Cronfa
Swansea University's Research Repository

Swansea University
Prifysgol Abertawe

Vulnerability and Repeat Victimisation in a Digital World: A Study of Computer Misuse and Fraud Reported in Wales.

Volume I of II

Sara Giro Correia

Submitted to Swansea University in fulfilment of the requirements for the Degree of Doctor of Philosophy.

Swansea University, 2020.

Copyright: The author, Sara Giro Correia, 2021.

In loving memory of:

Adelina Elias Correia, Maria Antónia Correia and Lusitano Correia

“À motié victime, à motié complice, comme tout le monde.”

[Half victim, half accomplice, like everyone]

Jean-Paul Sartre

Les mains sales, Paris, Gallimard, 1948

“[The Victims’ Code] forms a key part of the wider Government strategy to transform the criminal justice system by putting victims first, making the system more responsive and easier to navigate. Victims of crime should be treated in a respectful, sensitive, tailored and professional manner without discrimination of any kind. They should receive appropriate support to help them, as far as possible, to cope and recover and be protected from re-victimisation.”

Ministry of Justice

Code of Practice for Victims of Crime, 2015

“Justice? -You get justice in the next world, in this world you have the law.”

William Gaddis

A Frolic of His Own, Poseidon Press, 1994

Summary

While the estimated volume and cost of fraud and computer misuse (F&CM) is astoundingly high, much remains unknown about patterns of victimisation, especially in relation to repeat, 'chronic' and/or 'vulnerable' victims. These 'unknowns' have both theoretical and practical implications. Theoretically, understandings of repeat victimisation (RV) and vulnerability remain under-developed and under-studied, particularly with respect to F&CM victims. In practice, the ways in which victim vulnerability is defined and assessed have a direct impact on what response victims of F&CM get from the Criminal Justice System. Too often, however, such policies appear to reproduce idealised notions of 'the victim' or assumptions of what kinds of victims and vulnerability ought to be recognised – rather than being driven by evidence.

This work is a study of F&CM victimisation. It draws on a sample of crime reports (n = 17,049), made within Wales to the UK's National Fraud and Cybercrime Reporting Centre Action Fraud, between October 1st 2014 and September 30th 2016. A mixed-methods approach is used, encompassing descriptive and bivariate statistics, generalised linear models, deterministic and probabilistic data linkage, as well as qualitative thematic analysis. Throughout, the socially constructed nature of crime categories and the concepts of 'the victim' and vulnerability are recognised, while remaining committed to empirically grounded discussion of findings and (where applicable) the replicability of the analysis.

The analysis in this thesis highlights flaws in the reporting system that negatively impact on analysis and police response. These include data quality issues and the lack of a robust system to identify vulnerable and repeat victims. It also demonstrates the unsustainability of an online/offline distinction with respect to recorded F&CM crimes, identifies patterns of RV and their implications for crime prevention. Finally, this thesis advances an original framework for understanding vulnerability in the context of F&CM victimisation and better target a victim response.

Declarations and Statements

1. This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

2. This thesis is the result of my own investigations, except where otherwise stated. Other sources are acknowledged by explicit references and a bibliography is appended.

3. I consent for this thesis, if accepted, to be made available online in the University's Open Access Repository and for inter-library loan, and for the title and summary to be made available to outside organisations, after expiry of a bar on access approved by Swansea University.

4. The University's ethical procedures have been followed in this thesis and ethical approval granted by School of Law Research Ethics and Governance Committee on 3 November 2016.

Signed: Sara Giro Correia (candidate)

Date: 21 December 2020

Table of Contents

ACKNOWLEDGEMENTS

This Ph.D. project was made possible through an innovative partnership with the Cybercrime Unit at the Southern Wales Regional Organised Crime Unit (SW-ROCU), and a Ph.D. studentship funded by the Economic and Social Research Council (ESRC), administered and supported by Swansea University and the ESRC Wales Doctoral Training Partnership.

The SW-ROCU were key partners in this project, first identifying the value of exploring the potential of Action Fraud crime report data and then advising and continuously supporting my research efforts. SW-ROCU sponsored the required level of security vetting to allow me to intern with the Cybercrime Unit for an initial three months, after which they provided unwavering support and valuable feedback as the work progressed over the years. This included inviting me along to numerous feedback sessions and encouraging me to co-present initial results at various law enforcement and industry fora. The team was always welcoming as I inevitably (and frequently!) returned to the lab and used their facilities to optimise methods and re-run analysis. For that I am forever in their debt.

While there were many officers and police staff without whom this thesis could not have been completed, I must single out DCI Gary Philips, DCI Paul Peters, DI Eddie May and, especially, DI Craig Gillespie. Their leadership and commitment to work in partnership with academia and industry to better serve the public are unwavering. I am also thankful for the help and support of crime analysts including Amanda Jones (who first alerted me to the issue of repeat victimisation) and Emma Kitto-Casey. Thank you!

In addition, this thesis would not have come together without the support and guidance of my two wonderful supervisors, Prof. Stuart Macdonald and Prof. Nuria Lorenzo-Dus. There is no way to truly repay their kind and constructive feedback, but I will note that they have both been recipients of Swansea's annual REIS award for Outstanding Supervision and in both cases, this could not be more deserved.

I am also grateful for the support of the research community at the Law School and in particular to Dr. Patrick Bishop and all the fellow researchers I shared this journey with (Jens, Joe W., Amy-Louise, Seán, Katy, Lowri, Joe J. and Helen, among others). In addition, the postgraduate research support teams at the school, Swansea University and the DTP have been nothing but incredible all these years. Thank you to you all!

Finally, my thanks and love to my mother Maria João, father Jorge Lima, sisters Matilde and Beatriz and to my partner in crime, Cate Hopkins.

Sara Correia, September 2021

LIST OF TABLES AND FIGURES

1. Figures

2. Tables

List of Abbreviations

ACFE: Association of Certified Fraud Examiners (USA)

AF: Action Fraud, the National Fraud & Cyber Crime Reporting Centre

AP: Aggrieved Party

BBC: British Broadcasting Corporation.

BRC: British Retail Consortium

CMA: The Computer Misuse Act 1990

CNP: Card Not Present (fraud)

CPS: Crown Prosecution Service

CSBS: Cyber Security Breaches Survey (UK Official Statistics)

CSEW: Crime Survey for England and Wales (UK Official Statistics)

DCMS: Department of Culture Media and Sport (UK)

E&W: England and Wales

ESRC: Economic and Social Research Council

EU: European Union

HMG: Her Majesty's Government (UK)

HOCR Home Office Counting Rules

ICT: Information and Communication Technology

IP: Internet Protocol

KAS: Knowledge and Analytical Services (Welsh Government)

LA: Local Authority

LSOA: Lower Super Output Area (ONS)

MO: Modus Operandi

MOJ: Ministry of Justice

MMS: Mass Marketing Scams

N: number of cases or base of calculation.

NCSC: National Cyber Security Centre

NCRS: National Crime Recording Standard

NFIB: National Fraud Investigation Bureau

NTS: National Trading Standards

NFIB: National Fraud Intelligence Bureau

NOL: Notifiable Offence List

ONS: Office for National Statistics

PCC: Police and Crime Commissioner

PRC: Police Recorded Crime

RAT: Routine Activity Theory

ROCU: Regional Organised Crime Unit

SD: Standard Deviation

SME: Small and Medium Sized Enterprise

SW-ROCU: The Southern Wales Regional Organised Crime Unit

UK: United Kingdom

UN: United Nations

US DOJ: United States Department of Justice

INTRODUCTION

1. Context & Motivation

The scale of Fraud and Computer Misuse (F&CM) in the United Kingdom (UK) and beyond is astounding. In part due to their volume, and in part due to their potential impact, these crime types have taken centre-stage both as policy priorities and in media coverage – albeit often bundled together under the generic heading 'cybercrime'. The Crime Survey for England and Wales (CSEW) estimates that adults (16+) experienced approximately 4.6 million incidents of fraud and 876,000 incidents of computer misuse (CM) in the year ending March 2020. Of these, 18% experienced a financial loss which was not fully reimbursed, and a small minority of losses were considerable (3% lost over £1,000). In addition, where individual's losses are reimbursed, they are often incurred by business, whose overall losses as a result of F&CM are staggering. Based solely on their reported volume and associated losses, these crime types deserve closer inspection. However, previous research has also highlighted that the impact of these crime types goes much beyond the direct financial loss they cause (Button & Cross, 2017). In particular, both fraud and CM can have serious consequences for victims' privacy and the safety of their personal information, which can lead to anxiety and negative health and wellbeing impacts, further losses and strained relationships with family and friends. At the same time, the large volume of F&CM cases and difficulties in the investigation and prosecution of such crimes (particularly where they are committed online or remotely), mean that few victims receive much of a response from the Criminal Justice System (CJS) and see 'justice' being done. A recognition that it is not possible to 'control' F&CM through traditional enforcement activity has led to an increased emphasis on prevention and increasing resilience to these crimes. Despite considerable improvements in the recording of F&CM however, the tension between providing a local response to a global problem and the challenges of coordinating a response among a plethora of stakeholders (e.g., police, financial institutions, tech companies etc.), means victims can be forgotten.

The limited availability of evidence around F&CM victims and how best to respond to their needs is particularly striking in the context of the many initiatives which aim to make the CJS more 'victim focused'. In recent years, a plethora of legislative and policy initiatives have been

framed as "putting victims first" (MOJ, 2015, p. 1). To list but a few, these have included: the developing of The Code of Practice for Victims of Crime, known as The Victims' Code (2015), the establishment of a Victims' Commissioner and a Victims' Minister; a Victim's Taskforce which has recommended the development of a Victims' Law (to enforce the Victims' Code); the development of the Victims' Information Service; Victims' Contact Scheme; Victim Care Units; the Victims' Right to Review Schemes run by both the CPS and the National Police Chief's Council (NPCC), a Victims' Service Commissioning Framework, Victim Liaison Units and Victims' Personal Statements. This myriad of legislation and initiatives give shape to what Hall (2009) calls victims' procedural and service rights. Procedural rights are rights to participate and influence decisions in the CJS, whereas service rights relate to the way victims are treated, along with the services and support to which they are entitled. Despite these legislative and policy initiatives however, recent work has highlighted how 'orthodox' cyber-criminology has remained focused on risk and matters of crime control, rather than the harms associated with these crime types, or socio-structural and socio-cultural context of those risks (Powell, Stratton, & Cameron, 2018). Furthermore, despite considerable improvements in the reporting of F&CM since the roll out of the National Fraud and Cyber Crime Reporting Centre Action Fraud (AF), discussions with practitioners and recent research (Pease, Ignatans, & Batty, 2018; Skidmore, Goldstraw-White, & Gill, 2020b) highlighted that patterns of victimisation and vulnerability are not adequately understood in relation to F&CM victims. As detailed in chapter two, there is a considerable lack of clarity when it comes to identifying 'repeat' and 'vulnerable' victims and defining what an adequate victim-response should be in such cases. At the same time, these concepts of 'repeat' and 'vulnerable' victim are key to determining victims' procedural and service rights.

Given recent improvements in the recording of F&CM in England and Wales, it was timely to use Police Recorded Crime (PRC) to examine victims' characteristics, repeat victimisation and the notion of vulnerability and their relation to the impacts or harms associated with these crime types, through a combination of quantitative and qualitative methods. In the first place, doing so has led to insights into the quality of AF data and how this may be improved to aid research and practice. Furthermore, this study explores (repeat) victimisation and the notion of 'vulnerability' by providing an analysis of F&CM victimisation reported in the four Welsh police forces, situated within the local policy context of England and Wales. These reports were made via AF by victims based in Wales, between 1st October 2014 and the 30th September

2016. While the limitations of AF data are explored and acknowledged, by focusing on victims who, by reporting their victimisation as a crime, have engaged with the CJS, the analytical gaze is turned squarely onto what it would mean to have a CJS system which is indeed focused on responding to victims' needs. The research results are contextualised within the changing and increasingly global stage within which these crimes take place and identify an agenda for continued and future research.

2. Approach

Quantitative victimology is often aligned with a realist ontology which assumes that an objective reality of victimisation exists "out there" for research to uncover. Such ontological leanings are associated with positivist epistemologies and the strength of the positivist approach lies in developing evidence-based models, which are generalizable to the wider population and from which clear solutions and recommendations can be drawn. For example, many studies have applied Routine Activity Theory to cybercrimes and fraud victimisation, emphasising 'target hardening' solutions, i.e. how to make crime victims more resilient to victimisation (Bergmann, Dreißigacker, von Skarczinski, & Wollinger, 2017; Grabosky, Smith, & Dempsey, 2001; Holt, Burruss, & Bossler, 2018; Leukfeldt & Yar, 2016; Paek & Nalla, 2015; Williams, 2016). Another example is research conducted within computer sciences, modelling cyber-attacks to better understand their architecture as well as their consequences or impact, and thus mitigate against the risks they pose (e.g. Bacher, Holz, Kotter, & Wicherski, 2008; Cooke, Jahanian, & McPherson, 2005; Ianelli & Hackworth, 2005). Such research also lends itself to clear recommendations and is therefore easy to translate into policy impact.

However, a realist ontology is not without limitations. It can leave unquestioned assumptions about what crimes and what experiences of victimisation are measured in the first place and prioritised for a response – as well as who benefits most from such assumptions. In writing this thesis, it was considered that questioning any such assumptions was as important as "measuring" (or "capturing") experiences of victimisation. This was best achieved by recognising the socially constructed nature of the "reality" of crime, victimisation and vulnerability. Most commonly, this is a position characteristic of the opposite end of the ontological scale, where a relativist ontology posits that the "reality" of the social world is socially constructed and relative to the (inter-subjective) understandings of the observer.

Within victimisation studies, this perspective often characterises studies which prioritise understandings of "victimhood" by victims themselves, elicited through in-depth interviews or focus groups. Such a position recognises that there isn't an absolute reality of crime out there – what constitutes a crime and how/what crime is measured is itself the product of a social construction (Bondt, 2014; Bryman, 2012). As such, a relativist ontology has been accompanied by a constructivist epistemology in this thesis and thus the use of qualitative methods such as thematic analysis (TA), often characteristics of such an approach.

However, while this thesis is aligned with a relativist ontology and a social-constructionist epistemology, it is committed to integrating empirical measurement and qualitative nuance and thus reclaiming the use of specific quantitative and qualitative methods, as ontologically and epistemologically neutral. The logic behind this commitment is two-fold: firstly, it is argued that recognising concepts as socially constructed does not preclude their measurement or the observation of associated statistical relationships; secondly, measuring those concepts and relationships opens avenues for critical engagement with the results and the very concepts they seek to measure. Measuring concepts can make visible how those concepts are being shaped by what is deemed important to be measured in the first place. This is particularly important where, as in this study, administrative data are re-purposed for quantitative statistical analysis. As such, making sense of the measurements, their strengths and limitations is crucial to the project of de-construction (and re-construction) of notions of crime, victimisation and vulnerability. Consequently, this thesis is situated somewhere between realism and relativism on the ontological scale, at a point which has been described as *critical realism* (Braun & Clarke, 2013; Matthews, 2014; Willig, 1999). Furthermore, it takes a pragmatic mixed-methods approach, choosing methods based on how useful they are to answer the research question in hand.

3. Research Aims & Questions

This thesis has one preliminary and three substantive aims. Before addressing the three substantive aims, a preliminary evaluation of the quality of Action Fraud recorded crime data was undertaken. The first substantive aim is to understand the volume of F&CM victimisation recorded in Wales and explore victims' characteristics. Secondly, to identify patterns of individual F&CM repeat victimisation (RV) recorded in Wales and the characteristics of repeat

victims. Thirdly, to develop an empirically grounded theoretical model of vulnerability in the context of individual F&CM victimisation in Wales.

The first aim of this thesis is to identify what patterns of F&CM reporting (in Wales, over the reference period) could be discerned from AF data. This included volume of reports, victims' characteristics and impacts, as well as offenders' *Modus Operandi* (MO). To meet this aim, the following research questions (RQ) and sub-questions are addressed in chapters four and five.

RQ1: What was the volume of reported F&CM in Wales over the reference period? (chapter 4, section 1)

Answering this question included an examination of the volume of F&CM across victim types, forces and throughout the reference period. The volumes of F&CM recorded in Wales vis-a-vis other crime types were also examined.

RQ2: What were the characteristics of victims who reported F&CM in Wales over the reference period? (chapter 4, section 2)

Victim types and their characteristics were examined across crime group (fraud versus CM) and individual F&CM categories.

RQ3: What financial and other impacts were reported by individuals and other victims of F&CM in Wales over the reference period? (chapter 4, section 3)

Including a quantitative examination of how losses varied across victim types and characteristics and a qualitative analysis of impacts beyond direct financial loss.

RQ4: What online/offline dynamics enabled F&CM in Wales over the reference period? (chapter 5, section 1)

This question considered association online/offline dynamics across victim characteristics, crime group and F&CM categories. Other MO features were also qualitatively analysed.

The second aim of this thesis was to consider patterns of repeat victimisation and the extent to which the characteristics of one-time and repeat victims differed. To meet this aim, the following RQ5 to RQ9 and sub-questions are addressed in chapter six. Finally, RQ10 addresses the third aim of this thesis in chapter seven.

RQ5: What was the extent and nature of individual F&CM repeat victimisation (RV) in Wales? (chapter 5, section 2.1)

Including the overall volume of RV and its distribution across crime group and crime categories.

RQ6: What were the characteristics of repeat individual victims? (chapter 5, section 2.2)

Compared the demographic characteristics of one time and repeat victims and considered whether RV varied with respect to the local area's socio-economic profile and levels of internet access.

RQ7: What was the impact of RV? (chapter 5, section 2.3)

Examined financial and other impacts associated with RV.

RQ8: What was the characteristic time-course of RV? (chapter 5, section 2.4)

Examined the time-course of RV vary across crime group/category.

RQ9: What were the mechanisms through which RV happened? (chapter 5, section 2.5)

A qualitative analysis of the mechanisms which underpin RV, i.e., what are the typical tactics used by offenders to repeatedly victimise individuals.

RQ10: How was vulnerability constructed within reports of F&CM? (chapter 6)

A mixed methods analysis dominated by qualitative thematic analysis which uncovered the ways in which vulnerability was constructed within crime reports.

4. Overview of Methods

This thesis was written based on a review of the literature and the empirical study of F&CM victimisation reported and recorded in Wales, United Kingdom (UK), over a two-year period between October 1st 2014 and September 30th 2016 (n = 17,049). Three overall methods were used within the research and analysis of this thesis. These included frequentist statistical methods (descriptive, bivariate and multi-variate methods), data linkage methods (including both deterministic and probabilistic matching) and qualitative Thematic Analysis (TA).

Firstly, quantitative descriptive, bivariate and multi-variate methods were used to gain a broad understanding of the quality of AF data, the observed patterns of reported crime and victims' characteristics. This part of the analysis led to the refining of research questions and the identification of the need to develop a linkage method which would enable the identification of repeat victims, as well as the need to explore the data qualitatively.

Secondly, a combination of deterministic and probabilistic linkage was performed to both add new variables from external, open-source datasets to the original data (including geographical groupings, an indicator of level of socio-economic deprivation and a measure of internet accessibility) and to link incidents reported by the same individuals over the time-period of reports sampled. This enabled further statistical and qualitative analysis of patterns and key themes characterising repeat victimisation.

Finally, qualitative analysis was used to add nuance to the results obtained from the statistical analysis and, crucially, to drive the construction of an empirically grounded theoretical model of individual vulnerability to F&CM victimisation and its impacts. Furthermore, some themes identified through the qualitative analysis, were further illustrated quantitatively.

While the three key methods were broadly deployed in the order identified above, this overview highlights how results from each method influenced the application of the others. Thus, this was not a strictly linear process and hence a truly mixed methodology.

5. Originality and Contribution

Firstly, this work makes a methodological contribution to the growing field of administrative data research. AF data presented an unprecedented opportunity to explore F&CM victimisation and contribute towards the victimology research agenda. An increasing number of projects are being developed to explore, demonstrate and utilise administrative data to its full potential e.g., the Office for National Statistics' Administrative data census project, or the recent 'Data First' partnership between Administrative Data Research and the Ministry of Justice, to make court data from England and Wales available to researchers. However, administrative data research generally and research with police recorded crime, are challenging (e.g. Hope, 2007; Levi, 2017; Levi & Burrows, 2008). As highlighted by David Hand, it is imperative to "evaluate the impact of [administrative] data quality on statistical conclusions" (2018, p. 10). As such, this work highlights flaws in the reporting system and discusses its impact on analysis and police response. These include data quality issues and the lack of a robust system to identify vulnerable and repeat victims. In addition, this work has uniquely applied a mixed methods approach, including a data linkage method, to the field of victimology and in particular to the study of F&CM victims.

Secondly, it has been hypothesised that the noticeable 'crime drop' since the 1990s has occurred at least in part because 'traditional' property crimes such as burglary, car theft,

'traditional' fraud and violent crimes such as assault were being replaced by 'cyber' or 'online' crime. The debate has its proponents (Caneppele & Aebi, 2019; Tcherni, Davies, Lopes, & Lizotte, 2016) and its sceptics (Farrell & Birks, 2018; Levi, 2017), albeit with nuance. In relation to F&CM, while there is no clear evidence to support the idea that offenders who used to commit burglaries are now 'retraining' as hackers, it may be more strongly argued that there has been a surge in what have been termed *hybrid crimes* (Caneppele & Aebi, 2019) and a corresponding fall in what may be described as offline-only crimes. This theoretical debate has implications for policy as these crime types create extensive demand on CJS services, while posing very particular challenges (e.g., they cross jurisdictions, digital evidence is easy to destroy and internet facilitates anonymity, to name but a few). This work provides empirical evidence which demonstrates the erosion of the online/offline dichotomy. Consequently, a narrow focus on "cybercrime" may lead to ineffectual prevention initiatives and the inadequate distribution of police resources.

Thirdly, this thesis adds to the body of work which examines the mechanisms of F&CM and the impact of these crimes on victims. Previous research has highlighted the tactics used by fraudsters and has pointed towards the wide range of impacts fraud has on victims (Button & Cross, 2017; Button, Lewis, & Tapley, 2009a, 2009b). While previous studies mostly focused on small survey samples and in-depth qualitative studies, this thesis adds to this literature by corroborating previous findings through the mixed-methods analysis of a large sample of crime reports. In particular, insights into the 'anatomy' of fraud (Whitty, 2015a) i.e., the mechanisms through which fraudsters engage and victimise individuals, or their *Modus Operandi.* In addition, in line with previous work (Cross, 2018), these findings highlight that fraud victims are far from the 'ideal victim' as conceptualised by Nils Christie (1986). In addition, this work contributes towards better understanding the human impacts of computer misuse, with respect to which there is little scholarship.

Fourthly, albeit with some notable exceptions (Whitty 2015b, 2019, Correia forthcoming), F&CM repeat victimisation and its theoretical and practical implications have largely escaped academic scrutiny (Pease et al., 2018). As such, this thesis makes both a theoretical and practical contribution towards better understanding repeat victims of F&CM. It does so by drawing on a large sample of reported crimes to analysis patterns of reported repeat victimisation, its impact and providing an analysis of how 'vulnerability' is constructed within

F&CM reports. The implications for theory and practice of the patterns of (repeat) victimisation observed are also highlighted.

Finally, having identified the need for an understanding of vulnerability which is both broader than the one deployed in the Code of Practice for Victims' of Crime (MOJ, 2015) and the mechanisms, impact and patterns of (repeat) victimisation, this thesis puts forward a theoretically informed but empirically driven framework for understanding and measuring *vulnerability to* and *vulnerability post* F&CM victimisation. It does so by drawing on *vulnerability theory* (Fineman, 2008, 2017) and the concepts of *capabilities* (Nussbaum, 2011; Sen, 1999) and *technological affordances* (Fayard & Weeks, 2014; Gibson, 1986; Hutchby, 2001).

6. Thesis Overview

Chapter one discusses and defines *cybercrime*, F&CM crimes. It problematizes the term 'cybercrime' and hypothesises the advantages of moving away from the label 'cyber', while acknowledging online and offline elements where applicable. Considering the availability of multiple definitions and typologies of F&CM, it develops the definitions and typology used in this study. Furthermore, this chapter provides an overview of the current landscape of response to F&CM in the UK. It examines police strategy and considers its impacts on the victims' journey and experience through the CJS, highlighting the strengths and weaknesses of the current victim response.

Chapter two explores the twin concepts of "victim" and "vulnerability" in relation to F&CM victims, both theoretically and empirically, setting the scene for the analysis that follows. It starts by exploring understandings of 'the victim' at the *micro-level* of individual experience and self-identification, the *meso-level* of institutional definition and operationalisation and finally the *macro-level* of cultural phenomena. In doing so it highlights the consequences for victims of misalignment across these and the limitations of current conceptualisations of 'the victim' as a single human agent. Crucially, it identifies the centrality of the concept of 'vulnerability' at all levels. It then goes on to explore F&CM through a 'vulnerability' lens and consider the under-explored phenomenon of F&CM repeat victimisation.

Chapter three details the mixed methodology used to best answer the research questions posed in this thesis, in line with the approach described in this introduction. In particular, it details the considerable steps taken to make the dataset ready for analysis. It also sets out the use of

both quantitative and qualitative methods including descriptive and bivariate statistics, Generalised Linear Models, the data linkage method used, as well as thematic and content analysis. Finally, it turns to the ethical considerations and limitations.

Chapter four provides an analysis of reported crime patterns and answers research questions one to three. Through statistical analysis, this chapter examines the volume of F&CM, crime categories recorded and the characteristics of those reporting crime to the police. It then goes onto to analyse the impact of F&CM on victims, through a mix of quantitative methods and qualitative thematic analysis.

Chapter five examines how F&CM is committed (including what mechanisms are used by criminals and whether they are committed online or offline) and presents an analysis of patterns of repeat victimisation (RV) and their relevance for crime prevention. With respect to the RV analysis, the unit of analysis is the victim (rather than the crime report), which was made possible by applying a data linkage method to link together reports made by the same individuals within the sampled data. This analysis begins to address a current research gap around understanding repeat victims of F&CM, so that a response can be provided which meets their needs. It was also a stepping stone to the theoretical model of vulnerability developed in chapter six.

The final chapter (six) provides the results of the thematic analysis of a sample of incidents reported by one-time and repeat-victims and considers the ways in which 'vulnerability' is constructed within these crime reports. Drawing together insights from the literature, the analysis in chapters four and five, as well as its own qualitative analysis, a multi-dimensional vulnerability framework is proposed. This aims to enable a better theoretical understanding of F&CM victimisation, as well as aid practitioners in meeting the needs of victims.

Finally, the thesis conclusion summarises key results and, in light of these, considers implications for theory, practice and future research. This concluding discussion brings together reflections on the quality of the crime report data, the observed victimisation patterns and the proposed vulnerability framework. It also draws some overall conclusions on the CJS response in the context of the F&CM 'justice network' (Button, Tapley, & Lewis, 2012) on how stakeholders may better work together in the future to improve the response to F&CM victims.

The second volume of this thesis includes seven additional appendices. The first sets out F&CM typologies which this thesis draws on in greater detail. The second documents the data cleaning and processing carried out on the raw sampled data through R markdown notebooks (integrated code, output and descriptive narrative). The third summarises the variables, used in the analysis. The fourth to sixth appendices provide R markdown notebooks for the data linkage, statistical and qualitative analysis respectively. Finally, the seventh appendix includes a detailed quality evaluation of the administrative Action Fraud data used in this thesis.

CHAPTER 1 – Fraud and Computer Misuse in a Digital Society

This thesis started as a study of "cybercrime" but evolved into a study of 'vulnerability' in the context of Fraud and Computer Misuse (F&CM) victimisation, across the online/offline continuum. This chapter sets out the rationale for this approach. It starts by presenting a working definition of cybercrime, how it is or not distinct from 'traditional' forms of crime and exploring the usefulness of the term. It goes on to problematise cybercrime in relation to F&CM and review previous literature challenging the online/offline dichotomy. While moving away from 'cybercrime', the author maintains the usefulness of analysing the prevalence of digital elements in the way crimes are perpetrated and experienced, with a view to understanding how victimisation is changing in an increasingly digital society and developing appropriate crime prevention and victim support frameworks.

The chapter's first section problematises 'cybercrime' and provides a brief analysis of the UK's legal framework, establishing the working definitions and typologies of F&CM relied on throughout the rest of the thesis. The second section turns its attention to responses to F&CM victimisation. The interaction between national, regional and local policing in the implementation of the four strands of the cybercrime policing strategy (Pursue, Prevent, Protect and Prepare) is explored. Key elements of the wider F&CM 'justice network' (Button, Tapley, et al., 2012) response are also considered. By exploring F&CM from the perspective of current victim-responses, gaps in knowledge and areas for improvement are identified.

1. Cybercrime and the Digital Society

1.1. The Scale and Impact of 'Cybercrime'

It has been hypothesised whether the noticeable 'crime drop' since the 1990s, illustrated in Figure 1 below, occurred partly because 'traditional' property crimes such as burglary, car theft, fraud and violent assaults were replaced by 'cybercrimes' including online fraud and computer misuse. The debate has its proponents (Caneppele & Aebi, 2019; Tcherni et al., 2016) and its sceptics (Farrell & Birks, 2018; Levi, 2017), albeit with nuance. In relation to F&CM, while there is no clear evidence to support the idea that offenders who used to commit burglaries are now 'retraining' as online fraudsters, it may be more strongly argued that there

has been a surge in what have been termed 'hybrid crimes' (Caneppele & Aebi, 2019) and a corresponding fall in what may be described as offline-only crimes. By 'hybrid', it is meant crimes which combine online and offline components (Caneppele & Aebi, 2019, p.70).

At the same time, the significant volume of F&CM in England and Wales was highlighted from 2017, as these crime types integrated the yearly crime estimates produced by the Office for National Statistics (ONS), based on the Crime Survey for England and Wales (CSEW).[1] Recent estimates indicate that adults experienced approximately 4.6 million incidents of fraud and 876,000 incidents of computer misuse in the year ending March 2020, bringing the overall crime estimate to 10.2 million estimated crimes (ONS, 2020b, Table A1). While fraud has not changed significantly, the CM estimate decreased significantly between 2017 and 2019. However, early indications are that these crimes increased considerably during the recent COVID pandemic (e.g., APWG, 2020). Nonetheless, while the volume of F&CM is large the evidence for the crime 'displacement' theory is limited.

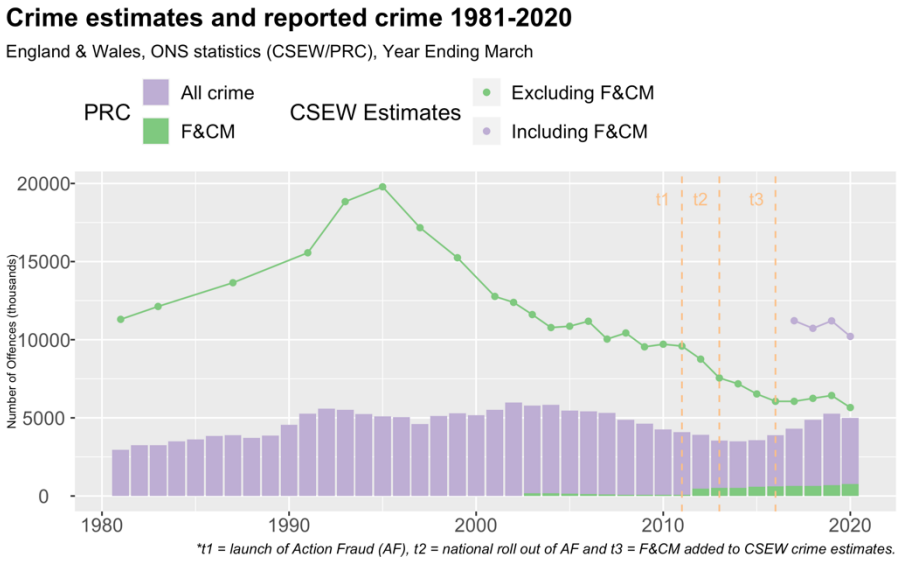

Figure 1 – CSEW crime estimates and police recorded crime (PRC), 1981-2020.

[1] Formerly known as the British Crime Survey, the survey was renamed as the CSEW in April 2012 to better reflect its coverage, as separate surveys are carried out in Scotland and Northern Ireland. Since April 2012, the responsibility for the CSEW has been transferred from the UK's Home Office to the Office for National Statistics (ONS) and its fieldwork and initial data preparation is contracted out. ONS then carries out further data preparation and analysis, which it publishes quarterly. As a mark of their quality, results are designated as "National Statistics" by the UK Statistics Authority.

Of those who experienced a loss in the year ending March 2020, "the majority (58%) incurred a loss of less than £250, with the median loss being £167, around a quarter (27%) incurred a loss of between £250 and £999 and the remainder (15%) incurred a loss of £1,000 or more, with 2% losing £10,000 or more" (Elkin, 2020). As such, while losses are concentrated at the low end of the scale, many suffered considerable losses. Furthermore, while often individuals' losses are reimbursed, 29% of CM incidents (106,000) experienced by 97,000 victims and 18% of fraud incidents (669,000) experienced by 602,000 victims resulted in losses which were not fully reimbursed (ONS, 2020c, Table F6). Additionally, the impacts of F&CM on individuals cannot be reduced to direct financial losses – there are indirect losses, emotional impacts and, in some cases serious health and social impacts to becoming a victim of F&CM (Button & Cross, 2017).

Alongside impact on individuals, large volumes of F&CM amounting to staggering losses are reported by businesses. As shown in Figure 2, Cifas and UK Finance, reported over 436,000 incidents of fraud in the year ending March 2020.[2] While Cifas does not publish losses, UK Finance indicated that their members lost £1.2 billion to F&CM in 2019 (UK Finance, 2020b). Furthermore, results from the Cyber Security Breaches Survey (CSBS) indicate that 46% of businesses and 26% of charities in the UK, suffered at least one cyber security breach or attack in the last 12 months (DCMS, 2020). Where breaches resulted in financial losses, the average (mean) cost of all such instances in in the year leading up to the survey was estimated at £3,230 overall and £5,220 for medium and larger firms. While this thesis is primarily focused on individual victims, as it will be seen, often there is more than one 'victim' and the extent of the impact of F&CM on businesses adds to the enormity of the volume and losses associated with these crime types. Furthermore, while larger organisations may absorb these losses (or pass on them onto consumers), these can be devastating for Small and Medium Sized Enterprises.

Figure 2 shows how the introduction of AF led to considerable improvements in recording practices, with the volume of recorded crimes increasing by over 160% between 2011 and 2013

[2] Cifas and UK Finance are two industry representative bodies who report fraud directly to the NFIB on behalf of their members. As it will be discussed, their membership primarily includes businesses which operate within the financial sector.

(ONS, 2020b, Table A5).[3] Despite these improvements however, F&CM remains considerably under-reported. It is estimated that, in the year ending March 2020, only approximately 8% of fraud and 2% of CM individual victimisation was reported to the police or AF (ONS, 2020b).

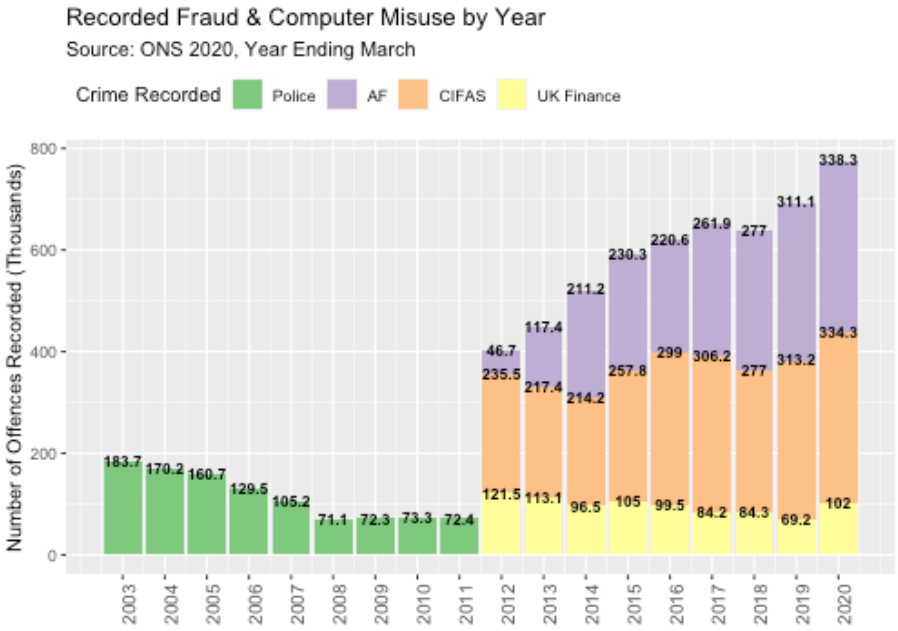

Figure 2 – F&CM recorded crime by Year, 2003-2020.

Unsurprisingly therefore, government efforts and investment have been directed at improving recording, awareness of and resilience to cybercrime and financial crime. Indeed, the government committed to spending £1.9 billion in cyber security between 2016 and 2021, a strategy due for renewal (HM Government 2016). This is, however, in a context where public-facing CJS institutions including the police, courts, prisons, victim support and probation services among others, have endured unprecedented budget cuts for over a decade. Furthermore, as will be discussed in detail, there is limited research on the characteristics of F&CM victims who come into contact with the CJS, especially those which may be considered 'repeat' or 'vulnerable' victims, as well as on the impacts of victimisation and how best to respond to victims' needs. Recent work has highlighted how to date, while cyber-criminology has focused on fraud and computer misuse, it has done so through a limited set of theoretical assumptions, drawing heavily on Cohen and Felson's (1979) Routine Activity Theory (Powell

[3] That is by comparing the volume of crimes reported directly to the police in 2011 to the volume of crimes reported to AF. If the additional reports made by the industry bodies Cifas and UK Finance, on behalf of their members, directly to the National Fraud Intelligence Bureau (NFIB) were taken into account, the increase would be even greater.

et al. 2018). As discussed in what follows, this is in part the result of a limited understanding of 'cybercrime' and a focus on crime control, over the social harms associated with crime and the socio-cultural and socio-structural characteristics of the 'Digital Society' (Powell et al. 2018). As such, while this thesis focuses on F&CM, its key motivation is to gain a better picture of the impact of these crimes on individuals, how they are made vulnerable to (re)victimisation and ultimately to reflect on what this means for the CJS, if it is to adequately address victims' needs.

1.2. Beyond 'Cybercrime' Orthodoxy

As with many heuristic devices, the concept of 'cybercrime' is contested. On one side it is argued that, since the early 1990s, the information and communications technology (ICT) *revolution* has resulted in far-reaching social changes affecting how crime is perpetrated, how victimisation is experienced and crime perceived (e.g. McGuire, 2007). More recently, in their book on 'digital criminology' Powell and colleagues have sought to covey how the landscape of crime and harms has and continues to change in what is today's 'Digital Society'. In other words, how 'technosocial cultures and practices come to bear [on the realities of crime and victimisation]' (Powell et al., 2018, p.32). On the other, scholars including Grabosky and Smith (1998; 2001), suggest that there is more continuity than change in the age of the *network society* (Castells 1996, 2010). Furthermore, "cybercrime" obscures a complex web of different crime types, policy priorities, harms and victim experiences. Similarly, the term 'fraud' is also broad and can take many forms. Thus, not only are both terms contested, but a plethora of typologies of both cybercrime and fraud exist, which will inevitably impact on how these crimes are measured and ultimately, on the priorities which emerge for response within policy and practice. As such, in the early stages of this work the author set out to define and problematise 'cybercrime' and establish a F&CM typology to be used in the analysis.

1.2.1. Defining Cybercrime

Borrowing from Wall (2007) and Yar (2006), cybercrime is understood to include criminally sanctioned illegal acts,[4] which in their preparation or performance, involve either the targeting of ICT networks and/or its constituent parts; and/or the use of ICT by the offenders, where it significantly transforms the scale of the crime and the ways in which offenders operate. This definition is compatible with that commonly used by UK law enforcement and adopted by the UK Home Office (McGuire & Dowling, 2013), which distinguishes between 'pure' cyber, or *cyber-dependent* crimes – i.e. 'new' crimes such as hacking or the spread of malware, arising from the development of ICT, where ICT is both the means and the target of the crime. Such crimes have also been referred to in the literature as high-tech crimes and, in the UK, may be termed computer misuse (CM) crimes, following the Computer Misuse Act 1990 (CMA 1990). Secondly, *cyber-enabled* crimes are those which (like fraud or cyber harassment) pre-date the existence of ICT but have, by its use, increased in scale or reach. Finally, in line with scholarship on cyber-terrorism (Gordon & Ford, 2002; Jarvis & Macdonald, 2015), crimes have also been described as *cyber-related,* where online activity may be involved in other ways, for example, where the Internet is used in the planning of crime.

While the distinction between *cyber-dependent*, *enabled* and *related* crimes was useful in developing early CJS responses to crime e.g., by enabling the identification of training and infrastructure needs, it has been suggested that this categorisation is too broad to have criminological value or explanatory power (Yar, 2006). In contrast, the typology developed by Wall (1999) distinguishes cybercrime with respect to the nature of the crime itself (2001, pp. 3-7), rather than the means by which it is committed.[5] It includes *cyber-trespass*, crossing boundaries into or damaging other people's virtual property, e.g., hacking, defacement, viruses; *cyber-deceptions and thefts*, stealing money or property, e.g., credit card fraud, intellectual property violations; *cyber-pornography*, breaching laws on child pornography, obscenity and

[4] This definition specifically refers to crimes as 'illegal' rather than 'deviant' acts, which Thomas and Loader also include in their conceptualisation of cybercrime, thus extending it to all those 'computer-mediated activities which are … considered illicit' (2000, p. 3 in Yar, 2006, p. 9). This is therefore a study of victims of crime (that which is illegal), rather than victims of deviance – that which diverges from usual or accepted social standards and may cause harm but is not (yet) criminalised.

[5] Although later Wall moved towards a categorisation somewhere between nature and mode of criminal offence including 1) Computer-Integrity crime, including criminal acts such as hacking, cracking and denial of service; 2) Computer-assisted crime, to include virtual theft and scams and 3) Computer Content Crime, including pornography, violence and offensive communications (Wall, 2007).

indecency e.g., possession and dissemination of indecent images of children or otherwise pornographic material; and *cyber-violence*, doing or inciting physical or psychological harm against others e.g., hate speech, harassment (Wall, 1999, p. 126). The first two may be classed as "crimes against property", the third as "crimes against morality" and the fourth as "crimes against the person" (Yar, 2006, pp. 10-11). To these Yar would add "crimes against the state" to include crimes such as cyber-terrorism, cyber-espionage and the revealing of state secrets (Yar, 2006, p. 11). The combined typology is illustrated in Figure 3.

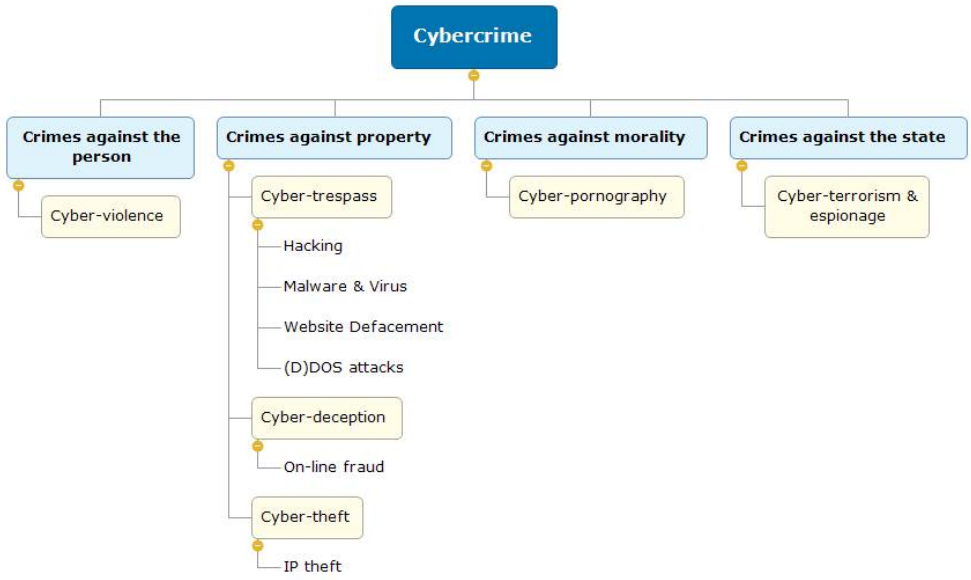

Figure 3 - Cybercrime working typology, based on Wall (2001) and Yar (2006).

The above categorisation allows for a focus on the social context of the crimes, the relationships between victim, perpetrators and other actors (e.g., website and phone providers), as well as for better comparisons to be drawn between online/offline crime. As a result, several authors have drawn on Wall (2001) and Yar (2006) when researching cybercrime offending and victimisation (e.g. Holt & Bossler, 2013). However, following Powell et al. (2018), this typology still over-emphasises a false online/offline dichotomy when increasingly, analysing the close interaction between online and offline elements provides new theoretical and practical understandings of crime and victimisation. This is further discussed in the next section. Furthermore, on a practical level, as the empirical analysis for this thesis progressed, the focus on 'cybercrime' became increasingly problematic, resulting in the abandonment of this term, in favour of the legal categories of fraud and computer misuse (F&CM).

1.2.2. Problematising ‘Cybercrime’

Grabosky and Smith (1998) have argued that the term ‘cybercrime’ obfuscates the nature of online criminality and victimisation. They considered various forms of illegal activity which takes place in ‘cyberspace’ and remained sceptical of their uniqueness. In their analysis, the nine types of what they described as 'telecommunication' crimes have not created new crimes but rather enabled types of criminal activity which pre-dated ICT "to be carried out more extensively, more efficiently, more quickly, with greater ease of concealment, and thus with greater difficulty of detection" (Grabosky & Smith, 1998, p. 210).[6] Accordingly, Grabosky applied Cohen and Felson's (1979) Routine Activity Theory (RAT) to cybercrimes and others extended it to the closely linked ‘lifestyle’ theory of criminal victimisation (Bergmann et al., 2017; Grabosky et al., 2001; Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011; Paek & Nalla, 2015; Williams, 2016). Following Cohen and Felson, crime – online and offline – happens when three elements come together: 1) motivated offenders, 2) suitable targets and 3) the absence of capable guardianship in the form of technical controls, police intervention etc. (Cohen & Felson, 1979). As such, analysis should focus not on the conduct itself, or whether or not it contains online elements, but on the motivations of offenders and the situational characteristics of victims, which are comparable to the motivations of 'traditional' criminals and victims (Grabosky & Smith, 1998; Grabosky et al., 2001). With respect to guardianship, cybercrime is also not distinct in addition to law enforcement, it involves "preventative efforts on the part of prospective victims, contributions by members of the general public or commercial third parties (such as insurance companies and private security services)" (Grabosky & Smith, 1998, p. 3; Grabosky et al., 2001). Furthermore, it is "often only when private efforts at crime prevention fail that the criminal process is mobilized" (Grabosky et al., 2001, p. 3). This suggests that 1) understanding and reducing cybercrime offenders’ motivation to commit crime is one strategy to reduce victimisation, alongside 2) *target hardening* by increasing the resilience of the victims and 3) effectively 'guarding' potential victims by increasing detection. The application to RAT to ‘cybercrime’ contexts is so widespread, that it might be referred to as the prevailing cyber-criminology orthodoxy.

---

[6] These included 1) Illegal interception of telecommunications; 2) electronic vandalism and terrorism; 3) stealing telecommunications services; 4) telecommunications piracy; 5) pornography and other offensive content; 6) telemarketing fraud; 7) electronic funds transfer crime; 8) electronic money laundering; and 9) Telecommunications in furtherance of criminal conspiracies.

However, the empirical testing of an RAT framework with respect to cybercrime victimisation has yielded mixed results (Leukfeldt & Yar, 2016). Firstly, a straightforward application of RAT to 'cybercrime' faces some challenges. As with other criminological approaches, RAT is focused on the 'where', 'who' and 'why' of crime. The answers to these questions are usually articulated with respect to the environment in which crime takes place, its *ecological assumptions* (Yar, 2006), and a specific crime event. In other words, crime is understood with respect to "particular places that have important defining social, cultural and material characteristics" (Yar, 2006, p. 18) – as well as situational characteristics, in the case of RAT – and it is these defining characteristics that explain the where, who and why of crime. However, cybercrime operates in a compressed 'time-space' continuum where attempts to remove the conditions under which crime can take place are likely to be frustrated. In addition, existing theories about 'who' the criminals are can be challenged in the context of cybercrime. As has been evidenced (e.g. Smith, Grabosky, & Urbas, 2004), concepts of "marginality" and "exclusion" that are used to explain why people offend in the "real" world are of limited use to understand cybercriminals, who are atypical given the relative socio-economic privilege, skills and resources required in order to commit cybercrime (Yar, 2006, p. 19).[7]

In relation to the theorising of victimisation, RAT also has considerable limitations. As shown in chapter two, the typical socio-economic profile of victims of F&CM is somewhat different to that of other crime types. In addition, recent work has articulated how viewing 'the victim' as a single entity, with particular characteristics that make them attractive targets, obfuscates the role of multiple actors in the construction of states of vulnerability (van der Wagen & Pieters, 2015, 2020). In their thought provoking pieces, van der Wagen and colleagues have therefore called for the re-conceptualisation of the cyber victim as a 'hybrid victim', not a single entity but a network of human and non-human entities, a 'cyborg'. In addition, RAT approaches to 'cybercrime' have been dominated by "individualistic, rational-actor and crime control concerns" (Powell et al., 2018, p.31), rather than the harms associated with these crimes, or how they are experienced in a Digital Society. As such, on the one hand, the case that the 'cyber' element is of no consequence, is unconvincing. Atypical patterns of victimisation and complex victimisation processes, which involve multiple stakeholders and

[7] Although the emergence of automated software tools to conduct cyber-attacks has changed this to some extend (Yar, 2006), lowering the level of technological expertise of cyber criminals, resources and a level of technical expertise is still required in order to deploy automated 'off the shelf' attacks.

victims, require revised theoretical frameworks for the understanding of victimisation and vulnerability, with implications for CJS policy and practice. On the other, the emerging critique of cyber-criminology orthodoxy highlights how understandings of cybercrime have led to a focus on limited crime types, the reliance on limited theoretical perspectives and the over-emphasising of an increasingly false online/offline dichotomy.

1.3. The Digital Society and Technological Affordances

While the term *cyberspace* is one that originated in fiction,[8] today it evokes the global network of computers and 'smart' devices including mobile phones and other objects (wearable tech, appliances etc.), connected via the Internet. Cyberspace is, however, more than the sum of its technologies and underpinning infrastructure – it is also the new social spaces created by the Internet, the "network of networks" (Castells, 1996, 2010). As such, cyberspace both contains and is contained by, the new social relations which develop within it. Inevitably, these social changes will affect what crime is committed, how it is committed, how it is experienced by victims and, importantly, how society responds. Castells theorised *the rise of the network society* in terms of how the ICT *revolution* changed the nature of globalisation, culture, institutions, the global economy and even our physical spaces (Castells, 1996, 2010). The *network society* may be described as the culmination of historical and globalising processes which led to today's society – one where, as a result of the new all-pervasive ICT paradigm, the network[9] as a form of social morphology has expanded throughout the entire social structure and overtaken all other forms of social action/interaction (Castells, 2010). Closely following Castells' argument that ICT has brought about "a new society" (Castells, 2000, p. 693) which prioritises networked information flows, is the sociological concept of the 'Digital Society'. This captures the idea that digital technology more broadly has created a society where tech is embedded into everyday assumptions and cannot be meaningfully separated from the 'analogue' world. At the time of writing, during a period of local lockdown due to the COVID19 pandemic, the socio-economic importance of networked information flows and the ubiquity of digital technology has never felt more 'real'. This new society has elements of

[8] First coined by William Gibson (1982) in the popular science and science fiction Omni Magazine and later popularised by his 1984 novel Neuromancer (Jordan, 2008; Wall, 2007).

[9] Defined as "a set of interconnected nodes", where the node unit will depend on the concrete network one considers – they may be stock exchanges, farms, media organisations, criminals etc (Castells, 2010, p. 501).

continuity (e.g., the global capitalist economy) but also elements of fundamental change which are *informationally* driven and resulted in the current morphology of the network.[10] In this context, several authors have begun to critically examine how the landscape of crime and associated social harms are changing in the new digital world (e.g. McGuire, 2007; Powell et al., 2018).

Considering such a pervasive societal transformation, it may become necessary to employ a broad definition of cybercrime which refers "not so much to a single, distinctive kind of criminal activity but more to a diverse range of illegal and illicit activities that share in common the unique electronic environment ('cyberspace') in which they take place" (Yar, 2013, p. 5). As previously noted, this includes new crimes which did not exist prior to networked computers, as well as crimes which pre-date the Internet but have been significantly "transformed" by it (Wall, 2007, p. 34). However, the relevance of 'cyber' goes beyond 'crime-as-conduct', to extend to the ways in which "new technologies and affordances" result in a "complex dialectic between the opportunities for harm and exploitation made available by new technologies (the many forms of cyber-crime and computer-enabled crime, and the other varieties of harm made feasible by new media – social media bullying, grooming, trolling and stalking, for example) and the regulatory and surveillance capacities of new technologies" (Sparks, 2020, p. 474). In essence, society as a whole and all crime with it has, to a smaller or larger extent, been transformed by digital technology.

Drawing on the work of ecological psychologist James Gibson (1986), much has been written about the *affordances* of environments and ICT, from a variety of perspectives including sociology (Hutchby, 2001), organisational studies (Fayard & Weeks, 2014), design (Norman, 1999) and, to a lesser extent, cyber security (Busby, Green, & Hutchison, 2017). Affordances describe the properties of an environment in relation to the capabilities of an organism (Chemero 2003). Technological affordances therefore, describe the possibilities for action

[10] According to Castells this change applies throughout all social relations, from the nation state, big corporations to local businesses. It is only by harnessing ICT to become horizontal and flexible structures that large corporations remain competitive in the global market. Without this 'spirit of informationalism' (Castells, 1996, p. 195), to drive innovation or 'creative destruction' (Webster, 2006, p. 105), even large corporations are threatened in the *network society*. This systemic volatility has, of course, far reaching consequences for employment and social relations. Critics of Castells, while acknowledging his considerable contribution to the study of modernity, point towards a range of issues including an "underestimation of the salience of class inequalities, the relation between continuity and change in his argument, and ambiguities as to what he understands by information, to a lingering technological determinism at the heart of his thesis" (Webster, 2006, p. 123).

which a given technology allows, with respect to the capabilities of an actor. This goes beyond a mere dispositional understanding of technology, towards one where affordances are seen as both features of technology and relational, i.e., constructed by actors based on their motivations and capabilities. Şahin et al. (2007) take affordances a set forward, incorporating the effect of an affordance into its definition. In the digital society therefore, cybercrime is characterised by the exploitation of a set of technological affordances, constructed through the motivations and capabilities of victims, offenders and the providers of the technology itself, and enabled by social practices and the regulatory and technological architecture of the informational networks of cyberspace. Consequently, the more embedded digital technology becomes, the harder the distinction between cyber-enabled, cyber-dependent and cyber-related crime is to draw. In fact, the online/offline dichotomy is increasingly recognised as a false one (Furnell & Dowling, 2019). For example, online stalking of victims, followed by the hacking and dismantling of an alarm system, may be a key and necessary step to the success of a burglary, changing, if not expanding, the scale and scope of a burglar's criminal operation – but burglary remains a crime tied to a specific geography. At the same time, such a crime may rely on the practices and infrastructures of the 'data economy', from individual's sharing of personal data, to its easy and searchable access by criminals, enabled by tech companies. Conversely, as this thesis shows, there are examples of hacking following a 'real world' burglary. Furthermore, victims often receive cold calls in real time, in their own homes, and are manipulated into giving a hacker access to their devices or online accounts. In such cases, the line between cyber enabled/dependant/related and 'traditional' crime is blurred. Finally, on one hand, regardless of the extent to which a crime takes place within an online environment, inevitably there is an offline site where the victimisation is experienced. Consequently, a victim-response relies on the availability of local services, which are challenging to reconcile with the compressed time-space of 'cyberspace'. On the other, it is possible to commit a crime which falls within the CMA 1990, while neither offender nor victim are connected to the Internet.[11] As such, a

[11] For example, where a perpetrator maliciously or recklessly infects a private network or 'intranet' with an impairing virus, this would be an offence under section 3 of the act – covering "unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer". The diminished *mens rea* element of "recklessness" as opposed to intent is significant. Penetration testing and academic experiments have demonstrated that individuals / company employees will often plug into their work or home machines, compromised USB drives 'planted' as bait. In fact, as external drive is assumed to have been the attack vector of the cyber-attack on the internet-isolated and top-secret Iranian nuclear facility, believed to have been the ultimate target of the un-claimed (but widely speculated to be a join USA-Israel effort) Stuxnet worm (Fildes, 2010).

'cybercrime' may occur without it being *placed* in the networks of *cyberspace*. For all these reasons, it is difficult to reconcile 'cybercrime' with attempts to focus on victims' experience and how best to respond to their needs.

1.3.1. Hybrid Crimes

The complex online/offline interactions suggest that 'cybercrime' is too broad to be useful. However, to empirically test and develop theory on one hand and to meet the informational needs of policy and practice on the other, the term 'cybercrime' must be capable of operationalisation. For this reason, Furnell and Dowling (2019) have argued that cyber-enabled crimes should be included in the 'cybercrime' category only where they have followed a cyber-dependent crime (e.g., fraud enabled by hacking), therefore excluding crimes such as cyber-harassment and cyber-stalking or online child sexual grooming from the cybercrime category. Such a classification could also substantially reduce the number of frauds which are labelled as 'cyber' frauds. However, while this definition provides theoretical clarity, establishing whether cyber-enabled crimes such as fraud followed a cyber-dependent crime would lead to considerable practical challenges in the recording and measuring of those crimes. Based on the Home Office Counting Rules (HOCR) for crime, most fraud types recorded by the police in England and Wales are capable of being preceded by (or indeed followed by) cyber-dependent crimes. However, the victim is most likely unaware that this was the case when reporting the crime. For example, many individuals in the sample collected for this study were contacted by offenders via phone under the pretext that their computer needed fixing and then paid to have it 'fixed'. In the process, offenders gained unauthorised access to victims' devices, which sometimes led to further cyber-dependant victimisation (e.g., installation of malware or accounts hacked). However, victims may be unable to tell either way. Furthermore, even where no hacking takes place, often the pretext of "cyber" is a key aspect of the MO (e.g., fixing a computer or a slow Internet connection). Likewise, restricting the 'cyber' label as suggested by Furnell and Dowling may not cover complex dynamics between data breaches, *phishing* emails and victimisation. As discussed below, *phishing* emails qualify as fraudulent 'false representations', which do not necessarily follow from cyber-enabled crime. However, *phishing* emails are often sent in the aftermath of widely covered news stories, such as the TalkTalk data breach of 2015 (Gibbs, 2015). Some individuals whose personal information was compromised suffered direct financial losses and thus were clearly the victims of cyber-enabled fraud. Many, however, were targeted by fraudulent "compensation" emails and phone

calls, which turned out to be fraudulent, allegedly perpetrated by an organised crime outfit (White, 2018), regardless of whether their details were compromised. In the first instance, there is a direct link between the hack and the loss. In the second, while the hack is indirectly connected, it is the pretext of "cyber" which enables the crime. In both examples therefore, recognising the "cyber" element would be key to crime prevention interventions/initiatives.

With the ubiquity of ICT and the increasing role of Internet of Things (IoT) smart devices, the online/offline distinction will become ever harder to draw (Furnell & Dowling, 2019). A recent news story covers a warning issued by the UK's National Cyber Security Centre (NCSC) regarding the risks of unchanged default security settings on poorly designed smart video devices including smart cameras and baby monitors (Corera, 2020). One such vulnerability allowed a hacker to speak to a young girl via the family's smart security camera (BBC, 2019a). Others have reported on vulnerable smart devices including children's toys (Laughlin, 2019) thermostats (Franceschi-Bicchierai, 2016), pacemakers (BBC, 2017; Goodin, 2018) and cars (Quach, 2020). It is thus not a great leap of imagination to anticipate smart devices being used to commit crimes as varied as burglary, child sexual exploitation or even arson and murder. It may be argued that the knowledge necessary to carry out such attacks would place them far beyond the capability of most criminals. However, that would be over-estimating the notoriously poor security features of many IoT devices[12] and under-estimating the ability of the cybercrime market to make hacking tools and services available to a 'non-expert' audience of criminals (Moore, Clayton, & Anderson, 2009).

This discussion leads to the conclusion that "cybercrime" must be understood at once broadly – to reflect how, in the 'Digital Society', digital technology increasingly permeates everyday life and continues to change social relations – and narrowly, in the sense that it is most useful as an analytical construct if it meaningfully distinguishes between crime types. Further, it has demonstrated some ways in which the online/offline dichotomy can be a false one with respect to F&CM. Therefore, as suggested by van Wilsem (2011), empirical work should seek to measure both online and offline elements, so as to make visible their interaction. This was confirmed through exploratory empirical analysis of the data in this study, which revealed the difficulties in attempting to classify reported crimes dichotomously as online *or* offline. As

[12] A situation which has led to a commitment from the UK government's DCMS for the introduction of new legislation to improve the security standards of smart devices.

such, rather than operationalising the term "cybercrime", this thesis focuses on Fraud and Computer Misuse crime categories, while examining the interaction of online ***and*** offline elements within the criminal *Modus Operandi* and the process of victimisation. Rather than a binary online/offline approach, sampled cases were coded with respect to whether there were salient online and offline, thereby identifying 'hybrid' crimes (Caneppele & Aebi, 2019).[13] The remainder of this chapter will summarise the legal definition of Fraud and Computer Misuse in England and Wales and establish the crime typology used throughout the thesis.

[13] Refer to the methodology chapter for further details of this coding.

2. Understanding Fraud and Computer Misuse

Following from the above discussion, this thesis focuses on patterns of victimisation in the context of Fraud and Computer Misuse (F&CM) offences, including online, offline and hybrid crimes. In what follows, the legal definitions of these crimes will be detailed. Broadly, fraud is understood in the context of this thesis in relation to the main fraud offence created by the UK's Fraud Act 2006 (FA 2006) and computer misuse as including the offences created by the Computer Misuse Act 1990 (CMA 1990). This section provides an overview of how these offences are defined in law and their implications for crime victims.

2.1. Legal Definitions of Fraud and Computer Misuse

2.1.1. Fraud

Fraud is a broad term which describes a variety of criminal behaviours ranging from one-off petty-fraud (e.g., a customer swaps price tags in a shop to pay less for an item), to medium-sized consumer frauds (e.g., an item misleadingly represented as an original luxury item online), to large-scale corporate conspiracies (e.g., the Enron accounting scandal of 2008). Any study of 'fraud' requires, therefore, a well-defined focus. Given the large volumes of fraud affecting individuals as noted in the introduction and the limited ability of the CJS to both prosecute offenders and protect their victims (see section two), this thesis focuses primarily on fraud reported by individuals.

The FA 2006 specifies that fraud may be committed in one of three ways: by false representation (s. 2), by failing to disclose information (s. 3), or by abuse of position (s. 4). In other words, the forbidden behaviour or *actus reus* of the main fraud offence is one of the three forms of conduct listed in the previous sentence. The forbidden intention or *mens rea* of the offence is two-fold: (1) intending to make a profit, cause a loss or expose another to a risk of loss; and (2) acting dishonestly. Of the three forms of conduct, the first is the most relevant to the context of 'cyber' and 'hybrid' individual victimisation. Here, a representation is false if it is untrue or misleading and the person making it knows that it is, or might be, untrue or misleading. A 'representation' may be understood as a statement made or implied as to a matter of fact, law or someone's state of mind. Alongside this, a representation is regarded as made if it (or anything implying it) is submitted in any form, to any system or device designed to receive, convey or respond to communications – with or without human intervention. As such,

fraud by false representation covers instances such as the use of another person's card details for purchases on-line, known as Card Not Present (CNP) fraud, or the sending of *phishing* emails where the relevant intent can be shown. However, the act of using another's identity without authorisation (often referred to as *identity fraud*) is not in itself a crime, until the requisite intent element can be shown.

Fraud is essentially an economic crime, and therefore does not extend to conduct which has no financial dimension (Law Commission, 2002). The general fraud offence is defined in terms of "gain" and "loss", which are in turn defined as extending only to gain or loss "in money or other property" (s.5). The *mens rea* element of acting 'dishonestly' is not defined in the FA, but it is a well-established legal concept.[14] Furthermore, this *mens rea* element signified a departure from the historic concept of 'deception' found in the old fraud offences and a shift from understanding fraud as a 'result crime' – a crime which took place when the fraudster obtained something by deception, i.e. the victim was in fact deceived – to a 'conduct crime', where the crime happens when the offender carries out the forbidden act with the required intention, regardless of whether or not the loss/gain occurs. In part, this change was needed to cover online fraud, as legal precedent established that machines could not be 'deceived'.[15] In practice however, *phishing* is only recorded as a crime by the UK's national reporting centre Action Fraud where there is a loss to the victim.

2.1.2. Computer Misuse

The CMA 1990 was introduced to address the new wrongs of 'cyber-trespass' including hacking, the spreading of malware and viruses, the disruption of on-line services through Denial of Service (DOS) attacks, etc. Existing criminal legislation in England and Wales proved ill-equipped to meet the challenges posed by behaviour falling within the cyber-trespass category, as attempts to apply the traditional law of theft, forgery and criminal damage to cases

[14] The test of dishonesty was originally found in the case of *R v Ghosh* [1982] 1 QB 1053, and it was what is described in law as a "subjective test". The jury had to consider two questions. Firstly, whether they considered the defendant's conduct dishonest, according to the standards of reasonable and honest people. Secondly, whether the defendant realised that reasonable and honest people would regard the conduct as dishonest. If the answer was affirmative to both these questions, then the defendant acted dishonestly. However, the test subsequently changed to become what is known as an "objective test" with the case *Ivey v Genting Casinos* [2017] UKSC 67 and this the question for the jury is simply "whether the defendant's conduct was dishonest by applying the objective standards of ordinary decent people", regardless of whether or not the defendant realised that their conduct was dishonest.

[15] For example the cases of *Davies v Flackett* [1973] RTR 8 and *Re Holmes* [2004] EWHC 2020 (Admin).

of computer misuse had limited to no success. However, the analogy between trespass on land and trespassing in cyberspace is figurative but without legal substance. In fact, trespass on land is a civil tort which only becomes a criminal offence in very specific circumstances.[16] In contrast, as will be shown below, there is no need to prove intent to commit a further offence in the case of 'cyber-trespass'. Here, the only intent required is to cause a computer to perform a function *without authorisation,* while *knowing* that the access was unauthorised. The concept of authorisation is thus the cornerstone of this act.

The CMA contains five main offences, three of which are of relevance to this thesis. The basic offence is "unauthorised access to computer material" (s.1). Whether this offence has occurred is determined in a three-part test: 1) the defendant causes a computer to perform any function (or enables another to); 2) that access was unauthorised and 3) the defendant knew that the access was unauthorised. Causing a computer to perform any function is illustrated in section 17(2) with respect to a number of examples including (c) using [the computer]. As such, the prohibited action (or *actus reus*) of the basic offence consists of a very low threshold of computer use – simply turning on the computer might constitute 'using it'. The second part of the test relates to the nature of authorisation. In short, the current legal position means that the purpose of access needs to be authorised, making the offence capable of extending to unauthorised use by insiders in a company – or authorisation received under a false pretext, as in the common case of remote access to devices provided to offenders by fraud victims. Finally, the third part of the test relates to whether the defendant knew that their access was unauthorised. Here, the defendant's knowledge is assessed using what is described in law as an 'objective' test – should the defendant have reasonably known that their access was unauthorised, as opposed to a 'subjective' test of what they did in fact know.

Furthermore, a defendant may be liable under the section two (s.2) offence where the unauthorised access under s.1 was carried out with the intention of facilitating a serious enough

[16] Trespass is the act of unjustified and unauthorised entry on another's land and is a tort which goes back to the case of Entick v Carrington (1765). Such an act constitutes a civil tort regardless of any injury or damage to the claimant. However, it is only under very specific circumstances that the tort of trespass becomes a criminal offence. These include failure to vacate premises on request of the lawful occupier (Criminal Law Act 1977, s.7), or a police officer (Criminal Justice and Public Order Act 1994, s.61); the CJPOA also provides for a number of aggravated trespass and other forms of trespassory gathering where it involves threats or actual interference with "any lawful activity" on that land (CJPOA, s.68); and finally there is criminal trespass where it contravenes an Antisocial Behaviour Order – an 'ASBO' – under s.1 of the Crime and Disorder Act. In contrast, the criminal liability for 'cyber' trespass is, as it will be further discussed, far wider than that for trespass on land.

further offence. For a s.2 offence to be committed, the further offence must be one for which (a) the sentence is fixed by law (e.g., murder); or (b) a person who has no previous convictions may be sentenced to imprisonment for a term of five years or more. In the courts' application of (b), the unauthorised access to online bank accounts and credit card databases are generally interpreted as indicative of an intention to commit fraud, often fulfilling the requirements of the s.2 offence (even where the false representation has not yet been made).

Section three (s.3) criminalises conduct such as disseminating computer viruses, deploying malware or carrying out (Distributed) Denial of Service ((D)DOS) attacks. To commit a s.3 offence, it must be established that the defendant committed an unauthorised act with respect to a computer,[17] with the further *mens rea* of having intended to impair, or having been reckless as to impairing, the operation of the computer. Here, recklessness is understood as a person knowingly taking an unjustifiable risk of causing the impairment of a computer.[18] The section clearly covers someone who intentionally or recklessly infects a computer with a virus or some other malicious software.

2.2. Implications for Victims

The above section demonstrated that both fraud and the concept of 'unauthorised access' underpinning computer misuse, are broadly defined. However, despite the breadth of the basic offence of unauthorised access, there may be circumstances where such hacking results in harm to individuals who are nonetheless not recognised as 'victims. Similarly, despite the broad terms of the offence of fraud under the FA 2006, there are situations where individual victimisation would not be recognised by CJS and other institutions (e.g. retailers or banks). However, this lack of recognition may have consequences in terms of the support and compensation victims can access.

One example is the potential impact on individuals of the data breaches such as the one suffered by the US-based company Equifax. On September 7th, 2017, the company disclosed that the personal information of over 143 million customers was compromised. The information

[17] Section 17(8) indicates that an 'unauthorised act' is any act which is not authorised. As such, even though the language used in section 3 is slightly different, the courts have applied the same understanding of authorisation explained with respect to the section 1 offence. In addition, an 'unauthorised act' also includes a series of acts.

[18] Following the *Cunningham* test in *R v Cunningham* [1957] 2 QB 396.

compromised included details such as social security numbers, birth dates, addresses and credit card details of individuals. In addition, Equifax eventually confirmed that an estimated 694,000 British citizens were also affected by the breach, 29,000 of whom had their driving licence number compromised (BBC, 2017d). As a result, millions of people could have had their identity used fraudulently by criminals and incur financial losses both directly if their credit card details were used to make purchases and indirectly if a fraudster acquired 'bad credit' in their name. However, in this case Equifax were the victims of the hack, not the individuals. Furthermore, where an individual's identity is fraudulently used to obtain services etc., it is the service provider that is defrauded, rather than the individual whose details are used. The misuse of one's personal information, often referred to as *identity fraud,* is therefore not a crime in itself. In this scenario, the low threshold of liability with respect to F&CM provides little redress for the individual victims whose details were compromised.

Another example is the potential impact of large infrastructure-level incidents on individuals. The *WannaCry* ransomware attack in 2017, for example, affected several organisations and services globally, including a number of National Health Service (NHS) hospitals in England and Wales. Exploiting a known but unpatched vulnerability in legacy Windows operating systems, the attackers caused a programme to be installed on vulnerable systems which encrypted data and demanded a ransom for their restitution. The attack affected thousands of computers and many organisations across the world, including 61 NHS trusts in the UK (BBC, 2017a, 2017b). This led to a significant number of services (including A&E) being disrupted and operations being cancelled (BBC, 2017c). Although it is not possible to say conclusively that any loss to human life, human illness or injury has resulted from this disruption, the attack did create a significant risk that this may result.[19] It is unclear, however, whether individuals who were victimised in such attacks would be recognised as victims and encouraged to access victim support services, seek compensation or who may play a role in such a response. It is also far from clear whether the software providers can be held accountable for sub-standard security and failures to 'patch' or enable the patching of vulnerable systems.

The implications of the legal definitions of F&CM for victims, the complexities of protecting individuals against these crime types and the role of the CJS vis-à-vis tech business and other stakeholders, require exploration which goes beyond the aims of this thesis. Nonetheless, this

section has highlighted the importance of recognising all victims of F&CM and where some of the gaps may be, given the legal landscape. The next section goes a step further by developing the typology of categories of F&CM which will be used in the rest of this thesis and considering the impact of existing typologies for victim recognition and visibility.

2.3. Towards a Working Typology

Despite its apparent simplicity, the consolidated UK criminal law on Fraud masks a level of complexity which becomes apparent when considering the myriad of fraud typologies developed by academia, industry and governmental bodies. As has already been highlighted, fraud may occur on a large or a small scale, over short or long periods of time, online, offline or a combination of the two, it may overlap with other crime types (e.g., typically computer crimes and money laundering, but also 'traditional' crimes such as burglary) and it can range considerably in terms of the complexity of the organisation of the criminal operation. As a result, a number of fraud typologies have been developed by official governmental sources (e.g. the National Fraud Investigation Bureau's fraud codes and Crime Survey for England and Wales fraud categories), by industry (e.g. ACFE, 2016; Cifas, 2017; FFA UK, 2017a) and by academics (e.g. Button et al., 2009b; Kuhl, 1998; Levi & Burrows, 2008; Stabek, Watters, & Layton, 2010). Crucially, each of these typologies was developed from a need to better understand specific victims, offenders or fraud types. As such, it was necessary to consider fraud categories against the research questions to be answered in this thesis and develop the working typology best suited to answer them.

2.3.1. Police F&CM Categories

Given that this work explores repeat victimisation and constructions of vulnerability within crime reports, it is logical to start by looking at how F&CM is categorised by the police. When a victim (or someone acting on behalf of the victim) reports F&CM, the crime is coded according to the categories as set out in the National Fraud Investigation Bureau (NFIB) F&CM codes.[20] At the time of writing, there are 15 NFIB fraud categories relevant to individual and business victims (some containing a further 24 sub-categories between them) and three

[20] See full list of NFIB fraud codes in Annex 1. A full description of each of these can be found in the Home Office Counting Rules.

computer misuse categories (with a further seven sub-categories between them). In total, this amounts to eight unique computer misuse and 41 unique fraud categories.[21] These were developed to be compatible with the UK's National Crime Recording Standard (NCRS), which is central to the Home Office Counting Rules (HOCR) for crime. The guiding principles of the HOCR reflect a macro-level approach to recording crime which aims to reduce double-counting. On the one hand, this constitutes a main strength of the system. On the other, as examined in detail in section two, it can lead to a failure to capture certain kinds of F&CM victimisation and vulnerability.

2.3.2. Industry Fraud Typologies

Two industry bodies Cifas and UK Finance (formerly Financial Fraud Action UK, or FFA UK) collect incidents of fraud from their members, some of which they report directly to the NFIB. The directly reported incidents are compatible with NFIB codes and are included in official crime report statistics. For their own purposes, however, these industry bodies regularly report on fraud affecting their members/clients against a broader fraud typology of their own (ACFE, 2016; Peaston, 2019; UK Finance, 2020b).[22] Comparing and contrasting industry typologies with the police and academic typologies mentioned above highlights their selectivity. Logically, industry bodies focus on fraud categories of particular relevance to their members and/or the services they provide. This may have the effect of over-representing such fraud types, as they are systematically collected on a large scale. However, it also highlights areas which would otherwise be less visible. One example is *identity fraud*, defined by Cifas as situations "when a fraudster abuses personal data to impersonate an innocent party, or creates a fictitious identity, to open a new account or product", of which there were 189,108 cases in 2018, accounting for 58% of all fraud cases Cifas recorded (Peaston, 2019, pp. 3-5). Another is *Authorised Push Payment* (APP) fraud where "a criminal persuades or tricks the victim into sending money directly from their account to an account which the criminal controls", often referred to as *social engineering* and of which there were 122,437 cases in 2019, amounting to losses of £455.8m (UK Finance, 2020a, p. 45). Both identity and APP fraud may be described as offender tactics, rather than fraud types in themselves, but their prevalence and impact mean

[21] Some of the categories have no sub-categories as such, the total number of categories is not a simple matter of summing up the sub-categories.

[22] See industry typologies summarised in Annex 3.

they are relevant to understandings of victimisation. At the same time, they may be understood as *technological affordances*.

2.3.3. Academic Typologies

In addition to the previously discussed cybercrime typologies, academic typologies of fraud tend to be more victim focused. One typology which distinguished between victim types was developed by Levi and Burrows (2008), in one of the earliest reviews to attempt to estimate the costs of fraud from a victim-centric perspective.[23] This rigorous typology aimed to 1) identify gaps in research, 2) identify harm against different groups and aggregate costs and 3) avoid double-counting. Because methods cut across various fraud types, they were not included in Levi and Burrows' typology. As such, the authors emphasised the need to distinguish between fraud types such as CNP fraud, and the methods used by fraudsters e.g., identity fraud. A distinct typology was utilised by Button, Lewis and Tapley (2009a) in a study which focused on understanding the impact of fraud on individual victims and small businesses. This typology divided fraud into three broad groups, *Mass Marketing Scams* (MMS), *Identity Frauds* and *Frauds Against Small Businesses*. In contrast to the previous typology, this one privileges the methods used by the fraudsters as the organising principle, resulting in three very broad groups. For the purposes of this thesis, these groupings were considered too broad.

2.3.4. A Working Typology

Fraud typologies are, to a large extent, driven by the purpose of the research/administrative exercise they serve. As illustrated above, a typology which is developed to estimate overall costs (such as Levi and Burrows'), a typology that aims to capture the impact of specific fraud types on industry (such as those used by Cifas and FFA UK) and a typology developed in order to best capture the impact of fraud on individuals (Button, Lewis and Tapley 2009) will each look very different. For the purposes of this research, it was useful to go beyond the UK legal definitions of fraud to a categorisation which helped highlight patterns of repeat victimisation and constructions of vulnerability. In addition, it was important that the typology used was both relatable to previous literature and capable of mapping against NFIB categories, so that research results may be directly relevant to CJS policy and practice. In order to maximise the relevance of the research results, it also had to be sufficiently detailed, without losing statistical

[23] See Levi and Burrows (2008) fraud typology in Annex I.

power due to some categories having too few cases. The typology summarised in Table 1, was developed to balance of each of these considerations.

Fraud	**Definition**
Advance-fee	Where fraudsters use telephone, mail or e-mail to target victims with a fictitious scenario and persuade them to pay a fee, in advance of either financial (e.g., in the case of lottery or lender loan frauds) or emotional recompense (e.g., in the case of romance fraud).
Business compromise	Fraud committed by an employee against their employer, or by a business against another business.
Card and banking	Fraudulent use of cheques, plastic card (including credit, debit, prepayment and store cards) and bank accounts.
Consumer	Fraud in connection with the purchase of goods or services (allegedly) rendered.
Investment	Investments in fraudulent 'opportunities' including investment in pensions, shares, pyramid schemes, time shares and others.
Other	All other fraud not covered elsewhere.
Public	Fraud against public authorities including fraudulent applications for grants and driver's licenses, benefit and tax fraud.
Retail	Fraud committed against retailers that does not involve online sales or cheque, or plastic card sales. It includes refund fraud, label fraud and obtaining goods or services with no intent to pay.
Services	Fraudulently applying for legitimate services including credit, insurance etc. It also includes fraudulently setting up direct debits from another's account.
Computer Misuse	**Definition**
Hacking	The hacking (i.e., unauthorised access) to a computer system. It includes the hacking of computers, servers, telephone systems, social media and email accounts, with and without blackmail.
Malware, Virus & (D)DOS	Criminal acts which impair the operation of a computer system including computer malware, viruses and (Distributed) Denial of Service attacks.

Table 1 – Analytical fraud categories used in this thesis.

Following Levi and Burrows (2008) and in line with HOCR, the methods used by fraudsters were analysed separately (through the qualitative analysis) rather than as fraud types. However, as suggested by industry typologies and the work of Button, Lewis and Tapley (2009), such

mechanisms of victimisation were considered key to a full understanding of the victimisation process.[24]

[24] Please refer to section four of Annex I for a detailed mapping of the categories used in this thesis to the original NFIB crime categories.

3. Responses to Fraud and Computer Misuse Victimisation

The landscape F&CM response within and beyond the CJS is somewhat fractured in England and Wales. This is unsurprising given the policing structure, the multitude of stakeholders involved, including a plethora of government and third sector support services to which crime victims can turn. Adapting the term used by Button et al. (2012), this may be referred to as the F&CM 'justice network'. This section provides an overview of the F&CM response landscape, providing a summary of the context which informed the analysis in the chapters that follow. As will be seen below, there are examples of multi-agency working and individual organisations have made important contributions towards ameliorating the impact of F&CM victimisation. However, to the extent it exists, the F&CM justice network is a loose one and primarily focused on traditional crime control activities (i.e., the investigation and prosecution of crime), with limited collaboration in and, in many cases, little ownership of, victim support. As such, the response to F&CM remains focused on the retributive triad of establishing what criminal offences have been committed, by whom, and what punishment they deserve. However, as discussed below, this is hardly 'victim-focused' and there are considerable challenges to this traditional policing approach. Drawing on previous work (Karagiannopoulos et al. 2019) and restorative justice principles (Braithwaite, 2004), there is a case to focus on the following four questions, adapted from restorative practices (Zehr, 1990, 2015): what harms are suffered, by whom, how to prevent and repair them, and who has the obligation/ability to do so. The next sub-sections analyse the Criminal Justice System (CJS) and other stakeholders are currently able to address these questions.

3.1. Criminal Justice System Response

Many F&CM victims will begin their 'journey' by calling the AF contact centre or reporting directly via the AF website.[25] Once reported, crime records are then passed onto the National

[25] In limited circumstances known as the "call for service criteria" where there is immediate enforcement action to be taken, local forces will record a case themselves. This includes a) where offenders are arrested by the police, b) where the offender is in the act of committing or has just committed the offence and c) where there is a local suspect, i.e. there are "viable investigative leads" to locate and apprehend a suspect (Home Office, 2020, p. 2). However, a record will also be submitted by the police to AF via the online reporting tool and flagged as having a call for service. In addition, where there is a call for service, local forces are required to provide the NFIB with outcome information. In the data sampled for this study, 12% of reports from business victims and 4% of those by individual victims were recorded with a "call for service".

Fraud Intelligence Bureau (NFIB). However, victims may also start by contacting financial service providers (e.g., banks), other government services (such as National Trading Standards), online marketplaces or other businesses, or third sector organisations (e.g., the Citizens' Advice Bureau). As they navigate their way through this network, there are considerable opportunities for victims to receive the support they need, but also to be lost along the way. In relation to the CJS, high levels of "attrition" have been documented along the F&CM victim's journey (Scholes, 2018, p. 4). *Attrition* is understood from the context to mean the gradual reduction in cases which remain engaged in CJS processes, as they progress from the reporting stage, to the point at which there is a judicial outcome. CJS "attrition" in the year ending March 2015 is illustrated in Figure 4.

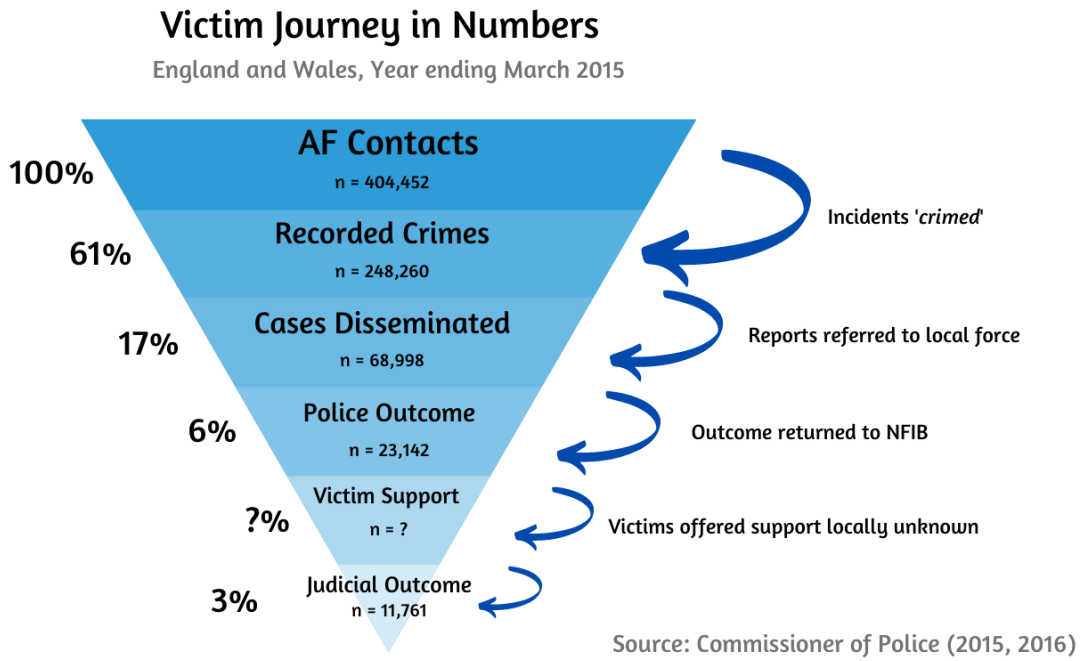

Figure 4 – The Victim Journey in Numbers.

This author's analysis of publicly available information revealed that the proportion of AF contacts which resulted in a recorded crime was approximately 61% in the year ending March 2015 and 63% in the year ending March 2016 (Commissioner of Police, 2015, 2016). These figures are not surprising as the police deal with a large and wide range of non-crime incidents, with the College of Policing suggesting "non-crime related incidents account for 83% of all Command and Control calls" (2015, p. 9). In addition, a very small minority of cases recorded as crimes ('*crimed*') reach a judicial outcome. Once *crimed*, the data enters the NFIB's "Known Fraud" database. Here, it remains until such time as a combination of algorithmic scoring and

human reviewing identifies the case as part of a bundle containing sufficient leads for investigation. Based on the initial algorithmic scoring case bundles are reviewed and optimised by NFIB Crime Reviewers. It is this bundle (rather than individual reports) that is sent (or "disseminated") to a specific local force for investigation, usually based on the location of suspects or, if unknown, the location of the victim. For crimes reported in Wales, the percentage of cases disseminated for further action has been estimated at 15%, in the two-years ending September 2016 (Correia 2019).

Attrition in the CJS is a result of the challenges of policing F&CM (section 3.1.1 below), the division of labour across the three levels of policing in England and Wales (national, regional and local), as well as the overall focus on 'Pursue' type activity (section 3.1.2 below). As a result, the response to F&CM must go beyond the traditional focus on investigation and prosecution of offenders. Each of these challenges is explored below.

3.1.1. Policing Challenges

Volume & Under-reporting

As previously noted, the volume of F&CM in the UK is astounding, even if only a minority is reported to the police. This volume inevitably creates considerable demand for the CJS and the wider F&CM justice network. However, it has also been noted that both F&CM are broad-ranging offences and, as shown throughout this thesis, their impact on victims can vary immensely. As such, the greatest challenge for CJS and other agencies, it is argued, is effective recording and prioritisation, to identify for investigation cases that represent serious and organised criminality, as well as those associated with victims who are especially vulnerable or in greatest need of support. However, the police's ability to effectively record and prioritise is limited by the previously noted under-reporting and, as shown in this thesis, the limitations imposed by the recording tools. Furthermore, as shown in Figure 4, in contrast to judicial outcomes, victim support provision is not systematically recorded or measured as a CJS outcome.

Cross-jurisdictional Cases

F&CM crimes span national boundaries, with victims and perpetrators often located across the globe. This creates challenges where different countries' legislation is misaligned and where police and stakeholders require information/evidence/actions from third parties, beyond jurisdictional boundaries. The sharing of information and evidence across national borders can

be a lengthy and costly process. Bilateral Mutual Legal Assistance Treaties set out the processes by which evidence can be accessed by the police across-jurisdictions, but these can be inefficient, complex and slow processes (e.g. Pullen, 2019; Woods, 2015). Furthermore, given the interaction between national, regional and local policing discussed below, cross-jurisdictional issues may arise within jurisdiction, as investigations and a victim-response may require the coordination of several autonomous police forces.

Anonymity and Pace of Technological Change

Offenders operating remotely cloud themselves in anonymity in several ways. They may use encryption technology to contact victims online, use multiple false identities, destroy digital evidence or (cold) call victims using Voice over IP (VOIP) technology – while masking their real IP address. Easily available tools and the pace at which technology changes make the policing of F&CM extremely challenging. Where law enforcement is successful in investigating F&CM crimes, and victims successful in improving their resilience to specific vulnerabilities, it is likely that offenders will move on to other technologies, often at a greater pace than that at which CJS agencies can move.

Low-risk, High-reward

The availability of cheap computers and "off the shelf" malware and other *exploits* (often open source or available for purchase from internet forums) means offenders do not need to be particularly gifted coders to become cybercriminals. Similarly, stolen credit cards or otherwise personal information with which to commit fraud can be obtained via the Internet at a relatively low cost. Alongside this, the low number of investigations and prosecutions (relative to reports) mean that the likelihood of being caught is also low. In addition, cybercrime is a relatively low-risk activity in itself, when compared other crimes, as offenders can operate from the safety of their own home, without being exposed to physical harm or social sanction. As such, these crime types are low-risk but high-reward.

Inter-Agency Working

Law enforcement must coordinate with multiple organisations to investigate F&CM and support victims, including other police forces nationally and internationally, and private sector organisations. In addition, security goes far beyond "public policing" and law enforcement relies on data and expertise from the private sector such as financial institutions, technology companies etc. which make up what have been called "security assemblages" (Schuilenburg,

2017). However, the members of these multi-agency partnerships will inevitably have competing priorities. As a result, police operations may be hindered (as well as helped) by the necessities and compromises required for such partnerships to work.

State-Actors

Offenders come in many shapes and forms. CM offenders range from the so-called "script-kiddies", to organised criminal enterprises and state(-sponsored) actors. The WannaCry malware for example, which impacted the UK National Health Service in 2017, has been hypothesized as a state-sponsored attack (Corera, 2017). There has also been considerable conjecture that the infamous Stuxnet attack on Iranian power plants was carried out by Western state actors (e.g. Fildes, 2010; Fruhlinger, 2017; McAfee, 2020). Likewise, several high-profile cases of fraud including bitcoin heists and the largest bank heist to date, targeting the Bank of Bangladesh in 2016, have also been allegedly linked to cyber state-actors (Rhysider, 2020). However, given the difficulties of "attribution", i.e., identifying who is responsible for cyber-attacks, the impact and capabilities of state actors remain difficult to measure.

3.1.2. Policing Strategy

In the context of the above challenges, F&CM policing strategy has four strands, following the 'four Ps' approach which originated in UK counter-terrorism policing: 'Pursue', 'Prevent', 'Protect' and 'Prepare'. 'Pursue' relates to the activity of investigating, prosecuting and disrupting offenders engaged in F&CM. 'Prevent' is concerned with preventing people from engaging in F&CM and includes raising awareness of the consequences of offending and, in the case of CM, initiatives to ensure talented individuals are diverted towards legal/ethical 'hacking'. The 'Protect' strand is focused on increasing protection for those who are at risk of (further) victimisation. Finally, the 'Prepare' strand is focused on improving resilience, in order to reduce the impact of F&CM in the future. Alongside this, F&CM policing is also framed by the Serious and Organised Crime Strategy, the National Cyber Security Strategy and the Code of Practice for Victims of Crime (known as the Victims' Code). The latter is discussed in greater detail in chapter two.

While the first two strands of policing are focused on offenders, Protect and Prepare activity are victim-focused, i.e. focused on increasing resilience to victimisation risk and harm. Furthermore, while 'Pursue' is the closest to more 'traditional' approaches to policing, the previous section has demonstrated the challenges of F&CM 'Pursue' activity. As such, the

suggestion that it is not possible for law enforcement to "arrest its way out" of the F&CM problem, often surfaces in discussions with law enforcement. As this section has also shown, an analysis of the typical victim journey supports this analysis. In this context, it is suggested that more emphasis on the Protect and Prepare strands is needed. However, while improvements have been made in relation to protecting and increasing resilience of businesses, the same level of activity is not found in relation to individual victims.

In addition, policing duties and responsibilities are generally localised, with Chief Constables across the 43 local police forces in England and Wales responsible for delivering local police priorities, established in conjunction with the publicly elected Police and Crime Commissioner (PCC). With respect to F&CM, however, responsibility for investigating and responding to victim needs is shared across a three-tiered police structure: the NFIB as the national coordinator (closely linked to the national reporting centre AF), the ten Regional Organised Crime Units (ROCUs) at a regional level and the 43 local police forces at the local level. The NFIB provides the strategic lead for investigations which are supported by the ROCUs, working with the forces within their regions. The 'Prevent' work is led by the ROCUs, as is 'Protect' activity aimed at businesses and organisations. Individual victim 'Protect'-type activity, however, falls within the jurisdiction local forces.

The AF reporting tool/form requests a variety of information from the victim including personal details, demographic characteristics, a measure of the impact of the crime on the victim, the amount of financial loss, a description of the incident and what is known about the alleged perpetrators. Where the victim self-reports via the website, the system will generate a report based entirely on the victim's own assessment and reporting of the situation. Where the victim calls the contact centre, the report is written by the trained staff. As previously noted, AF reports are then submitted to the NFIB's 'Known Fraud' system, where an algorithm identifies inter-related cases with potential leads for investigation. These 'bundles' are then disseminated to a local force or partner agency for investigation. In most cases, this will be the force where the suspect, rather than the victim, is located.

As shown elsewhere (Correia 2019), only a small number of cases are disseminated for intelligence or victim support. However, the NFIB team returns a full list of cases reported by victims within the forces' respective jurisdictions. This was done monthly at first but is now done weekly. As previously noted, responding to victims' needs falls within the jurisdiction of local forces. This expectation is clearly set out in policy terms as responsibility for allocating

funding for victim services is within the remit of the local Police and Crime Commissioners. However, whether and how local forces are discharging this responsibility across the country is unclear. The separation of F&CM investigation and victim-response, combined with the priority given to 'Pursue' type work and/or other crime types in the context of limited resources, results in a lack of ownership of the F&CM victim response. In addition, as will be shown throughout this thesis, the victim data returned to local forces is not optimised for the provision of a victim response.

3.1.3. Beyond 'Just Deserts'

Influenced by the 'Just Deserts' theorists, early work on how victims understood justice as "distributive" of "retributive", i.e., whether the victim believed the offender was sufficiently punished. Later scholarship demonstrated that a 'just' criminal justice process was also important to victims and that in fact, procedural justice (Thibaut & Walker, 1975) enabled victims to cope with the impact of victimisation. Procedural justice from a victim perspective is thus characterised by several aspects including the victim having a voice and control over decisions, trust in the CJS institutions, being treated with dignity and respect and that the criminal justice decisions are neutral, i.e. based on facts and made without bias (Wemmers, 2010). Others have sought to add a further dimension to victims' understandings of justice referred to as interactional justice. This refers to the way in which the procedures are implemented or "the quality of interpersonal treatment [victims] receive during the enactment of organizational procedures" (Bies & Moag, 1986, p. 44). Finally, Greenberg's (1993) taxonomy of justice included information justice, referring to the extent to which procedures are explained to the victim and they are kept informed and configural justice, whether criminal justice outcomes are configured towards achieving equity, responding to need, reducing conflict etc. Such an understanding is more compatible with a restorative justice orientation towards identifying what harms are suffered, by whom, how to prevent and repair them, and who has the obligation/ability to do so (Zehr, 1990, 2015). As this section has demonstrated however, the current system is delivering little retribution or restoration for victims. Nonetheless, there are several examples of victim-focused approaches, including Sussex Police's Operation Signature, as well as key victim-focused initiatives developed by the wider F&CM *justice network* in recent-years. The next section elaborates on these further.

3.2. Victim-Focused Responses

Despite the previously mentioned challenges of policing F&CM, the above sub-section shows that the current policing structures are still predominantly designed to deliver on 'Pursue' outcomes – i.e., investigations leading to prosecutions and convictions. Nonetheless, there are some examples of a victim-focused response, including initiatives across the F&CM 'justice network'. While ROCUs have generally focused their 'Protect' activity on businesses, some initiatives have developed at the national and local force level around protecting individual victims. Two such initiatives include the Economic Crime Victim Care Unit (ECVCU) and Operation Signature, first launched by Sussex Police and subsequently adopted as a model by other forces, including South Wales Police. In addition to the activity of law enforcement, however, there are several other agencies/stakeholders involved in 'Protect'-type activity including National Trading Standards, Royal Mail and the financial industry. In what follows, current victim-focused responses will be discussed in greater detail.

3.2.1. Police 'Protect' Activity

While there is limited guidance at the national level to inform the identification of victims which require additional support, the launch of the Economic Crime Victim Care Unit (ECVCU) bucks the trend. The ECVCU compromises a team of victim support advisors whose role is to support "vulnerable people who have fallen victim to fraud and cybercrime, with the aim being to make them feel safer and reduce the possibility of them becoming a repeat victim" (Action Fraud, 2018). The initiative started as a pilot in London and was then expanded to a telephone service in the West Midlands and Greater Manchester. Based on discussions with stakeholders, advisors review victim data for these three forces and make an assessment of victim vulnerability based on the victim's self-report and a series of key-word text searches. When the data sampled for this study was collected, individuals reporting via AF were asked three questions to help determine vulnerability including 1) Have you been a previous victim of fraud?; 2) Are you at risk of losing money? and 3) Are you a regular target of fraudsters? At the time of visiting the team, the ECVCU staff based at City of London Police reviewed all cases where these questions are answered affirmatively (level 1), while their colleagues in Scotland review the remaining cases (level 2). Since then, the vulnerability scoring has evolved, but the principle of a vulnerability-score-based triage remains.

In addition, several examples of good practice can be found within local forces, including Operation Signature, launched in 2014 by Sussex Police and adopted/adapted by a number of forces since, including South Wales Police in November 2017 (South Wales Police, Personal Communication, 2018). Operation Signature is a "campaign to identify and support vulnerable victims of fraud within Sussex" (Sussex Police, 2018). It involves identifying victims vulnerable to fraud, providing them with protection advice, working in partnership with statutory and voluntary organisations to signpost victims to other services and training new officers on how to identify and support victims. To deliver this, Sussex Police appointed a Financial Abuse Safeguarding Officer and the PCC funded two roles within the charity Victim Support to work with vulnerable repeat victims (Sussex PCC, 2017). Within Wales, some aspects of Operation Signature were adapted by South Wales Police, including its methodology for identifying vulnerable victims (see chapter two). This involves, firstly, a risk assessment of all victim reports in line with THRIVE principles[26] which leads to the allocation of cases to the victim's local Basic Command Unit (BCU) area; and secondly, a victim visit and the Op. Signature risk assessment. This risk assessment requires the visiting officer to fill in a questionnaire available to officers via a mobile application, which collects considerable detail about the victim's circumstances. These data are linked to a scoring matrix which places the victim on a high, medium or low risk category. At this point, the data are returned to the force's Action Fraud Single Point of Contact (SPOC), who then refers those deemed to fall within the high-risk category to the relevant partner agency for further support. The extent to which partner agencies can respond to this need, is an area for future research.

3.2.2. Phone Blockers

First launched as a pilot scheme in 2017 and funded by DCMS, the National Trading Standards' Scams Team makes phone blocking devices freely available to individuals who are considered vulnerable and are being targeted by nuisance and fraudulent phone calls (Eastbourne Herald, 2016). The blocking devices are provided by the company trueCall. They stop calls containing recorded messages, silent calls and, where the option is activated, completely block calls from numbers not on a list pre-identified by the homeowner (known as 'white-listing'). Although

[26] West Midlands Police developed and introduced the THRIVE model (Threat, Harm, Risk, Investigation, Vulnerability and Engagement) for their call management centres, where they risk assesses each call and provide an appropriate response based on that assessment (NPCC 2017).

information is limited on the features of these particular blockers, trueCall's website suggests that calls can be recorded and the white-list edited online, features which in themselves carry privacy and security risks. Nonetheless, the pilot is reported to have blocked over 100,000 calls to 214 vulnerable individuals in the space of a year, who had previously lost a total of £970,042 to nuisance calls and, of which, only 1% experienced further losses during the pilot (NTS, 2018, 2019). In the most recent phase of the project, individuals are invited to apply for these call blockers via the NTS' *Friends Against Scams* campaign website in March 2020, with an early referral option made available to local stakeholders e.g., through the Wales Against Scams Partnership. Individuals considered vulnerable for the purposes of this scheme are loosely defined and include those suffering from dementia, mental health issues, recent bereavements, or who are otherwise deemed to be at risk of becoming victims of fraud.

3.2.3. Fraudulent Mail Prevention

Fraudulent mail is a widespread social engineering method used predominantly in Mass Marketing Scams (MSS) to establish contact with potential victims. Where MMS mail campaigns are identified by Royal Mail, letters are confiscated before delivery. In addition, National Trading Standards (NTS) works with Royal Mail to identify and alert vulnerable and repeat victims of fraudulent mail, in particular the elderly. When a referral is made by NTS to the local authority's Trading Standards Services (TSS), they will visit/contact the individual to ascertain whether or not they were victimised, alert them to risk or actual fraud (they may not know or believe they have been victimised) and record information on previous losses.

3.2.4. The Banking Protocol

The Banking Protocol, first trialled in London in October 2016, was rolled out nationally in March 2017. Where banks adhere to the protocol, bank staff are trained to stop suspicious transactions, which may be indicative of fraud. Where fraud is suspected, customers are asked a series of questions, the responses to which may trigger the protocol. When this is activated, the bank staff will call the local police and are guaranteed a priority response, with several arrests having been reported in the media. According to UK Finance, the protocol has resulted in banks preventing £19 million in fraud in the first half of 2020 and a total of £116 million and 744 arrests since its introduction (UK Finance, 2020a).

3.2.5. The Financial Abuse Code of Practice

The Financial Abuse Code of Practice is another initiative of the financial industry launched in August 2018, taking forward the recommendations of the (2016) Financial Services Vulnerability Taskforce. This voluntary code was designed to, among other things, ensure greater awareness of financial abuse in its various forms (e.g., by intimate partners, family members, in the context of domestic abuse or the financial abuse of the older population), encourage disclosure, as well as a consistent and adequate response across the sector once abuse is disclosed by a customer (UK Finance, 2018).

3.2.6. APP Code

The greatest known losses to fraud victims as reported by financial institutions in the UK are associated with 'card not present' and 'authorised push payment' (APP) fraud. The first refers to bank card details being used without the authorisation of the customer, while the second refers to situations where individuals are socially engineered into authorising a payment to a fraudster. To address the issue of APP fraud, the multi-agency Authorised Push Payment (APP) Scams Steering Group developed a voluntary code for financial institutions (officially the Contingent Reimbursement Model Code 2019). Under this code, victims of APP will be fully reimbursed by the bank or payment service provider of which they are customers, "provided they did everything expected of them under the Code" (APP Scams Steering Group, 2019b). This includes taking action following warnings from providers, not making payments without a reasonable belief that it was legitimate and not acting with gross negligence. In addition, the code states that vulnerable victims should be refunded regardless of whether they have complied with these expectations. At the time of its launch, "eight payment service providers, representing 17 consumer brands and over 85 per cent of authorised push payments" signed up to the code (APP Scams Steering Group, 2019b). Although this code only applies to frauds to have happened since its launch date (28 May 2019), and therefore would not be applicable to the victims sampled in this study, this is a welcome scheme and its development an example of successful multi-agency work.

4. Conclusion

On the one hand, the term 'cybercrime' is widely adopted by the media, policy makers, academia, law enforcement and the general public. It is therefore of paramount importance to engage with it. On the other hand, this chapter has shown how the term perpetuates an increasingly false on/offline dichotomy, which fails to fully capture many individuals' victimisation experiences. From the victims' standpoint, every 'cyber-dependent' crime is placed within 'real' space – they interact with the offender in a defined time-space and often experience losses, be it in the form of tangible or intangible property. Likewise, cyber-enabled crime such as Dating or Investment frauds involve *social engineering* methods. Such crimes have a socio-emotional dimension quite apart from the online methods used. As such, the term 'cybercrime' may be described both as under and over-inclusive. Theoretically, it obscures more than it clarifies, as it fails to capture online/offline interactions and 'hybrid' victims (van der Wagen & Pieters, 2020). Furthermore, while cyber-criminology orthodoxy has focused primarily on crimes such as online fraud and computer misuse, it has done so primarily through limited theoretical perspectives and a crime control lens (Powell et al. 2018). However, such a perspective sheds limited light on the notion of vulnerability. Finally, prevention messaging which over-relies on the concept of 'cybercrime' may overlook on/offline dynamics key to victims' experiences and thus alienate individuals in need. It is thus concluded that while "cybercrime" remains a useful (if not unavoidable) starting point for discussion, it is more fruitful to study the interplay of the online and offline elements of crime, without making strong assumptions about what crime types are 'cyber' in nature.

As a result, while the relationship between online/offline is explored empirically, this thesis operationalises specific crime categories within the broad crime types of fraud and computer misuse (F&CM). Fraud is defined in accordance with the FA 2006 and, drawing on Levi & Burrows, summarised as "the mechanism through which a fraudster intends to obtain financial advantage, cause loss or expose another to the risk of loss, by implicitly or explicitly acting dishonestly" (2008, p. 299). Computer misuse refers to the main offences under the CMA 1990, the first three of which focus on the key concept of unauthorised access/acts and were examined in some detail in this chapter. This chapter has shown that focusing on F&CM is considerably more precise than examining 'cybercrime'. Nonetheless, F&CM offences are still broad and associated with low thresholds of liability. As such, a F&CM typology was developed in this chapter for use in the empirical study conducted for this thesis. This typology draws on

previous literature (Levi & Burrows, 2008; Button, Lewis and Tapley, 2009) and is capable of mapping against NFIB crime codes. In addition, it was refined throughout the analysis to preserve detail, without losing statistical power.

Despite this, however, legal definitions may result in individuals who are 'harmed' as a result of F&CM and hence, as discussed in chapter two, classed as 'victims' are not always recognised as such by CJS agencies. This results from the administrative needs of CJS agencies to avoid double counting and from the conceptualisation of 'the victim' as a single agent. However, recent cyber-attacks such as the WannaCry ransomware and the Equifax breach, demonstrate that 'the victim' is a hybrid of individuals, machines and organisations (van der Wagen & Pieters, 2020). In both examples, the incidents were related to unpatched but known technical vulnerabilities. Such vulnerabilities are often beyond the control of the individuals they affect and are a manifestation of the technological *affordances* of ICT systems. A useful vulnerability framework must therefore be capable of shedding light on the role of multiple actors and a full range of vulnerability dimensions, including the role of such affordances.

Finally, the need to understand vulnerable and repeat victims was set out against the broad landscape of F&CM response in E&W. This chapter provided the necessary context to understand the current landscape of the CJS response to F&CM. It first considered the volume of reported crime which enters the CJS and its 'journey' from crime report to possible court outcome. It also reviewed the policing strategy, to identify where the responsibility for a victim-response rests within the three-tiered structure of F&CM policing. Finally, several victim-focused initiatives aimed at preventing individuals from becoming victims of F&CM were introduced. The chapter illustrated the difficulties of taking a traditional 'Pursue'-style approach to policing F&CM and highlighted some of the best practice around protecting vulnerable and repeat victims within the broader F&CM 'justice network'. As will become clear from the analysis in chapters four and five, many of the initiatives highlighted above target key points of the 'anatomy' of a fraud including the ways in which offenders make contact with victims, where the victim is about to pay a fraudster or, where victimisation has occurred, the circumstances under which the victim might be compensated for their losses. On the whole, the initiatives discussed above provide a blueprint for the kind of multi-agency working which is required to effectively reduce the impact of F&CM on victims. As will be discussed throughout this thesis (and particularly in chapter two), however, there are several

‘blind spots’ in current understandings of what makes someone vulnerable in the context of F&CM victimisation.

There can be no doubt that F&CM crimes present new and developing challenges for policing and other CJS agencies, the result of which is a high level of ‘attrition’ in the traditional ‘Pursue’ type activity, with few reported cases being investigated and prosecuted. Consequently, the response to F&CM must go beyond traditional policing. However, it is clear that ‘Protect’ type activity and the victim-response more broadly is inconsistent across England and Wales. In part, this results from the need for a multi-agency and localised response. Furthermore, despite some best practice, there is a clear gap in evidence-based methods through which to identify vulnerable victims. As discussed further in the next chapter, vulnerability is often understood in rather narrow terms which do not necessarily capture the realities of victimisation or victims’ support needs. This is a gap which this thesis hopes to fill. The concepts of ‘victim’ and ‘vulnerability’ are further examined in the chapter that follows.

CHAPTER 2: Victims and Vulnerability

This chapter defines and explores the concepts of 'victim' and 'vulnerability' in the context of F&CM victimisation. Here, a 'victim' is someone who has suffered a harm, as a result of a criminal act, which falls within the F&CM categories set out in chapter one. However, even where the remit of study is thus limited, who has the power to claim the victim label, to apply it and how these decisions are made are central questions to a critical victimology (Walklake 2007).[27] Such questions remain under-explored in the context of F&CM victimisation. The process of being victimised is referred to as victimisation and the mechanisms through which someone is victimised (e.g., social engineering, hacking, cold calls etc.) are referred as the *Modus Operandi* (MO) of the crime. The term 'vulnerability' has its roots in the Latin word *vulnus*, meaning "wound". Criminological work on vulnerability has focused overwhelmingly in areas such as sex work (e.g. Munro & Scoular, 2012), hate crime (e.g. Chakraborti & Garland, 2012) and the relationship between vulnerability and fear of crime (Ferraro, 1995; Killias, 1990). However, this chapter demonstrates that understanding vulnerability is key to improving the response to victims of F&CM. Furthermore, it is a concept which crosses disciplines including globalisation studies (Turner, 2006), development studies (Chambers, 1983) and legal theory (Fineman, 2008). Drawing from this multi-disciplinary body of work is both enrichening and illuminating to understand vulnerability in the context of F&CM victimisation.

Like typologies of F&CM, typologies of 'the victim' are many and varied (e.g. Christie, 1986; Fattah, 1991; Mendelsohn, 1956, 1976; von Hentig, 1948). However, for the purposes of this thesis, it was useful to conceptualise 'the victim' as operating at three district levels of analysis: the *micro* (individual), *meso* (institutional) and *macro* (cultural) levels. In what follows, the first two levels will be explored in detail, with references to the third where applicable. In doing so, this chapter highlights the role of the concept of 'vulnerability' across all levels. Consequently, it is argued that the terms *victim* and *vulnerable* are twin concepts. Furthermore, as it will become clear from the discussion that follows, one group of victims which are

[27] The field of victimology extends to 'general victimology' encompassing wider victimisations such as those resulting from natural disasters and war (Hall, 2009a, p. 4).

considered vulnerable within victim policy are repeat victims, those victimised more than once within a given time period. However, being a (repeat) 'victim' and being 'vulnerable' is not entirely equivalent and vulnerability remains under-theorised with respect to F&CM victims (Skidmore, Goldstraw-White, & Gill, 2020a, 2020b). This chapter disentangles these concepts to achieve a greater depth of understanding of F&CM victimisation, on which the rest of this thesis is grounded.

1. The Individual Micro-Level

At the micro-level, 'the victim' arises from an inter-subjective perception and/or experience of harm, which results from crime. As such, understanding the range of harms associated with F&CM is key to understanding victim experiences. Furthermore, "experiential victimisation" (Walklake, 2011, p. 181) is linked to the individual's own experience and self-assessment of their own vulnerability to criminal victimisation, including the harms they have/might suffer and how they have/might cope with those harms. However, this self-perception and experience does not happen in a vacuum and will be influenced by interactions with others. As such, the individual experience is linked to the meso and macro-levels of analysis. Firstly, at the micro-level of analysis, 'the victim' is understood as an individual who firstly, had an experience of criminal victimisation i.e., was 'harmed' or negatively impacted by a criminal act. Secondly, the individual must accept the status of 'the victim'. Accepting this label, from this author's constructivist perspective, requires the victim to reflect on and interpret their own experience as one of victimisation, which inevitably depends on the individual's knowledge and social context, their ability to communicate the experience to others, as well as others' response (Strobl, 2010). This includes recognition, or lack there of, of 'the victim' status at the institutional meso level. However, F&CM victimisation carries considerable stigma, especially with respect to fraud (e.g. Button & Cross, 2017; Cross, 2015, 2018). As such, individuals may actively seek to disassociate themselves from 'the victim' label – even when others seek to impose it on them. In what follows, previous literature is reviewed, to explore the victim impacts of F&CM experiences and they might reject 'the victim' label. It is suggested that accepting the 'victim' status requires individuals to see themselves as vulnerable and perceive the victimisation experience as reflecting and/or exacerbating that vulnerability.

1.1. The Impact of F&CM Victimisation

Crime is known to result in a wide range of harms or impacts on the victim's wellbeing (Spalek, 2006) and F&CM is no exception. For some, these crimes have little or no impact (Button & Cross, 2017; Button et al., 2009a). Examples of this may include where the risk of loss is accepted by the victim when making an 'investment' or an online purchase. However, F&CM can also have serious negative impacts for victims. In a review of the evidence, Blakeborough and Correia (2018) summarised these as including financial loss, emotional distress (stress, anxiety, feelings of mistrust), strained relationships with family and friends, worsening physical and mental health issues and, at its extreme, suicide or suicidal ideation (see Button & Cross, 2017; Button et al., 2009a; Kerr, Owen, Nicholls, & Button, 2013). This sub-section summarises the known impacts of F&CM and crime more generally, on individual victims. Furthermore, it shows how these impacts are linked to individuals' self-acceptance as victims.

Psychological and emotional impact

Victimisation experiences can lead to a breakdown of the individual's understanding of the world which may lead to individuals rejecting the victim label altogether (Strobl, 2010). This may be explained through the Belief in a Just World theory (BJW), which suggests that most people believe they live in a just world where people get what they deserve (Lerner, 1980; Lerner & Simmons, 1966). Other psychological impacts may be the loss of a sense of control, often coped with through feelings of self-blame and/or favourably comparing one's own experience with that of others (Spalek, 2006). Additionally, emotional impacts previously shown to be associated with fraud victimisation include feelings of anger towards the perpetrators (Button, Lewis, & Tapley, 2014; Spalek, 1999), stress or worry (Pascoe, Owen, Keats, & Gill, 2006), upset (Button et al., 2009a) and ridicule or embarrassment (Button, Lewis, et al., 2014). Research on *Mass Marketing Fraud* also captured feelings of stress, anxiety, and loss of self-esteem, because of victimisation (OFT, 2006). On one hand, these emotional states may allow individuals to 'take control' of the situation. On the other, they can adversely impact on the victims' health and wellbeing.

Physical and mental health

The impact of fraud on some individuals mental and physical health has also been documented, while the impacts of CM are less well understood. Fraud victimisation has been linked to depression (Button et al., 2009a; Ganzini, McFarland, & Bloom, 1990) and, in a minority of

cases, suicide attempts or ideation (Button, Lewis, et al., 2014). Furthermore, the psychological strain of fraud victimisation has also been linked by victims to the deterioration of physical health and the manifestation of physical symptoms such as nervous skin conditions (Button et al., 2009a; Spalek, 1999).

Relationships

Fraud victimisation can also result in relationship strain or breakdown (Button, Lewis, et al., 2014). For example, the individual's relationships with friends and family may become strained due to the financial impact of these crimes, the victims' concealing of the victimisation or, in extreme cases where the individual denies victimisation and continues to engage with the fraudsters. The latter may be particularly acute in situations where the criminals manipulate the individual into isolating themselves from loved ones. As discussed elsewhere in this thesis, it is particularly challenging to respond to the needs of these "designated victims" (Strobl, 2010, p. 6)(see section two below).

Fear of crime and repeat victimisation

Victims may also become fearful of, or more *vulnerable* to, repeat victimisation. One theory within the vast 'fear of crime' literature suggests that fear of crime is associated with prior victimisation (e.g. K. A. Fox, Nobles, & Piquero, 2009; Keane, 1995; Rountree, 1998; Skogan, 1987), described as the 'victimisation thesis' (Brands & van Wilsem, 2019, p. 7). There is a small but growing body of research into fear of online crime, including on inter-personal online crimes such as harassment/stalking (e.g. Henson, Reyns, & Fisher, 2013; Randa, 2013) and online fraud (e.g. Brands & van Wilsem, 2019; Brunton-Smith, 2017; Virtanen, 2017; Yu, 2014). However, the existing work has yielded mixed results with respect to how prior victimisation and vulnerability affect fear of online crimes, as well as what individual characteristics are associated with increased fear of online crime (Virtanen, 2017).

While fear of F&CM is beyond the scope of this thesis, this is certainly an area for further research. Furthermore, research is needed to establish whether the vulnerability dimensions/factors identified in chapters to come are correlated with individual's fear of F&CM. Moreover, prior victimisation has been demonstrated to be a high predictor of future victimisation (S. D. Johnson, 2008; Tseloni & Pease, 2004), suggesting such fears are well founded. More recently however, it has been argued that self-perceptions of vulnerability

(rather than prior victimisation) are best placed to explain differences in fear of crime (Farrall, Jackson, & Gray, 2009). Repeat victimisation is discussed in detail in section four below.

Behavioural impacts

Previous research has shown that perceived risk of victimisation partially mediates individuals' willingness to use ICT (Böhme & Moore, 2012; Hille, Walsh, & Cleveland, 2015) and online banking and shopping (Brands & van Wilsem, 2019). There is evidence that this perceived risk (or 'fear') is increased with prior experiences of victimisation (Brunton-Smith, 2017) and may lead to avoidance behaviours (Riek, Abramova, & Böhme, 2017). These reflect the results of an earlier study of *Mass Marketing Fraud,* which found that over half of fraud victims surveyed changed their purchasing or payment behaviour following victimisation (OFT, 2006). Similarly, in an interview study of over 700 victims, Button et al (2009) also found that most victims had changed their behaviour as a result of a victimisation experience. Victims changing their behaviour is not necessarily negative and could signal increased guardianship. At the same time, the increased reliance on digital services means that increased feelings of anxiety and lack of confidence online, can considerably constrain individuals' lives.

Secondary and indirect victimisation

Secondary victimisation refers to instances where victims' subjective experience of victimisation is not recognised or properly understood by those around them, resulting in further negative outcomes (e.g., distress, anxiety, further victimisation), which could otherwise have been avoided or ameliorated. Secondary victimisation can therefore "be understood in the context of coping" (Strobl, 2010, p. 15) and relates to the way in which CJS agencies and others respond to a victimisation experience. Indirect victimisation refers to the harms suffered indirectly because of criminal acts e.g., by the close relatives or friends of the individuals who are victimised. As shown in section two below, there is little recognition for either secondary or indirect victims of F&CM.

Other impacts

Finally, F&CM victimisation may also lead to actual or fear of violence, damage to reputation, or criminal liability for victims themselves. Individuals can experience damage to their reputation when criminals use their identity to commit crime, and/or experience considerable anxiety at the possibility. Button et al. (2010 as cited in Button & Cross, 2017) include the testimonial of an individual in London who was (very publicly) suspected of downloading child

pornography because his identity was used by criminals to do so with grave subsequent impact on his life and wellbeing. They also include examples of individuals who are concerned about the ways in which others may use their personal information. Fraudsters often use victims' details to fraudulently obtain credit which then impacts on victims' credit rating and require considerable time and effort to rectify the situation, with potential for long-lasting reputational losses. Furthermore, victims of F&CM have also experienced fear as a result of threats of violence, threats of legal action and blackmail (Button & Cross, 2017). Finally, in some cases where fraud victims have been manipulated into laundering money for offenders, victims themselves have faced criminal charges and/or been imprisoned.

1.2. The Self-Rejecting 'Victim'

Individuals may recognise that a crime has been committed 'against them' and perhaps even report it, without accepting 'the victim' label (Fohring, 2018). Several reasons may explain why F&CM victims, who experience any number of the previously mentioned impacts, reject 'the victim' status. Firstly, being victimised may directly challenge the individual's own beliefs, be it a sense of "personal invulnerability, that the self is good and the world is safe and just" (Fohring, 2018, p. 153) or, in the case of some fraud victims, that the 'relationship' built with the fraudster was genuine, rather than based on deception. Drawing on the Belief in a Just World theory (BJW) (Lerner, 1980; Lerner & Simmons, 1966) and the work of psychologists such as Janoff-Bulman (1995), it is understood that most individuals subscribe to three core beliefs including "personal invulnerability, that the self is good and the world is safe and just" (Fohring, 2018, p. 153). Furthermore, being a victim of crime is, for most individuals in the UK, a rare event. As being victimised is something that mostly happens to 'other people', BJW beliefs are reinforced. BJW theory can also explain why others may be inclined to engage in 'victim-blaming' behaviour (Aguiar, Vala, Correia, & Pereira, 2008; I. Correia & Vala, 2003; Loseman & van den Bos, 2012), something which has been well documented towards victims of fraud (Button & Cross, 2017). Thus, by distancing themselves from the victimisation experience, both victims and those around them are able to preserve their core beliefs (Fohring, 2018; Strobl, 2010).

At the same time, self-denial of 'the victim' status may reflect the corresponding lack of recognition by others. Cross (2013, 2015) for example, has argued that stereotypical perceptions of fraud victims as motivated by greed on one hand and gullible and/or uneducated

on the other, will dissuade individuals from seeing themselves as victims and rather assume they are somehow culpable and therefore deserving of their own victimisation. This can lead to situations where rejecting the victim label is a mechanism of coping with the experience of victimisation. Coping is achieved by either supressing the experience (if that can be considered 'coping') or processing and 'overcoming' its negative impacts (Fohring, 2018). Being "a victim" is a loaded term associated with passivity, which may therefore be disempowering.[28] The rejection of 'the victim' label can therefore be a means of rejecting the stigma of victimisation. However, while there is stigma associated with being 'greedy' or 'gullible', the rejection of the victim label as a way of 'taking control' of the situation has not been observed in relation to fraud victims. Cross (2016) has found that some older victims chose not to disclose their experience to friends and family for fear that this may lead to judgements about their mental capacity and ultimately result in restrictions being imposed on their day-to-day lives. In such circumstances, it is difficult to say whether the individual is 'taking control' of the situation and managing the consequences of their victimisation – or simply avoiding them due to the stigma associated with becoming a victim, or fear of being further disempowered. In other words, avoidance may be questioned as an adequate coping strategy. At the same time, it has been argued that overcoming victimisation experiences is also a social expectation (Strobl, 2010). In this respect, the victims' silence, combined with a 'keep calm and carry on' attitude, might in fact allow them to continue with their 'normal' pre-victimisation life. In parallel, experiences and risk of victimisation may have become so 'normalised' as to not register in the same way (Genn, 1988) – although this may also be interpreted as a coping mechanism.

Victims' own associations between being victimised and "vulnerability", "powerlessness" or "weakness" (Fohring, 2018, p. 157) suggest that accepting 'the victim' label involves understanding oneself as a *vulnerable* subject, vis-à-vis criminal activity. This is not however, a welcome status, and societal pressures lead individuals to distance themselves from being labelled as weak or vulnerable, and instead stress 'surviving' or 'coping' mechanisms, which ironically also make them less suitable for recognition as a victim by others (Fohring, 2018, p. 158). Nonetheless, this indicates that understanding what makes individuals more vulnerable

[28] This is particularly common in studies and campaigns relating to the victims of sexual offences and domestic violence, where the term "survivor" is preferred as it does not have the same (often gendered) connotations of passivity, weakness and helplessness (Walklate, 2007b, p. 27).

is the key to supporting them to overcome the impact of criminal victimisation. At the same time, dispelling the 'myth' of invulnerability to F&CM may lead to victims (and those around them) being kinder to themselves. It also suggests that being a 'victim' is not static – individuals may journey beyond the vulnerable state caused/exacerbated by criminal victimisation, acceptance and non-acceptance. A victim-focused response should support them in that journey.

1.3. Non-Human and Multiple Victims

Finally, recent work has challenged the view of 'the victim' as a single, human agent, with respect to CM and cyber-enabled fraud (van der Wagen & Pieters, 2015, 2020). Highlighting that multiple actors are often victimised e.g., those who manage computer systems, the computers themselves and the end user, Wagen and Pieters argue that 'the victim' of these crime types is best understood as *a network*, rather than a single agent. Furthermore, they argue that such a conceptualisation highlights the limitations of common online/offline and victim/offender dichotomies. As such, they call for a re-conceptualisation of 'the victim' as a 'hybrid' which includes multiple agents, some of which human, some non-human, some 'real' and some 'virtual'. Consequently, the F&CM vulnerability framework developed in chapter six, accounts for more than individual *embodied* vulnerabilities and encompasses their interaction with machines.

2. The Institutional Meso-Level

At the institutional meso-level, 'victims' are those labelled as such by criminal justice and other agencies. Here, the current legal and policy framework defines victims of F&CM in terms of harms suffered and states of *vulnerability*. The gap between the micro-level experience and the meso-level labelling means that, on one hand the individual may see themselves as a victim but not be recognised as such. One the other, victims may reject the victim label when others seek to impose it on them. Each corresponds to what Strobl called "the rejected victim" and "the designated victim" respectively (2010, p. 6). As noted above, self-perception as a victim of F&CM will be shaped by how and whether a victimisation experience is validated through interaction with the CJS and other agencies, as well as with informal support networks including family and friends. In turn, this inevitably impacts on the support victims can access. While there is far from a full picture of the "rejected victims" of F&CM, some research points towards examples of how negative attitudes towards victims of fraud permeate the interactions some victims have with family, friends and CJS agencies (Button et al., 2009a; Cross, 2016). This suggests that some F&CM victims may indeed be rejected.[29] Additionally, instances of the 'designated victim' have also been documented in relation to fraud victims who are 'in denial' about being victimised, despite evidence suggesting that a fraud has been committed, which has adversely impacted on them (Button, Lewis, & Tapley, 2012). Practitioner accounts (Deem & Lande, 2018) and qualitative explorations of the experiences of victims and their friends and families (Button, Lewis, et al., 2012), have highlighted situations where victims are repeatedly exploited by fraudsters, but fail to accept this reality.

While institutional labelling will include some and exclude others who self-identify as victims, it is at this meso-level that experiences of victimisation are measured within the population and differences between groups observed, enabling an analysis of which groups are more likely to become victims of F&CM. Risk profiles have been developed by researchers and practitioners and groups at higher risk of victimisation or greater "victim proneness" (Walklate, 2011, p. 180) are often referred to as "vulnerable". Several key variables are considered of criminological relevance within the literature at this aggregate level, including social class, age,

[29] In addition, as detailed in Annex VII, the application of the Home Office Counting Rules for Recorded Crime (HOCR) effectively excludes some victims e.g., those who are harmed through 'identity fraud' are not, in most cases and legally speaking, viewed as 'the victims' of crime.

gender and ethnicity – although the importance of these factors, vis-a-vis classism, ageism, sexism and racism has been questioned (Walklake 2007). Nonetheless, such risk profiles are useful in the development of awareness campaigns targeting specific 'at risk' sub-groups. As such, *vulnerability to victimisation*, understood as risk of victimisation based on measured characteristics, plays a role in understanding risk of victimisation and defining policy and practice priorities. However, such patterns are not well understood with respect to victims of F&CM and do not always capture the previously discussed heterogeneity of victims' experiences. Recognition and measurement at the meso-level, it is argued, are currently ill suited to enable practitioners to identify victims in need of support and how to help them become more resilient to F&CM. This section considers the known characteristics of F&CM victims at this aggregate level and how 'the victim' and 'vulnerability' are defined in policy and legislation.

2.1. Victim Characteristics and Routine Activities

2.1.1. Demographic & Environmental Characteristics

In the year ending March 2019, 1.8% of all adults were estimated to have had at least one experience of CM victimisation (ONS, 2020d). However, this was significantly lower for the 75+ age group (0.8%) and men reported significantly more cases of CM than women (2% and 1.6% respectively). Other characteristics significantly associated with CM victimisation included marital status other than being widowed, having higher qualifications, and working in managerial and professional occupations, residing in the 20% least deprived areas in both England and Wales, spending more time outside the home and visiting local bars. Additionally, levels of victimisation varied geographically, with higher victimisation among those living in the South and East of England and lower within the Northeast of England, when compared to all regions. Surprisingly given disparities in Internet access, it was also significantly associated with rural (2.3%) rather than urban areas (1.7%). No significant difference was found with respect to ethnic group (except for White victims being significantly more likely to experience unauthorised access than Asian/British Asian victims), country of birth, disability or sexual orientation.

In the same period, 6.8% of all adults were estimated to have been victims of at least one fraud, including bank and credit account, consumer and retail, advance fee and other frauds (ONS, 2020d). The proportion of victimisation was highest for the 35-55 age groups (over 8%) and

significantly lower for the 65+ age groups (4.8% for 65-74 and 3.6% for the 75+ age group), with no significant differences between men and women for either online or offline frauds. The significance of the age variable holds for both online and offline fraud, although an even lesser proportion of older victims reported online frauds. Victims of fraud were also significantly less likely to be economically inactive or widowed, more likely to be in managerial and professional occupations, have high qualifications, more likely to spend more time outside the home and visit bars. Additionally, there were significantly less victims in the Northeast regional of England when compared to Wales and all other English regions, but no difference was found between urban/rural areas. Furthermore, there were significantly more victims in the 20% least deprived areas in England, but no differences were found with regards to deprivation levels within Wales. As with CM, no significant difference was found with respect to ethnic group, country of birth or disability, and no clear pattern emerges with respect to sexual orientation. The association of greater educational achievement with increased risk of victimisation to online fraud echo a survey study of individuals in the UK conducted by Whitty (2019). However, the age statistics are at odds with work suggestion a higher risk of victimisation for older age groups (e.g. Bolimos & Choo, 2017; Deem & Lande, 2018; James, Boyle, & Bennett, 2014; Titus & Gover, 2001; Victim Support, 2015b).

2.1.2. Routine Activities and Guardianship

In line with Cohen and Felson's (1979) Routine Activity Theory (RAT), several studies have indicated that F&CM victimisation is associated with 'risky' routine activities, while others focused on the absence of capable guardianship (Bergmann et al., 2017; Grabosky et al., 2001; Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011; Paek & Nalla, 2015; Williams, 2016). This theory posits that crime can be explained by the coming together of three distinct factors: a) motivated offenders, b) suitable targets/victims and c) the absence of "capable guardians against a violation" (L. E. Cohen & Felson, 1979, p. 589). Of these, the latter two factors are relevant to understanding victimisation. Furthermore, the concept of 'suitable target' is further broken down into the following components: 1) the *value* or the "material or symbolic" desirability of the target; 2) whether the target is *visible* to the offender, 3) whether the target is *accessible* to the offender and 4) and finally the level of *inertia* of the target "against illegal treatment by offenders" (L. E. Cohen & Felson, 1979, p. 591). The concept of guardianship is more loosely defined to include any structures of everyday life which discourage crime including the presence of other people, security measures and police presence.

The suitability of applying an RAT framework to 'cybercrime' was considered by Leukfeldt & Yar (2016). In addition to reviewing 11 other studies applying RAT to cybercrime, they conducted their own an empirical study on a large sample of individuals (n = 9,161). Their analysis shows that RAT cannot explain cybercrime victimisation across a variety of cybercrimes which included instances of cyber-trespass (hacking and malware) and cyber-deceptions (identity and consumer fraud). Visibility, operationalised as the level of internet usage and the extent of respondents participation in a number of on-line activities was the only RAT element which had a significant effect across all cybercrimes considered. Furthermore, the significance of the RAT framework overall was evaluated to differ greatly between the cybercrimes considered. The authors concluded that RAT was more suitable to measure cyber-trespass type crimes such as malware infection than cyber-deceptions such as identity fraud.

The above results are aligned with a survey study by Bergmann et. al. (2017) which found that individual and household factors, as well as online and prevention behaviour, influence the risk of victimisation with respect to cyber-dependant or cyber-trespass type crimes. However, they also concluded that the effects differed between the three types of cyber-dependant crimes considered (malware infection, ransomware infection, and misuse of personal data) and therefore these crime types should be studied separately. With respect to risky activities, a small sample study by Hutchings and Heyes (2009), indicates a correlation between computer use and receiving phishing emails. Pratt et al. (2010) found that the effect of demographic characteristics (e.g. age, gender, education, marital status) on the likelihood of being targeted by online fraudsters, is fully mediated by indicators of routine online activities. Another study by Reyns (2015) in Canada, found that an increased online presence placed users at more risk of online victimisation, but this was aggravated rather than prevented by online guardianship. Other studies showed that routine activities were also associated with an increased likelihood of being a victim of 'identity fraud' (Reyns & Henson, 2015) and that risk factors can vary between identity fraud sub-types (Burnes, Deliema, & Langton, 2020). For example, a small survey study by Deliema et al. (2019) found that victims of *Investment* fraud in America traded more frequently in stocks and purchased more investments through unsolicited calls, emails, television adverts, or "free lunch" seminars.

2.2. 'The Victim' and 'Vulnerability' in Law

2.2.1. The Victim

The definition of victim in England and Wales is not far from that adopted by the United Nations (1985), which includes those who suffered harms as a result of criminal activity.[30] In particular, section 53(3) of the Domestic Violence, Crime and Victims Act 2004 specified that whether a) "no complaint has been made about the offence;" and b) "no person has been charged with or convicted of the offence", is immaterial to the recognition of a victim of crime (or anti-social behaviour). However, while reporting a crime to the police in the UK is not necessary for a victim to be able to access victim services, in practice a police referral is the most common way in which these services are accessed.[31] As such, it is unclear whether victim services are made available to those 'rejected' for not meeting the victim criteria as set out in the HOCR. Furthermore, EU Directive 2012/29/EU also defines victims primarily in terms of direct harms experienced due to criminal acts, but it has placed increased emphasis on the importance of addressing secondary and repeat victimisation.[32] Reflecting these developments, the definition of the victim in the UK's Code of Practice for Victims of Crime ('the Victims' Code') includes a) "a natural person who has suffered harm, including physical, mental or emotional harm or economic loss which was directly caused by a criminal offence" or b) "a close relative of a person whose death was directly caused by a criminal offence" (MOJ, 2015,

[30] A crime victim includes "persons who, individually or collectively, have suffered harm, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their fundamental rights, through acts or omissions that are in violation of criminal laws operative within Member States, including those laws proscribing criminal abuse of power" (UN, 1985).

[31] For example, the charity Victim Support reported having received 297,521 support telephone calls directly from victims, in contrast to 1,190,160 police referrals in the year 2014/15 (Victim Support, 2015a). No comparable information has been provided in more recent annual reports by the charity Victim Support. However, as discussed elsewhere, the Coalition and Conservative governments moved away from the single provision model of the previous Labour governments where Victim Support delivered most victim services across the country. Without a single unified provider across England and Wales, it is likely that an even greater proportion of crime victims access support services through police referrals. This is an inevitable result of the fragmentation of the service delivery, particularly as the information about local services is available through the internet, but not easily accessible for those without the required digital skills to find it.

[32] While the Framework decision mentioned secondary victimisation twice, once in the preamble and another time in the legal provisions and made no reference to repeat victims, the directive mentioned secondary victimisation 17 times and repeat victimisation 18 times, 7 each in the actual legal provisions.

p. 1).[33] In addition, for the purposes of the code, a criminal offence includes "an offence that is committed, or subject to criminal proceedings, in England and Wales" (MOJ, 2015, p. 1). However, there is no explicit reference to secondary victimisation in the Victims' Code which, given their high degree of "attrition" through the CJS (Scholes, 2018) (see chapter one), is particularly concerning for F&CM victims.

2.2.2. Vulnerability

EU Directive 2012/29/EU cemented the existing minimum standards on rights, support and protection of victims of crime, while also emphasising the need to identify and provide an enhanced response to victims and witnesses considered 'vulnerable'. According to this directive, vulnerable victims require special protections and include those who have been, or could be, repeatedly victimised (Article 18). In addition, support services should be available to all victims "in accordance with their needs, […] before, during and for an appropriate time after criminal proceedings" (Article 8), including the provision of information on compensation, referral to specialist services, the provision of emotional and where possible psychological support, general practical advice and advice on how to prevent secondary and repeat victimisation (Article 9). Furthermore, states must ensure that "measures are available to protect victims and their family members from secondary and repeat victimisation, from intimidation and from retaliation, including against the risk of emotional or psychological harm, and to protect the dignity of victims during questioning and when testifying" (Article 18). As a result, an assessment of the micro-level factors which make victims more *vulnerable* to secondary and repeat victimisation, intimidation or retaliation is required, in order to determine the level of support which should be provided for the adequate protection of victims (Article 22). As such, while the general provisions under Articles 8 and 9 refer to the impact of the crime on the victim before, but also and after the incident of victimisation (*vulnerability to* and *vulnerability post* victimisation), the provisions under Articles 18-22 are more narrowly focused on *vulnerability to further victimisation*.

The above principles are mirrored in the Victims' Code, which recognises three categories of victims which should be prioritised for a response. These include "victims of the most serious

[33] This Code is issued by the Secretary of State for Justice under section 32 of the Domestic Violence, Crime and Victims Act 2004. It implements relevant provisions in a number of EU Directives, including Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime.

crimes", "persistently targeted" (or repeat) victims and "vulnerable or intimidated victims" (MOJ, 2015, p. 13). As is further explored in the next section, this is a narrow conception of vulnerability and thus F&CM victims may fall within the second and third categories, but only in very limited circumstances. Furthermore, the Code requires law enforcement to "conduct a needs assessment at an early stage to decide whether victims fall into one of the three priority categories" (MOJ, 2015, p.40). However, as demonstrated in chapter one, there is little evidence that victims of F&CM received a response tailored to their needs. Brexit notwithstanding, the service standards established in European legislation and the commitment to prioritising vulnerable victims is reflected in the new Victims Strategy (MOJ, 2018). It renews the commitment to a 'needs assessment' (MOJ, 2018, p.17), with particular attention to repeat victims, which should be followed by referral to victim support services, as required. It also notes that Victim Services are available to victims of crime regardless of whether or not they reported the crime (through self-referral) but that "there is a lack of consistent standards" (MOJ, 2018, p.22) in their provision. The importance of self-referral to victim support services is particularly relevant to victims of F&CM, as these crimes are demonstrably under-reported (see methodology). However, while the strategy also notes that nearly half of all crime victimisation reported in the CSEW relate to F&CM crimes, it is silent on how victimisation to these crime types will be specifically tackled. In particular, while it sets out to "ensure that services provide victims with a quality service, based on their needs" (MOJ, 2018, p.25), it limits its commitments to continuing to pilot the Economic Crime Victim Care Unit (ECVCU) for victims within the Manchester and the West Midlands police force areas. As such, it is unclear how inconsistent victim support to F&CM victims across England and Wales will be tackled. In addition, under the European Withdrawal Act 2018, the UK will only retain in its body of law directly applicable elements of the Treaties, EU Regulations and legislation implementing EU Directives. In the absence of a 'victims' law' implementing directive 2012/29/EU, the above-mentioned rights are not legally enforceable.

2.3. Vulnerability in Policy and Practice

As shown above, the notion of vulnerability plays a key role in understanding and shaping the response to F&CM victimisation. However, Skidmore et al. (2020b) have noted that there is considerable variation in the way the term is defined by stakeholders. Looking across definitions used by those who play a role in the F&CM 'justice network' (Button, Tapley, et

al., 2012) (Table 1), it becomes apparent that while no general definition is provided, the way in which vulnerability is operationalised within the Victims' Code is very limited. In contrast, law enforcement and other organisations define vulnerability in broader terms and recognise a wider variety of vulnerability dimensions and indicators.

UK Government

No general definition of vulnerability is provided, but the following groups are identified as vulnerable in the Victims' Code (the Code) (2015) and the UK Victim Strategy (2018).

Victim Category	Definition/Indicators	Vulnerability Dimensions
Serious crime	Victims of crimes resulting in the death of a close relative, victims of domestic violence, hate crime, terrorism, sexual offences, human trafficking, attempted murder, kidnap, false imprisonment, arson with intent to endanger life and wounding or causing grievous bodily harm with intent (MoJ 2015, p.14)	Impact
Persistently targeted*	A victim that has "been targeted repeatedly as a direct victim of crime over a period of time", particularly where "deliberately targeted" or the "victim of a sustained campaign of harassment or stalking" (*Ibid.*)	Repeat Victimisation
Young victims	Victims under 18 years of age at the time of the offence (following section 16 of the Youth Justice and Criminal Evidence Act 1999)	Embodied
Physical or cognitive disability	Where the quality of the victim's evidence is likely to be affected because they: i) suffer from a mental disorder within the meaning of the Mental Health Act 1983. ii) otherwise have a significant impairment to intelligence and social functioning or iii) have a physical disability or are suffering from a physical disorder (*Ibid.*). (following section 16 of the Youth Justice and Criminal Evidence Act 1999)	Embodied
Intimidated victims	Where the quality of the victim's evidence will be affected because of fear or distress about testifying in court. The assessment will take into account any negative behaviour towards the victim, the nature of the offence (victims of a sexual offence or human trafficking are automatically considered to be intimidated), as well as "the victim's age and, if relevant, the victim's social and cultural background, religious beliefs or political opinions,	Situational; Structural

	ethnic origin, domestic and employment circumstances" (*Ibid.*, p.14) (following section 17 of the Youth Justice and Criminal Evidence Act 1999)	
Seriously injured victims	Victims so badly injured because of a criminal offence that they are unable to communicate	Impact
Victims with disabilities	Victims with any disability	Embodied
Language barrier	Where the victim does not understand, or speak, English.	Embodied

Dyfed/Powys Police Force

General definition: "A person is vulnerable if, as a result of their situation or circumstances, they are unable to take care of or protect themselves from harm or exploitation" (FOI Request).

Relevant situation/circumstances include the categories that follow – grouped by this author.

Victim Category	Definition/Indicators	Vulnerability Dimensions
N/A	Adverse Family Circumstances, Adverse Community Circumstances, adverse Cultural Influences, Immigrant Status, Isolation, Lack of Power, Lack of Support, Language Barriers, Poverty, Risky Behaviour, Alcohol & Substance Misuse.	Relational; Structural; Situational
Relationship with offender	Coercive Control, Grooming, Presence of Abuser.	
Minority Status	Difference, Disability, Ethnicity, Gender, Mental Health, Religion, Sexual Orientation, Age.	Embodied

Gwent Police Force

General Definition: "A Person is Vulnerable if, as a result of their situation or circumstances, they are unable to take care or protect themselves from others, from harm or exploitation." (FOI Request)

Victim Category	Definition/Indicators	Vulnerability Dimensions
N/A	Not Known	Not Known

South Wales Police

General Definition: "A person is vulnerable if, as a result of their situation or circumstances, they are unable to take care of or protect themselves from harm or exploitation" (FOI Request).

While there is no definitive list of indicators and "each case is assessed on its own merits" (FOI Request), the individual's situation or personal circumstances include the aspects that follow (Personal Communication 2019).

Victim Category	Definition/Indicators	Vulnerability Dimensions
Socio-economic disadvantage	Personal circumstances: Social isolation; Poor social / communication skills; History of offending; Repeat victim; Self-neglect; Living Conditions; Bereavement; Poor education	Relational; Structural

Ill health & disability	Health and disability: Learning disability; Physical disability or illness; Mental health needs; Drug/alcohol misuse or dependency; Intoxication	Embodied
Minority status	Personal Characteristics: Gender / transgender; Sexual orientation; Ethnic background; Age; Disability; Religion / belief	Embodied; Structural
Socio-economic disadvantage	Economic circumstances: Financial, Unemployment, Housing	Structural

Victim Support

General definition: None provided. However, the groups that follow are referred to as vulnerable, in addition to those previously identified by the Victims' Code (Victim Support 2017).

Victim Category	Definition/Indicators	Vulnerability Dimensions
Repeat Victims	"Some individuals are particularly vulnerable [to repeat victimisation], either because of where they live or work, or their physical characteristics or personal circumstances." (2002 p.3), individuals struggling with mental health issues (2013)	Repeat Victimisation
Socially disadvantaged	Groups including "young households, single parents, those on low incomes or unemployed, those from minority ethnic groups and those living as tenants" (2002, p.10)	Structural
Mental Illness	Those with severe mental illnesses (2013, p.12)	Embodied

Age UK

General definition: Risk of being harmed, often increased in later life due to diminished resilience due to factors such as the ones that follow. (AgeUK 2015, 2018)

Victim Category	Definition/Indicators	Vulnerability Dimensions
N/A	"social engagement, financial resources, physical health and ability, cognitive and mental health and social and family support" (2018 p.1). However age or any of the factors above "should automatically be equated with vulnerability" (2018 p.2).	Relational; Structural; Embodied

Multi-Agency APP Code

General definition: "All Customers can be vulnerable to APP scams and vulnerability is dynamic. The reasons for dynamics of vulnerability may include: the personal circumstances of the Customer; the timing and nature of the APP scam itself; the capacity the Customer had to protect themselves; and the impact of the APP scam on that Customer". (APP Code 2018, p. 13)

Victim Category	Definition/Indicators	Vulnerability Dimensions
N/A	A Customer's personal circumstances which lead to vulnerability are varied, may be temporary or permanent, and may vary in severity over time.	Embodied; Relational

N/A	APP scams may include long-running APP scams or in the moment APP scams.	Situational
N/A	The capacity of a Customer to protect themselves includes their knowledge, skills and capability in engaging with financial services and systems, and the effectiveness of tools made available to them by Firms.	Embodied; Guardianship
N/A	The impact of the APP scam includes the extent to which the Customer is disproportionately affected by the APP scam, both financially and non-financially.	Impact

Table 2 – Definitions of vulnerability by CJS and other agencies.

As illustrated in Table 2, the vulnerability within in the UK Victims' Code (2015) is defined in considerably narrower terms than those used by law enforcement and other stakeholders. While law enforcement and others consider a wide range of vulnerability dimensions and factors, victim policy emphasizes *embodied* vulnerability, repeat victimisation and the physical impacts of victimisation to violent crime. The ways in which vulnerability is defined within policy and operationalised in practice are further explored in what follows.

2.3.1. Vulnerability in The Victims' Code

The Victims' Code makes specific mention of particular groups who have extra entitlements, including those who should receive an enhanced response – and may thus be categorised broadly as vulnerable. As noted above, there are three broad categories of victims that are entitled to an enhanced service under the code: 1) victims of the most serious crimes, 2) persistently targeted victims and 3) vulnerable and intimidated victims. In limited circumstances, F&CM victims might fall under the second and third categories. As seen in this section however, this framework excludes most such victims.

The first and second categories are predominantly defined in terms of the nature and magnitude of the *harms* suffered and do not apply to property offences such as F&CM. The most serious crimes include those resulting in bereavement, as well as domestic violence, hate crime, terrorism, sexual offences, human trafficking, attempted murder, kidnapping, false imprisonment, arson with intent to endanger life and wounding or causing grievous bodily harm with intent (MOJ 2015, p.14). In the second category, a persistently targeted victim is one that has "been targeted repeatedly as a direct victim of crime over a period of time",

particularly where "deliberately targeted" or the "victim of a sustained campaign of harassment or stalking" (MOJ 2015, p.14). As such, some victims of F&CM may be classed as persistently targeted victims.

With respect to the third category, victims are vulnerable they if they are under 18 years of age at the time of the offence, or if the quality of the victim's evidence is likely to be affected because they i) suffer from a mental disorder within the meaning of the Mental Health Act 1983; ii) otherwise have a significant impairment to intelligence and social functioning or iii) have a physical disability or are suffering from a physical disorder (MOJ 2015, p.14). [34] As such, vulnerability is predominantly defined in terms of *embodied* characteristics (see section 3). Finally, the category of intimidated victims applies where the quality of the victim's evidence will be affected because of fear or distress about testifying in court. The Code indicates that an assessment of whether a victim is intimidated will take into account any negative behaviour towards the victim, the nature of the offence (victims of sexual offences or human trafficking are automatically considered to be intimidated), as well as "the victim's age and, if relevant, the victim's social and cultural background, religious beliefs or political opinions, ethnic origin, domestic and employment circumstances" (2015, p.14). While it is theoretically possible that F&CM victims may fall under this category, it is unlikely that they would be considered high enough in a "hierarchy" of intimidation which is illustrated with examples of serious physical violence.

In order to discharge its responsibilities towards victims, the Code states that the police must: "conduct a needs assessment at an early stage to decide whether victims fall into one of the three priority categories" (p.40).[35] However, while all victims should be assessed as to vulnerability, most of the rights the Code affords vulnerable victims are only engaged if and when they become witnesses in criminal proceedings. As such, an "early stage" could be interpreted as referring to the decision to prosecute, rather than when F&CM crimes are reported. Finally, as established in chapter one, very few cases of F&CM ever make it as far as prosecution. When they do, many are likely to be resolved before the individual is required to

[34] In in line with section 16 of the Youth Justice and Criminal Evidence Act 1999, which determines eligibility for the court to grant "Special Measures" to witnesses in criminal trials.

[35] This needs assessment originates from EU Directive 2012/29/EU which established the need to provide an enhanced response to victims and witnesses considered vulnerable and thus required assessment of "vulnerability" and "harm" (Article 22). Brexit notwithstanding, this assessment priority of vulnerable victims is also reflected in the new Victims Strategy 2018.

give evidence in court. As such, the third category of vulnerable victim recognised in the Code will only be applicable to victims of F&CM in a small number of cases and in very limited circumstances. Overall therefore, the national framework for victims' rights and entitlements remains inadequate to meet the needs of F&CM victims. In great part, this is a result of the understanding of vulnerability within the Code and, as seen below, how this is used in practice.

2.3.2. Vulnerability and Policing

Table 2 above highlights that comparatively to the Victims' Code, police forces in the Southern Wales region consider a much wider range of vulnerabilities – at least in theory.[36] All three forces define a person as vulnerable "if, as a result of their situation or circumstances, they are unable to take care or protect themselves or others from harm or exploitation". In addition, some of the forces have developed their own list of factors which may constitute relevant vulnerability factors, with some variation between them. In practice however, the groups which are assessed for vulnerabilities is also restricted. South Wales police for example, focus their vulnerability assessment "on those victims who are over the age of 70 and deploy specific keywords in their report which indicate aspects of vulnerability" (SWP, 2019). The need to prioritise response is not surprising, given the limited availability of resources. However, it is unclear that the groups prioritised for response are defined based on evidence that they are especially vulnerable, rather than what Christie (1986) described as idealised conceptualisations of 'the victim'. Furthermore, previous work has highlighted a lack of consistency in the definition and application of vulnerability needs assessments to fraud victims, across police forces in England and Wales (Skidmore et al., 2020b).

Finally, the definition used by South Wales police aligns with the broader vulnerability framework in the Victims' Code, in its identification of repeat victims as vulnerable. As seen in Table 1, this is also reflected in the conceptualisations of vulnerability used by other stakeholders including Victim Support. However, as further explored in section four, while repeat victimisation (RV) may be an indicator of vulnerability to victimisation, identifying and measuring RV overall is not straightforward. Furthermore, while RV demonstrates a higher risk of victimisation, it does not necessarily signal greater impact post-victimisation. As with

[36] This information was compiled through a mix of desk-based research, personal communications with law enforcement and other stakeholders and a Freedom of Information Request made to the relevant forces. The request was fulfilled or partly fulfilled by three of the four Welsh police forces.

the previous discussion about ‘vulnerability’ in practice, the understanding of vulnerability deployed in practice lacks rigorous theoretical grounding. As such, in what follows, the concept of vulnerability will be problematised from a theoretical perspective.

3. Problematising Vulnerability

Vulnerability is a combination of a state of exposure to risk of harm, with a reduced capacity for defending oneself from or coping with the risk of harm materialising (Chambers 1989, Munro & Scoular, 2012). In the context of this thesis, it is either a) an increased susceptibility to the negative impacts of F&CM victimisation, i.e., a greater risk of being victimised; and/or b) an increased susceptibility to harms which are directly related to or exacerbated by experiences of F&CM victimisation. As previously noted, groups identified to be at higher risk of victimisation, or characterised by greater "victim proneness" (Walklake, 2011, p. 180) are often referred to as “vulnerable”, i.e., category a) of vulnerability. Furthermore, a considerable body of research has focused on those who are *repeat victims* as a marker of greater vulnerability *to victimisation* (see section four below). This section argues that vulnerability *to victimisation* (or victimisation risk, measured statistically in terms of the likelihood of being (re)victimised given a specific group/population) should be distinguished from vulnerability *post-victimisation* which (concerning the victims’ actual experience of being victimised and their resilience to the negative impacts of crime). The latter relates to a wider set of circumstances which make the individual more susceptible to harm, beyond the direct experience of victimisation. However, addressing both types of vulnerability is essential to a victim-focused approach to F&CM.

3.1. Defining Vulnerability

Chambers defines vulnerability as “exposure to contingencies and stress, and difficulty coping with them. Vulnerability has thus two sides: an *external* side of risk, […] and an *internal* side which is defencelessness, meaning a lack of means to cope without damaging loss" (1989, p. 1, emphasis added). The first part of the definition is both too broad, given the term “contingencies”, and too specific in its reference to “stress”. The second part however mirrors the previous discussion on understandings of ‘the victim’, as vulnerability can be understood in terms of the ‘objective’ assessments of risk (the external side), often at the *meso* level, and the inter-subjective self-perception of the impact of victimisation, relative to the victim’s ability to recover (the internal side). This definition is also useful in that it sets out the logical timeline for response: first, targeting prevention measures at those at high risk or *vulnerability to victimisation*; second, targeting support at those who are victimised, to enhance the victim’s capability to cope with impacts *post-victimisation*. Of course, the operationalisation of ‘risk’

as objective and external to the individual may describe differences in risk across sub-groups of the population, but it does not explain the reasons for such differences. Furthermore, while vulnerability *post-victimisation* emphasises the individual's capability to deal with victimisation impacts, it does not immediately make salient how structural factors *external* to the individual e.g., socio-economic deprivation or the availability of a social network of support, define what those capabilities are in the first place. It also fails to account for the socio-cultural macro-level factors which result in some victims being more readily recognised than others. However, these are important dimensions in understanding and adequately responding to F&CM vulnerability.

The 'fear of crime' literature explains variations in self-perceptions of vulnerability to criminal victimisation with respect to the anticipated likelihood of harm and impact of the suffering caused by becoming a victim (Butler, 2006; Green, 2007; Killias, 1990). Killias (1990) understands the term 'vulnerability' as a multi-dimensional phenomenon, including physical, social and situational factors. These factors influence victims' self-perceptions of vulnerability in terms of their perceived exposure to the risk of victimisation, their perceived control of the situation (such as means of defence or escape) and their anticipation of (the magnitude) of harm resulting from victimisation (1990, p. 98). Together, these factors explain variations in self-perceptions of vulnerability, which in turn explain variations in fear of crime among individuals. The first dimension (perceived exposure to risk) aligns with Chamber's *external* side, while the others align with the *internal* side of vulnerability. However, Killias does not define vulnerability as such, and does not provide an exhaustive set of vulnerability factors capable of operationalisation. Additionally, while Killias' approach directs the analytical gaze towards the multiple-dimensions which influence vulnerability, he does not fully capture the notion of differing capabilities to deal with the negative impacts of victimisation as a key to identify and support *the most* vulnerable. As with the definition put forward by Chambers, Killias' fails to highlight how vulnerability may (or not) be created and recognised by the institutions that surround victims and the structural factors which shape their lives and therefore their ability to overcome the negative impacts of victimisation. Finally, his approach favours the crime 'event' as a unit of analysis, rather than understanding victimisation as a process. As noted by Genn (1988) and further examined in section four below, key aspects of the victims' experience are lost by focusing on crime events. Furthermore, emphasising victimisation as a process, including its relational and contextual aspects, highlights that vulnerability is not

static, but changeable over time and within each social context. Only thus can vulnerability be truly understood and addressed. Here, Fineman's (2008) vulnerability theory is very helpful and will therefore be further discussed below.

3.2. A Vulnerability Lens

This section considers whether the concept of vulnerability is capable of providing a lens through which the needs of victims can be identified and addressed. In this respect, Fineman's (2008) vulnerability theory helps to articulate an answer. Drawing on Turner (2006), Fineman conceptualises vulnerability as a universal human condition, which results from individuals' *embodiment* (see below) on one hand and inter-dependence on the other, within a precarious environment of risk and uncertainty. Vulnerability is an "openness to physical or emotional harm" applicable to all, a "continuous susceptibility", which means that despite invulnerability beliefs at the *micro* level and idealised conceptions of the victim at the *macro* level, "there is no position of invulnerability" (Fineman, 2017, p. 11). It is also a condition of dependency – accepting the vulnerable-self is recognising one's dependence on others (family, colleagues, institutions), which is anathema to the liberal ideal of the autonomous subject. As such, Fineman argues that law and policy should be centred around the 'vulnerable subject', rather than assuming the subject to be free and unencumbered. An echo of this idea is found in the often-repeated mantra that everyone is, to some extent, *vulnerable to* F&CM victimisation. As such, the conceptualisation of "vulnerability as the human condition" may enable individuals, law enforcement and other agencies to make sense of experiences of F&CM victimisation, without recourse to either stigmatising or idealised notions of 'the victim'.

However, saying that we are all vulnerable to being victimised does not mean that we are all going to experience that vulnerability at the same rate, or in the same way. Vulnerability in general, and with respect to F&CM victimisation in particular, is asymmetrical. There are inequalities with respect to how much crime individuals experience individually and collectively, as members of population sub-groups. In line with Chambers (1989), the instance of being victimised is viewed as a harm in itself (referred to as *vulnerability to victimisation*). A focus on this type of vulnerability aims to reduce risk of victimisation and is geared towards crime prevention and crime control. However, as well as different risks of being victimised, there are also differences in terms of how well-equipped different individuals are to cope with victimisation and, in some cases, victimisation may create new or exacerbates old vulnerability

factors i.e., circumstances which increase susceptibility to harm such as illness, financial difficulties or social isolation. This may be referred to as *vulnerability post-victimisation*. The universalist approach could have risked obfuscating the how victimisation differently impacts on specific groups, as well as the heterogeneity of victims, their circumstances and needs post-victimisation. However, this paradox is identified by Fineman, who describes vulnerability as at once universal and particular. Following Fineman (2008, p. 13), what makes vulnerability particular to the individual is their access to "assets of resilience" which, as discussed further below, mirror the idea of "capabilities" introduced by the economist Amartya Sen (1999) and further developed philosophically by the legal scholar Martha Nussbaum (2006, 2011). Capabilities or assets of resilience, enable the individual to cope with the impacts of being victimised and it is the role of the state, CJS agencies and other institutions to ensure all victims have access to those assets. As such, while there is considerable stigma associated with the notion of vulnerability to F&CM, a vulnerability lens provides a framework through which to identify the assets of resilience needed to meet the needs of victims. As such, this lens is well suited to the victim-focused approach identified in chapter one, i.e., to identify what harms have been suffered as a result of F&CM, by whom, how to prevent and repair them, and who has the obligation/ability to do so.

In line with Fineman's (2008, 2017) vulnerability analysis, Green (2007) extended the concept of harm suffered by crime victims in of terms their ability to cope or recover from the impact of victimisation. Furthermore, in their outreach work, Karagiannopoulos and colleagues (2019) identified that a focus on resilience increased engagement from (potential) victims of F&CM. Likewise, Skidmore et al. (2020b) discuss the financial, emotional and physical harm caused by fraud in terms of the victims' resilience or ability to recover. In the context of F&CM, a relatively small loss for one individual may represent a devastating loss to another, depending on their material means and respective ability to 'bounce back'. Likewise, recovering from the negative emotional impact of a long-running dating fraud, may require considerably more social and emotional capabilities, than being victim to a rogue on-line sale. Another key example is old age, often assumed to be synonym with greater vulnerability, with little recognition of the varying access to "assets of resilience". However, previous work has fallen short of articulating whether, when and how the state, through its criminal justice system and the wider 'justice network' (Button, Tapley, et al., 2012), have a responsibility to provide victims with the necessary capabilities to cope with F&CM vulnerability. It is argued that

considering the plight of crime victims through a vulnerability perspective directs attention towards problem-solving and focus on enabling victims to cope and/or heal.

The above notwithstanding, the vulnerability lens is not without its critics. In the context of the regulation of sex work, Munro and Scoular (2012) highlight that the 'universal versus particular' lens may in fact be too focused on individuals and distract attention from the underlying, structural causes of vulnerability. As a result, rather than being mobilised within the policy arena as "a mechanism by which to identify, problematize and compel state responses to a universal condition of precarious dependency", it might instead be used "as a category of neo-liberal governance which legitimates state encroachment whilst constructing 'vulnerable' individuals as 'risk-managers' (Munro & Scoular, 2012, p. 189). Consequently, policy interventions may be designed to provide (at least in appearance) a response to the universal condition of vulnerability, rather than actually addressing the needs of the most vulnerable. This critique echoes the theses of "adaptation to failure" (Garland, 2001) and "governing through crime" (Simon, 2006) which are said to characterise the current status quo of CJS policy. In fact, while vulnerable victims have come to occupy centre stage in victim policy and (to a lesser extent) the response to F&CM, the implications of the individual-universal duality have not been fully understood, or the assumptions made in the applied understandings of vulnerability critically examined. Consequently, on one hand, the universality of vulnerability has not been adequately leveraged to challenge the stigma associated with being a victim of F&CM. On the other, static and *embodied* vulnerability factors such as age and education have been prioritised in both policy and research over dynamic/relational factors such as financial deprivation and isolation. In addition, 'objective' assessments of vulnerability (regardless of whether they are based on empirical evidence) have been prioritised over victims' own experiences.

Nonetheless, having considered the ways in which understandings of 'the victim' rely on the concept of 'vulnerability' from the micro to macro levels, it is argued that a vulnerability lens can serve to highlight who is recognised as vulnerable within the CJS and who is unable to claim that status, creating the space for a discussion of what structural vulnerability factors are at play, while recognising the importance of the subjective experience. The universal/particular dichotomy is a reminder that any statistical modelling of vulnerability will always tend to make visible those victims who are more commonly vulnerable, but inevitably miss 'un-standardised' vulnerability. Nonetheless, it is important to recognise "the dangers of any

uncritical adoption of a discourse of vulnerability, without an interrogation of who is recognised to be vulnerable, under what conditions and why, as well as of the broader socio-economic and state agendas that are served by the responses imposed" (Munro & Scoular, 2012, p. 200). To do this effectively however, it is important to consider as wide a range of vulnerability dimensions as possible and how these can be operationalised. Several dimensions of vulnerability are therefore identified across criminological and other scholarship including situational, embodied, relational and structural, as discussed in turn below. These informed the vulnerability framework developed in chapter six.

3.3. Vulnerability Dimensions

Situational Vulnerability

As previously discussed, Routine Activity Theory (RAT) has been extensively applied to a variety of F&CM crimes, albeit with mixed results (Bergmann et al., 2017; Grabosky et al., 2001; Leukfeldt & Yar, 2016; Paek & Nalla, 2015; Williams, 2016). There is strong evidence that certain online and offline activities make individuals more vulnerable to F&CM by virtue of increased 'exposure' to risk. By the very nature of the approach, some of the 'activities' measured in RAT studies are very frequent, day-to-day 'routine' actions, which cannot be avoided without having an overwhelmingly negative impact on the wellbeing of the would-be victim. As such, from a victim-perspective, RAT leaves the option of improving guardianship. However, there is less certainty regarding the effects of increased guardianship on these crime types. Most likely, this is because the approach does not immediately capture situations where the recognised individual victim has little control over guardianship arrangements or, in the case of fraud, where they are manipulated into lowering their guard. For example, individuals' personal details may be obtained by fraudsters via a data breach and subsequently exploited. Similarly, individuals may be exposed to risks of hacking or malware infection where new software vulnerabilities are found and exploited by criminals, before a patch is available. In these circumstances, the individual has little control to increase guardianship – as do law enforcement and other CJS agencies. Finally, a focus on the situational aspects of the crime does not consider how the crime impacts differently on different individuals. As such, while important, situational factors on their own cannot fully explain vulnerability to/post victimisation, or enabled adequate responses.

Embodied Vulnerability

Fineman (2008, 2017) identifies two ways in which universal vulnerability becomes particular to the individual. The first is through embodied inequalities or the ways in which the characteristics of the body shape the subjective experience of vulnerability. Embodiment is a key concept for some schools of phenomenology (Merleau-Ponty, 2012) which describes how the "subjective experience of one's own body is different from the objective or scientific picture of a body in physiological terms" (Blackburn, 2016). Embodied inequalities may be understood as the physical characteristics which render individuals differentially vulnerable, such as being very young or very old, using a wheelchair, gender, or the colour of one's skin. Embodied differences in vulnerability may be horizontal i.e., they may vary across social groupings at a given time and place. They may also be vertical i.e., an individual will be variably vulnerable across time within the self from birth to death, being a child, an adult, elderly, disabled, ill etc. It is variations in the latter that make vulnerability a universal human condition (Fineman 2008, 2017).

As previously discussed, characteristics such as being young and highly educated have been associated F&CM victimisation, while no difference was found in terms of variables such as ethnicity. In addition, a greater proportion of males experienced CM victimisation. As shown in chapter four however, the typical profile of victims who report F&CM to the police are older and overwhelmingly white, with no significant differences in terms of gender. In part, these differences may be explained by the limitations of recorded crime, vis-à-vis the limitations of victimisation surveys (see Annex VII). However, mirroring the discussion of the concept of 'the victim', individuals are not vulnerable simply due to the physical 'facts' of their condition, but because of how they experience these inter-subjectively, in their particular social and situational contexts. Old age for example, is connected with physical and cognitive decline, which could lead to individuals being exploited by hackers and fraudsters. However, it may also involve social isolation as family may be unable to care for older family members or lack the time to ensure they have understood how to operate devices safely. At the same time mobility declines, reducing contact with friends which may have helped, but may now also be increasingly ill, immobile or pass away. As such, while conditions which define embodied vulnerabilities may be understood as 'static' (e.g., old age, illness), the subjective experience of those conditions can be changed. Therefore, the focus on embodiment rather than mere

physicality, takes the debate beyond describing what characterises victims, to focus on whether and how the subjective experiences associated with those characteristics can be improved.

Furthermore, the way in which embodied characteristics and harm suffered are identified and measured is contested (Green 2007) and often driven by statistical assumptions. Statistical analysis linking crime and harms experienced using CSEW data for example, equates the risk of harm from criminal victimisation experienced by the individual and generalises this to "the risk of and harm done by crime to social groups [to which the individual is assumed to belong] and vice versa" (Walklate 2011, p. 183). In other words, the analysis assumes that belonging to that specific group is a relevant (if not determining) factor in being vulnerable, despite the victim's actual experience. Equating the experiential with the structural makes some groups (e.g., the elderly) more visible than others (e.g., young people) as vulnerable victims of crime (Walklate 2011). In doing this, the nuance in the victims' actual experience is lost, as is the role Christie's (1986) "ideal victim" in determining priority of service. This highlights the need to take into consideration the *embedded*/*relational* and the *structural* aspects of vulnerability.

Relational & Structural Vulnerability

Studies of victimisation often focus on situational and embodied, over the relational and structural factors, which may contribute to vulnerability to and post victimisation. In this way, the "status or condition of 'vulnerability'—particularly in policy discourses—will often be reserved for specific individuals or groups ('the vulnerable') who are deemed, whether for innate or circumstantial reasons, to be peculiarly exposed to risk, uncertainty or negative outcomes" (Munro & Scoular, 2012, p. 196). It is well known, for example, how much of the impetus behind victimisation surveys was the ability to challenge what could be perceived as unfounded (and thereby irrational) fears of crime among some low-risk groups (e.g., the elderly). However, vulnerability cannot be reduced to risk or likelihood of victimisation based on embodied characteristics. An individual's reaction to risk and experiences of victimisation is also shaped by the "agency/structure dialectic" (Wisner, 1993, p. 129). This means that their feelings and experiences of vulnerability to criminal victimisation are strongly shaped by a system of social relationships which, in turn, are spawned by broader structural factors. On the one hand, vulnerability will be experienced differently based on the social networks an individual has access to, for support. It will also be experienced differently based on the relationship between the victim and the suspect, particularly where they are known to the victim. On the other, access to such networks is dependent on the social, political and economic

factors which structure/define relations of power and authority (Palm, 1990) and create or perpetuate "clusters of disadvantage" (Chambers, 1983, p. 111). If anything, vulnerability is as much a result of relational and structural factors, as it is of the situational aspects of the crime and the victims' embodied characteristics.

Fineman's vulnerability theory also highlights the need to look beyond embodied vulnerabilities to how vulnerability is "embedded" through the social relations and institutions one occupies (2008, 2017). This perspective shines a new light on the role that the state, the CJS and other stakeholder organisations should take in responding to vulnerable victims of F&CM. For example, individuals are more or less vulnerable, depending on whether they have a stable income, help from friends and family, or access to financial welfare support. In fact, Fineman sees the social world and particularly state institutions, as structures designed to help people withstand vulnerability, i.e., be resilient to harm. Building on Kirby's (2006) work, As previously noted, Fineman suggests this is achieved through "assets of resilience", the support mechanisms which social relations and state institutions provide individuals to enabled them to withstand "internal or external shock"; these assets may be material, social capital or emotional, among others (Fineman, 2008, pp. 13-14). In this way, vulnerability gives rise to harm and suffering, but also to positive outcomes such as empathy, social cohesion, intimacy, innovation and pleasure (Bergoffen, 2011; Fineman, 2012; Grear, 2010).

Vulnerability theory strongly echoes Sen's capabilities approach, which focuses the discussion of social justice around "judging individual advantage in terms of the capabilities a person has, that is, the substantive freedoms he or she enjoys to lead the kind of life he or she has reason to value" (1999, p. 87). In other words, capabilities are opportunities for functioning at the desired level of wellbeing, or what is feasible for any person to do/be/become. Nussbaum (2011) develops the philosophical aspects of the approach and argues that social justice necessitates that individuals be provided with a baseline or minimum threshold of ten central capabilities (primarily but not exclusively by states and their institutions).[37] At the same time,

[37] The ten central capabilities include 1) *life* or being alive for a normal length of time; 2) *bodily health,* including living healthily and having access to adequate shelter; 3) *bodily integrity*, including freedom of movement, security from violence, sexual satisfaction and choice in matters of reproduction; 4) *senses, imagination and thought*, including the use these abilities and the freedom to develop and express them; 5) *emotions*, including the ability to develop, have and express feelings without fear or anxiety; 6) *practical reason*, or being able to form

maintaining respect for human dignity requires that individuals should ultimately have the choice of whether or not to use those capabilities. As such, capabilities include an element of opportunity which is external to the individual, as well as an "internal preparedness" (Nussbaum, 2011, p. 61) to use those capabilities, which when combined is observable through the individual's actual functioning. Due to this duality, capabilities must sometimes be inferred from "patterns of functioning" (Nussbaum, 2011, p. 61). Fineman's assets of resilience are broadly equivalent to a negative framing of Nussbaum's capabilities. Fineman thinks of societal relationships and institutions as responding to vulnerability, Nussbaum as enabling human flourishing, but both focus on the role of the state in addressing vulnerability, ensuring minimum standards are met and inequalities of access addressed. By helping individuals to overcome vulnerability, assets of resilience enable capabilities to be used by individuals or, where they have been compromised by adversity such as an instance of F&CM victimisation, restored. Where social relations and institutions fail to provide these assets, or where these assets are unequally distributed, vulnerability is said to be *embedded* through social relations and institutions.

Given that inequalities exist with respect to how assets of resilience are distributed within society, Fineman posits that it is for the state to monitor these differences and address not just discriminatory practices, but also the conferring of special privileges on certain groups (2008, 2017). In many ways, this responsibility has been reflected in the judgments of the European Court of Human Rights in Strasbourg, where states' positive obligations towards individuals have been recognised in terms of institutionally rendered vulnerabilities in the form of "prejudice and stigmatization" on one hand and "social disadvantage and material deprivation" on the other (Peroni & Timmer, 2013, p. 1065 and 1067). As shown in section 2.3, the situational and embodied aspects of vulnerability are privileged in policy and practice over relational and structural dimensions. However, while the embodied vulnerabilities associated

---

and live by one's own conception of the good life; 7) *affiliation*, including a) the freedom to identify, live with and engage with others and b) being able to develop self-respect and being treated with dignity regardless of affiliation and/or identity; 8) *other species*, or being free to live in accordance with a concern for the natural environment 9) *play*, or the ability to engage in recreational activities; and 10) *control over one's environment* including a) by participating in the political process and b) through being able to hold rights over property, seek employment and be treated with dignity at work and be free from unjustifiable interference with one's liberty (Nussbaum, 2011, p. 34). The discussion of the impact of F&CM in chapters two and four illustrates that these crime types can adversely impact on several of the capabilities identified by Nussbaum, including life, bodily health and integrity, emotions, play and control over one's environment.

with old age may play an important role (e.g., loss of physical and/or cognitive capacity), it may be that embedded vulnerabilities such as poverty and social isolation – or conversely the maldistribution of material assets and social capital with respect to the older population – constitute the more important focus for intervention.

The role of the state in addressing the vulnerability, including its relational and structural dimensions is of course, contested. Also contested, is the notion that there can be no criminal justice without social justice. This is not the place to articulate the arguments for and against the legitimacy of 'big' and 'small' state intervention to achieve security and/or it link to social justice. However, it should be clear to the reader that it is assumed that criminal justice can only in fact be 'just' where the wider circumstances and harms suffered by both victims and offenders are considered and ultimately addressed. This conviction stems from the underlying principle of the social contract – individuals obey the law under the condition of protection offered by the state. However, that protection cannot be limited to negative freedoms (e.g., freedom from criminal victimisation) and must extend to substantive or positive freedoms (e.g., the freedom to continue to live a good life if and when victimised). Arguably, if a victim's life and wellbeing cannot be satisfactorily restored post-victimisation, it is hardly satisfactory that the crime has been punished. Furthermore, in the context of F&CM, where the difficulties of a crime control approach are many, as discussed in chapter one, an approach based on victim welfare may in fact be the most meaningful type of response.

4. Repeat Victimisation

Early work into repeat victimisation (RV) highlighted that as much as 14% of the population were repeat victims and they reported 70.9% of the incidents recorded on the then British Crime Survey (Farrell, 1992, p. 92). More recently and in the context of the previously described crime drop (see chapter one), it has been noted that while the overall volume of crime has decreased, the proportion of crimes experienced by the top 10% of the most victimised households increased from 57% in 1994 to 72% in 2012 (Ignatans & Pease, 2016). RV has since been examined across a variety of crime types including violent crime (Johnson et. al 1974, Ziegenhgen 1976), racially motivated crime (Sampson & Phillips, 1991), domestic violence (Brimicombe, 2016b) and domestic burglary (S. D. Johnson, 2008; Polvi, Looman, Humphries, & Pease, 1991). With respect to F&CM, ONS have reported that, based on experimental statistics, 13% of F&CM victims were repeat victims in the year ending March 2020 (ONS, 2020a, Table D7). Furthermore, a representative study of the UK population indicated that 26% of fraud victims became repeatedly victimised in their lifetime (Whitty, 2015b) and a more recent study of victims and non-victims found that 45% of fraud victims were repeat victims (Whitty, 2019). Others have referred to those who experience high levels of repeat victimisation and/or are unable or unwilling to protect themselves from it as "chronic victims" (Button, Lewis, et al., 2012).

With the notable exception of the studies mentioned above, few have focused on how RV affects victims of F&CM. However, previous literature indicates that patterns of RV reveal important information for the development of general crime prevention initiatives. Specifically, in the context of limited resources, identifying repeat victims will allow for the targeting of crime prevention resources where they may have the effect of reducing crime overall. This is because being a victim is, "for whatever […] combination of reasons, a good predictor of swift future victimisation" (Farrell & Pease, 1993, p. 2). Furthermore, research indicates that RV does not occur randomly (Hindelang, Gottfredson, & Garofalo, 1978; Sparks, 1981; Sparks, Genn, & Dodd, 1977) and is associated with specific demographic characteristics (Ignatans & Pease, 2015, 2016). However, despite the numerous studies of RV, policy makers' interest in understanding it has declined since its peak in the 1990s (Pease et al., 2018). Furthermore, while the insights from the previously mentioned scholarship are extremely useful, crime prevention must be tailored to crime types, victims' circumstances and available local resources. As such, it has been noted that the study of cybercrime "through a repeat

victimisation lens is overdue" (Pease et al., 2018, p. 259). This section reviews the literature on RV including how the term has been defined, the patterns identified in previous literature and its implications for policing. It also sets out what this thesis adds to existing knowledge on repeat victims of F&CM.

4.1. Extent of Repeat Victimisation

Different terms have been used, often inconsistently, to refer to the experience of being a crime victim more than once including "revictimisation, multiple victimisation, repeat victimisation, multi-victimisation, repetitive victimisation and recidivist victimisation" (Farrell & Pease, 1993, p. 5). In this thesis, the terms repeat and multiple victimisation are used, in part adapting the definitions employed in the CSEW, which defines a repeat victim as someone who was the victim a specific crime type more than once (within crime-type victim), in the previous 12 months (ONS, 2020e). This is distinguished from multiple victimisation which is where someone experiences more than one crime of different types in the previous 12 months (across crime-type victim). As this thesis is limited to an analysis of F&CM, the term repeat victim is used to include victims who reported more than one fraud, those who reported more than one computer misuse crime, but also those who reported a mix of fraud and computer misuse crimes within the time reference period.

While there is little research into repeat victims of F&CM, the CSEW provides an indication of the levels of RV. Recent CSEW figures suggest that an estimated 743,000 adults experienced 876,000 incidents of Computer Misuse in E&W, in the year ending March 2020 (ONS, 2020b). This means that approximately 1.6% of adults experienced at least one CM crime within that period, with the majority of victims experiencing one incident (89%), 10% experiencing between two and four and 1% five or more incidents (ONS, 2020a, Table D7) . Among the CM crimes measured, there was a significant 22% decrease in victims of computer viruses which unauthorised access to personal information (i.e., 'hacking') stayed the same. For fraud, the estimates are larger, with an estimated 3.1 million victims experiencing 3.7 million fraud incidents in the same period, amounting to 6.6% of all adults in E&W experiencing at least one incident of fraud (ONS, 2020b). Overall, the majority of victims were only victimised once (88%), 11% were victimised between two and four times and 1% were victimised five or more times (ONS, 2020a, Table D7). The same dataset indicates that ¼ of both F&CM incidents were experienced by repeat victims. As such, while a considerable proportion of F&CM is

experienced by repeat victims, among those, a few experience a particularly high number of victimisations. These statistics suggest a significant proportion of RV which is indicative of the need to further explore RV with respect to F&CM and understand how it may impact on victims and crime prevention strategies. The known patterns of RV are explored further below.

4.2. Patterns of Repeat Victimisation

Previous research has highlighted the usefulness of measuring RV for crime prevention and several key insights are worth noting. Firstly, studies have suggested that a large proportion of crime is experienced by a small number of repeat victims (Farrell, 1992; Farrell, Tseloni, & Pease, 2005; Sidebottom, 2012). These in turn suggest that where crime prevention strategies are designed to reduce RV, they will "prevent a large proportion of all offences from being committed" (Farrell, 1992, p. 86). Furthermore, failed attempts to fit the distribution of RV to variations of the Poisson model suggest it does not happen by chance (Farrell, 1992, 1995; Genn, 1988; Sparks et al., 1977) and it is associated with specific demographic characteristics (Ignatans & Pease, 2015, 2016). Generally, previous research indicates that the characteristics that distinguish repeat from one-time victims are the same ones that distinguish victims from non-victims. For example, previous research has indicated that there are significantly more females who are one-time victims of domestic abuse, but also that significantly more females are repeat victims of such crimes (HMIC, 2015). As shown in section 2.1, CSEW figures indicate that the F&CM victim profile is considerably different to that of other crimes, with the typical victim being male, older and of higher socio-economic status (ONS, 2017c). In the only study known to the author to directly addresses this issue with respect to victims of online fraud, Whitty (2019) found that, with the exception of guardianship behaviours, the distinsguishing activities repeat victims carried out online as well as their socio-demographic and psychological characteristics were the same as those which distinsguished victims from non-victims. With respect to guardianship behaviours (e.g. reading anti fraud advice and scam alerts), this study also found that the direction of correlation was the oposite to what was expected – victims exhibited higher levels of guardianship behaviours than non-victims and repeat victims exhibited higher guardianship behaviours than one-time victims. Whitty suggests this may be an indication of the lack of effectiveness of the available esafety advice. In addition, there may also be a time-lag effect in that those who have been victimised then increase their guardinaship behaviours.

Furthermore, patterns of RV vary between crime types such that victims of domestic abuse are more likely to be re-victimised than victims of other crime types (Walby, Towers, & Francis, 2016). As previously noted, following a 'flag' or 'boost' approach (Pease et al., 2018, p. 258; Tseloni & Pease, 2003), this may be either because those individuals were more vulnerable to victimisation in the first place, or because being a victim made them more vulnerable to further victimisation, or else a combination of the two. That said, identifying victims as vulnerable to victimisation based solely on demographic characteristics may be divisive and yield too many false positives to be of practical use. In addition, quantitative RV patterns do not necessarily capture its processes or mechanisms. Genn's (1988) work in particular shows that in a context where criminal victimisation normalised to the point of being seen by victims as 'a part of life', counting how many instances of victimisation the victim remembers or reports provides little insight or meaning.

Another insight from previous research is the association between high rates of RV ('hot dots') and geographical concentrations of crime ('hot spots') (Trickett, Osborn, Seymour, & Pease, 1992). According to this evidence, what distinguishes high crime areas is not that more individuals are victims of crime, but that more victims of crime are repeatedly victimised. As such, protecting victims from repeat victimisation will coincide with areas where crime is highest and thus result in crime reduction. This has led to the growth in research into 'near repeats', predicting where crime will take place next, based on where it has previously taken place geographically. For example, the prediction of where the next burglary will take place, based on the location of previous burglaries – because burglars will target specific geographic areas and dwelling characteristics. However, where crimes with a significant online component, the spatial element is less relevant to victim selection – although, as it will be seen, it is often a part of the MO. As such, RV rather than near-repeat victimisation is a more useful metric of crime concentration, to determine where crime prevention resources should be deployed (Pease et al., 2018).

Finally, RV has been shown to happen relatively soon after the first victimisation for several crime types including burglary and property crime (Polvi, Looman, Humphries, & Pease, 1990; Reiss, 1980), racial attacks (Sampson & Phillips, 1991) and domestic violence (Farrell, 1992). Similar findings also indicate that repeats happen relatively swiftly with respect to computer misuse offences (Moitra & Konda, 2004). This suggests the risk of RV is highest immediately after the prior victimisation.

4.3. Repeat Victims and Vulnerability

The relationship between vulnerability and RV may be (quantitatively) understood in two ways, the 'flag' approach and the 'boost' approach (Pease et al., 2018, p. 258; Tseloni & Pease, 2003). The first understands RV as an indicator which *flags* a victim as especially vulnerable to victimisation. The victim has characteristics which make them a more appealing or more likely target, irrespective of previous experience and thus being a repeat victim signals vulnerability factors which precede the crime itself. The second suggests that being victimised once increases the likelihood of being victimised again and therefore risk of victimisation is *boosted* by prior victimisation (Johnson, 2008; Tseloni & Pease, 2004). This is most likely because the same offenders will target the victim again. Johnson (2008) concludes that repeat victimisation results from a combination of the two. At the same time, other work (Farrell, 1992; Genn, 1988) shows that RV is a process which cannot be easily reduced to a series of distinct events. Doing so might lead to the mechanisms of RV not being fully understood.

Furthermore, regardless of whether RV is a 'flag' or a 'booster', it says little about the victims' ability to cope with the negative impacts of victimisation (vulnerability post-victimisation) or the kinds of support which would enable coping and the return to normalcy after the victimisation experience. However, such a response may be necessary in the case of some repeat victim who may also be classified as 'chronic' victims. Hope and Norris defined 'chronic victims' in statistical terms to represent a "small class of respondents with the highest probability of being frequently victimized, representing the extremely attenuated right-hand tail of the [probability] distribution" (2013, p. 559). In the context of fraud, the term has also been used qualitatively, to refer to victims who "fall into a pattern of repeated falling for the same or similar frauds" (Button, Lewis, et al., 2012, p. 53). In addition, the 'chronic victim' of fraud has also been characterised by being unable or unwilling to accept that they have been victimised (Button et al., 2009a) or "[becoming] essentially 'addicted' to the fraud and repeatedly [sending] money, even when family, friends and official bodies are advising them against their involvement" (Button & Cross, 2017, p. 102).

The idea of "chronic victims" suggests that that RV, at the higher end of its distribution, is a 'flag' for pre-crime vulnerability. However, the 'relationship' which fraudsters establish with victims and, as it will be seen in chapter five, the continuing narrative between incidents may also 'boost' the risk of further victimisation. Also compatible with a 'boost' approach is the

suggestion that once victimised for the first time, some victims are added to 'suckers' lists' by criminals (Button & Cross, 2017; Button et al., 2009b, p. 5; Cross, Richards, & Smith, 2016; Cross, Smith, & Richards, 2014), who trade these between themselves, resulting in these victims being repeatedly targeted. However, the empirical evidence is limited with respect to both chronic victims and suckers' lists. They remain hypothesis which are inferred indirectly from higher-than-average levels of RV and the multiple incidents connected by an evolving narrative e.g., as with recovery fraud following another type of fraud (Cross et al., 2016).

5. Conclusion

In this chapter, the twin concepts of "victim" and "vulnerability" were explored in more detail both theoretically and empirically, setting the scene for the analysis that follows. Understandings of 'the victim' were explored across three theoretical levels, the *micro-level* of individual experience and self-identification, the *meso-level* of institutional definition and operationalisation, and finally the *macro-level* of cultural phenomena. In doing so this chapter highlighted the consequences for victims of misalignment between these levels and the limitations of current conceptualisations of 'the victim' as single human agents. Understanding the victim across these three levels has opened the door for a focus on how the concept is constructed and thus understood by victims' themselves as well as other actors, while moving away from typologies focused on the victims' role (or culpability) in their own victimisation. This allows for a plurality of constructions to co-exist and makes visible where they are not aligned. Additionally, this analysis has shown how often the misalignment stems from the gap between the objective 'fact' of victimisation as defined in law and by agencies' 'labelling' of victims and the inter-subjective construction of 'victimhood' by victims and those around them, both of which are influenced by cultural norms about who is an 'ideal victim' (Christie, 1986). Unfortunately, others have shown that F&CM victims often lack the characteristics which would confer them legitimacy as 'ideal victims' and thus their needs are unlikely to be prioritised in policy and public discourse (Cross, 2018).

At the *micro* level, an individual self-identifies as 'a victim' where they believe they have suffered a harm as a result of a criminal act and accept this experience as evidence of a state of vulnerability, which amounts to victimisation. This acceptance is inter-subjective because it is linked to how the individual interprets their subjective experience of victimisation, in relation to their interaction with the interpretations by others. What is clear from this discussion is that

both the victims' own self-perception and the response of those around them are inevitably shaped by the *meso* and *macro*-level understandings of 'the victim'. Furthermore, the evidence suggests that there are psychological and social incentives for individuals to reject the victim label and that these may be particularly relevant in the case of F&CM victimisation. This may, to some extent, explain why F&CM are considerably under-reported. It also raises the issue of whether a focus on vulnerability may dissuade victims from seeking and/or accepting support. Finally, recent work has highlighted the limitations of conceptualising 'the victim' as a single human entity, where there may be multiple and even non-human 'victims'. In part, this is rooted in the liberal, social-contract theory tradition, within which one of the primary functions of the criminal law is to protect the most basic welfare interests of individuals, hence the need to establish 'harm' to the singular (individual) victim.

At the *meso* level of institutional recognition or labelling, being able to claim the 'victim' status is, with some exceptions, also contingent on an individual suffering a harm resulting from a criminal offence. The extent to which this happens in practice, however, is constrained by information needs e.g., avoiding the double counting of bank and card fraud, as well as operational realities. Assessments of vulnerability have thus become a way to mediate demand on police resources, on one hand to meet victims' heterogeneous needs, on the other to help target and prioritise resources. However, there is considerable variability with respect to how vulnerability is understood and measured by law enforcement and other stakeholders and the vulnerability frameworks used tend to be based on static characteristics (such as age) which lack a robust empirical grounding (S. Correia, 2019; Skidmore et al., 2020b). For example, to the extent that there is a victim hierarchy reflecting idealised notions of victimisation, older victims of F&CM appear to be are generally favoured. However, depending on how victimisation and vulnerability are measured, age can appear to be positively or negatively correlated with F&CM victimisation. Furthermore, the concept of vulnerability as understood within the Victims' Code {MOJ, 2015 #291}, excludes victims of F&CM in all but very limited circumstances. As a result of this narrow view, victims may experience greater negative outcomes, for a longer period, than they might have otherwise. This suggests the need for greater conceptual clarity on what is meant by vulnerability and how vulnerability is assessed but also an understanding which better captures vulnerability in the context of F&CM. Given its role in defining 'the victim', the meaning of vulnerability was then explored through the lens of Fineman's (2008, 2017) vulnerability theory.

From an initial working definition of vulnerability as "openness" (Fineman, 2017, p. 11) or susceptibility to harm, this analysis revealed vulnerability to be a multi-dimensional concept which cannot be reduced to *embodied* characteristics such as age, gender or ethnicity. The vulnerability lens showed that in policy and in practice, understandings of vulnerability tend to favour measures of the (type of) *harm* suffered, *embodied* characteristics and *situational* factors, over *relational* and *structural* vulnerabilities. As such, there is a need to move away from discretionary interpretations of the term towards want that recognises it for its multi-dimensionality and complexity. In addition, it has been suggested that in relation to victims of F&CM there are two types vulnerability which are best considered separately: *vulnerability to victimisation* and *vulnerability post-victimisation*. Vulnerability to victimisation is focused on varying degrees of risk and control which influence how likely someone is of becoming a victim – either once or repeatedly. Risk and control are strongly mediated by embodied and situational factors. This is distinguished from vulnerability post-victimisation, which is concerned with the victims' ability to cope with new or exacerbated harms, which result from F&CM. This understanding provides a bridge between many different understandings of vulnerability and captures the paradox at the heart of the concept – that is both universal and particular to victims' circumstances. This is key to establishing an adequate response and processes within the CJS to meet the challenges posed by F&CM victimisation.

Understandings of 'the victim' at the *micro*, *meso* and *macro* levels influence and reinforce each other. However, micro and macro level understandings are crystallised at the meso-level of the institutional label – somewhere at the intersection of individual experience and cultural understandings of the victim, individuals are recognised as victims and labelled as such by CJS and other institutions. Furthermore, it is at this level that decisions about the implementation or dispensation of victim rights are made. As shown, vulnerability assessments trigger that what Hall (2009) terms victims' procedural and service rights. Procedural rights are rights to participate and influence decisions in the criminal justice process, whereas service rights relate to the way victims are treated and the services and support they are entitled to when they engage with the CJS. However, as noted above, there is considerable variation with respect to how vulnerability is understood and operationalised to provide a response to victims of F&CM. As such, victimhood "is something that has to be achieved and involves a process from the individual recognizing that they have been victimised and thus may claim the label, through to being socially and/or in policy terms recognised as a victim" (Walklate 2007, p. 28). In other

words, self-perception and the choice to report crime are necessary but not sufficient conditions to accessing victim services. The ways in which victims are selected and their needs prioritised give form to what has been described as a "hierarchy of victimisation" (Carrabine et al., 2004, p. 117) and are linked to the macro-level 'idealisations' of the victim.

As such, F&CM crime reports constitute a useful point of departure to develop a better understanding of which experiences of victimisation are recognised and how vulnerability is constructed at the meso level. It also allows for an examination of which victims are considered *vulnerable* and how vulnerability is identified by law enforcement agencies. As noted, understandings of 'the victim' across the micro to macro levels can be at odds, with some who consider themselves victims not being recognised and vice-versa. As such, there is a need to think critically about situations where the different levels of understanding of the victim do not align. While patterns of F&CM victimisation emerge at the meso-level, victims' needs are heterogeneous. It would be a fallacy to apply such patterns directly to the individual's experience. The individual, inter-subjective and 'experiential' (Walklake, 2011, p. 181) nature of such experiences and fears highlight the need to explore experiences of F&CM victimisation beyond standard patterns. To critically consider such patterns, this thesis goes on to explore qualitatively "what this standardization makes visible and renders invisible and how it connects to the deep-rooted assumptions of what it is that can be asked" (Walklate, 2007b, p. 64). As such, it contributes to the plugging of the evidential gap with respect to F&CM vulnerability.

Finally, this chapter addressed the relationship between vulnerability and repeat victimisation (RV). RV is one factor recognised within the Victims' Code as an indicator of victim vulnerability and which may be applicable to F&CM victims. Based on CSEW data, it demonstrated that while under-researched, a significant proportion of F&CM crimes are experienced by repeat victims (approximately 25%) and that a significant proportion of F&CM victims are estimated to be repeat victims (13%). Previous research suggests that RV may be both a 'flag' or a 'booster' of victimisation risk, referred to as *vulnerability to victimisation*. As such, understanding patterns of RV has the potential to inform crime reductions strategies. At the same time, the ways in which RV measurements influence the visibility of patterns of certain victim groups is of paramount importance as it may over or under-state RV experiences. Furthermore, more research is needed to understand the minority of victims who experience extreme levels of RV and which may be referred to as 'chronic' victims. For these victims, addressing *vulnerability post-victimisation* may be as important as attempting to intervene in

order to protect them from further victimisation. In chapter five, this thesis takes steps towards closing this evidential gap.

CHAPTER 3: Methodology

1. Research Questions and Mixed-Methods Research

This thesis is situated within a constructivist, *critical realist* perspective. It takes a constructivist approach as it understands crime, victimisation and vulnerability as socially constructed concepts (the *critical* aspect). Nonetheless, it recognises the importance of measurement in furthering conceptual understandings and enabling the development of evidence-based criminal justice responses (the *realist* endeavour). Measurement furthers understanding in so far as the process of measurement lays bare assumptions of what 'counts' as crime and who counts as a (vulnerable) victim. As such, measurement is a vehicle for critical engagement with socially constructed categories. Furthermore, measurement is "currency" in policy-making contexts, relied upon to determine the fair prioritisation of resources. This applies to the prioritisation of crime types based on volume and impact and of the victim support provided, based on vulnerability assessments. As such, a mixed-methods approach was aligned with the author's epistemological perspective and well-suited to meet the aims of this thesis.

Mixed-methods involves combining qualitative and quantitative methods "for the purposes of breadth and depth of understanding and corroboration" (Johnson , Onwuegbuzie , & Turner 2007, p. 123). Arguably, most research uses mixed-methods by for example, engaging with previous literature, utilising qualitative data to develop quantitative instruments, or deriving quantitative summaries from qualitative data (Creswell, 2010). Consequently, mixed-methods is not seen by some scholars as a stand-alone paradigm.[38] Regardless, the author considers privileging the use of a plurality of methods to be a unique approach. As Johnson and Onwuegbuzie suggest, one should "choose the combination or mixture of methods and procedures that works best for answering […] research questions" (2004, p. 17). Accordingly, each method used in this thesis was chosen for its contribution to answering particular research

[38] A research paradigm is understood here as "a set of beliefs, values and assumptions which a community of researchers has in common regarding the nature and conduct of research" (R. B. Johnson & Onwuegbuzie, 2004, p. 24).

questions. Furthermore, the idea of *triangulation* that lies at the core of mixed-methods is well established. Triangulation consists of using multiple methods within a research design for the purposes of validation of results and their interpretation (Campbell & Fiske, 1959). This is done in recognition that no method is perfect and, in an attempt to address these imperfections. Validity is thus achieved where a "proposition can survive the onslaught of a series of imperfect measures" (Webb, Campbell, Schwartz, & Sechrest, 1966, p. 3).[39] In this way, it is hoped that "the bias inherent in any particular data source, investigator, and particular method will be cancelled out" (Denzin, 1978, p. 14). This is also the core principle of the 'scientific method'. Inevitably, there are a wide variety of configurations of mixed-methods research, where one method may be more or less dominant (Teddlie & Tashakkori, 2009). In this thesis, quantitative methods dominated the first stages of research, while qualitative methods dominated the final stages. Table 3 summarises the research questions (RQs) and sub-questions, as well as the respective analysis chapters and methods used throughout this thesis.

	Question & Sub-Questions	**Methods**
RQ1	What was the volume of reported F&CM in Wales over the reference period? (chapter 4, section 1) i. How did the volume of recorded F&CM vary across victim types? ii. Was the volume of F&CM recorded in Wales significantly different across forces? iii. How did the volume of crime reported in Wales vary over the reference period? iv. Was the volume of F&CM recorded in Wales significantly different to other crime types?	Descriptive and bivariate statistics; GLMs.
RQ2	What were the characteristics victims who reported F&CM in Wales over the reference period? (chapter 4, section 2) i. What victim types reported F&CM in Wales? ii. What were the demographic characteristics of individuals across the crime groups? iii. What were the demographic characteristics of individuals across crime categories?	Descriptive and bivariate statistics; GLMs.
RQ3	What financial and other impacts were reported by individuals and other victims of F&CM in Wales over the reference period? (chapter 4, section 3) i. How did direct losses vary between victim types and individual characteristics?	Descriptive and bivariate statistics; GLMs; TA.

[39] 'Validity' is in itself a complex and contested construct, particularly where the 'validity' of knowledge produced through a social-constructivist lens is questioned by more positivist traditions. Nonetheless, the term is used here in the broadest possible sense to mean research findings which are internally coherent, while making a contribution towards a given area of study such as F&CM victimisation.

	ii. What impacts beyond direct losses can be identified from crime reports? (qualitative)	
RQ4	What online/offline dynamics enabled F&CM in Wales over the reference period? (chapter 5, section 1) i. Was there an association between the online/offline Modus Operandi (MO) and victim characteristics? ii. What online/offline dynamics characterised each of the crime categories considered? iii. To what extent were online/offline elements driving these crimes? iv. What other the key MO features can be identified? (qualitative)	Descriptive and bivariate statistics; GLMs; TA.
RQ5	What was the extent and nature of individual F&CM repeat victimisation (RV) in Wales? (chapter 5, section 2.1) i. What is the extent of RV within the sampled data? ii. Did the distribution of RV vary across crime categories?	Descriptive and bivariate statistics; data linkage; GLMs.
RQ6	What were the characteristics of repeat victims? (chapter 5, section 2.2) i. What were the demographic characteristics of repeat-victims and how did these differ from one-time victims? ii. Did RV vary with respect to the local area's socio-economic profile and level of internet access? iii. Which crime categories and victim characteristics were best suited to predicting individual RV?	Descriptive and bivariate statistics; data linkage; GLMs.
RQ7	What was the impact of RV? (chapter 5, section 2.3) i. Was there an association between RV and the financial loss suffered by victims? ii. What other RV impacts can be identified from F&CM crime reports?	Descriptive and bivariate statistics; data linkage; GLMs; CA.
RQ8	What was the characteristic time-course of RV? (chapter 5, section 2.4) i. What was the overall/typical time-course of RV? ii. Did the distribution of time-course vary across crime group/category?	Descriptive and bivariate statistics; data linkage; GLMs.
RQ9	What were the mechanisms through which RV happened? (chapter 5, section 2.5)	Data linkage; TA and CA.
RQ10	How was vulnerability constructed within reports of F&CM? (chapter 6)	TA and CA.

Table 3 – Research questions and respective methods used.

The methods used in this thesis included a review of existing literature and published statistical datasets, the statistical analysis of a two-year sample of AF recorded crime, the linkage of these reports to identify repeat victims, the Thematic Analysis (TA) of the free-text incident descriptions of a sub-sample of reports and the validation of key qualitative insights through Content Analysis (CA). Quantitative and qualitative methods were used both simultaneously and sequentially (Morse, 1991). Simultaneously, as quantitative and qualitative methods were selected to answer the research questions to which they were respectively best suited, with limited interaction between them. Quantitative methods were best suited to answer research

questions one to eight with the exceptions of RQ3(ii) and RQ4(iii)), while qualitative methods were used predominantly to answer questions nine and ten. The quantitative methods, including descriptive, bivariate and multi-variate analysis, used *R statistics* software and *R markdown* to document statistical coding and analysis.[40] The qualitative TA was aided by the analysis software NVivo. At the same time, sequential triangulation was also used in the sense that the results of one method influenced the interpretation of the results of the other. On one hand, the qualitative data played an important role in "interpreting, clarifying, describing, and validating quantitative results, as well as through grounding and modifying" (R. B. Johnson, Onwuegbuzie, & Turner, 2007, p. 115). On the other, quantitative content analysis facilitated an assessment of the generalisability of key insights derived from qualitative analysis. As such, the 'hybrid' and pragmatic mixed-methods approach resulted in greater validity and more in-depth research findings. Surprisingly, despite notable exceptions (e.g. Holder, 2016; Ranapurwala, Berg, & Casteel, 2016), examples of mixed methods in F&CM victimology and RV research are rare, with most studies focusing on either large quantitative studies or small qualitative but in-depth analysis of the victims' experiences. In this way, this thesis makes a unique methodological contribution in its application of a mixed-methods approach to the study of F&CM vulnerability and RV. In what follows, the data collection process and analysis methods are described in detail, followed by a reflection on legal and ethical considerations, as well as the strengths and limitations of this methodology.

[40] R Statistics is an open-source statistical programming language which is widely used in the physical sciences and increasingly by social scientists. As will be explained, R Markdown provided a framework to integrate R code, results, and prose commentary into this thesis (see Annexes). In combination, R Statistics and Markdown thus allow for transparency and the replicability of the statistical analysis.

2. Data Collection

The data collected included all F&CM reports (n = 17,049), made to AF within the four Welsh police forces (Dyfed/Powys, Gwent, North Wales and South Wales), between 1st October 2014 and the 30th September 2016 (the 'reference period').[41] As it will be seen, of these, n = 11,841 were identified as reports pertaining to individual victims. The start date was determined by what data was available to the Southern Wales Regional Organised Crime Unit (SW-ROCU). In addition, it was considered by the research partners and the researcher that by 2014 the quality of the Action Fraud data should have stabilised, as the service had been rolled out nationally from April 2013. Finally, the researcher requested a two-year sample ending in September as this allowed for comparison with CSEW estimates for the same period.

The dataset was collated from monthly extracts of crime reports made by victims to AF and subsequently shared with local police forces by the NFIB, via the NicheRMS system.[42] With the exception of data pertaining to North Wales, it was from this system that the SW-ROCU extracted the sampled data for collation and analysis by the author (the 'raw' dataset).[43] In addition, the author added variables to the raw dataset through coding and (deterministic) linkage to open source data, while a more sophisticated linkage method was applied to link reports made by repeat victims.

The final dataset thus provided a snapshot in time of crime reports and respective law enforcement response and may be described as police recorded crime (PRC), as well as administrative (linked) data. The limitations of using administrative data and specifically PRC in research are known (Flatley, 2013; Levi & Burrows, 2008). At the same time, there are also considerable benefits in making use of the richness of AF data. Section seven of this

---

[41] As detailed in Annex II (section 2), the raw data supplied by the ROCU included incidents reported between the 1st June 2014 and the 30th November 2016 (n = 20,376). For the reasons stated below, this reference period was adjusted and duplicates removed resulting in a total sample of n = 17,049 incidents.

[42] NicheRMS is an operational platform provided by Niche Technology Incorporated, a private Canadian corporation founded in 1992 and based in Winnipeg, Manitoba. NicheRMS is used by police services in the United States, Canada, the United Kingdom, and Australia (Niche Techonology, 2019).

[43] As the North Wales police force falls within the jurisdiction of the North West (TITAN) ROCU, SW-ROCU facilitated a request to this local force which provided North Wales data separately. The data was provided to the author by SW-ROCU in four separate batches between August 2015 and August 2017. The first batch of data included crimes reported by victims in Gwent, Dyfed Powys and South Wales between June 2014 and November 2015. The second batch added crimes reported up until February 2016 for the same forces. The third batch included data for reports in North Wales for the equivalent period of June 2014 to February 2016. Finally, the fourth batch included reports for all four Welsh police forces between February and November 2016.

methodology details the ethical approval procedures and the legal, security and ethical considerations considered and acted upon throughout this research. In addition, the final section discusses the limitations of this study's design.[44]

[44] The strengths and limitations of Action Fraud data are considered throughout this thesis and are the subject of detailed analysis in Annex VII.

3. Data Processing and Sample Characteristics

3.1. Data Processing

Extensive data processing was required to make the raw data ready for analysis. These processes included variable re-naming, adjusting the reference period, removing erroneous duplicate entries, standardising missing values, formatting variable types and ordering the dataset by date. After standard processing, basic quality assurance was performed by calculating variable the proportion of missing and unique values per variable and the total number of records contained in each batch supplied to the author (Annex VII). Finally, through linkage, new variables were added and repeat victims identified. As such, the variables used in the analysis that follows this chapter were either *original variables*, derived from the original variables through re-classification (*derived variables*) or coded from original variables through the application of coding rules (*coded variables*). In addition, several variables including geography, internet access and socio-economic indicators, were linked from external open-source datasets (*linked variables*). In total, the original dataset contained 28 and the final dataset 51 variables.

The required data processing was made possible by using R tools, particularly packages of the 'Tidyverse' collection (Wickham et al., 2019), which provide a range of data science functionally. Furthermore, all processing was documented using R Markdown, which provides a framework for combining code, results, and prose commentary, thus allowing these to be integrated into this thesis and ensuring reproducibility (Allaire et al., 2020; Xie, Allaire, & Grolemund, 2018). The data processing carried out to prepare the dataset for analysis is detailed in the R Markdown notebooks in Annex II (data cleaning and derivation) and Annex IV (data linkage). Annex III includes a list of all dataset variables including classification (e.g., numeric, categorical etc), along with variable descriptions. A summary of the processing and linking of key variables is included below.

3.1.1. Original Variables

Age Variable

Age on the day of reporting was known for n = 9,714 individual reports. As this appeared to be automatically calculated based on the victim's date of birth (dob), impossible/unlikely age values were indicative of possible errors in the dob recorded. In particular, two records

contained a negative age value, three were recorded as zero and five were equal to or larger than 114. In early discussions with SW-ROCU, it was noted that values of 114 or above were generated by call operators in lieu of dob 'not known'. As such, the decision was taken to re-code values equal to or lower than 0, as well as over 100 as missing.

3.1.2. Derived Variables

Crime Group and Crime Category

Reports in the original dataset of recorded crime were classified in line with the Home Office Counting Rules for Recorded Crime (HOCR). In total, this amounted to 8 unique categories of computer misuse offences and 41 unique fraud categories. Given that working with 49 categories would be theoretically unwieldy and statistically impractical, the original HOCR categories were grouped by similarity of MO, with reference to existing F&CM typologies, resulting in nine categories of fraud and two categories of computer misuse (please refer to chapter one, section 1.4). As the HOCR categories are considerably more granular than those in the literature, they were grouped in order to be, to the extent that it was possible, compatible with existing typologies, particularly Levi & Burrows (2008), Button, Lewis and Tapley (2009), Wall (1999) and (Yar, 2006). That said, this typology was also data-driven in the sense that throughout the analysis it was developed to maximise statistical power.

Police Response Variables

Crimes reviewed by an NFIB Crime Reviewer (see chapter one, section 2.1) included a complete record for at least one of the following variables: '*disseminated',* indicating referral to a police force; '*partner'* for referral to partner agency; '*outcome',* the immediate outcome of the referral or alternative action; and '*call',* a subsequent update of outcome. Following standard processing, these variables were combined to aid analysis. Firstly, a variable (*disseminated_all*) combined *disseminated* and *partner*. Secondly, a new *outcome_derived* variable was derived to combine *outcome* upon NFIB review, with *call*. Where there was a record for both *outcome* and *call*, the latter was given priority as this was the most recent. Finally, to overcome the difficulties created by the missing values across all police response variables, the variable *action_type* was derived to classify the action taken overall, combining

all police response information into eight categories.[45] This variable favoured the classification in *outcome_derived*, supplementing this with "Referred to Partner" where there was a *partner* referral, but *outcome* was missing (n = 11) and "Force Miscellaneous" where there was a *dissemination* but *outcome* was missing (n = 20).

3.1.3. Coded Variables

Several key variables were not directly available but were coded based on original variables. The coding was iteratively designed until the author was satisfied with its accuracy, through a combination of automated coding and manual review.[46] Inevitably, some error will remain, including false positives, false negatives and unknowns. Despite limitations however, few cases were identified as misclassified once records were linked to identify reports made by the same individual and examined in detail, suggesting a low level of false positives. Coding methods for victim type, gender and MO Group are described below.

Victim Type

Meeting the aims of this study required identifying victim type. This was coded according to a series of pre-defined rules, applied sequentially, in order to identify whether reports were made businesses, public sector organisations, charities or individuals as summarised in Table 4 below.[47]

Rule Description	**Businesses**	**Public**	**Charities**	**Individuals**	**Missing**
1) Code "Business" where crime category applicable to businesses only.	810	NA	NA	NA	16,239
2) Code "Business" where victim address contained one of the designated key words.	1,924	NA	NA	NA	15,125
3) Code "Business" where victim name contained one of the designated key words.	302	NA	NA	NA	16,747
4) Code "Public" where analytical crime category was "Public Fraud".	1,978	109	NA	NA	14,962
5) Code "Charity" where crime category only applicable to charities.	1,972	109	57	NA	14,911

[45] Force Miscellaneous; Enforcement & Investigation; Victim Care; Prevention; Intelligence; Filled; Referred to Partner and No Investigation.

[46] Given the need to rely on identifiable information to carry out this process, this was performed within SW-ROCU secure environment, prior to the anonymisation of the data (see section 8).

[47] Full coding details in Annex II, section 4.9.

6) Code "Individual" where victim type is still missing and victim has a title (e.g., Mr).	1,972	109	57	11,841	3,070

Table 4 – Victim type coding rules and frequencies.

The above coding rules and the key word list were developed iteratively by manually reviewing random samples of the resulting coding. This coding is not error-free as illustrated by the 3,070 cases which could not be coded. Given the coding rules, it is likely that these are overwhelmingly individual victims whose records were missing a title and thus individual victims are likely under-estimated. In addition, it is possible for a sole-trader, trading under their own name, to be misclassified as an individual victim. However, few false positives were identified on manual review of a random sample of cases.

Gender

Victims' gender was also of criminological interest but unavailable directly. The variable gender was therefore coded in two steps, prior to anonymisation (Table 5).[48] Firstly, gender was coded based on the title recorded along with victims' name: Mrs, Ms and Miss were coded as "female"; Mr was coded as "male" and Dr as "missing". Secondly, where gender was still missing, new gender codes were imputed based on the victim's first name, extracted from the full name variable and then coded using the R package *gender* (Blevins & Mullen, 2015; Mullen, 2016). This provides a dictionary of the most probable gender, based on first name. The results of this coding are presented in the table below.

	Female	**Male**	**Missing**	**% Missing***
Step 1	6,150	6,472	4,427	25.29
Step 2	5,821	6,305	4,923	28.88
Total	7,741	8,297	1,011	5.93

Table 5 – Records coded male/female per coding stage.

***Represents % of total number of records, including reports from all victims.**

There were limitations to this approach as the probabilities of gender used in R package *gender* were derived from the U.S. Social Security Administration baby name data, per year of birth.

[48] See Annex II, section 4.5 gender coding method in detail.

As the underlying data dictionary is not optimised for the Welsh population within the study's reference period, it is likely to underperform with respect to non-English and Welsh names. In addition, it is limited by the gender binary assumptions of the underlying name-gender dictionary. As such, the second method will tend to favour records for cis-English-White victims. Nonetheless, using this method reduced the proportion of missing values from 25.29 to 5.93%, thereby improving the quality of the statistics produced.

MO Group

Following from the discussion in chapter one and to explore the online/offline dichotomy, all records were coded (true/false) to indicate whether there was evidence that they contained online and/or offline elements (Table 6). Records were coded *true* for online elements if they met one of three conditions: 1) the crime targeted computers/networks or their constituent parts, 2) computer/networks were key to the crime's MO, or 3) computer/networks were the pretext used to commit the crime. All incidents assessed to meet the above criteria based on the NFIB category description were automatically coded as having an online element.[49] Finally, where there was evidence that computers/networks were used to commit the crime based on a search of keywords within incident descriptions (Gordon & Ford, 2002; Jarvis & Macdonald, 2015), these were also coded for online elements. Keyword lists for both online and offline coding were developed based on the review of the literature on the mechanisms of F&CM, followed by iteration between automated coding and manual review of multiple random sub-samples of cases (n = 100). This process was repeated until the number false positives and false negatives amounted to 5% or less of the random sub-sample.[50]

	NFIB Category	**Key Word Search**	**Combined Total**
Online	6,656	8,015	9,402
Offline	3,922	6,053	8,216
Unknown	NA	NA	894

[49] These included all Computer Misuse crimes and crimes where the pretext of networked computers was key, namely the NFIB category of Computer Software Fraud (although this was also coded for offline elements given that a phone call is the method of first contact), see Annex I.

[50] As documented in section 4.8.4.4 of Annex II, the percentages of estimated false positives and false negatives for reports coded for online elements were 3% and 0% respectively; for reports coded for offline elements, they were 4% and 5% respectively.

Table 6 – Records coded on/offline per coding stage.

In addition, following van Wilsem (2011), the data were coded *true* for offline elements (variable *offline_all*), so as to make visible the online/offline dynamics. Records were coded as containing offline elements where the MO relied on and the crime could not be committed without non-internet enabled communications, or prior a relationship between the victim and the suspect(s). This included where there was evidence of face-to-face communication, telephone or texting. In addition, offline coding included cases where there was evidence of a known suspect/offender (e.g., family members or (ex)partners), as this suggested an offline relationship. Furthermore, similarly to the process described above, coding of offline elements was carried out based on a combination of identifying NFIB categories which necessitated an offline element and a key-word search of the incident descriptions. Finally, the variable *mo_group* was derived from the previously coded *online_all* and *offline_all* variables, categorising records which contained evidence of only online elements, only offline or mixed on/offline elements.

3.1.4. Linked Variables

Linked data (2006) is understood as structured data which is matched with additional data via shared identifiers (deterministic matching), or through statistical methods (probabilistic matching), in order to add additional information/variables to a dataset. Several new variables were added to the dataset through deterministic matching including ONS geography data, Ofcom data on internet connectivity data and socio-economic indicators from the Welsh Index for Multiple Deprivation (WIMD). In addition, a more complex linkage methodology using both exact and probabilistic matching was developed and optimised to identify the crime records reported by the same individual victims (section five below).

Geography Data

Data pertaining to the statutory administrative area known as the Local Authority (LA), as well as the standard statistical Lower Layer Super Output Areas (LSOAs) and Middle Layer Super Output Areas (MSOAs), were downloaded from ONS Postcode Directory (ONSPD), via the UK Data Service web portal. The Directory "relates postcodes (as at the third Friday of the month prior to each release) to administrative and electoral areas as at the preceding May" (ONS, 2016a, p. 5). The November 2016 release of ONSPD was chosen as it most closely matched the end of reference period. Geography data for Wales was added to the sampled

dataset by linking on the common variable *postcode* within the SW-ROCU's secure premises, prior to the data being anonymised for further analysis at the University. While regularly updated, the ONSPD does not constitute Official Statistics and will inevitably contain errors in the form of missing and inaccurate data. Nonetheless, the ONSPD matched 100% of the sampled dataset, indicating a negligible level of error.

Internet Connectivity Data

Internet connectivity data for LAs in Wales was downloaded from Ofcom's Open Data portal (Ofcom, 2017b). This data was originally collected by Ofcom from the main UK telecoms operators (BT, Virgin Media, Sky, TalkTalk, Vodafone and KCOM) and represents a snapshot in time taken in June 2016 (Ofcom, 2017a). Data from June 2016 was chosen as it most closely matched the end of the reference period. Internet connectivity data was then added to the crime reports dataset by linking from the Ofcom data on the common variable for LA code. The variables linked from Ofcom's data are described in Annex III based on Ofcom (2017b) metadata.

Following linkage, an overall measure of internet access (*net_access*) was derived on a four-point scale from poor to very good, by LA. This measure was derived in two steps. Firstly, the percentage of premises able to receive information at the various Mbit/s levels recorded was computed (e.g., those able to receive 2Mbit/s were calculated as 100 – percentage unable to receive 2Mbit/s), as these were more intuitive measures than the original variables. Secondly, a new variable was created by coding the overall level of internet access in the area according to the rules detailed in Table 7.

Rule	**Internet access**
1) Less than 90% of premises receive 2 Mbit/s or 5 Mbit/s	Poor
2) Less than 95% of premises receive 2 Mbit/s and 5 Mbit/s	Poor
3) Cases not covered by all other conditions	Medium
4) More than 90% of premises but less than 95% receive 30 Mbit/s	Good
6) At least 95%of premises receive 30 Mbit/s	Very Good

Table 7 – Rules for local internet access measure

The variables used in the construction of the above measure have several limitations. Firstly, broadband infrastructure is not fixed, and it was not possible to ascertain exactly how this data

was collected by Ofcom, or the ways in which errors could occur in the collection/processing at source. Furthermore, the overall measure applies to LAs rather than individual victims. Nonetheless, this data provides a proxy measure of variations in Internet access across LAs.

Welsh Index of Multiple Deprivation

WIMD data was downloaded and linked to the sampled dataset (StatsWales, 2014a). The index is an official statistic which measures the concentrations of different types of deprivation across eight domains, at the previously mentioned LSOA level across Wales. The combination of the results across domains gives an overall relative deprivation ranking for each LSOA i.e. it identifies areas from the most to the least deprived (StatsWales, 2014b). As there are 1909 LSOAs in Wales based on the 2011 Census, the WIMD ranking ranges from 1 (the most deprived area) to 1909 (the least deprived area).

The 2014 WIMD ranking data was sampled because it was the only full update of the index which was carried out within the reference period of the crime reports dataset. As such, WIMD data was added to the crime report dataset by linking on the common variable *lsoa11*. The WIMD is limited as an indicator in that it "identifies areas where there are concentrations of several different types of deprivation" (Jones, 2014, p. 1). As such, this variable provides a measure of social-deprivation for the area where F&CM crimes were reported, rather than identify individual victims who are multiply deprived. However, it remains useful to understand whether certain F&CM categories are associated with lower or higher levels of deprivation at this aggregate level.

3.1.5. Variable List and Description

Annex III includes a list of all dataset variables including classification (e.g., numeric, categorical etc), along with variable descriptions. For ease of reference, the variables are grouped as pertaining to a) crimes and MOs, b) police response, c) victim characteristics, and d) situational context.

3.2. Sample Characteristics

Once duplicates were removed (n = 147), a sample of n = 17,049 cases used in the analysis which follows this chapter.[51] The characteristics of the sample are summarised in Table 8 below.[52]

	Full sample (n = 17,049)		**Individual victims (n = 11,844)**	
	Mean or %	SD	Mean or %	SD
Force				
Dyfed/Powys	17.98%	0.38	20.58%	0.40
Gwent	18.46%	0.39	20.19%	0.40
North Wales	22.77%	0.42	15.78%	0.36
South Wales	40.79%	0.50	43.46%	0.50
Quarter				
Year 1 – Quarter 1	7.04%	0.26	3.94%	0.19
Year 1 – Quarter 2	14.18%	0.35	13.17%	0.34
Year 1 – Quarter 3	14.93%	0.36	16.41%	0.37
Year 1 – Quarter 4	12.22%	0.33	12.07%	0.33
Year 2 – Quarter 1	10.93%	0.31	9.46%	0.29
Year 2 – Quarter 2	12.04%	0.33	12.80%	0.33
Year 2 – Quarter 3	13.87%	0.35	15.02%	0.36
Year 2 – Quarter 4	14.79%	0.35	17.13%	0.38
Victim type				

[51] Duplicates were removed based on the crime unique reference number (the NFRC code). In a discussion with a Crime Reviewer at the National Fraud Intelligence Bureau (NFIB) (personal communication, June 4, 2018) it was established that it was possible for an NFRC number to appear twice where a case is disseminated to more than one force (e.g., to one force for investigation and to another for victim support). However, on close examination, all cases containing duplicate NFRC codes were in fact just complete duplicates of each other, with no indication of more than one dissemination. In addition, all duplicates related to cases reported in the month of December 2014 (in South Wales, Gwent and Dyfed/Powys). As this indicated a system glitch, duplicates were simply removed from the analysis.

[52] *Due to missing values for age, n = 9,543. **Due to missing values in loss variable, n = 11,874 for all victims and n = 8,230 for individual victims.

Business	11.55%	0.32	N/A	N/A
Charity	0.33%	0.06		
Individual	69.47%	0.46		
Public Org.	0.64%	0.08		
Not Known	18.01%	0.38		
Gender				
Female	N/A	N/A	48.86%	0.50
Male			50.96%	0.50
Not Known			0.18%	0.04
Age				
*Age**	N/A	N/A	50.47	18.62
Age category				
0-19	NA	NA	2.86%	0.17
20-24			5.56%	0.23
25-29			5.43%	0.23
30-34			5.74%	0.23
35-39			5.66%	0.23
40-44			6.16%	0.24
45-49			6.67%	0.25
50-54			6.85%	0.25
55-59			6.74%	0.25
60-64			6.94%	0.25
65-74			13.68%	0.34
75-84			6.82%	0.25
85+			1.45%	0.12
Not Known			19.43%	0.40
Ethnicity				
Asian	N/A	N/A	1.83%	0.13
Black			0.65%	0.08
Mixed			0.41%	0.06
Other			0.41%	0.06
White			63.22%	0.48
Not Known			33.48%	0.47
Crime group				
CM	7.68%	0.27	8.11%	0.27
Fraud	92.32%	0.27	91.89%	0.27

MO Group				
Mixed	26.05%	0.44	31.05%	0.46
Offline Only	22.14%	0.41	17.56%	0.38
Online Only	29.10%	0.45	31.70%	0.47
Not Known	22.71%	0.42	19.68%	0.40
Crime category				
Advance-fee fraud	19.05%	0.39	21.32%	0.41
Business Compromise	0.88%	0.09	NA	NA
Card and Banking fraud	5.51%	0.23	4.84%	0.21
Consumer Fraud	40.62%	0.49	45.15%	0.50
Hacking	4.99%	0.22	5.46%	0.23
Investment fraud	1.92%	0.14	1.98%	0.14
Malware, virus & (D)DOS	2.69%	0.16	2.65%	0.16
Other fraud	16.52%	0.37	15.93%	0.37
Public fraud	0.64%	0.08	NA	NA
Retail fraud	3.27%	0.18	NA	NA
Services fraud	3.91%	0.19	2.67%	0.16
Direct financial loss				
*Pounds sterling (£)***	258752.9	15894479	3960.87	64031.57
Repeat report				
No	NA	NA	93.04%	0.25
Yes			6.96%	0.25
Actioned				
No	85.22%	0.35	85.32%	0.35
Yes	14.78%	0.35	14.68%	0.35
Action type				
Enforcement and Investigation	9.83%	0.30	9.04%	0.29
Filed	1.98%	0.14	2.38%	0.15
Miscellaneous	0.18%	0.04	0.19%	0.04
Intelligence	1.03%	0.10	0.94%	0.10
No Investigation	0.42%	0.06	0.39%	0.06
Prevention	1.08%	0.10	1.43%	0.12
Victim Care	0.26%	0.05	0.31%	0.06
NA	85.22%	0.35	85.32%	0.35
Deprivation index (WIMD)				
Most (1) to least (1909)	956.83	533.67	960.11	544.41

WIMD category 1				
Low Deprivation	NA	NA	24.48%	0.43
Medium Deprivation			51.31%	0.50
High Deprivation			24.21%	0.43
WIMD category 2				
Low Deprivation	NA	NA	24.48%	0.43
Low-Medium Deprivation			26.09%	0.44
Medium-High Deprivation			25.22%	0.43
High Deprivation			24.21%	0.43
Internet connectivity				
Poor	8.36%	0.28	9.40%	0.29
Medium	23.94%	0.43	23.18%	0.42
Good	18.76%	0.39	14.66%	0.35
Very Good	48.95%	0.50	52.76%	0.50

Table 8 – Sample summary statistics.

Of the few continuous numerical variables included in this dataset, none were normally distributed. Normality was visually verified by analysing via histograms and the respective Q-Q plots (minus outliers) for the variables age, loss and WIMD. In addition, the lack of normality was quantified by calculating the skew, kurtosis and applying the Shapiro-Wilk test of normality (W) (Table 9).[53]

	Mean	**Median**	**Skew**	**Kurtosis**	**W**
age	50.47	51	-0.03	-1	0.97***
loss	3960.42	155	62.89	4636.87	0.02***
deprivation	960.11	964	-0.01	-1.17	0.96***

Table 9 – Summary statistics for numeric variables age, loss and deprivation (individuals).

In a normal distribution, skew and kurtosis are zero. As such, the skew of age and deprivation indicates a slight concentration towards higher values (meaning older age, lesser deprivation) and the kurtosis scores indicate a flat and lightly tailed distribution. For loss, the considerably

[53] ***significant at the p-value < 0 .001 level.

high positive value of skew indicates that values are very concentrated towards the lower end of loss (the left side of the x-axis) and the high positive value of kurtosis indicates a pointy and heavy-tailed.[54] Variables age ($W = 0.97$, p-value < 0.001), loss ($W = 0.02$, p-value < 0.001) and deprivation ($W = 0.96$, $p < 0.0001$), were all significantly non-normal according to the Shapiro-Wilk test.[55] However, for large samples such as this one this test "can be significant even when the scores are only slightly different from the normal distribution" (Field, Miles, & Field, 2012, p. 185). Nonetheless, based on the visual analysis of the histograms and Q-Q plots, each of these variables were assumed to be non-normally distributed (for histograms and Q-Q plots, see Annex V).

[54] Several transformations were unsuccessfully attempted to normalise the loss data including log, square-root and reciprocal transformations (see section 9.1.2 of Annex V).

[55] The Shapiro-Wilk test of normality tests the null hypothesis (H_0) that there is no significant difference between the distribution of a variable of interest and the normal distribution, based on that variable's mean and standard deviation. As such, where the p value is significant ($p < 0.05$) the null hypothesis is rejected, supporting the alternative hypothesis that there is a significant difference between the variable's and the normal distribution.

4. Descriptive, Bivariate and Multivariate Analysis

As previously noted, quantitative analysis was used to answer specific research questions. In broad terms, the questions which could be answered through quantitative methods related crime types being recorded, victim characteristics, the relationship between the two, as well as patterns of RV. The quantitative analysis involved exploring relationships between variables designated as outcome (and known as dependent or response variables) and explanatory (also referred to as independent or predictor variables) and a series of statistical procedures to determine the statistically significant and strength of these relationships (or their effect size). Furthermore, where possible, results were broken down further to establish what was driving key effects. The methods used included descriptive, inferential and statistical modelling techniques (namely Generalised Linear Modelling or GLM).

4.1. Descriptive and Bivariate Analysis

A descriptive statistical analysis of the dataset was undertaken in the first instance (see previous section). In addition to summarising the data, calculating measures of central tendency and dispersion of the data, where appropriate, variables were tested for statistical assumptions regarding the shape and homogeneity of the distribution, as well as independence of cases (detailed in Annex V). Inferential bivariate analysis was then carried out in order to draw conclusions about the wider population (victims reporting instances of F&CM) and to examine differences, similarities and relationships between variables (Calder, 1996). Hypotheses about relationships between individual/environmental characteristics and crime categories were developed from the descriptive statistics and a review of the literature. These were tested using inferential statistical techniques, in line with a frequentist statistical approach.[56]

While the dataset analysed included all crimes reported within the Welsh forces, following Brimicombe (2014, 2016a, 2016b), this was treated as a sample of records delimited by the

[56] The Frequentist approach assumes that the distribution of the population data are similar to that of the sample data. However, as the true population mean cannot be known, this approach requires the development of a null hypothesis (H0), i.e. where there is no relationship and the population mean would be 0. In this way, the null hypothesis can be rejected or accepted. Where it is rejected, the analysis lends weight to the alternative hypothesis (H1) that there is a relationship between the variables. Using Frequentist methods however, H1 cannot be accepted or rejected in its own right. Bayesian methods could be used in order to accept or reject H1 directly, but these make different assumptions which some authors find problematic (Lee, 2012, p. xxii) and Bayesian statistics are still not widely used in criminology.

reference period and therefore subject to sampling errors. As such, statistical techniques were used to assess the likelihood that the observed differences and relationships could have arisen by chance or, in other words, the level of certainty with which the findings may be treated. As the dataset contained a variety of categorical (e.g. gender), interval (e.g. number of repeats) and ratio (e.g. loss and age) data, statistical tests were carried out as appropriate including *chi-square* (associations between categorical variables), the *Wilcoxon-Mann-Whitney* test (associations between two groups for non-normal ratio data), the *Kruskall-Wallis* test (associations between more than two groups for non-normal ratio data) and the *Spearman rank* correlation coefficient (for non-normal interval data). Furthermore, the relationships identified with these statistical procedures were key to developing hypothetical models tested through a Generalised Linear Model method, as described below.

4.1.1. Statistical Testing

Chi-Squared Tests

The dataset used in this analysis contained a considerable number of categorical variables suitable for Pearson's chi-squared (χ^2) analysis (Fisher, 1922; Pearson, 1990). The chi-squared test compares the observed distribution of a categorical variable (with two or more levels) in a contingency table, against the expected frequency if the difference between its levels/categories were due to chance i.e., tests the null hypothesis (H_0) that there is no relationship between two categorical variables. It is accepted statistical practice to reject H_0 if the probability of a chance result is more than 5%, i.e., the *p-value* is greater than 0.05. However, as the χ^2 tends to yield significant results with large samples (Field et al., 2012), the higher significance level of 0.01 is used throughout this thesis. Finally, it should be noted that in frequentist statistics, rejecting H_0 does not prove H_1, but rather it lends support to its claim.

Two assumptions must be met for the χ^2 test to be valid. The first concerns the independence of the observations. The test assumes that each individual observation (i.e., each case recorded) contributes to only one cell in the contingency table (each observation is either Fraud or CM, Male or Female etc). As it will become clear in the chapters to come, due to repeat victimisation, some observations in the data were not independent (estimated at x% of reports by individuals). As such, only unlinked reports were used in the χ^2 analysis. However, the potential for missed links (false negatives) remains a source of uncertainty/error within this

data and a limitation of the analysis. As discussed in section 5 of this methodology, the extent of missed links could not be reliably established.

The second assumption of the χ^2 is that the sampling distribution approximates the χ^2 distribution. In a large sample such this one, this is not usually an issue and it is accepted that where the minimum expected frequency in any contingency table cell is greater than five, the sampling distribution is close enough to the χ^2 distribution (Field et al., 2012). However, where samples are smaller and for 2x2 tables more generally, the χ^2 test tends to result in an overestimation of the relationship i.e. the rejection of a true H_0, known as a *false positive* or a Type I error (Field, 2009, p. 691). One correcting method in 2x2 tables, is to calculate χ^2 using Yate's (1934) correction for continuity, a method used where applicable.[57] As discussed in the next section, statistical significance was determined when the *p-value* was less than .01 and the effect size (or practical significance) determined using the odds ratio, which also indicated the direction of the effect.

For larger contingency tables, following Howell (2013), it was considered acceptable to have up to 20% of expected frequencies below five, given that no expected frequencies were below one (Field et al., 2012, p. 818). While this meant a loss of statistical power – i.e., tests in these circumstances may have failed to detect a genuine effect (a "false negative"), the greater risk of "false positives" was minimised. As with 2x2 tables, χ^2 tests on larger contingency tables were considered statistically significant when the *p-value* was less than .01. The practical significance or effect size of the result was determined based on *Cramér's V*. The direction of the effect was considered drawing on the z-scores of standardised residuals. However, as this becomes more challenging as the size of the contingency table increases, the analysis of large tables was supplemented by GLM effect plots (see section 4.2).

The Wilcoxon rank-sum test

The Wilcoxon (1945) rank-sum test, is considered the non-parametric equivalent of the independent t-test.[58] It was used to test whether the distribution of a non-normal continuous

[57] Alternatively to Yate's correction, a more accurate p-value where the sample is too small can be achieved by using Fisher's exact test (Fisher, 1922). This method works well for 2 x 2 contingency tables and can be used for larger tables. However, it is a computationally intensive process which, in some cases, may never finish. Where this was the case, it was not be feasible to carry out a χ^2 analysis.

[58] This test is very similar to the Wilcoxon-Mann-Whitney rank test (Mann & Whitney, 1947).

outcome variable (e.g. financial loss), was the same across two groups such as males/females (H_0), or significantly different (H_1). This test works on the principle of ranking the data in the continuous/outcome variable from lowest to highest value and then carrying out the statistical analysis to produce the test statistic W, based on these ranks. In this study, the W statistic and associated *p-value* were calculated using the R function *wilcox.test(),*where a p-value greater than 0.05 means there is no significant difference between groups. Given the size of the sample, the distribution of W was assumed to approximate the normal distribution and a continuity correction applied (Field et al., 2012, p. 659). [59]

The Kruskal-Wallis Test

The Kruskal-Wallis test measures associations between more than two groups (e.g., MO group has three levels/groups) and a non-normally distributed ratio data variable (e.g., age or loss). It is therefore the non-parametric equivalent to the parametric ANOVA test. Once again, it is based on ranking the data and then summing the ranks for each of the groups, denoted as R_i. The R values are then used to calculate the test statistic H based on the established formula (Kruskal & Wallis, 1952). This statistic has a chi-squared distribution and test results are thus reported in a similar way to a chi-squared test, with a *p-value* greater than 0.05 denoting that there is no significant difference between groups.

The Spearman Rank Correlation Coefficient

The Spearman rank correlation coefficient r_s (Spearman, 1910) tests for a significant correlation between two numeric interval data variables, where they are not normally distributed (e.g. loss and age variables used in this study). As with the afore-mentioned tests, this test "works by first ranking the data" for each variable to be correlated "and then applying Pearson's equation [or correlation coefficient] to those ranks" (Field et al., 2012, p. 223). Like Pearson's correlation, r_s varies between 0 and +/- 1, where 1 represents a perfect correlation and the +/- whether it is a positive or a negative correlation. The *p-value* of less than 0.05 indicates whether this calculated coefficient is statistically significant.

[59] By default, R uses the normal approximation method with a continuity correction, rather than the Monte Carlo method to calculate p-values where the sample size is greater than 40.

4.1.2. Effect Size & Results Breakdown

Finding statistical significance means it is probably not a chance result but says little about the social relevance or practical size of the difference, or what exactly is driving it, the result breakdown. Even if often lacking in social and criminological research (Bernardi, Chakhaia, & Leopold, 2016; Bushway, Sweeten, & Wilson, 2005), discussion of effect size or the substantive meaning of the statistical relationship is as, if not more important, than a discussion of statistical significance.[60] Doing so avoids what Cohen (1994, p. 997) described as "the ritual of null hypothesis significance testing – mechanical dichotomous decisions around a sacred 0.05 criterion". To avoid this pitfall, an effort has been made to always distinguish between *statistical* and *substantial* significance by reporting on both p-values and effect size. In addition, where possible *post hoc* tests were carried out to provide a breakdown of this effect.

Effect Size

Field et al. state that effect sizes provide an "objective and (usually) standardized measure of the magnitude of an observed [i.e. statistically significant] effect" (2012, p. 57). As it will be seen, 'objective' here does not mean a clear consensus on what constitutes a large or small effect, but rather that, having decided on a standard by which to judge whether an effect is big or small, measures of effect size permit different studies to be compared directly, even where the methods and variables are not exactly the same.

Two types of measures of effect size were used. Firstly, tests of the r-family, based on Pearson's correlation coefficient r, such as Cohen's r, *Phi* and (its extension) *Cramér's V*. Similarly to a correlation, these effect size test statistics vary between 0 and 1, where 1 represents the strongest possible association between the variables. In the case of *Phi*, the test statistic varies between -1 and +1, also indicating the direction of the association. Secondly, odds-ratios (for Chi-squared (χ^2) tests) were provided where applicable.

While there is no scientific consensus on whether an effect size should be classified as small medium or large, and it can depend on subject matter, the most common classification used is that of Cohen (J. Cohen, 1988, 1992). A large effect means a difference between groups which is very apparent to the 'naked eye', a medium effect one which is somewhat apparent and a

[60] In fact, some journals including *Basic and Applied Social Psychology* have banned statistical significance testing on their publications!

small effect one which would not be detectable by simply looking at the two groups. Table 10 summarises the effect size guidelines suggested by Cohen (J. Cohen, 1988) and Rea and Parker (2014), which were used in this thesis.[61]

	Negligible	**Small**	**Medium**	**Large**
*Cohen's r**	0 – < 0.10	0.10 – < 0.30	0.30 – < 0.50	≥ 0.50
*Cohen's h**	0 – < 0.20	0.20 – < 0.50	0.50 – < 0.80	≥ 0.80
*Odds ratio**	0 – < 1.55	1.55 – < 2.8	2.8 – < 5	≥ 5
Cramér*'s V and Phi (Φ)***	0 – < 0.10	0.10 – < 0.20	0.20 – < 0.60	≥ 0.60

Table 10 – Effect size guidelines.

As previously noted, the nature of the data analysed in this thesis meant that in many cases χ^2 tests were used to examine associations between variables. Where the degrees of freedom are the same between multiple χ^2 tests, the value of the test statistic can be compared directly between them, to gauge the relative effect sizes. Between tests with the same degrees of freedom, the higher the value of χ^2, the larger the effect. However, by computing *Cramér's V*, the size of the effect is standardized, so effects may be compared where different degrees of freedom apply and the absolute size of an effect may be gauged.

Alternatively, for 2x2 tables χ^2 comparisons and in some cases of 2 x k tables,[62] the odds ratio provides a more intuitive measure of effect size and the direction of the effect. The odds represent the probability of an event over the probability of its opposite – e.g., being male and reporting CM over being male and not reporting CM. The odds ratio is simply the ratio between the odds of two possible successes – e.g., the odds of being male and reporting CM divided by the odds of being female and reporting CM. As such, the odds ratio between any two pairs of binary categorical variables provides a clear indication of the effect of the relationship between the variables.

[61] *Adapted from Cohen (1988). ** Adapted from Rea and Parker (2014).

[62] As well as for 2 x k contingency tables in situations where the levels of one variable are ordered and therefore there is an obvious reference group (Howell, 2013).

To calculate effect size of a significant relationship identified with the Wilcoxon rank-sum test, the z-score R used to calculate the p-value was converted into and effect size estimate, r, using Rosenthal's (1991, p. 19) equation:

$$r = \frac{\mathrm{z}}{\sqrt{\mathrm{N}}}$$

in which z represents the z-score (calculated by the statistical programme R) and N is the number of total observations on which z is based.

The Kruskal-Wallis Test, post hoc tests can be conducted to determine what is driving any associations found with this test by essentially performing a series of Wilcoxon rank sum tests between pairs of variable levels (Siegel & Castellan, 1988). Unfortunately however, there are no clear ways to determine the effect size of statistically significant differences found with this test in any meaningful way (Field et al., 2012, p. 685).

Results Breakdown

In addition, while effect size measures indicate the size of the effect overall (e.g., an association between RV and age), they do not show whether the effect is driven by specific groups (e.g., a specific age category). As such, further statistical analysis was carried out to provide a more detailed analysis of the results, breaking them down where appropriate.

For 2x2 χ^2 comparisons, the odds ratio is sufficient to understand the direction of the effect, but this becomes meaningless with a larger number of categories. In this case, the standardized residuals (SDs) are considered instead. The residual is the difference (or the error) between what the model predicts (the expected frequency), and the data observed (the observed frequency). These values are standardized by dividing them by the square root of the expected frequency as per the formula below, where *i* represents the rows and *j* the columns in the contingency table:

$$standardized\ residual = \frac{observed_{ij} - expected_{ij}}{\sqrt{model_{ij}}}$$

SDs behave like *z scores* in that if the value lies outside of ±1.96 then it is significant at $p < .05$, if it lies outside ±2.58 then it is significant at $p < 0.01$ and if it lies outside ±3.29 then it is significant at $p < 0.001$ (Field et al., 2012). The plus or minus sign indicates the direction of the relationship of the association (positive or negative). As such, R was used to compute the

standardized residuals as part of the χ^2 output, particularly where contingency tables were larger than 2x2 tables.

However, the estimation of the strength of relationships between variables using χ^2 is a rough one. As noted, it is difficult to interpret where contingency tables are larger than 2x2, even where SDs are used. In addition, tabular analysis cannot estimate the proportion of variance explained by interaction effects between variables (Calder & Sapsford, 1996, p. 266). In contrast, the effect displays produced with the Generalised Linear Models (GLMs) discussed below, provide more sensitive and precise techniques of estimation of effect sizes and interaction effects.

4.2. Generalised Linear Models

The realities of F&CM victimisation are complex and call for the analysis of the combined effect of multiple variables, with multiple levels between them. Where a variable has many levels (e.g., age categories), the direction of effects can be challenging to interpret and communicate. Furthermore, answering the research questions posed in this thesis required going beyond bivariate analysis, to consider multi-variate relationships – where the effect of multiple variables considered together. To address these challenges, the Generalised Linear Modelling (GLM) technique was use, aided by the *R Commander* interface developed by Fox and Weisberg (2011). As the name indicates, this technique is a generalisation of linear regression modelling (which assumes normally distributed and continuous outcome variables), to the modelling of outcome variables which come from the wider exponential family of probability distributions.[63] Given that the dataset used in this study consisted predominantly of non-normally distributed data, including many categorical variables, the GLM technique was particularly useful in its analysis.[64] The most common GLMs used therefore included the modelling of binary variables (e.g. one-time/repeat victim) using a logistic regression model, or the modelling of count data (e.g. number of reports made) using a Poisson model.[65] In what follows, the key features of GLM analysis used are described in more detail, including question

[63] As well as the normal distribution, the exponential family of probabilistic distributions includes the log-normal, exponential, gamma, chi-squared, beta, Bernoulli, and Poisson distributions, among others.

[64] Although GLMs still assume that the errors of the resulting model are normally distributed.

[65] In other words, the Poisson distribution describes the number of events which occur in a fixed time interval.

representation, model assumptions and parameters and determining model and variable significance.

4.2.1. Question Representation

In line with GLM analysis, the first step was to represent research questions/hypothesis in an equation-based format which explicitly identified the relationships being statistically tested. For example, the model **repeat report ~ crime category + age*gender** tested the hypothesis that this combination of explanatory variables (crime category, along with the interaction between victim age and gender) approximately predicted the outcome variable. In broad terms, GLMs work by mapping the effect of one or more explanatory variables onto an outcome variable (Y) via a link function which transforms Y in such a way that makes this mapping possible (see next sub section). In the above example, a logit link function transforms the probability of the outcome (repeat victim/one-time victim), so that it can be mapped to the (linear) effects of crime category and the interaction between age and gender. The resulting statistics produced through a GLM would refer to the relationship between a report by a repeat victim and crime category, after the interaction between victim age and gender is taken into account (in other words, *controlled* for). The interaction represents the combined effect of two variables, for example the statistics for age*gender would refer to the relationship between the interaction factor age*gender and repeat reports, after crime category is controlled for. As it will be seen below, this allows for measuring the significance of both individual variables and the overall model.

4.2.2. Model Assumptions & Parameters

Once question/hypothesis were, the choice of GLM was based on the (assumed) distribution of the outcome variable (Y).[66] Common models used include ordinary least squares (OLS) regression (if Y is continuous and normally distributed), Poisson regression, also known as log-linear regression (if Y is a count), Logistic Regression (if Y is a binary category), proportional-odds regression (if Y is an ordered categorical variable) and multinomial regression (if Y is an unordered multi-categorical variable). The ~ symbol in the GLM equation represents the link

[66] Assumptions regarding the (approximate) distribution of Y are tested once the model is run, through goodness of fit analysis, i.e. by testing how well the model fits the observed data. In addition, residuals should be normally distributed.

function associated with each of these model types: an identity link is used to model a continuous response variable; a log link is used to model a count response variable; and a logit (or *log-odds*) link is used to model a categorical variable (Hutcheson, 2018). Where the outcome variable was crime category, an unordered categorical variable, meaning a Multinomial regression model (MLM) using a logit link would be appropriate.

Using the model parameters obtained with a GLM, the model can be statistically represented as a linear model equation. For example, a simple **Financial Loss ~ Age** model would use an identity link function (if loss were normally distributed) and be statistically represented as:

$$Loss = b_0 + b_1 Age$$

Where β_0 estimates the financial loss when age = 0 and β_1 estimates the change in financial loss for a unit increase in age.

As with χ^2, GLMs assume independence of the observations and therefore only unlinked reports were used in the models. Once again, the potential for missed linked observations having been included in the GLM analysis is acknowledged as a limitation of this analysis.

Contrast Coding

Where the outcome variable is categorical, instead of modelling the variable directly, the logit (or log-odds) of the probability of each of its levels is modelled.[67] As such, modelling categorical variables (ordered and unordered) requires re-coding each level of a variable into "dummy" variables, referred to as contrast coding. Dummy-coding may be done by hand, although when GLM models are computed in via the *R Commander* interface (J. Fox & Weisberg, 2011), R will compute these dummy variables automatically (in the background, without adding them to the dataset) and allows for user-defined "contrasts" to be set.

The most common approach to the contrast coding of the outcome variable is to choose one level of the outcome variable as a reference category, to which each of the remaining levels is compared (a technique known as *treatment* contrast coding). This is relatively straightforward where the outcome variable is a binary category. Where the outcome variable has more than

[67] Logits (or log-odds) represent the mathematical log of the odds ratio, which is the probability of an event, over the probability of a non-event. Logits are useful for statistical analysis because taking the log-odds of a sample of data (i.e., applying a log transformation to the data), results in a normal distribution of the residuals, therefore meeting the assumptions of many statistical methods.

two (unordered) levels, the multinomial logistic regression model (MLM) is used. This is an extension of the logistic regression model for binary data. Here, an arbitrary reference level within the outcome variable is chosen and multiple models are simultaneously computed to compare each level to the reference. An MLM is therefore essentially a series of logistic regressions.

While treatment coding is the most commonly used, other coding techniques can enhance the analysis (Hutcheson, 2011). When there is no obvious reason to choose a level as the reference category for example, it may be useful to carry out other types of contrast coding. In this analysis, Helmert and Orthogonal Polynomial coding were also used. In the former, each level within a categorical variable was compared to the average of the previous levels, a type of coding appropriate for ordered categorical variables as it takes the order of the categories into account. In the latter, each level was compared to several linear and non-linear distributions, to identify trends including linear, quadratic and cubic trends.[68]

4.2.3. Variable and Model Significance

When modelling relationships, it is important to determine both which parameters make a significant contribution towards reducing the deviance of the model (for multivariate models) and whether the overall model is significant. The standard output of a GLM model in R presents the model parameters and significance of each variable (through the ANOVA Type III tests). In addition, the overall significance of the model is also calculated (with the ANOVA Type II tests). Whether or not the overall model is significant is established by testing whether the deviance explained by the model is significantly greater than the null model, using a χ^2 test. As such, despite electing the type of model depending on the outcome variable, GLMs are conceptually very similar, as is their output, making this a coherent analytical framework to compare models which include different types of data.

Variable significance

As with simple OLS regression models, the relative contribution (or effect size) of each variable is expressed through the relative size and direction (positive or negative) or their respective β coefficient values. Along with the β values, the standard GLM output also provides

[68] This should only be used where the categories within the explanatory variable can be reasonably assumed to be equally spaced e.g. the variable "quarter" derived from reported date in this data (Hutcheson, 2011).

a measure of the statistical significance of each variable with respect to Y. This significance is expressed, depending on the type of GLM chosen to match the characteristics of the outcome variable, in terms of z-scores, t scores and F statistic, along with respective *p-values*. For categorical outcome variables in particular, the statistical significance of each category to the prediction of the response variable is estimated using the z-distribution. As such, in logit models of categorical outcome variables, the β coefficients are not presented as probabilities but as the log-odds of probability and are therefore not immediately interpretable. As such, to aid interpretation, the marginal effects or residual deviance is also provided. Furthermore, the effect size (or substantial significance) of each variable can be clearly and intuitively visualised through effect plots, a key strength of the GLM approach.

Graphical interpretation of effect size

To aid interpretation and communication of results, GLMs are interpreted through graphs (effect plots) produced with a package developed by John Fox (2003) for the statistical programming language R, based on his earlier methodology (Fox, 1987). Complex models, including both ordered and unordered categorical variables, categorical variables with multiple levels or main effects and interactions, can be more easily visualised and interpreted (J. Fox, 2003). GLM effect plots on their own allow for the direction, size and significance of the relationships being modelled, to be visually inferred (Hutcheson, 2018).

While the standard statistical output is provided in log-odds, effect plots show the probability of the outcome variable over the range of each explanatory variable in the model, making the relationships in the data easier to comprehend. In addition, unlike the standard statistical output, the effect displays show the higher-order effects only (those that should be interpreted) and absorb their lower-order relatives (J. Fox, 2003). The meaning graphed relationships which would have been difficult to grasp from coefficients alone (particularly for a non-statistical audience) can thus be visualised. This feature makes this type of analysis particularly useful for this study, as it models several categorical outcome variables. Effect displays were thus used both as an analytical tool (to identify relationships) and to communicate research results.

Overall model significance

The statistical significance and effect size of the overall model (i.e., the combination of all variables in the model) is assessed based on deviance across all GLM models. The deviance is simply a measure of the difference between the values predicted by the model and the actual

values observed. This may be expressed as follows (where d represents the difference between predicted and observed values, or the residual, for each observation):

$$Model\ Deviance = \sum_{i=1}^{n} d_i^2$$

If the model provides a good prediction of the response variable, the deviance will be relatively small. As such, deviance is a measure of the goodness of fit of the model. The goodness of fit of the model can be determined by comparing the deviance of nested models. In other words, the deviance of the model which includes the explanatory variable is compared to the deviance of a model in which that variable is not included. In the previous example of the model **Financial Loss ~ Age**, this goodness of fit measure would compare the deviance of the proposed model $Loss = b_0 + b_1 Age$, to the deviance of the model: $Loss = b_0$, and determine whether the 'effect' of the proposed model was to increase or decrease model deviance. The standard R output for GLMs provides the deviance of the proposed model (Residual Deviance) and the deviance of the nested model (Null Deviance). In addition, the significance of the difference between the two will be provided by asking R for the Analysis of Deviance table (ANOVA Type II), which tests for significance using chi-square. The overall model-fits are thus represented in the form of deviance and are tested for significance using chi-square. In the analysis that follows, analysis of deviance tables (ANOVA Type II) were thus produced to test the significance of each model.

5. Linking Repeat Reports

By applying a within-dataset linkage method, a new *victim index* variable was created to identify individuals and added to the reported crimes dataset. By "merging" or aggregating data on this index, it was possible to analyse individual victims (rather than reports) and compare repeat and one-time victims, in order to answer RQs5-9. The linkage method used followed three key stages (Christen 2012). Stage one (*pre-linkage*) included choosing the variables best suited to perform the linkage, as well as cleaning, parsing and standardising the data as required for the next stages. Stage two (*linkage*) included developing the method for linking the incidents per se, by identifying which reported incidents may belong to the same victim, known as *matching*. Here, a combination of deterministic, score-based and probabilistic matching was used (Harron, Goldstein, & Dibben, 2015). The final *post-linkage* stage involved an examination of the matching process through clerical review, the estimation of linkage error rates and an analysis of the resulting linked dataset of repeat victims. Throughout, the functionality provided by the R-Statistics *'RecordLinkage'* package (Borg & Sariyar, 2020; Sariyar & Borg, 2010) was used.[69]

5.1. Pre-Linkage

5.1.1. Choosing and Parsing Matching Variables

The pre-linkage stage included choosing the *matching* or *identifier variables* which individually or in combination allowed the author to ascertain whether records belonged to the same victim. Three factors were considered including variable completeness, distinguishing power (or uniqueness) and validity. Completeness was calculated as 100 minus the percentage of missing data in each variable. *Distinguishing power* was based on the percentage of unique observations within each variable (e.g., gender has less levels and therefore considerably less distinguishing power than dob). Finally, variable validity was determined based on the consistency with which it was judged to have been recorded. This in turn was based on whether there was form-validation on input into the AF database (score 75), discrete multiple-choice

[69] The linkage method is provided in full through R markdown in Annex IV.

categories (score 25), or no validation at all such as with free-text entries (score 0).[70] An average quality score was then calculated for each variable (as exemplified in Table 11). Based on final quality scores, victim address, postcode, name, age and dob were identified as the most suitable variables for linkage.

Identifier	% Complete	% Unique	Validity	Quality Score
address	100.00	97.84	75	90.95
postcode	100.00	83.76	75	86.25
full name	100.00	91.03	0	63.68
age	82.00	66.79	25	57.93
dob	80.56	64.56	25	56.71

Table 11 – Top quality identifiers for linkage.

5.1.2. Creating match-keys

Exact matching on the above variables would only identify matches where these variables were complete and recorded without error. Given that records would be unlikely to agree on these identifiers by chance (Grannis, Overhage, & McDonald, 2002), the result would be a high level of confidence on the matches found (few false-positives), but a high level or missed-matches (or false-negatives). The performance of deterministic matching based on multiple match-keys sought to reduce false-negatives by allowing for some missing data or small errors in the matching variables (Grannis et al., 2002). Match-keys were created by slicing and/or concatenating together identifier variables into new match-keys. Table 12 summarises match-keys used, their quality score and the inconsistencies each was designed to address.[71]

[70] Form validation refers to automated content checks on form fields so that the input is only accepted if it conforms to a valid format: e.g. a valid address or date.

[71] The linkage quality score for each match-key was calculated in the same way as the quality score for individual linking variables above: the average between completeness, uniqueness and validity. Completeness and uniqueness were calculated exactly as before. Given that each match-key resulted from a (partial) concatenation of other variables, an average validity score had to be calculated for each match-key, before the final quality score could be computed.

	Match-Key	Score	Inconsistencies addressed
1	Full Name, Dob, Address	77.19	None - exact agreement
2	Forename, Surname, DoB, Sex, Postcode	73.88	Full Name discrepancy
3	Forename initial, Surname initial, DoB, Sex, Postcode District	73.72	Name / postcode discrepancies
4	Forename tri-gram, Surname tri-gram, DoB, Sex, Postcode Area	73.78	Name discrepancies / movers in area
5	Forename initial, DoB, Sex, Postcode	75.81	Surname discrepancy
6	Surname initial, DoB, Sex, Postcode	75.78	Forename discrepancy
7	Forename, Surname, Age, Sex, Postcode Area	73.77	Dob discrepancy / movers in area
8	Forename, Surname, Sex, Postcode	73.78	DoB missing / incorrect
9	Forename, Surname, DoB, Sex	69.69	Movers out of area
10	Forename, Surname, DoB, Postcode	73.87	Sex missing / incorrect

Table 12 – Exact/deterministic linkage match-keys.

5.2. Linkage

5.2.1. Exact Matching

Having determined what match-keys to use, exact matching was performed using the *compare.dedup* function from the *RecordLinkage* R package (Borg & Sariyar, 2020). Firstly, on the combination of full name, address and dob, resulting in 380 links. Subsequently, exact matching was performed on each match-key, resulting in the number of matches detailed in Table 13. Matches from each iteration were combined and de-duplicated to arrive at a final set of 609 unique matched pairs.

	Match-Key	Matches
1	Full Name, Dob, Address	380
2	Forename, Surname, DoB, Sex, Postcode	427
3	Forename initial , Surname initial, DoB, Sex, Postcode District	499
4	Forename tri-gram, Surname tri-gram, DoB, Sex, Postcode Area	476
5	Forename initial, DoB, Sex, Postcode	502
6	Surname initial, DoB, Sex, Postcode	514
7	Forename, Surname, Age, Sex, Postcode Area	469
8	Forename, Surname, Sex, Postcode	476
9	Forename, Surname, DoB, Sex	438
10	Forename, Surname, DoB, Postcode	433
	Total combined matches	609

Table 13 – Number of exact/deterministic matches per match-key used.

However, exact matching only allowed for very specific errors and therefore relying solely on this approach had the potential to result in a large number of missed matches (or false negatives). As such, a score-based probabilistic matching method was used.

5.2.2. Score-Based Matching

Score-based matching refers to matching records based on a threshold *matching score* being reached, which is designed to consider both partial agreement between matching variables, as well as the relative importance of each variable for the linkage. Agreement scores were calculated by the *compare.dedup* function of the RecordLinkage R package, which calculates a comparison pattern (or vector) for each pair of matched records. In the example below (Table 14), a score of zero represents no agreement between records, one represents exact agreement and a number between zero and one represents partial agreement on a specific variable. The reported crimes index 7425 and 7450 are compared, resulting in the comparison vector $\gamma = (0.7, 0.08, 1, 1, 1, 0, 1, 0, 1)$. If either of the records being compared contained a missing value for

a given variable, this would result in a score of zero.[72] In simple score-based matching, a score of zero would also have been assigned if the variables disagreed in any way. Here, the approach was refined by utilising functionality to perform phonetic and string comparisons.[73]

ID1	ID2	DOB	Email	Forename	Gender	Postal Area	Surname	Mobile	Name	YOB
7425	7450	0.7	0.08	1	1	1	0	1	0	1

Table 14 – Example of score-based match comparison.

RecordLinkage's phonetic function mapped victim names into new strings representing their pronunciation, so that similar sounds were coded with the same phonetic code, using the commonly used English-language *soundex* algorithm.[74] The algorithm attributed a score of zero to names where the corresponding phonetic codes did not match and a score of one where the names matched phonetically (even where they did not alphabetically). In addition, *RecordLinkage* also allowed for the use of string comparators, to identify partial agreement between strings, through the edit distance algorithm developed by Levenshtein (1966).[75] This algorithm measures the 'distance' between strings, meaning the number of deletions, insertions or substitutions required to transform one of the strings being compared into the other. Using phonetic and string comparators reduced the number of false negatives (missed links) as it took into account a wider range of recording and spelling errors.

Furthermore, *blocking* variables were also defined to reduce the number of comparisons required and make the matching process more efficient to run given the constraints of time and computational power (Sariyar & Borg, 2010). Blocking reduces computed comparisons to

[72] This is the default behaviour of the *RecordLinkage* package (Sariyar and Borg 2010). Although it may have been desirable to score such cases (possibly a score of 0.5 to denote the possibility of match), this would have required further pre-processing of the data which was not possible given the time and resource constraints when carrying out the linkage.

[73] A 'string' is a common data type recognised by multiple computer languages which consists of alfa-numeric characters. Assigning data types to each variable (e.g. string or integer) defines the kind of operations which can be performed on that variable by the software. In this case, the application of the string comparator function.

[74] This algorithm was developed by Robert C. Russell and Margaret King Odell (Odell, 1956) and its implementation draws from the US census. As further discussed in the limitations section, this will thus likely result in better matching for individuals with English names.

[75] The function *levenshteinSim* was used. The alternative string comparator 'Jaro distance', also available within *RecordLinkage*, was considered but testing revealed that the edit distance was better at identifying different spellings of the same name.

those pairs of matched cases which meet defined *blocking* criteria. As such, instead of calculating matching vectors (and later scores) for all possible pairs, these are computed only for pairs which agreed on the blocking criteria. Multiple iterations of the probabilistic linkage method progressively relaxed the blocking criteria, until it was determined that the method was resulting in a sufficient number of matches. Table 15 illustrates the effect of the iterative matching process on the number of resulting matched pairs.

	Matching variables*			**Matched pairs**
	Blocking variables	**Phonetic comparators**	**String comparators**	
1	YOB Postcode First Name	Last Name	Address Line 1	499
2	YOB Postcode First Name Trigram	Last Name	Address Line 1 Mobile Email	523
3	Postcode Bigram First Name Trigram	Last Name	Address Line 1 DOB Mobile Email	106,257

Table 15 – Iterations of score-based matching.

***Variable names: DOB = Data of Birth; YOB = Year of Birth; First Name Trigram = First 3 Letters of First Name; Postcode Bigram = First 2 Letters of Postcode.**

Finally, rather than simply adding up agreement scores, probability methods were used to determine the weight that each comparison element should be given, to represent the different likelihoods that records may have matched by chance, based on the variables being compared. The next section describes how the final matching score was computed to identify the 'true' links among all matched pairs.

5.2.3. Probabilistic Matching

The probabilistic approach links records according to probabilistic rules, by assigning weights to each comparison pair corresponding to the probability that the match is true, given the agreement of the identifiers. Score-based probabilistic matching provided a consistent method for matching records using a range of identifiers assuming typographical errors (Winkler, 2015), extending the number of matches identified. As previously demonstrated, variables

differed in terms of their quality for matching. To take this into account, Newcombe and colleagues (1959) introduced a method based on odds ratios to estimate the weight that each comparator should have in calculating the final matching score of each pair of records being compared. This idea was formalised mathematically by Fellegi and Sunter (1969), through a method based on traditional probability theory. Following this approach, rather than simply calculating matching scores for each variable and the total matching score for each pair of crime records, weighted scores (also called matching weights) were computed based on probabilistic matching. This provided a systematic approach to establishing the relative importance of each variable being compared.

5.3. Post-Linkage

5.3.1. Threshold Setting

Having probabilistically determined matching scores for each pair of records, threshold setting to determine true matches was done through manual review. In order to minimise error, the data were inspected, and minimum and maximum thresholds set, defining a range of "possible links" requiring further manual review. Firstly, record pairs were sorted in descending order of matching score. Then, two thresholds (minimum and maximum) were set dividing the dataset of matched pairs into three regions. This was supported by the function *getPairs* of the *RecordLinkage* R package, which shows matched record pairs along with their weight. These weights we distributed as illustrated below (Table 16, Figure 5).

Min.	1st Qu.	Median	Mean	3rd Qu.	Max.
-13.13	-13.13	-13.13	-11.19	-10.24	37.42

Table 16 – Distribution of Probabilistic Matching Weights.

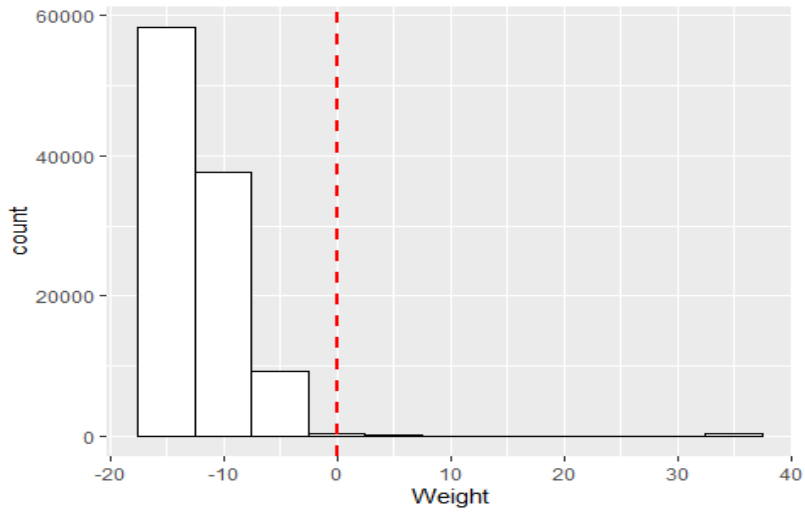

Figure 5 - Distribution of Probabilistic Matching Weights.

The manual review was conducted by organising the matched pairs from low to high matching scores and conducting visual comparisons of full name, address and date of birth. To determine the maximum threshold, the top of the sorted list of pairs (in descending order) was inspected for the highest score that did not match. When non-matches began to appear frequently, the upper threshold was fixed. Likewise, continuing to look through the list, the minimum threshold was fixed when matches became moderately rare. Following this procedure, a minimum threshold of 3.56 and a maximum threshold of 17 were found and each of the matched pairs classified as "non-links" (n = 105,604), "links" (n = 535) or "possible links" (n = 118) using the *emClassify* function. Classified pairs of matches in the bottom region (below the minimum threshold) were automatically rejected as false matches; matched pairs in the top region (above the maximum threshold) were automatically accepted as representing true matches; the middle region was then manually reviewed to determine whether each pair is a true or false match.[76] Ultimately however, probabilistic matching only added a further 18 matches to the total of linked pairs, resulting in a final 627 links between matched incidents (609 had been found through exact and rule-based matching).

[76] To do this, all records pairs which constituted "possible links" were extracted and manually reviewed to determine whether they should be classed as links or non-links. In addition, cases were manually reviewed where variables which were expected to match did not (e.g. where the variable "gender" did not agree between two linked records). These included matched cases with the following inconsistent variables: police force (2 matches), victim type (41 matches, 37 due to missing values), ethnicity (168 matches, 165 due to missing values) and gender (29 matches, 15 due to missing values). Missing values were completed through imputation and incorrect values were re-coded as appropriate as detailed in section 3.6.2 of Annex IV.

5.3.2. Linkage Error

Linkage error can occur, resulting in false links (false-positives) or missed links (false-negatives). In addition, where linkage error is not random, it can result in biased estimates. This section documents the metrics used to determine linkage error in this study. The implications of the linkage error for analysis are further discussed below. Among the commonly used linkage quality metrics are *precision* and *recall* (or sensitivity) (Christen & Goiser, 2007). Precision represents the proportion of classified matches that are true matches and is calculated as follows:

$$Precision = \frac{True\ Positives\ (TP)}{True\ Positives\ (TP) + False\ Positive\ (FP)}$$

Recall on the other hand, represents the proportion of true matches that have been classified correctly and is calculated as follows:

$$Recall = \frac{True\ Positives\ (TP)}{True\ Positives\ (TP) + False\ Negatives\ (FN)}$$

Linkage error can thus be estimated via clerical review of a random sample of matches (Newgard, 2006). By manually reviewing pairs it is possible to determine which they should have been classed as links or non-links. By comparing the reviewed link status to the link status obtained via the linkage methodology, precision and recall can be calculated. Assuming that the sample of comparison matched pairs is random, it can reasonably be assumed that the error measures are representative of the overall dataset (Harron et al., 2015). As such, a sample of 100 pairs of matches and non-matches were extracted for clerical review and both the precision and recall rates were calculated at 100%. As the sample for review was taken from the set of comparison pairs on which exact and/or probabilistic matching was performed, this was not truly random as these were limited to the pairs that fulfilled the blocking criteria (n = 2730). Without blocking however, there were over 70 million possible comparison pairs which would result in a random sample which included very few matches.[77]

[77] Calculated as $n\,(n-1)/2$, where n represents the number of incidents to be matched. This results in $11841\ (11841-1)/2 = 70{,}098{,}720$ possible comparison pairs.

5.4. Limitations

Based on the available variables, it was only possible to attempt linkage for reports made by individuals for whom a combination of the name, DOB and address/postcode could be relied upon to form the basis of the linkage. These could then be supplemented with less accurate and/or differentiating variables such as mobile/email and gender respectively. In relation to other victim types such as businesses however, DOB would be meaningless and no other unique reference such as company/charity number was provided. Furthermore, it was considered that there was too much inconsistency in relation to how name/address/postcode could be recorded given the observed variability in what and how business name was recorded, as well as the fact businesses can operate from multiple locations. As such, the repeat victim analysis was limited to reports from individual victims.

Furthermore, the estimation of RV found among F&CM reports to the police would likely be conservative, even if the data was 100% accurate and complete. The reason behind this is twofold. Firstly, the approach taken to the linkage was one of minimising false positives. This was reflected in the choice of considerably high minimum and maximum thresholds used to classify matches as 'true links' and is reflected in the results of the quality measures applied to the linkage. Secondly, the sample of data on which the linkage was performed was limited to two years and thus the linkage will only capture individual victims who reported repeatedly within this timeframe.

Finally, the limitations regarding the quality of AF data and the nature of PRC discussed in detail in Annex VII, also impacted on the quality of this linkage. Linkage accuracy was limited by recording errors and the completeness of the crime records. In particular, this linkage methodology required complete values for name, date of birth and postcode. The percentage of recorded incidents for which all of these variables were available was approximately 85% of the total number of records that could have been considered for matching. In addition, as discussed in detail in Annex VII, given that the dataset comprises only cases which victims reported to the police, the analysis that follows from this linkage methodology cannot be generalised to all repeat victims.

Despite these limitations, this method has not, to the best knowledge of the author, been applied to this particular use-case and has therefore enabled new insights into the characteristics of victims of fraud and CM who repeatedly report to the police. In addition, it highlights the ways

in which simple improvements in the recording of these crime types would enable a greater insight into the characteristics of victims more generally and repeat victims in particular.

6. Thematic Analysis of Incident Descriptions

Thematic analysis (TA) was used to analyse free-text incident descriptions within a sub-sample of crime reports (n = 332). TA describes a systematic method for "identifying, analysing and reporting patterns (or themes) found in qualitative data" (Braun & Clarke, 2006, p. 79). These themes relate to the overarching ideas, concepts or issues which describe the content of unstructured data. As such, TA was ideal to analyse incident descriptions and answer several research questions in this thesis. As summarised in Table 17, this included research question (RQ) 3(ii), which aimed to achieve an understanding of the wider impacts of F&CM victimisation. Similarly, RQ4(iv) and RQ9 aimed to better understand the *Modus Operandi* of offenders. Finally, RQ10 examined how the concept of *vulnerability* was constructed within reports. Through TA, the answers to these questions were allowed to emerge from the data (albeit through the author's interpretative gaze), going beyond pre-define categories and concepts.

	Research Question
RQ3(ii)	What impacts beyond direct losses can be identified from crime reports?
RQ4(iv)	What other the key MO features can be identified?
RQ9	What were the mechanisms through which repeat victimisation happened?
RQ10	How was vulnerability constructed within reports of F&CM?

Table 17 – Research Questions asnwered through TA.

The above questions were approached in two distinct ways. Following (Reicher, 2000), the first three (RQ3(ii), RQ4(iv) and RQ9) had an "experiential", while the last question (RQ10) had a "critical" focus. By experiential it is meant that the analysis focused on capturing the detail of victim impact and criminal MOs, as they were expressed in the data. As such, the "voice" within the data and its meaning-making were prioritised and accepted, resulting in the generation of descriptive thematic codes. In this way, the qualitative analysis supplements the insights gathered quantitatively. In contrast, in answering RQ10 "an interrogative stance [was adopted] towards the meanings or experiences expressed in the data (...) [seeking] to understand the factors influencing, and the effects of, the particular meanings or representations [of vulnerability] expressed" (Braun & Clarke, 2013, p. 21). The focus in answering this question was on how the language used shaped and created, rather than merely reflected reality (Weedon, 1987). In other words, capturing the representation and construction of concept of

"vulnerability" in the data – through explicit or implicit meaning, drawing on the author's own interpretative analysis.

One important limitation of this analysis relates to the reliance on a relatively small sub-sample of incident descriptions, as further examined and explored below. In addition, following from the discussion in chapter one, section 3.1, the incident descriptions in this sample captured the "voice" of several populations. The voice may be that of the Action Fraud call handler, where the report was made over the phone by the victim, or someone else on behalf of the victim. Alternatively, it may be that of the victim or a friend/family member themselves, where the report was made online, through the AF website. Finally, it may also be that of a law enforcement agent, in the less frequent event of an officer taking a crime report and submitting it through the online tool to AF on behalf of the victim. As such, there were varying levels of hermeneutics involved and the themes identified cannot be clearly attributed to any one of these populations. Nonetheless, these themes represent key understandings of 'victimisation' and 'vulnerability', as shaped by the current recording practices.

TA was conducted in six stages, adapted from Braun and Clarke (2006, 2012, 2013): 1) sub-sampling; 2) reading and familiarisation; 3) systematic coding; 4) identification of themes; 5) review of themes and production of a thematic map; and finally, 6) defining and reporting of themes. While qualitative analysis is an interpretative endeavour, these stages ensured that the analysis was carried out methodically and thus "in a way that is theoretically and methodologically sound" (Braun & Clarke, 2006, p. 78). The analytical steps taken in each of the TA stages are further explained below. Where applicable, these were aided by the computer assisted qualitative analysis software NVivo and coding summaries including in Annex VI. The next sub-sections detail these stages in more detail.

6.1. Sub-Sampling

The first TA stage was sub-sampling, as due to data access restrictions, it was not possible to code and analyse all reports by individual victims (n = 11,841). As previously mentioned, data cleaning and standardisation took place during the preceding quantitative part of the analysis, including the anonymisation of incident descriptions. Due to the access restrictions, the researcher had to manually verify that personal information was removed from each incident description, before they could be extracted for further analysis at the university. As such, instead of seeking to anonymise the full sample, a sub-sample of cases was therefore selected

for TA, using purposive and simple random selection techniques, within the time available for this task, in such a way as to best answer the research questions. Reports by repeat victims were needed to capture the repeat victimisation mechanisms and constructions of "vulnerability". Furthermore, it was considered important to review the reports of those with a higher incidence of repeat reporting, as this may constitute an indicator of greater vulnerability to victimisation. As such, all reports made by victims who reported three or more incidents were purposively selected for TA (58 victims, 208 incidents). At the same time, a random selection of 22 repeat victims who reported two incidents (44 incidents), totalling 252 incidents reported by 80 repeat victims were also selected for TA. In order to capitalise on the TA reading and familiarisation stage (see below), it was decided that the same sample of one-time victims should be used to answer all qualitative research questions. As such, an equal number of reports from one-time victims (n = 80) were also randomly selected for TA to ensure a balanced sample of repeat and one-time victims. Altogether, a sub-sample of 160 victims who reported 332 incidents between them were thus selected for TA. While this is a relatively small sub-sample of the full sample (3%), the use of a combination of random and purposive sampling was intended to maximise the utility of this sample. The anonymised TA sample was then transferred to the University and uploaded to the qualitative analysis software NVivo as a dataset. All incident descriptions were made available for open coding, each report classed as an individual case and all other variables classed as case attributes (more on these designations below).

6.2. Reading and Familiarisation

The first stage of the analysis involved reading and re-reading the text of the incident descriptions sampled for TA. Each description was read several times and notes made on key concepts and ideas. The aim of this reading stage was to begin the process of making sense of the data, thereby uncovering its meanings. This required asking 'critical' questions of the data throughout the reading (Braun and Clarke, 2013) and summarised in Table 18.

	Active Reading Questions
RQ3(ii)	What aspects victim impacts are salient within reports? Are these surprising/unexpected in any way?
RQ4(iii)	What aspects of the MO are salient within each crime category? Are these surprising/unexpected in any way?
RQ9	Is there a nexus between the different reports by the same victim?

	How may the salient characteristics of this nexus be described?
RQ10	What are the different ways in which victim vulnerability is expressed or implied? Why might the victim's experience and their vulnerability be described in particular ways? What assumptions (if any) are made in these descriptions? In what ways do constructions of victimhood and vulnerability mirror the theory/policy understandings of the victim/vulnerability? How do they differ?

Table 18 – Critical questions considered during stage two of TA.

Data familiarisation was carried out on paper and was the first step in making sense of the data. However, the notes produced were a product of the researcher's subject matter knowledge, subjective experiences and beliefs, rather than the result of systematic engagement with the data. Nonetheless, they were considered a resource as they allowed the researcher to be reflexive and consider whether they could be validated or negated by the codes and themes identified through the systematic coding that followed, aided by NVivo.

6.3. Systematic Coding

The systematic coding of the entire dataset that followed used the computer assisted qualitative data analysis software NVivo. This stage consisted of systematically "identifying aspects of the data that relate[d] to [the] research questions" (Braun & Clarke, 2013, p. 205). A code is a label, a short phrase or word which "captures the essence" of what the data contains (*Ibid.*). Using NVivo, each sentence within each incident description was coded first in relation to each of the questions identified above. The aim was that when the entirety of the sample was coded, each code was distinct but at the same time, the codes in their entirety were comprehensive so as "to capture both the patterning and the diversity within the data" (Braun & Clarke, 2013, p. 211). Were the data to be lost forever, the full list of codes (Annex VI) would provide a complete picture of their content. As such, while coding summary tables are used to communicate the analytical process, the relevance of the themes and codes is determined by their definition and explanatory value, rather than their number.

While systematic coding is itself an interpretative analytical exercise, codes can be broadly described as "data-derived" or "researcher-derived" (Braun & Clarke, 2013, p. 206), although they can overlap. Data-derived codes, also referred to in the literature as open coding (e.g. Vaismoradi, Turunen, & Bondas, 2013), are semantic – they are directly derived from the explicit meaning of the words/phrases found in the data. As such, they reflect the participant's

language and concepts found in the data. In contrast, researcher-derived codes reflect what the researcher identifies as implicit meanings within the data (albeit through their textual materiality), drawing on the theoretical framework which informs the research (also referred to as axial coding). Given the nature of the research questions, most codes relevant to RQ3(ii), RQ4(iv) and RQ9 were data-derived, while most codes related to RQ10 were researcher-derived. Finally, the data coded for each code were collated together using NVivo's functionality.

6.4. Identifying Themes

Themes were then identified across the previously established codes and underlying data, with the aim of highlighting salient and broader patterns, relevant to the RQs. Following Braun and Clarke (2006, 2012, 2013), this was done by reviewing the codes and the data collated therein and grouping them into themes by identifying similarities and overlaps, as well as overarching "concepts, topics or issues which several codes relate to" (Braun & Clarke, 2013, p. 225). As such, while the codes capture one idea, a theme is typically a "central organising concept" (Braun & Clarke, 2013, p. 223) which contains several different codes. At the same time, it is possible for a code to become a theme where it is large and complex enough (Charmaz, 2006) and for a theme to include sub-themes. Themes became salient due the frequency with which they occurred. This stems from the assumption that recurring ideas "capture something (...) socially meaningful" (Braun & Clarke, 2013, p. 223). Additionally, themes were also identified where they were meaningful for answering the RQs (Buetow, 2010). Finally, some aspects stood out despite not being considered an organising concept if they added meaning or explanatory power to the data. For example, age was salient as a feature of this dataset but themes around how age led to different experiences of victimisation provided greater explanatory power. This highlights how the identification of themes is an interpretative endeavour in TA, which emerges from the interplay between the author's theoretical underpinnings and their interpretation of the data. At the same time, by conducting this analysis systematically and reflexively, the result is an internally coherent analysis which allows for a more nuanced understanding of the "reality" which crime reports capture. At the end of this stage, a list of "candidate themes" was generated for review in the stage that followed, to ensure internal coherence.

6.5. Thematic Mapping & Review

NVivo's 'nodes' were used to visualise the thematic map of the candidate themes, by considering they related to each other and the underlying data. This allowed the author to consider the relationship between themes – which "can be hierarchical or non-hierarchical (lateral)" (Braun & Clarke, 2013, p. 230). It also helped identify themes and sub-themes, which was a useful resource in reviewing the themes to ensure the analytical insights being produced were internally coherent. At this stage, the full sample of data was re-read in light of the candidate themes, to select those which best captured the meaning of the dataset in relation to the research questions. This required reflection on how each theme related to the others and how it contributed to the overall analytical narrative. This was an iterative process which involved several re-reads of the data in light of the candidate themes, until the researcher was satisfied with the 'fit' between the themes and the data overall. At the end of this stage, a set of distinct and coherent themes had been identified, along with a clear sense of how these fit together to answer the RQs.

6.6. Defining and Reporting Themes

The final stage of the qualitative analysis involved naming and defining themes and finally the write up of analysis and discussion. Theme names were chosen to communicate creatively and succinctly their contribution towards the full explanatory narrative which resulted from the analysis. Each theme was defined, setting out its boundaries, as reported in subsequent chapters and summarised in Annex VI. Furthermore, themes and codes are visually illustrated through tree maps and thematic diagrams. Table 19 summarises themes and codes per research question (i.e. the number phrases coded), as well as how many times crime reports were coded for each theme. Throughout this thesis, NVivo's data query functionality was used in addition to the count of phrases coded, to identify the number of crime reports coded to each question, theme and sub-theme.

	Overall Themes	*Sub-themes*	*Phrases Coded*	*Crime Reports Coded*
RQ3(ii)	4	NA	196	184
RQ4(iv)	2	6	632	435
RQ9	3	NA	185	167
RQ10	3	8	701	543
Cumulative Total	12	14	1714	1329

Table 19 – Overall coding summary.

Finally, the analysis was written up by identifying extracts to best illustrate each theme and bringing these themes together in the form of an overall explanatory narrative. This narrative interprets the significance of each theme in answering the research question: it tells "the reader *what* is interesting about the data – and particular data extracts – and *why* that is" (Braun & Clarke, 2013, p. 253). Once again, this was an iterative process of going between the name of the themes, their definition, illustrative content and narrative role. Furthermore, this included reflecting on existing literature and theoretical concepts, bringing into focus how insights related to other scholarly works and adding depth to the analysis. The overall themes which emerged in relation to each RQ are summarised and explored in the following chapters.

7. Legal & Ethical Considerations

Following Israel and Hay (2012) and with reference to the ESRC's Framework for Research Ethics (2015), four key ethical principles were considered throughout the course of this research including the non-maleficence (or the 'no harm') principle, confidentiality, the principle of informed consent and research integrity. The research project was also subject to Swansea University's ethical approval procedures and approved in November 2016.[78] Furthermore, a Memorandum of Understanding was established with SW-ROCU for the sharing of the data. This section discusses the implementation of these principles and mechanisms.

7.1. Non-maleficence and Confidentiality

Following the principle of non-maleficence, this research could not have proceeded ethically, if it was likely to result in harm to participants (i.e., F&CM victims). The dataset used in this study contained sensitive, personal identifiable information (PII) and business sensitive data which could result in harm to participants if disclosed. If identified, victims may be targeted further, and it could lead to reputational damage for businesses. As such, the most significant risk to participants in this study was loss of anonymity, by having personal details made public either from the dataset itself, via "statistical disclosure" or disclosure through the excerpts used to illustrate the qualitative analysis. As such, the researcher took all possible measures to minimise risk of disclosure before, during and after analysis. As this project involved access to PII, agreed terms for sharing of participant information were required to manage risk of harm both during and after data collection (Israel & Hay, 2012), these were formalised in a Memorandum of Understanding with South Wales Police.

In this study, the first step towards confidentiality was anonymity, i.e., ensuring data could not be traced back to victims. Anonymity is particularly important for criminologists working with administrative datasets such as recorded crime, especially where these data have been linked to other datasets, as the information for each participant becomes more detailed (Willenborg & de Waal, 2012). As noted above, the principle of confidentiality is closely linked to the principle of non-maleficence. To mitigate against the risk of loss of anonymity, the researcher

[78] Notification of approval received on 3 November 2016.

first conducted a robust risk assessment of potential harms arising from data linkages of administrative datasets (Laurie & Stevens, 2014) and considered how to anonymise the dataset, including what units of analysis to use, the size and characteristics of the communities / samples and whether there was any identifiable information in free text fields. As a result of this assessment, it was agreed with the research partners that PII data would be completely removed from the dataset before it was securely transported from police premises to the University. As a result, large sections of the methods used (including data cleaning, validation and linkage) were carried out in the SW-ROCU secure lab, prior to full anonymisation. Consequently, these stages of the research were subject to time constraints and the ability to spend time using SW-ROCU facilities.

Once these stages were concluded, the data was fully anonymised before being transferred to the University. This included the removal of many variables including name, dob, address, contact details and free-text descriptions. Smaller samples of data including incident descriptions used for TA were individually anonymised by the researcher, one-by-one removing all disclosive information. Once anonymised, strict data-security measures for the transfer and storage of the data at the University were adopted. Finally, all outputs were reviewed for disclosive or identifiable information prior to submission. The security measures adopted are discussed further below.

7.2. Security and Data Transfer

Prior to commencement, the research partners sponsored the author to obtain the required level of security clearance, as a condition for data access. Once vetted, the researcher was allowed to visit the SW-ROCU secure computer lab to undertake the necessary work as described above. The anonymised dataset was the transported to the University in a digital format, on an encrypted USB device. After that, the data was stored on the University drive allocated for the author's personal use and, at the request of the ethics committee, accessed via a designated desktop PC in the Postgraduate Research Room at the Law School.

On the university systems, the anonymised data are be covered by the institutions' Information Security Policy which includes password-protection, anti-virus, regular patches to protect against breaches and a response team in the event of a suspected or actual data breach. Furthermore, all data on USB drives and on the University intranet is encrypted at rest. On

completion of this thesis, the anonymised data will be kept on an encrypted drive in a locked cabinet at the University for a period of five years, after which it will be destroyed.

7.3. Informed Consent

Participants should explicitly consent to taking part in research (or in this case consent to their data being used), and that this choice be informed (Israel & Hay, 2012). In other words, the participant freely agrees to take part in full cognisance of the purpose of the research project, the research methods to be employed, what participation involves, where and when it will take place, possible risks involved in participation, the possible outcomes of the research, as well as participants' rights and entitlements – such as the right to withdraw consent.

In the case of research using large administrative datasets such as this study however, obtaining informed consent from each participant was unfeasible. Participant consent was implicit or tacit in so far as the research was conducted in collaboration with law enforcement and aimed to improve crime prevention and better the victim response. Participants would therefore have agreed to the terms and conditions of accessing police services. However, this was not 'informed' as the individuals whose data were used were not individually contacted to provide their consent to their data being used for the specific research projects. It could thus be argued that administrative data should simply not be utilised in research as it compromises individual rights.

On the other hand, rights to freedom and autonomy are under-pinned by other rights and arise in a context of social interdependence. It was considered that, subject to the non-maleficence principle discussed above, it would in fact be unethical to consider that individuals' right to freedom and autonomy (established in Article 1 of the Universal Declaration of Human Rights (UDHR)), should take precedence over the greater good of many, considering that this research aims to improve services for future victims. Additionally, the right to freedom and autonomy is not absolute and it does not necessarily supersede other rights such as the right to security under Articles 3 and 23 of UDHR, the right to family life under Article 16, or the right not to be arbitrarily deprived of their property under Article 17(2). Therefore, while informed consent

was not obtained, the rights of future victims were considered not just an ethical justification but an ethical imperative in favour of using AF data in research.[79]

7.4. Research Integrity

Research integrity must be at the heart of any research endeavour, for without integrity, including sound, transparent and independent methods, research can be of no value for either the furthering of knowledge or policy. As such, research integrity features within the ESRC's *Framework for Research Ethics* (2015) which states that research "should be designed, reviewed and undertaken to ensure recognised standards of integrity are met, and quality and transparency are assured."; and that research should be independent from "any conflicts of interest or partiality should be explicit."

With respect to the former, this research has been conducted with a particular emphasis on design integrity and transparency. This is reflected in the choice of methods and tools. It was a commitment to transparency and replicability that led to the choice of a scripted statistical analysis in "R" and the use of r-markdown to document all steps of statistical programming and coding (see annexes 2 to 5). In addition, alongside a considered reflection on the strengths and weaknesses of the data and the method used, the researcher will seek to deposit the anonymised dataset, with the permission of the research partners, with the UK Data Service.

With regards to research independence, accessing the administrative data to carry out this research, both required and engendered a relationship of trust between the researcher and the police partners. This relationship could influence the research in so far as that the police may be interested in results that can be operationalised or, further still, results which will enable

[79] From a legal perspective, when the sampled AF data was collected by the police, this would have fallen under the 'crime and taxation' exemption under the Data Protection Act 1998 (DPA); this provision means that the police are exempt from the first data protection principle (fair and lawful processing) but must satisfy one of the legitimising factors provided in schedule 2 of the Act. In this regard the police may rely on sch.2(5)(a) that the data processing is necessary for the administration of justice. As such, explicit consent of the data subjects is not required to legitimise the data processing conducted by the police. Likewise, similar exceptions apply in the context of the more recent General Data Protection Regulation (GDPR), which came into force while this research was underway. Furthermore, the processing of the data carried out by the author did not rely on the legal basis of consent, but rather on public interest.

them to make a case for particular reforms or more resources. Maintaining ethical research conduct thus requires the researcher to disclose this potential for influence and to take a reflexive approach as to its impact on the research results. As such, throughout this project, the researcher attempted to develop the research in a direction which could in fact have a positive impact on policy and practice, without losing sight of how police priorities may need to be considered critically. On one hand, ensuring research findings are relevant and applicable to policy and practice, is partly an ethical responsibility towards participants in the context of using administrative data without explicit consent. At the same time, the researcher sought to maintain their independence, demonstrated through the ways in which this thesis is situated within the relevant literature and used appropriate and transparent methods.

8. Strengths & Limitations

This methodology was not without limitations. As discussed throughout this chapter, each of the specific quantitative and qualitative methods used had limitations. However, by using a flexible mixed-methods approach, the author has produced the best possible evidence that was possible using AF data, thus demonstrating its richness and potential for further research. Nonetheless, by far the most considerable limitation of this study relates to the quality of the dataset itself, which is intimately related to the ways in which the data were collected by AF. The quality of AF dataset is discussed throughout this thesis, in relation to the results presented, including how adequate it is to identify (repeat) victimisation patterns. In this respect, the limitations of the data which were identified are in themselves research findings. In addition, a detailed account of an initial quality evaluation is provided in Annex VII.

Despite these limitations however, this methodology enabled the identification of repeat victimisation patterns and led to rich insights with respect how vulnerability is constructed at the reporting stage of the victims' CJS journey. At the same time, in line with the 'scientific method', the robust and transparent methods used contribute to the field and enable falsification. Finally, as noted at the start of this chapter, a mixed-methods approach allowed for the triangulation of findings across the different types of analysis undertaken. In so far as the analysis produced reconciled findings through a variety of methods, this work is methodologically robust and internally coherent.

CHAPTER 4: Recorded Fraud and Computer Misuse

This chapter provides an analysis of the recorded F&CM crime patterns over the reference period and seeks to answer research questions (RQs) one to three and respective sub-questions. RQ1 concerned the significance and volume of F&CM recording and is the focus of section one; RQ2 related to the characteristics of individual victims and is the focus of section two; finally, RQ3 concerned the financial and other impacts of F&CM and is answered in section three. Quantitative and qualitative methods were used both simultaneously and sequentially (Morse, 1991) in this chapter. Simultaneously, methods were selected to answer the research questions to which they were respectively best suited, with limited interaction between them. At the same time, the qualitative insights into the impact of F&CM crimes add depth to the quantitative analysis and thus were sequentially integrated into the overall analysis. Before presenting the results and discussion, the relevant research questions will be re-stated in full, and the methods used in this chapter summarised.

Research Questions

RQ1: What was the volume of reported F&CM in Wales, over the reference period?

i. How did the volume of recorded F&CM vary across victim types?
ii. Was the volume of F&CM recorded in Wales significantly different across forces?
iii. How did the volume of crime reported in Wales vary over the reference period?
iv. Was the volume of F&CM recorded in Wales significantly different to other crime types?

RQ2: What were the characteristics of victims who reported F&CM in Wales, over the reference period?

i. What victim types reported F&CM in Wales?
ii. What were the demographic characteristics of individuals across the crime groups?
iii. What were the demographic characteristics of individuals across crime categories?

RQ3: What financial and other impacts were reported by individuals and other victims of F&CM in Wales, over the reference period?

i. How did direct losses vary between victim types and individual characteristics?
ii. What impacts beyond direct losses can be identified from crime reports? (qualitative)

Methods Summary

To answer RQ1 and RQ2 and sub-questions, as well as QR3i, a mix of bi-variate and multi-variate analysis was carried out on a sample of all Action Fraud crime reports, made by victims within the four Welsh police forces (Dyfed/Powys, Gwent, North Wales & South Wales),

between 1st October 2014 and 30th September 2016 (the reference period), a sample size of n = 17,049 cases. Of these, n = 11,844 were identified as pertaining to individual victims (rather than public entities, businesses or other corporate entities).

To answer the above questions, bivariate relationships were tested using the appropriate statistical tests, primarily chi-squared, but also Kruskal-Wallis, Kolmogorov–Smirnov and Wilcoxon rank sum tests. Annex III includes a list of all variables used in the analysis, including classification (e.g., numeric, categorical etc), along with variable descriptions. Measures of statistical significance and effect size are provided throughout. Statistical significance is measured through p-values, whereas effect size was interpreted with reference to the measures and guidelines in Table 10 (see chapter three, section 4.1.2). In addition, the R statistics *effects* package was used in combination with R *commander* to produce effect plots of Generalised Linear Models (GLMs). GLMs were used particularly where traditional bivariate analyses was inconclusive with respect to the size and/or direction of the effect (particularly for chi-squared tests on larger than 2x2 contingency tables).

Finally, thematic analysis of a sub-sample of incident descriptions (332 incidents reported by 160 victims) was undertaken to answer QR3ii and thereby better understand the wide range of impacts F&CM has on victims. As noted in the previous chapter, TA was conducted in six stages, adapted from Braun and Clarke (2006, 2012, 2013): 1) sub-sampling; 2) reading and familiarisation; 3) systematic coding; 4) identification of themes; 5) review of themes and production of a thematic map; and finally, 6) defining and reporting of themes.

1. Volume of Recorded Fraud and Computer Misuse

Between the 1st of October 2014 to the 30th of September 2016 (henceforth 'the reference period'), n = 17,049 F&CM reports were made within the four Welsh police forces (Dyfed/Powys, Gwent, North Wales and South Wales). Most reports were made within the South Wales Police force area (40.79%), followed by North Wales (22.77%), Gwent (18.46%) and Dyfed/Powys (17.98%). While no equivalent data was published for the first year of this sample, the counts for the second year (Table 20), match those published by ONS, suggesting that no systematic errors occurred in data collection (Table E9, ONS, 2017b).[80] Furthermore, Figure 6 illustrates the breakdown of crimes recorded, by victim type.

Police Force	**n(F&CM)**	**Fraud rate**	**CM rate**	**F&CM rate**
Dyfed/Powys				
2015	1,541	2.72	0.27	2.99
2016	1,525	2.82	0.14	2.96
Gwent				
2015	1,515	2.39	0.21	2.59
2016	1,632	2.67	0.12	2.79
North Wales				
2015	2,041	2.68	0.25	2.94
2016	1,841	2.43	0.22	2.65
South Wales				
2015	3,151	2.15	0.24	2.39
2016	3,803	2.69	0.20	2.89
All forces				
2015	8,248	4.89	0.49	5.38
2016	8,801	5.38	0.36	5.74

[80] There was an exact match between the counts within this sample and the counts of crimes recorded by AF and referred to the NFIB for the year ending September 2016, as published by ONS, for Dyfed/Powys (n = 1,525), Gwent (n = 1,632) and South Wales (n = 3,803). For North Wales the ONS published figure was n = 1,903 while the sampled figure was n = 1,841 (a different of 3.3%). As the North Wales data was acquired separately as explained in the methodology, this may be due to an error in the processing of the data before it reached the author. However, this was considered a small error within the overall sample.

Table 20 – Recorded crimes and rate recording per 1,000 people.

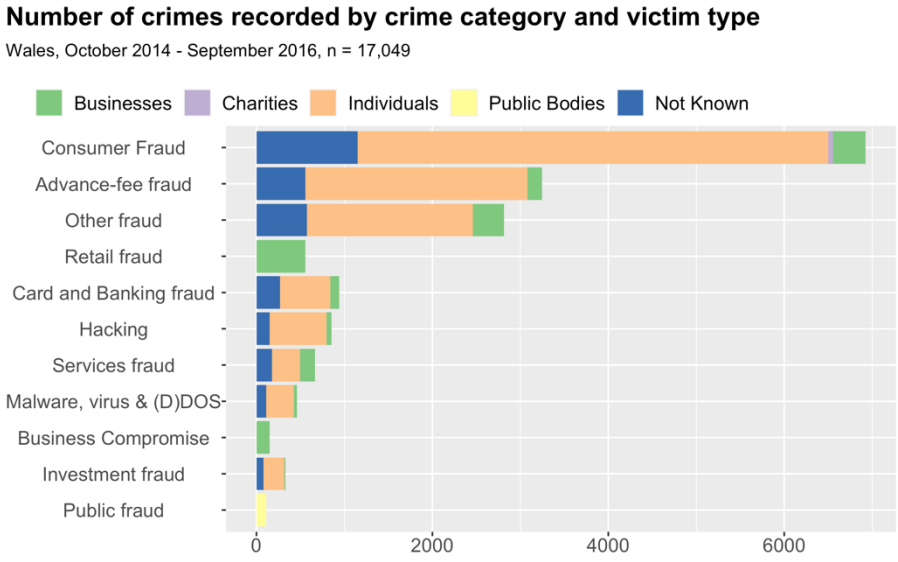

Figure 6 – Number of crimes recorded by crime category and victim type.

Most reports were coded as having been made by individuals, making this data particularly well suited to the study of individual victimisation. Furthermore, there were differences between the crime categories reported across victim types. This is unsurprising as some categories were coded only to specific victim types. In line with the aims of this thesis however, most of the analysis that follows this section focuses on the crime types reported by individuals (n = 11,844).

1.1. Change Over Time

Overall, there was an increase in the total number of recorded F&CM between the first and second year sampled. On average, approximately six crimes were reported per 1,000 people, per year. As Figure 7 demonstrates however, breaking down the recording rate per month and crime group shows that fraud is comparatively more frequent than CM. In addition, as is further explained below, the recording rate of fraud dipped considerably between July-August 2015, when AF call centre services were limited. The same impact is not visible for CM, presumably as CM victims might have continued to report via the online reporting tool. Furthermore, it took nearly a year (10 months) for fraud recording rates to return to pre AF-crisis level, suggesting the disruption had prolonged effects on reporting behaviour and/or recording practices. Given the impact of this external event and the relatively short reference period, it is not possible to identify any clear seasonal effects, such as whether the increase over the

spring/summer months is a regular occurrence. Nonetheless, this sub-section considers the volume of recorded F&CM in more detail.

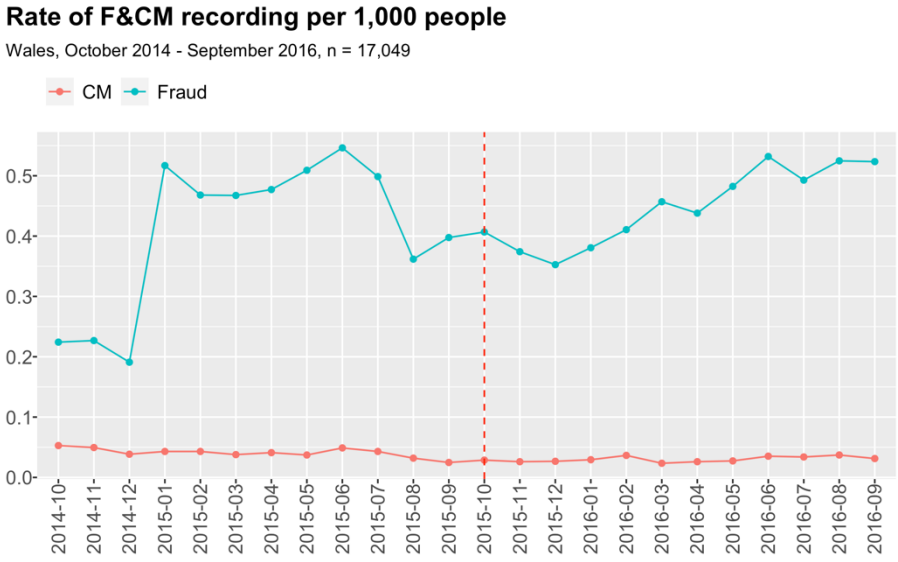

Figure 7 – Rate of F&CM recording per month.

The rate of recording of fraud is considerably higher than that of CM, which is in line with the greater prevalence of fraud victimisation shown in the CSEW figures in chapter one. At the same time, due to the effect of the National Crime Recording Standard (NCRS), this may conceal cases which include CM offences, but fraud was registered as the main offence. One aspect of the NCRS is the *principle crime rule* which states that in cases where there is "sequence of crimes in an incident, or a complex crime, [which] contains more than one type of crime", then "the most serious crime" should be counted (Home Office, 2020a, Section F). This is the crime carrying the maximum sentence on conviction or, where the maximum sentences are equivalent, the greatest sentence most likely to be prescribed on conviction. Given the relatively higher severity of fraud over most CM offences, this principle tends to favour the recording of fraud over CM when both are reported.[81]

In addition, as shown in Table 20, the rate of crimes recorded per 1,000 of the population in each force, was greater in Dyfed/Powys.[82] Looking at the rates of recording over time however, it appears that while the recording rate for fraud increased for most forces (excluding North

[81] Please refer to Annex VII, for a full discussion of the effect of the NCRS and HOCR on the quality of AF data.

[82] The population within each force was calculated using the ONS mid-year population estimates for 2016 (ONS, 2018), cross-referenced with the local-authority-to-police-force lookup table from December 2016 (ONS, 2019).

Wales), the rate CM decreased in each of the Welsh forces. Furthermore, while there were considerably more reports within the South Wales force in absolute terms, Figure 8 shows that similar variations were found across forces when rates of recording per 1,000 people were considered, with two dominant trends. Firstly, there was a sharp increase in the rate of reporting between December 2014 and January 2015 in all forces but North Wales. Discussions with practitioners indicated that this may reflect the implementation period of the AF. While rolled out nationally from March 2013, it appears AF took longer to be fully implemented across all forces than initially expected. Most Welsh forces were no exception to this, with levels of reporting very low in the first quarter of the first year sampled. As such, where subsequent analysis considers changes over time, the first quarter of the first year has been removed from the analysis.

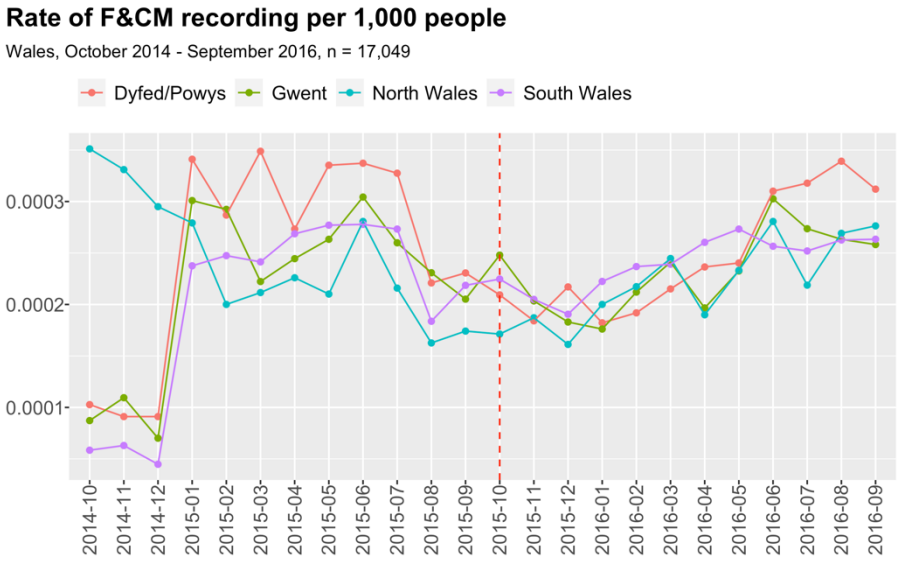

Figure 8 – Rate of F&CM recording by force.

Secondly, the decrease between July-August 2015 coincides with Broadcasting Support Services Ltd (BSS), the company then running the AF call centre service, suddenly going into administration (Out-Law.com, 2015). An interim service was provided by Concentrix between August 2015 and April 2016, which subsequently became the long-term provider when the overall AF contract was awarded to IBM (Owen, 2015), who continued to sub-contract the call centre to Concentrix. The impact of this crisis on crime recording is further illustrated in Figure 9, by plotting the frequency of reports per quarter (each quarter containing a three-month period). The same graph also shows how the decrease in recording was sharper for Dyfed/Powys, but this was also where recording levels were quicker to recuperate. As

discussed below, this may be because F&CM represents a higher proportion of the total crime reported within this force.

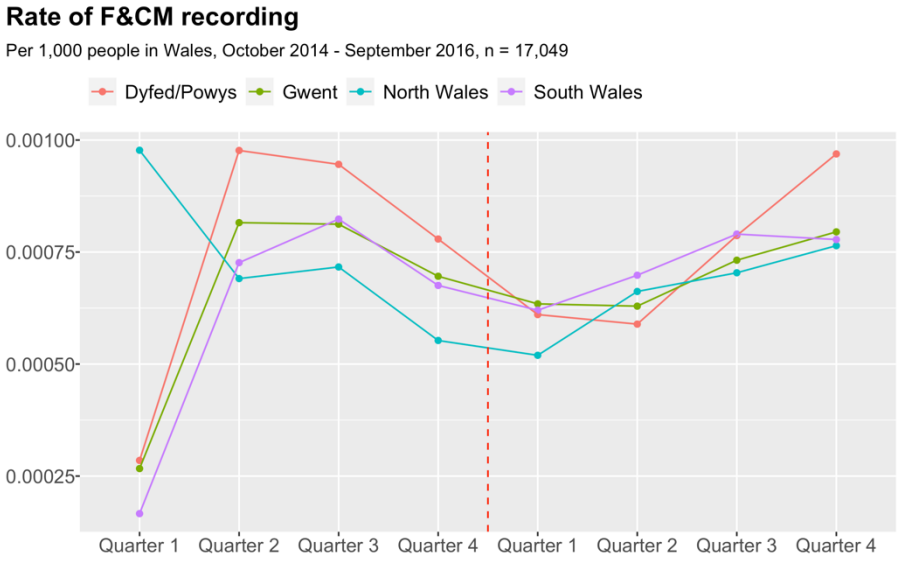

Figure 9 – Rate of F&CM recording per quarter.

Consequently, the increases in reporting both in the first quarter of year one and over the second year of the sample are likely indicative of the availability of the reporting service, rather than a true reflection of victims' reporting behaviour or the extent of victimisation. This highlights how volatile administrative data can be to external events and corroborates previous literature suggesting caution in interpreting trends in the volume of recorded crimes (e.g. Hope, 2007; Levi & Burrows, 2008; MacDonald, 2001; UKSA, 2014). Interpreting sudden spikes and drops in crime reports must be carefully considered against any possibility that they were driven by changes in the collection and/or processing of the data by AF and NFIB respectively. To truly gauge reporting behaviour from this data would require the AF system/service to have been stable throughout the reference period, which it was not. Given the periods of reduced service and volatility which the AF service experienced during the reference period, it is reasonable to assume that the volume of recorded F&CM captured in this study is lower than it would otherwise have been. External events can impact the recording of crime both directly and indirectly. While it has been argued that there has been a spike in AF reporting during the current COVID19 pandemic (Buil-Gil, Miró-Llinares, Moneva, Kemp, & Díaz-Castaño, 2020) for example, such analysis should consider seasonal effects, as well as the availability of AF services. Furthermore, if organisations to which individuals would alternatively report (e.g.,

banks or online shops), are temporarily unavailable or harder to reach, AF reporting may increase.

1.2. Comparison with Other Crime Types

RQ1(iv) set out to compare the volume of F&CM, to the volume of other crimes recorded in Wales over the reference period. Based on ONS published data (Stripe, 2020), this was equivalent to approximately 8% of the volume of other crimes recorded in Dyfed/Powys, 4% in Gwent, between 5-6% in North Wales, and around 4% in South Wales (Figure 10).[83] While these are small proportions, most crimes recorded in Wales fall into the *violence against the person* or the *criminal damage and arson* categories. In 2016 for example, violence against the person accounted for 26.01% and criminal damage and arson for 17.49% of all crime (excluding F&CM) recorded (Stripe, 2020).

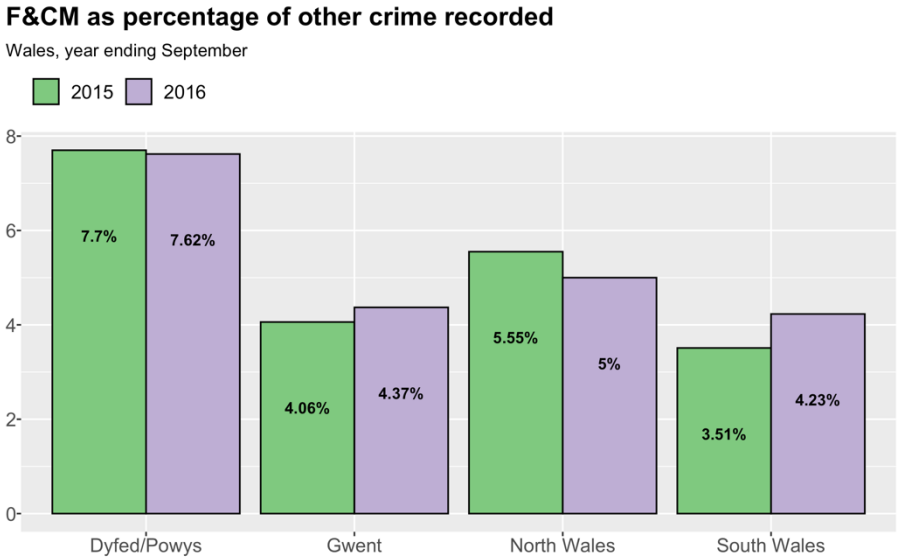

Figure 10 – F&CM as percentage of other crime recorded.

Comparing the F&CM reports made by individuals across Wales to other property crimes affecting individuals however, fraud stands out. Figure 11 shows rates of recording for six property crimes against individuals in each Welsh force, where one line (dots) relates to the

[83] This total recorded crime figure includes a wide range of crimes recorded by the police including violent and property crimes against individuals (e.g. homicide, violence against the person, personal theft or domestic burglary) and other victims (e.g. shoplifting, robbery or non-domestic burglary). It also includes crimes such as vehicle crimes, bicycle theft and possession offences (e.g. drugs and weapons).

year ending 2015 and the other (triangles) to the year ending 2016.[84] Where the rates are the same for 2015/2016, dots and triangles overlap and only one line is visible. As illustrated, recording rates for fraud are considerably higher than most other property crimes, across all forces. Domestic burglary, however, has a higher rate of recording than both F&CM in all forces but Dyfed/Powys.

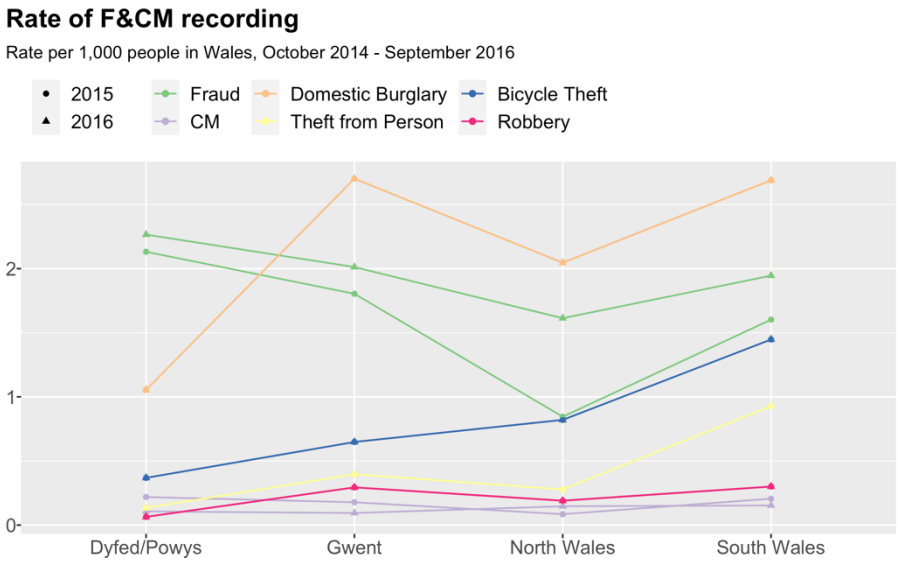

Figure 11 – Rate of recording of property crimes against individuals.

Furthermore, as previously noted, this graph shows that the recording rate for fraud has visibly increased between the first and second years sampled – while the other crime types, including CM, show little or no difference between years (hence the overlapping lines). In short, the recording rate for fraud was higher than for most other property crimes targeted at individuals and increased between the two years sampled. However, as noted above, fraud may have been recorded as the main offence where it was enabled by CM.

[84] The rates here are slightly different to those presented in Table 20 because the calculations were restricted to crimes identified as reported by individual victim only, on account of the comparator crimes being personal property crimes.

2. Victim Characteristics & Reporting Behaviour

RQ2 concerned the characteristics of F&CM victims. To address this question, this section explores individual characteristics associated with F&CM victimisation within the sampled cases, through quantitative analysis. Firstly, it considers the overall volumes of reports by victim type. Secondly, it explores how victim characteristics differ between victims of fraud and of CM. Finally, it then examines the characteristics of individuals by crime category, i.e., sub-categories of fraud and CM.

2.1. Victim Types

As noted in the methodology, to answer RQ2(i), as well as the remaining sub-questions, the data were coded with respect to whether reports were made by individuals, public sector victims, businesses, charities or the victim type was unknown. The percentage of reports by victim type is summarised in Figure 12 below. Of the total sample (n = 17,049), it was not possible to establish the category of victim in approximately 18% of cases. The majority of reports were coded as pertaining to individual victims (69.47%), others related to businesses (11.55%), charities (0.33%) or public institutions (less than 1%). AF data are therefore demonstrably best suited to exploring individual victimisation. Furthermore, the small proportion of reports from businesses is indicative of their considerable under-reporting of F&CM, especially given the volumes recorded by organisations such as UK Finance and Cifas, noted in chapter one.[85]

[85] While UK Finance and Cifas report a large proportion of cases directly to the NFIB, these reports are made primarily on behalf of the financial and insurance industries. Furthermore, as noted in Annex VII, it is not always clear whether the 'crimes' recorded by industry organisations would meet the legal definition of a crime as set out in the NCRS and the HOCR.

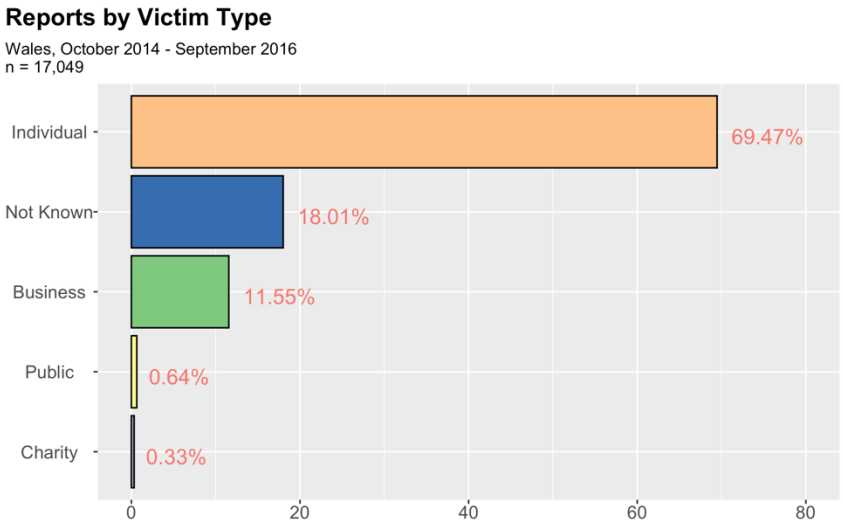

Figure 12 – Percentage of reports by victim type.

A statistically significant difference was found with respect to whether Individuals or Businesses were more likely to report CM or Fraud (χ^2 (1) = 33.35, p < .001).[86] Based on the odds ratio, individuals are approximately 1.93 times more likely to report a case of CM than business victims (n = 13,814), representing a small effect size. This effect can be clearly visualised in Figure 13, through the effect plot of the binomial logit model *Crime Group* ~ *Victim Type* GLM (χ^2 (1) = 38.64, p < .001).[87]

[86] Yates continuity correction applied.

[87] Refer to Annex V, Part III, section 2.2.2 for full model parameters.

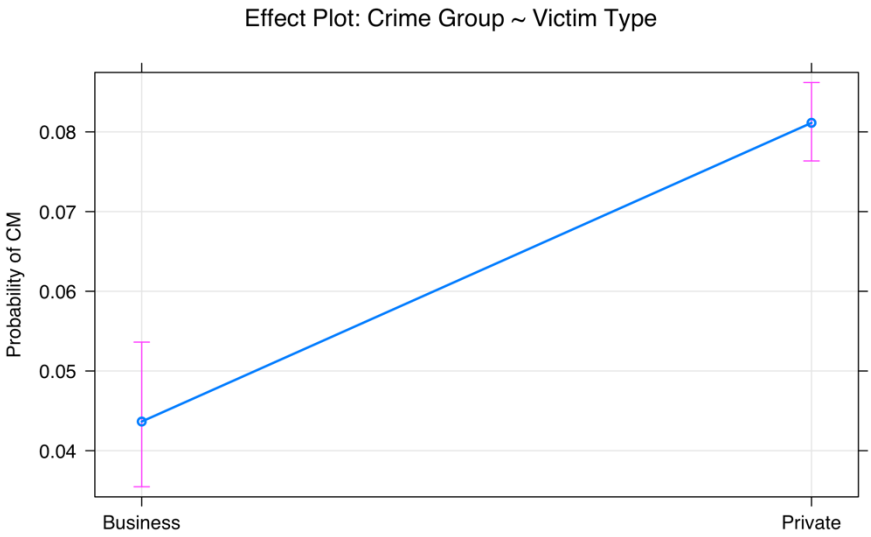

Figure 13 – Effect display of GLM model *Crime Group ~ Age Category* (Model 1).

Given the policy emphasis on cyber resilience for businesses, it is surprising that businesses report proportionately less CM than individuals. However, it is suggested that this may be a result of higher rates of businesses under-reporting CM, rather than businesses experiencing less incidents. Higher rates of under-reporting of CM incidents may be explained by businesses focusing their attention on self-investigation of incidents with the aim of patching vulnerable systems, as well as having greater recourse to cyber insurance where losses justify a claim.[88] In addition, consumer legislation is still grappling with notions of product liability in the context of intangible/digital products and thus consumers have little recourse with respect to unsafe/defective products (Krebs, 2018). The next sub-section considers the characteristics of individual victims in greater detail.

2.2. Victim Characteristics

In this section, victim characteristics are considered in greater detail and, where possible, compared with the local demographic characteristics and known profiles of F&CM victims. In

[88] Although insurance companies may also require that their business clients make a crime report. In addition, further research is needed to investigate whether reports from businesses have increased since the coming into force of the EU's General Data Protection Regulation on 25 May 2018, as this has placed greater responsibility on businesses to protect personal data and report breaches. Unfortunately, this fell outside this work's reference period.

doing so, this section answers RQ2(ii) and identifies and explores several hypotheses regarding individuals' reporting behaviour

2.2.1. Age

Where victim age was known, half were below 51, also close to the mean average of approximately 50 years of age (n = 9,543). These parameters did not change greatly between the two years sampled. Based on the mean and median age however, victims in the Dyfed/Powys area were somewhat older (Table 21). A non-parametric Kruskal-Wallis test found a significant difference in victims' age across police force areas (χ^2 (3) = 163,07 p < .001). However, as noted in the methodology (section 4.1.2), the effect size of this test cannot be easily determined. As such, age was recoded into a categorical variable, allowing for a clearer visualisation of the age distribution and effect size/direction, while also not subject to normality assumptions (Table 22).

	n	Min	Median	Mean	Max.	SD
Full Sample	9,543	9	51	50.47	97	18.62
2015	4,380	12	51	50.69	97	18.61
2016	5,160	9	51	50.29	95	18.57
Dyfed/Powys	2,074	12	54.49	57.00	93	18.33
Gwent	1,968	12	49.84	50.00	95	18.20
North Wales	1,280	14	51.80	53.00	90	18.40
South Wales	4,217	9	48.39	48.00	97	18.61

Table 21 – Distribution of age variable for individual victims, without outliers.

Age Category	n(CM)	n(Fraud)
0-19	39	299
20-24	75	584
25-29	68	575
30-44	213	1866
45-59	217	2183
60-64	64	758
65-74	85	1536
75-84	31	777

85+	5	164

Table 22 – Table of F&CM reports per age category.

The effect of age was thus explored in relation to crime group for individual victims (n = 9,539). A chi-squared test also supported a statistically significant difference between the number of frauds and CM reports recorded across age groups, with a small effect size (χ^2 (8) = 76.49, p < .001, *Cramér*'s V = 0.09). The binomial logit GLM model *Crime Group ~ Age* (χ^2 (8) = 84.22, p < .001) was also computed, enabling a clearer interpretation of the breakdown of this relationship via the effect plot (Figure 14).[89] In line with the online/offline results in the next chapter, the probability of reporting CM (over Fraud) is significantly higher for the younger age groups and changes significantly for groups over 65. Furthermore, re-running the model using polynomial contrasts suggests there is a negative linear trend between age category and the probability of CM. However, as indicated by the error bars below, this trend should be interpreted with caution.

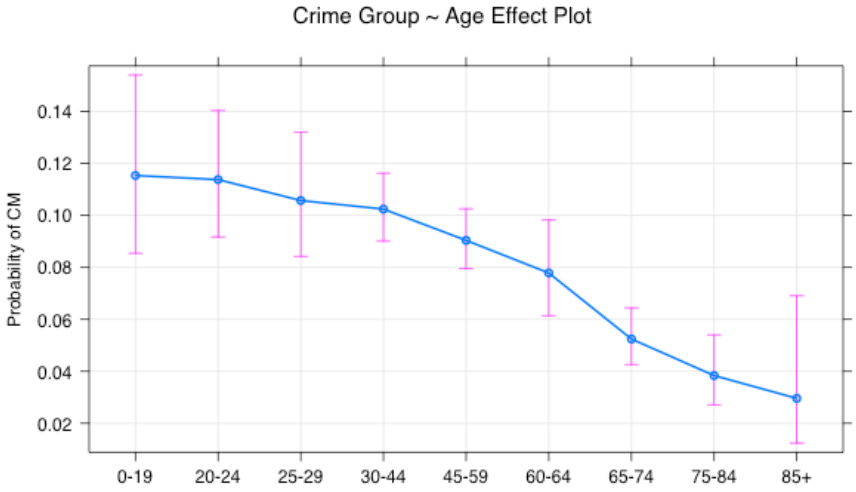

Figure 14 – Effect display of GLM model *Crime Group ~ Age Category* (Model 2).

The use of age categories also allowed for the distribution of age among victims to be compared to that of the Welsh population according to the last census (Figure 15).[90] Despite limitations in the comparison, the graphs illustrate that that the distribution of age within crime reports

[89] Refer to Annex V, Part III, section 2.3.2 for full model parameters.

[90] Apart from individuals under 20 years old, age was re-coded into the categorical age variable to reflect the age categories used in the Census of England and Wales. Given the low number of cases relating to individuals under the age of 20 in the sample however, these were grouped together in one category (0-19 years).

differs significantly from the distribution of age within the Welsh population. [91] Most obviously, the 0-19 age group is under-represented and the 65-74 age group over-represented within the sample of reports.

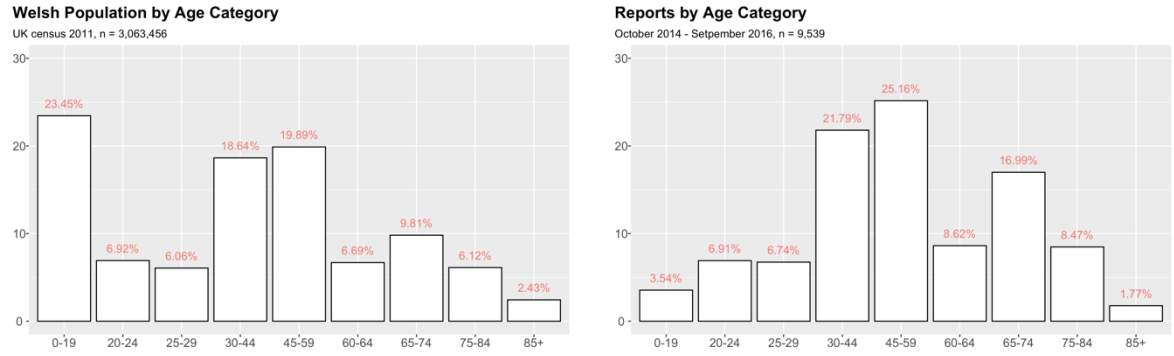

Figure 15 – a) Welsh population by age category (2011 UK Census); b) Percentage of reports by age of individual victim.

This was confirmed with a Kolmogorov–Smirnov (KS) test. The highly significant *p value* in this test (D = 1, p-value < .001 (two-sided test)) means the null hypothesis that the distribution of age in the data sample is the same as in the Welsh population, can be rejected. This test has been shown to produce false negatives both with very small and very large sample sizes. A similar conclusion however, was reached using the chi-squared test to compare the proportion of reports by age category, between the sample and the Welsh population (χ^2 (7) = 47.64, p < .001, *Cramér's V* = 0.3) resulting in a statistically significant result and a medium effect size.[92] The standardised residuals indicate that difference appears to be driven by the 0-19 age category being significantly under-represented in the sampled records (p < .001).[93] As such, the under-representation of the younger age group is likely to reflect differences within the population of reporting victims, rather than wider variations in the Welsh population.

[91] While the unit of analysis for the census is individuals, the unit of analysis with respect to this sample is crime incidents. As it is discussed in chapter six, a significant number of reports (8%) were identified as relating to repeat victims. These victims would have been counted more than once with respect to the distribution of victims' age within the sample. In addition, as we approach the next decennial census in 2021, the 2011 census is, at the time of writing, almost ten years out of date.

[92] Due to the small number of cases, the last two age categories were combined into a +75 age category.

[93] Standardised residuals behave like z scores; if their value lies outside of ±1.96 then it is significant at p < .05, if it lies outside ±2.58 then it is significant at p < .01 and if it lies outside ±3.29 then it is significant at p < .001. The plus or minus sign indicates the direction of the relationship of the association (positive or negative respectively).

Some insight with regards to reporting behaviour can also be gained by comparing the distribution of recorded F&CM in Wales by age group for the second year sampled (Figure 16), to CSEW experimental statistics on the distribution of F&CM victimisation across age (Figure 17). Overall, CSEW experimental statistics for the year ending September 2016 suggested that 6.3% of all adults in England and Wales were victims of fraud and 3.4% of all adults were victims of CM (ONS, 2017a). However, as illustrated in Figure 17, the estimated proportion of victimisation varied with age and across crime group.

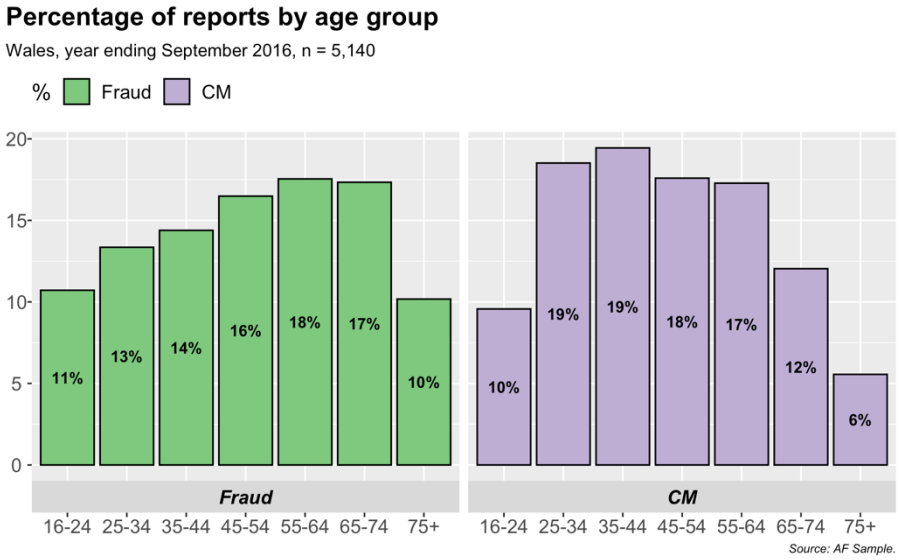

Figure 16 – Percentage of sampled reports by crime group and age group.

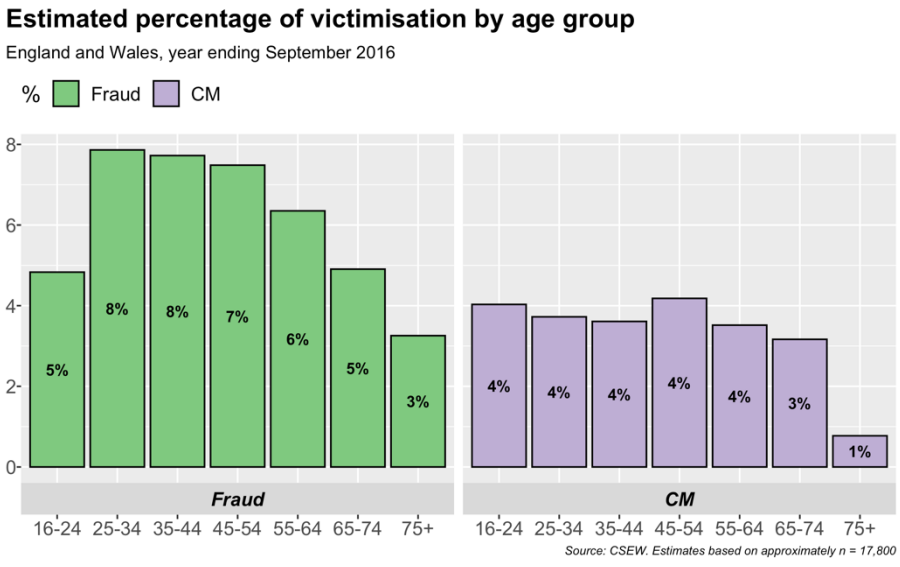

Figure 17 – Percentage of estimated CSEW victimisation within age group.

The proportions are not directly comparable as Figure 16 provides the proportion of incidents reported in Wales, while Figure 17 relates to the estimated proportion of all individuals who were victimised across England and Wales, within each age group. With that caveat, the shape of the distributions suggests that for CM reporting may be lower for the 16-24 and the 65-74 age groups (only 16+ adults are sampled for the CSEW), but the overall shape of the distributions are similar. With respect to fraud however, the distributions appear like a horizontal mirror inversion of each other, suggesting that while younger groups suffer the highest proportion of victimisations, it is the older groups who tend to report being victimised. This finding is in line with Ross et al.'s (2014) meta-analysis of 14 studies exploring the association between older age, vulnerability and likelihood of fraud victimisation, as well as with Schiebe et al. (2014), who concluded that there is no strong evidence that older individuals are more susceptible to fraud, they simply report more.

The reasons why older individuals are more likely to report F&CM are beyond the scope of this study. However, this age profile matters in terms of providing a victim response – to avoid secondary victimisation, CJS institutions must be ready to meet the needs of older victims, particularly older victims of fraud. With some exceptions, few studies have sought to capture the experiences and needs of victims of (online) fraud generally or of older victims of fraud in particular (Button et al., 2009a; Cross et al., 2016). Nonetheless, research on ageing and older people within other disciplines has both theorised old-age vulnerabilities (Grundy, 2006; Schroder-Butterfill & Marianti, 2006) and, by understanding its multiple dimensions, challenged the equivalence between being 'old' and being 'vulnerable' (Bozzaro, Boldt, & Schweda, 2018). On the one hand, increasing individuals' resilience to the impacts of F&CM victimisation will require addressing vulnerabilities which may be associated with older age. On the other, old age is not synonymous with being vulnerable and vulnerabilities unrelated to age cannot be ignored. The vulnerability framework developed through the qualitative analysis in chapter six aims to reconcile the multiple dimensions of F&CM vulnerability.

Age v. Gender

The gender breakdown of the sample was evenly split between reports from male (50.96%) and female (48.86%) victims, reflecting that of the Welsh population (KAS, 2012). Furthermore, while a significant difference was found between the proportion of male and females across age category, this was not at the required $p < 0.1$ level (χ^2 (7) = 15.97, $p < .05$, *Cramér's V* = 0.04). The standardised residuals suggested that there was a greater probability

of male victims in the youngest (0-15), as well as the 65-74 age groups, while the probability of female victims was greater for the 45-54 age group ($p < .05$). However, given that there are more older women within the Welsh population at the time of the last census (Figure 18), no difference still means that male victims were over-represented within the oldest age category.

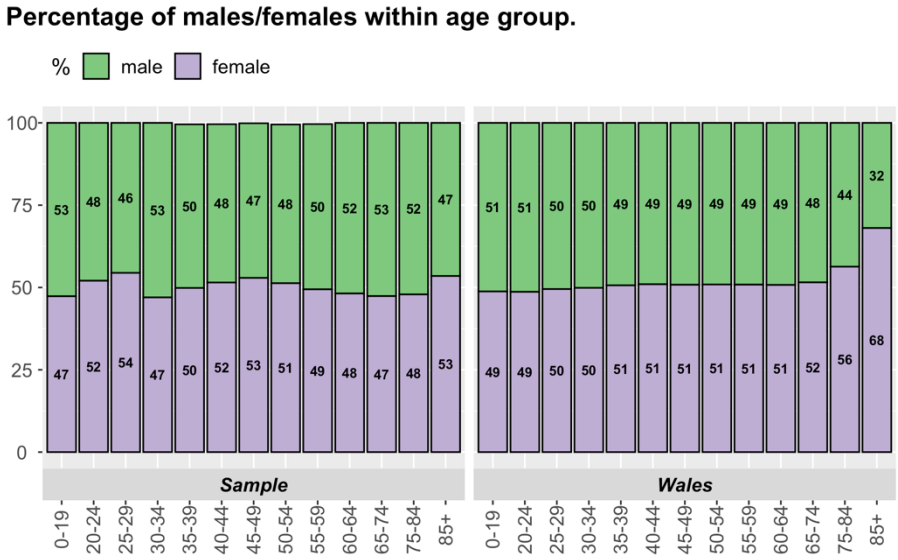

Figure 18 – Percentage of gender by age group (sampled reports and Welsh population).

In addition, the analysis of the binomial logit model GLM *Crime Group ~ Age * Gender,* revealed no significant interaction between age and gender with respect to the likelihood of a victims reporting fraud vis-à-vis CM (χ^2 (1) = 0.730, $p > .05$). This is illustrated in the effect plot below, as the probability of Fraud increases with age for both males and females and there is considerable overlap between error bands (Figure 19).[94] Furthermore, while not directly comparable, experimental statistics based on CSEW data for the year ending September 2016 (Table E3, ONS, 2017a) also suggest that there is little difference in the proportion of F&CM victimisation across age group and gender (Figure 20), with the exception of male victims in the 75+ age category, who are estimated to experience double the proportion of fraud than females in the same age group. As such, this analysis suggests that while older individuals are generally over-represented within crime reports due to their reporting behaviour, the relatively large number of males in the oldest categories (75+) may also reflect a higher likelihood of F&CM victimisation for older males.

[94] Refer to Annex V, Part III, section 2.4.4 for full model parameters.

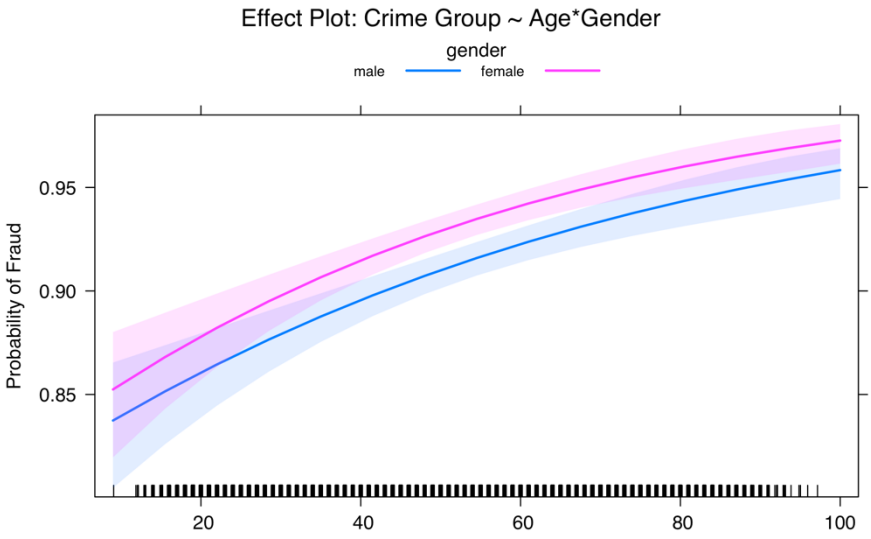

Figure 19 - Effect display of GLM model *Crime Group ~ Age*Gender* (Model 3).

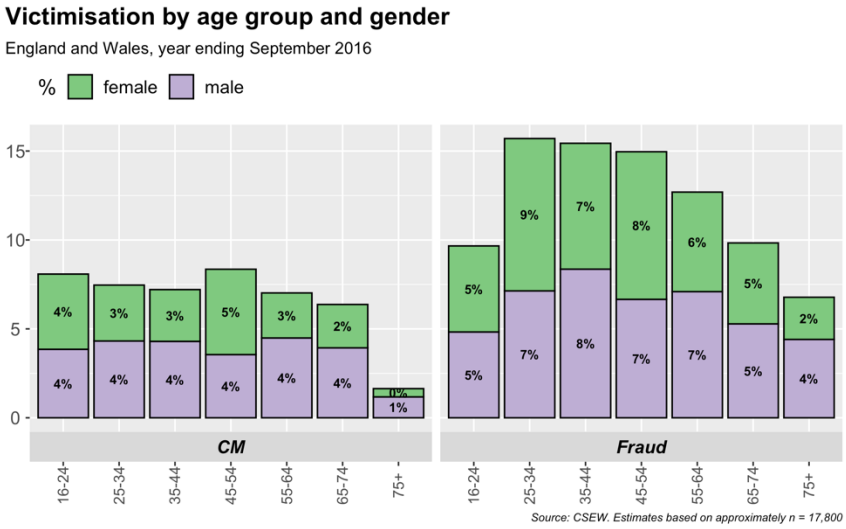

Figure 20 – Percentage of estimated victimisation within age group by gender.

2.2.2. Ethnicity

Where victims' ethnicity was known, approximately 3.3% were made by Black, Asian or Minority Ethnic (BAME) victims.[95] However, the 2011 census estimated that approximately 4.4% of the population usually resident in Wales identified as BAME (Jackson, 2012), suggesting BAME victims are somewhat under-represented within AF data. At the same time,

[95] It is acknowledged that the term BAME is problematic but it was used I line with the practice of the Office for National Statistics.

the breakdown of BAME groups was similar to that of the overall population in Wales, with reports from 1.83% *Asian*, 0.65% *Black*, 0.41% *Mixed* and 0.41% *Other* victims.[96] However, due to the combined level of missing values with respect to victim type and ethnicity (23.26%), these observations are not conclusive. In addition, this analysis is limited by the low numbers within each BAME category. These categories were therefore merged into one BAME group, in order to meet statistical assumptions.

With all the above caveats, a chi-squared test indicated that there was no significant difference between White/BAME ethnic groups with respect to the reporting of Fraud or CM cases (χ^2 (1) = 0.09, $p > .05$).[97] Based on the odds ratio, White victims were approximately 1.09 times more likely to report a CM case than those of BAME backgrounds (n = 7,879), representing a negligible effect size. As such, based on the chi-squared and odds ratio, no statistically significant or substantial difference was found between ethnic groups reporting F&CM.

That said, experimental CSEW statistics (Table E3, ONS, 2017a) suggested that a higher proportion of ethnically Black adults became victims of F&CM in 2016, as did a lower proportion of individuals who identified as Asian, when compared to their White counterparts (Figure 21). All things being equal, Black victims should therefore also be over-represented within crime report data. That they are not, suggests that, similarly to other crime types, F&CM may be particularly under-reported among Black individuals. However, CSEW figures include England as well as Wales and the former includes a much larger BAME population and the 2016 results were experimental. The most recent data suggests that there are no differences in the levels of F&CM victimisation across ethnic groups (ONS, 2020d). As such, further research is necessary to establish whether Black individuals are disproportionately victimised, or disproportionately under-report F&CM.

[96] The 2011 census estimated the minority ethnic population of Wales to be approximately 2.3% Asian, 0.6% Black, 1.0% Mixed and 0.5% Other (Jackson, 2012).

[97] Pearson's Chi-squared test with Yates' continuity correction.

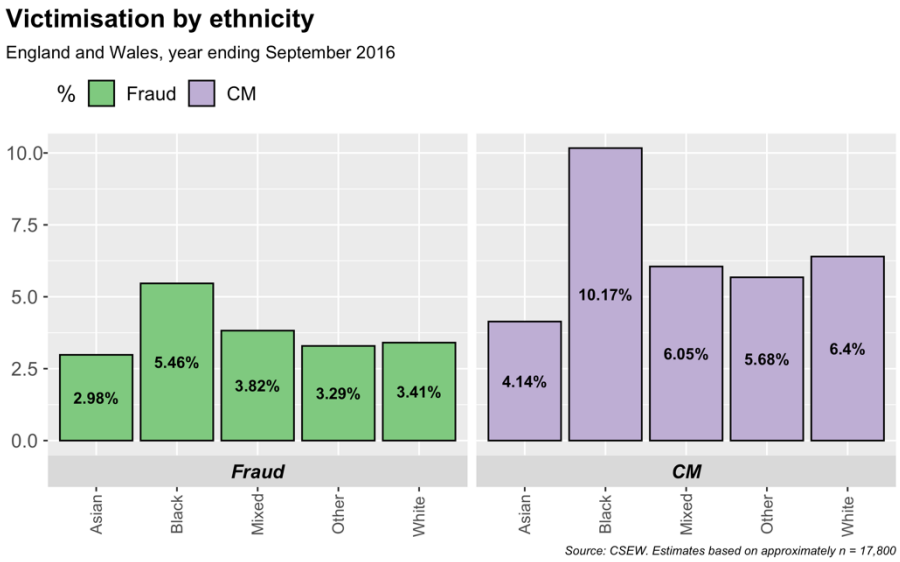

Figure 21 – Percentage of estimated victimisation within age group by ethnicity.

It is well documented that the social construct of race is a consistent predictor of attitudes towards the police, with BAME individuals significantly less likely to trust the police than their white counterparts in White-majority societies and the UK in particular (e.g. Bowling, Parmar, & Phillips, 2003; Brown & Reed Benedict, 2002; Roux, 2018). Such feelings are inevitably historically and socially contextualised and may be aggravated during particularly racially charged historical moments such as the current post-Trump, post-Brexit moment, where police brutality against Black individuals and a sense that the CJS does not work for victims or offenders are catalysts for the Black Lives Matter and the Defund movements. Lack of trust in the police and other CJS institutions may be exacerbating under-reporting of F&CM among BAME groups. As such, the extent to which BAME positionalities i.e., subjective experiences of collective race identities, shape experiences of F&CM victimisation, is also under-researched.

2.2.3. Gender

Reports from individuals were evenly distributed between males (50.96%) and females (48.86%), with a relatively low number of missing values (0.18%), following the data derivation exercise previously described. A statistically significant difference was found between males and females with respect to whether they report fraud or CM, but this was not at the .01 level (χ^2 (1) = 4.09, p < .05). In addition, based on the odds ratio, males are approximately 1.15 times more likely to report a case of CM than female victims (n = 11,823), representing a negligible effect size. Nonetheless, as with ethnicity, future qualitative research

is needed to understand the extent to which gender as a collective identity affects victimisation experiences. Speaking directly to victims would enable an exploration, for example, of whether experiences of secondary victimisation where F&CM is reported to the police, are in any way gendered.

2.2.4. Deprivation

The average Welsh Index of Multiple Deprivation (WIMD) score of 960.11 was observed across individual reports (where 1 represents the most deprived and 1909 the least). As also explained in the methodology, these scores were re-coded into four categories representing the first, second, third and fourth quartiles of deprivation (low, low-medium, medium-high and high deprivation). Overall, 24.48% of reports were associated with a low deprivation area, 51.31% with a medium deprivation area (including 26.09% Low-Medium and 25.22% Medium-High deprivation) and 24.21% with a high deprivation area.

Levels of deprivation varied considerably across the four Welsh police forces however, as confirmed by a statistically significant chi-squared test, with a medium effect size (χ^2 (9) = 1272.2, $p < .001$, *Cramér's V* = 0.19). Given the number of categories involved in the comparison however, it was challenging to interpret the direction of this effect based on the standardised residuals. This was aided by the effect plot of the multinomial logit model *WIMD Category ~ Police Force* (χ^2 (9) = 1321.7, $p < .001$) (Figure 22).[98]

[98] Refer to Annex V, Part III, section 2.7 for Chi-squared standardised residuals and full GLM parameters.

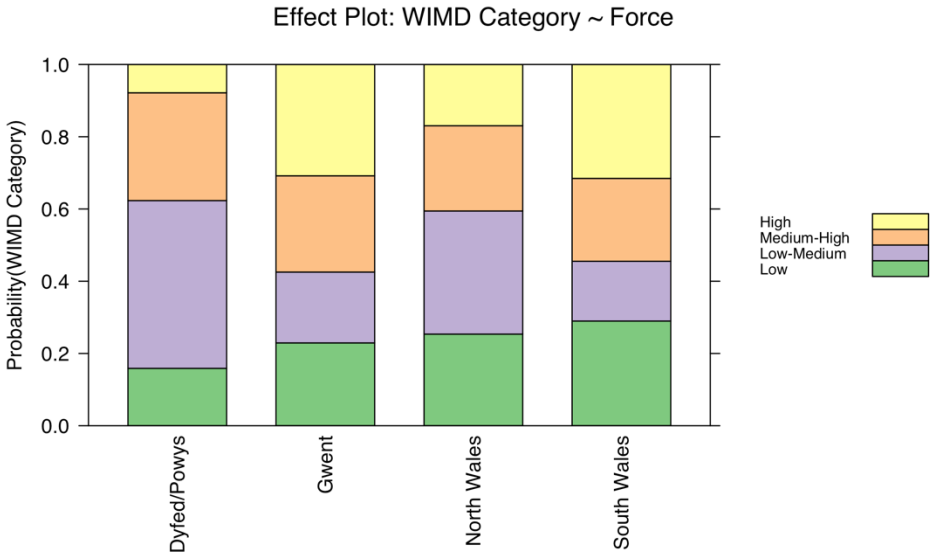

Figure 22 – MLM model *WIMD Category ~ Police Force* effect plot (Model 4).

As illustrated, reports from victims in the Dyfed/Powys police force area were concentrated in the Low-Medium deprivation category, with a very low probability of any report being made from a Highly deprived area. In North Wales, the picture is similar, but the probability of High deprivation is greater. In the Gwent and South Wales however, the probability of reports from Highly deprived areas is much greater.

Furthermore, Table 23 shows the summary values describing the distribution of the WIMD score, by crime group. Judging by the mean and median values, it appears that fraud reports are in slightly less deprived areas. However, the Wilcoxon rank-sum test failed to yield a statistically significant difference between the distribution of deprivation scores across F&CM (W = 5076112, p-value > .05).

	n	mean	sd	median	3Q	max	range	skew	kurtosis
Fraud	10,883	962.35	543.71	968	1421	1909	1908	-0.02	-1.16
CM	961	934.84	551.95	901	1419	1909	1907	0.07	-1.19

Table 23 – WIMD measures of central tendency by crime group.

Corroborating these results, no association was found between crime group and WIMD score re-coded into a (high/medium/low) category (χ^2 (2) = 0.55, p > .05). As such, no significant statistical or substantial difference was found between level of deprivation and the reporting of Fraud or CM. However, it should be noted that this measure of deprivation relates to the victim's locality, rather than their personal circumstances. In addition, future research might

compare the levels of deprivation in areas with high F&CM reporting, to those where other crime types are most reported.

2.2.5. Internet Access

A much starker difference was found with respect to the levels of internet access associated with each police force area. A chi-squared test revealed both a statistically significant and substantially large difference between the levels of internet access across police force area (χ^2 (9) = 13629, p < .001), the *Cramér's V* (0.61) indicating a large effect size. Again, this effect can be most effectively visualised through the effect plot of the multinomial logit model *Net Access ~ Police Force* (χ^2 (9) = 15713, p < .001) (Figure 23).[99]

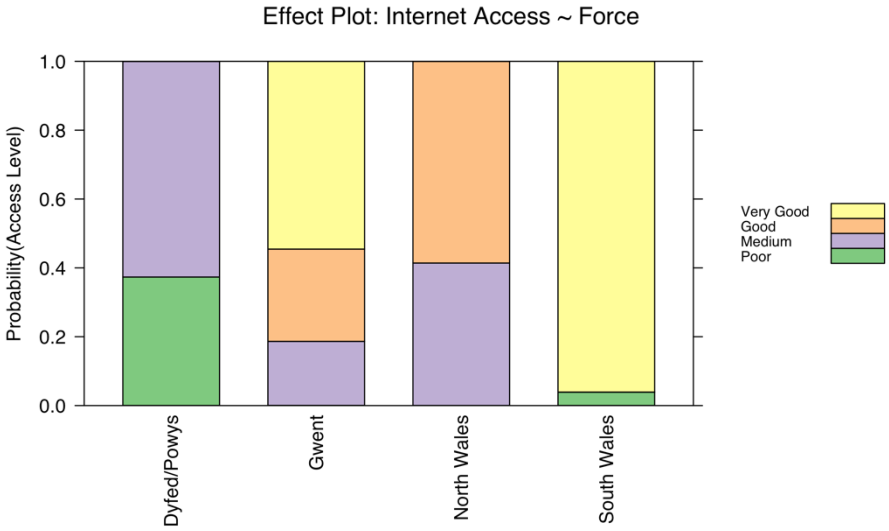

Figure 23 – MLM model *Net Access ~ Police Force* effect plot (Model 5).

The Dyfed/Powys area stands out once again, with all reports coming from areas with Poor or Medium access. This is followed at some distance by North Wales, where there is a greater than .5 probability of Good access. However, these results pale in comparison with reports from Gwent, most probability from areas with Very Good Access and South Wales, where probability of Very Good access was overwhelming. Furthermore, a chi-squared test indicated that there was a statistically significant difference between reports of F&CM, depending on the degree of internet access within the victim's LA area (χ^2 (3) = 10.87, $p < .05$, *Cramér*'s V = 0.03). However, this difference was not at the p < .01 significance level used in this study and

[99] Refer to Annex IV, Part III, section 2.8.1 for Chi-squared standardised residuals and full MLM parameters.

the effect size based on *Cramér*'s *V* was negligible. Nonetheless, to the extent that a difference was found, unsurprisingly, the standardised residuals indicate that it is driven by CM victims being significantly more likely to have Very Good internet access ($p < .01$). As above, future research might compare the levels of internet access in areas with high F&CM reporting, to those where other crime types are most reported.

2.3. Victim Characteristics and Crime Categories

Addressing RQ2(iii), this section explores whether the previously discussed individual and environmental characteristics are associated with particular fraud or CM categories.[100] Combined with the analysis that follows of the impact of each crime type on victims (sections 3.2 and 3.3 below), section four goes on to summarise the typical victim profile for each crime category.

2.3.1. Fraud Victim Characteristics

Age

A statistically significant difference with a small effect was found with respect to the age profile of victims across fraud categories (χ^2 (30) = 275.88, $p > .01$, *Cramér*'s $V = 0.08$).[101]. Although some indication of the direction of this effect was apparent through the standardized residuals, given the number of categories, this is best illustrated through effect plot of the multinomial logit model *Fraud Category ~ Age* (χ^2 (30) = 283.35, $p < .001$).[102]

[100] Due to the small numbers, CM categories were combined into one category of *Hacking* and another including *Malware, Virus & (D)DOS*,

[101] As above, the younger (0-19) and older (85+) age categories used elsewhere in this study were combined in order to meet the assumptions of the chi-squared test.

[102] Helmert contrasts were used to take into account the ordered nature of the age variable. Refer to Annex V, Part III, section 2.11.1 for Chi-squared standardised residuals and full MLM parameters.

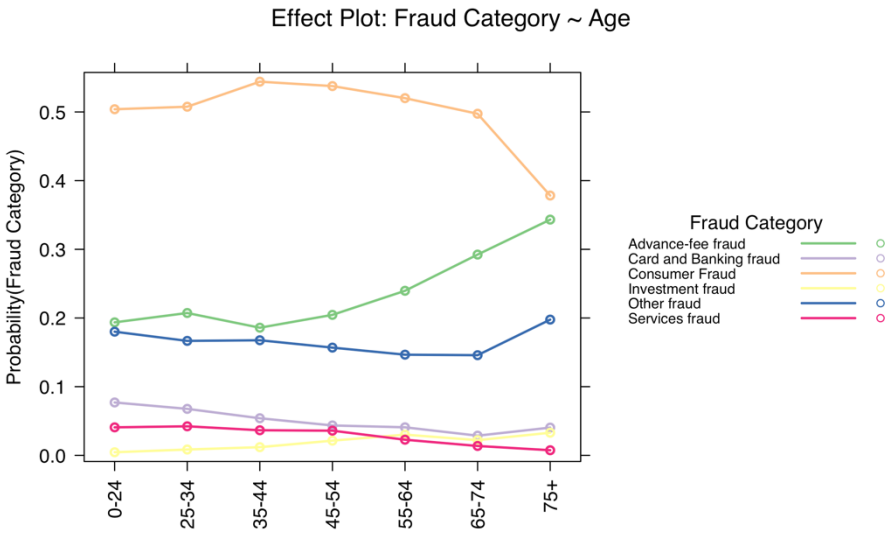

Figure 24: Effect display of MLM model *Fraud Category ~ Age* (Model 6).

As Figure 24 shows, the effect was driven by the *Consumer* and *Advanced-fee* fraud categories. The probability of the first dropped considerably for the 75+ victims, while the probability of the second increased linearly with age, from age group 45-54 onwards.

Ethnicity

A statistically significant difference was also found with respect to the types of fraud reported across the binary ethnicity classification of White/BAME, but this had a negligible effect size (χ^2 (5) = 16.44, $p < .01$, *Cramér*'s $V = 0.04$). To the extent that a difference was found, the standardized residuals indicated that this was driven by *Advance-fee* fraud reports being significantly more likely to come from White victims ($p < .01$). However, these observations must be interpreted with caution given the high percentage of missing values (33%).

Gender

A statistically significant difference with a small effect size was found with respect to the fraud types reported by male and female victims (χ^2 (5) = 52.71, $p < .01$, *Cramér*'s $V = 0.07$). Here, the standardized residuals indicated that this was driven by *Advance-fee* fraud reports being significantly more likely to come from females and *Investment fraud* reports from male victims ($p < .01$). The odds ratio indicated that the odds of females reporting *Advance-fee* fraud were 1.19 times larger than those of male victims (a negligible effect), while the odds of male victims reporting *Investment* fraud were 2.28 times larger than those of females (a small effect).

Deprivation

Judging by the mean and median values in Table 24, it appears that *Card/Banking* and *Services fraud* were associated with relatively more deprived areas. However, as illustrated in Figure 25, the distribution of the WIMD variable was similar across fraud categories. This was confirmed with a Wilcoxon rank-sum test for non-parametric data, which failed to yield a statistically significant result (W = 104708, p-value > .05).

	n	mean	sd	median	3Q	max	range	skew	kurtosis
Advance-fee	2525	922.7	537.32	903	1373	1909	1907	0.09	-1.15
Card/Banking	573	889.59	543.71	864	1369	1909	1908	0.12	-1.18
Consumer	5347	978.44	541.43	992	1432	1909	1908	-0.04	-1.15
Investment	235	1001.62	512.09	1015	1431	1905	1901	-0.15	-1.03
Other	1887	999.28	554.97	1046	1474	1909	1907	-0.16	-1.16
Services	316	888.94	553.96	882.5	1361.50	1899	1895	0.07	-1.24

Table 24 – WIMD measures of central tendency by fraud category.

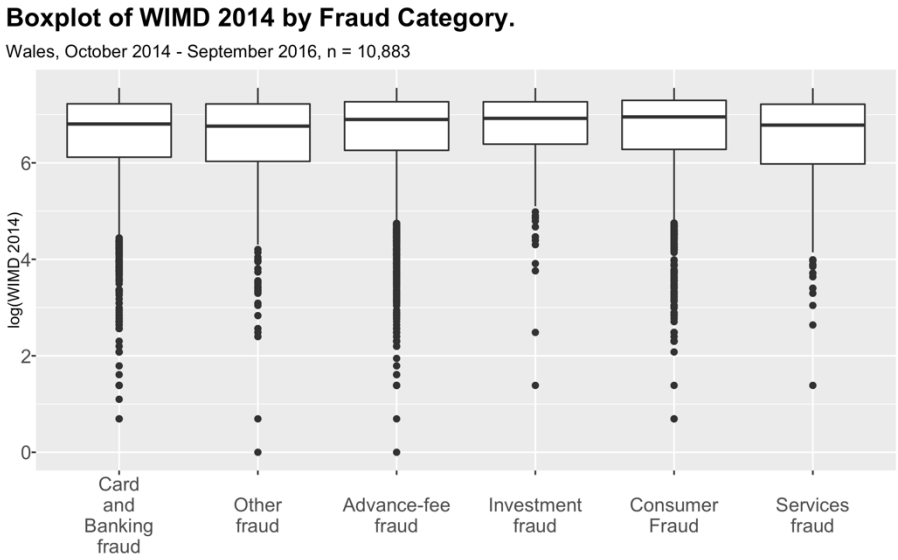

Figure 25 – Boxplot of WIMD 2014 by fraud category.

Furthermore, while a Kruskal-Wallis test found a significant difference in deprivation scores across fraud categories (χ^2 (5) = 44.23, p < .001), the effect size of this test cannot be easily determined. Through the effect plot of the *Fraud Category ~ WIMD* (χ^2 (5) = 44.14, p < .001) multinomial logit model however, it became clear that while the model itself was statistically significant, the probability of each fraud category did not change much as WIMD score

increased. This is illustrated in the relatively constant size of the bands in Figure 26 below.[103] However, as noted in the methodology this is an imperfect measure as it relates to the victims' LSOA, rather than their personal circumstances.

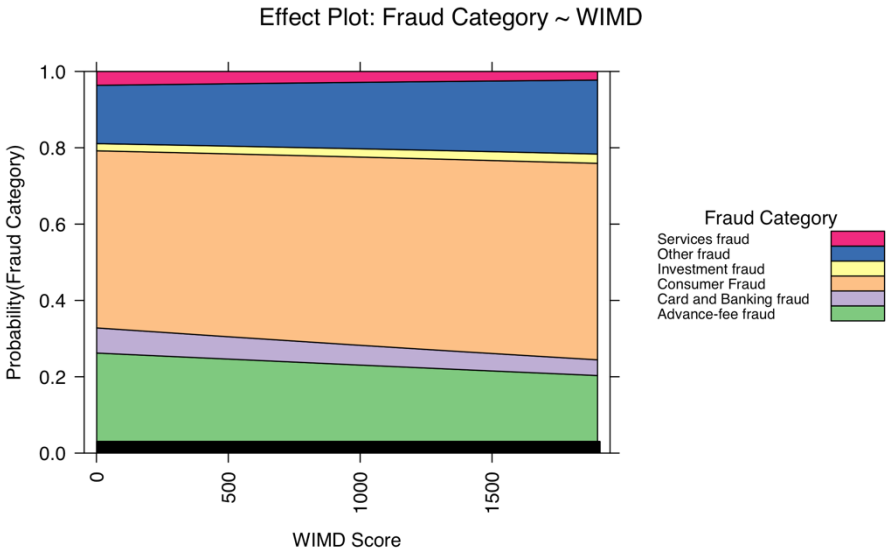

Figure 26: Effect display of MLM model *Fraud Category ~ WIMD* (Model 7).

Internet access

With respect to internet access, a chi-squared test indicated that while there was a statistically significant difference between the number of reports made by fraud category, depending on the level of internet access in the victim's LA, the effect size of this difference was negligible (χ^2 (15) = 47.88, $p > .05$, *Cramér*'s $V = 0.04$).

2.3.2. Computer Misuse Victim Characteristics

Age & Ethnicity

Victims of CM were found to be younger than fraud victims. However, while a significant difference was found with respect to the age profile for victims of *Hacking* and *Malware, Virus & (D)DOS* attacks, this was not at the $p < .01$ level ((χ^2 (6) = 13.94, $p > .05$).[104] Furthermore, the effect size was small (*Cramér*'s $V = 0.13$). Similarly, no significant differences were found with respect to ethnicity across CM categories (χ^2 (1) = 0.02, $p > .05$).

[103] Refer to Annex V, Part III, section 2.11.4 for Chi-squared standardised residuals and full MLM parameters.

[104] Given the small number of cases in the younger (0-19) and older categories (85+), these were combined in order to meet the assumptions of the chi-squared test.

Gender

With respect to gender, a statistically significant difference was found between CM categories (χ^2 (1) = 4.75, $p < .05$), but this was not at the $p < .01$ level used in this study. Furthermore, based on the odds ratio, males were approximately 1.37 times more likely to report a case of *Malware, Virus & (D)DOS* (n = 957), which is indicative of a negligible effect size.

Deprivation

Judging by the mean and median values in Table 25, it appears that based on the average deprivation scores Hacking reports are in less deprived areas. However, as illustrated in Figure 27, the distribution of the WIMD variable was very similar between the two CM categories. This was confirmed with a Wilcoxon rank-sum test for non-parametric data, which failed to yield a statistically significant result (W = 104708, p-value > .05).

	n	mean	sd	median	3Q	max	range	skew	kurtosis
Hacking	647	944.98	557.82	898	1440.50	1909	1907	0.07	-1.22
Malware, Virus & (D)DOS	314	913.94	539.94	903	1374.25	1886	1878	0.05	-1.14

Table 25 – WIMD measures of central tendency by CM category.

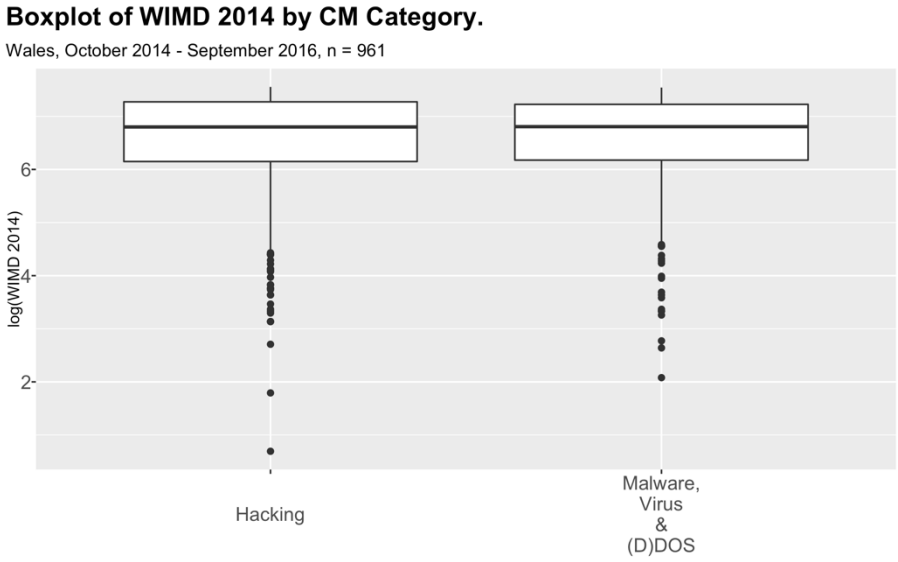

Figure 27 – Boxplot of WIMD 2014 by CM Category.

Corroborating these results, no association was found between CM categories and WIMD score re-coded into a (high/medium/low) category (χ^2 (2) = 1.78, $p > .05$). As such, no significant statistical or substantial difference was found between level of deprivation and the reporting of CM categories.[105]

Internet access

A chi-squared test indicated that there was no statistically significant difference between reports made by CM category, depending on the level of internet access in the victim's Local Authority area (χ^2 (3) = 5.75, $p > .05$).

[105] As above, it should be noted that this measure of deprivation relates to the victim's locality rather than their personal circumstances.

3. Impact of Fraud and Computer Misuse

The third research question posed in this thesis concerned the reported financial (RQ3(i)) and other impacts (RQ3(ii)) of F&CM. In approximately half of the sample, no direct financial loss was recorded. Where such losses were recorded, the data show high dispersion, with losses concentrated at the lower end of the scale, while a few extreme cases skew mean averages. As it will be seen, this was true across crime type, victim type and individual characteristics. Nonetheless, there were variations between sub-groups of reports within the sample and these are explored in section 3.1 below.

While patterns of direct loss are an important piece of the puzzle in understanding F&CM impact, direct losses are an imperfect measure of victim impact. [106] Firstly, the full extent of direct losses may be unknown to the victim at the time of reporting. Secondly, indirect losses may be more significant than direct losses. Furthermore, the range of impacts of F&CM go beyond financial loss. These wider impacts are examined in section 3.2, through the thematic analysis (TA) of the incident descriptions of a sub-sample of cases.

3.1. Direct Financial Loss

3.1.1. Loss by Victim Type

Overall, 49.5% of the crimes sampled reported a direct financial loss. This included 61% of business, 70% of charity, 49% of individual and 8% of public sector reports. Conversely, 19.32% of business and 28.52% of individual reports recorded no loss, a significant difference confirmed through a chi-squared test (χ^2 (1) = 90.32, p < 0.01).[107] The odds ratio showed this to be a small effect, as the odds of individual victims reporting no loss were only 1.6 times higher than those businesses. Furthermore, as illustrated in Table 26, losses were highly dispersed for all victim types, with considerable differences between mean and median values, as well as large standard deviations and ranges. Furthermore, the skew and kurtosis further

[106] Within this section and respective sub-sections the term “loss” is used to mean “direct loss”, unless otherwise stated.

[107] Pearson's Chi-squared test with Yates' continuity correction.

indicated that these data were not normally distributed.[108] The high dispersion and the effect of a few large losses is also illustrated by the long whiskers in Figure 28.

Victim Type	n	mean	sd	median	3rd quartile	range	skew	kurtosis
Business	1,202	22,947.68	487,658.70	299.50	2,700	16,784,964	33.81	1,158.34
Charity	39	2,409.23	7,295.86	5	125	30,999	3.07	8.34
Individual	5,854	5,568.50	75,864.90	350	1,547.50	4,999,999	53.10	3,302.38
Public	9	333,335,086	499,998,685	500	1,000,000,000	999,999,994	0.59	-1.81
Not Known	1,512	8,030.15	49,342.29	420	3,000	1,424,939	20.22	508.34

Table 26 – Distribution of loss by victim type (sd = standard deviation).

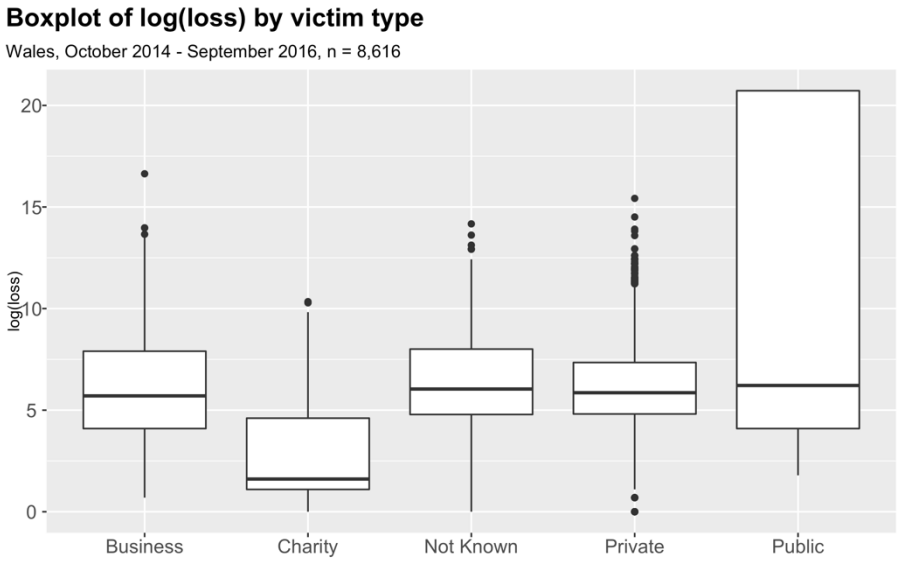

Figure 28 – Boxplot of Log(Loss) by Victim Type.

***The log transformation was applied to allow for a better visualisation, given the level of dispersion and the number of outliers.**

[108] In a normal distribution, the skew and kurtosis values are 0. Positive skew values indicate a higher than expected concentration of values to the left of the graph (in this case towards the lower end of loss). In addition, positive values of kurtosis indicate a pointy and heavy-tailed distribution.

Unsurprisingly, there were differences between the magnitude of losses reported by individuals and businesses, with business victims reporting higher average losses.[109] However, both Table 26 and Figure 28 show that median loss values were relatively similar between these victims. As the median value cuts the data in half, this means that of all that reported a loss, half of the reports from individuals were below £350 and half of all reports from businesses below £299.50 – a not dissimilar amount. In contrast, the mean individual loss was £5,568.50 and the mean business loss £22,947.68. This is a much larger difference, but it is skewed by a small number of very high loss values, particularly for business victims. Given the dispersion of the data, the median provides a better indication of the "typical" loss than the mean.[110]

Outliers

There was no reason to believe that the higher values of loss recorded resulted from systematic error. However, to avoid a few extreme values skewing the results, extreme cases were removed in the subsequent analysis. Of the business reports who reported a loss greater than £0 (n = 1,202), based on z-cores, 0.14% of the sample or 2 cases of losses were superior to £1,170,000.[111] For individuals' reports, there were 28 outliers among cases reporting a loss (n = 5,854), all of which amounted to losses equal or superior to £150,000. Table 27 summarises the financial loss data for each group with outliers removed.

	n	mean	sd	median	3Q	max	range	skew	kurtosis
Business	1,199	7,054.33	37,796.83	299	2,630	854,860	854,858	17.18	349.6

[109] Losses reported by victims whose 'type' was unknown, while not dissimilar to individual victims, had to be discarded from the analysis, as were the few reports made by those classed as "public sector" and "charities", given the small number of reports. As such, the focus of the analysis that follows is limited to losses experienced by businesses and individuals.

[110] It should be noted that the variability of the size of the boxes and whiskers (Figure 28) indicated that there was no homogeneity of variance between losses reported by individual and business victims. This conclusion was formalised using Levene's test (1960). The test's result indicated that for reported loss, the variances were significantly different between individual and business victims $F(4,8611) = 1075$, $p < .0001$. As noted in the methodology (section 6.2), this precluded the use of an OLS model to further explore differences in loss reported by these two groups.

[111] Outliers were identified by using both the Interquartile Range (IQR) rule, as well as z-scores. The IQR rule stipulates that data values more than 1.5 times below the first quartile or above the third quartile are outliers. Z-scores standardize a dataset by converting a variable's data points into scores if the distribution had a mean of 0 and a standard deviation of 1. By doing this, we can establish which data-points fall within important limits. Any absolute z-score greater than 3.29 is an outlier (Field et al., 2012, p. 146).

Individuals	5,824	2,916.96	9,569.29	349	1,500	143,000	142,999	6.95	61.43

Table 27 – Distribution of loss for individuals and businesses.

Even after removing outliers however, the distribution of loss for businesses and individuals remained non-normal and highlight dispersed. It is unsurprising therefore that the Wilcoxon rank-sum test, used to compare the distributions of financial loss between the two independent groups (individual/business victims who reported a loss > £0, n = 7,023), yielded a significant difference, but a small effect size (W = 3352221, p-value < .05, r = -0.03). This result thus lends support to the conclusion that the apparent differences between losses reported by businesses and individuals result from the effect of a small number of high values.

Loss categories

Three reasons led to the re-coding of the numeric loss variable into loss categories. Firstly, given the dispersion of the data, it was easier to visualise the distribution of loss by converting the loss variable into categories. Secondly, using a categorical variable avoided the extreme values mentioned above skewing results, without their complete removal. Finally, a categorical variable allowed for statistical tests which were not subject to assumptions of normality. The proportion of business/individual reports recorded for each loss category is shown in Figure 24. Considering only those cases where there is a reported loss above £0, the modal category is a loss equal to or less than £150 for both groups. Moreover, considering the cumulative percentages for all reports by individuals and businesses, in approximately 50% of cases the loss ranged between £1 and £300 and in approximately 70% of cases the loss ranged between £1 and £1000. In addition, the loss categorisation highlights some differences between the losses reported by individual and business victims, with a greater proportion of reports by business victims at both extremes of loss.

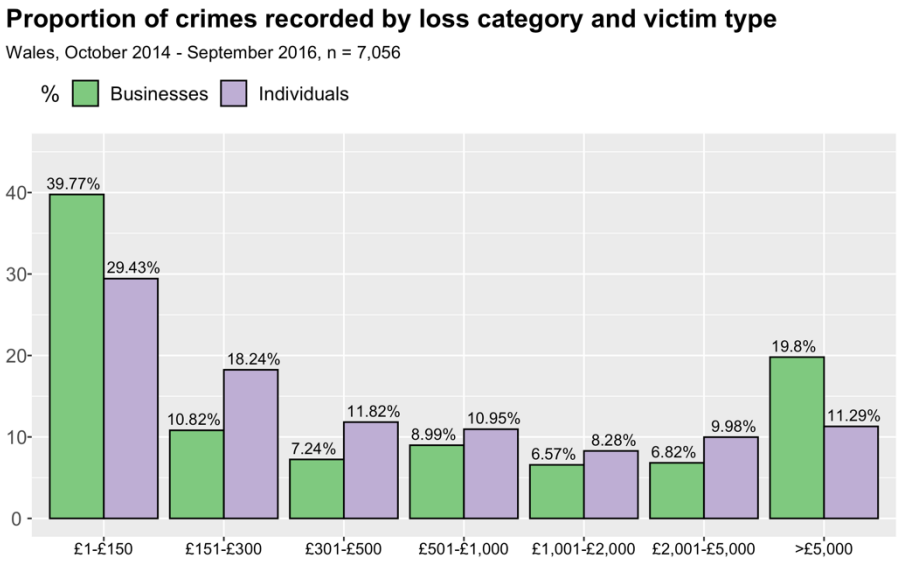

Figure 29 – Proportion of crimes recorded by loss categories, within victim type.

A chi-squared test was used to test the association between the loss category variable and victim type. The difference between the categories of loss reported by businesses and individuals were found to be statistically significant but the effect size small (χ^2 (6) = 159.99, p < .001, *Cramér's* V = 0.16). Nonetheless, interpreting the chi-squared result by looking at the standardized residuals confirms that this difference is due to business victims being more likely to report losses at the highest end of the spectrum, while the opposite is true of individual victims, where losses are significantly more concentrated at the lower end of the scale, for all but the £1-£150 category (p < .01).

3.1.2. Loss by Crime Group and Crime Categories

Levels of direct financial loss reported by individuals and businesses (n = 13,814) were compared across crime group, crime categories and MO group. Firstly, differences in the proportion of no loss reports were investigated, as summarised in Figure 25. A series of chi-square tests revealed a statistically significant difference between the levels of loss/no loss reports across crime group (χ^2 (1) = 453.91, p < .001), crime category (χ^2 (9) = 895.76, p < .001, *Cramér's* V = 0.25) and MO group (χ^2 (2) = 520.51, p < .001, *Cramér's* V = 0.22). Within crime group, the odds of a CM report being a no loss report were 4.82 times those of fraud report, a medium-sized effect. *Cramér's* V also suggested a medium effect size for the difference between loss/no loss reports across crime categories and MO group. Furthermore, the standardized residuals showed that all differences depicted in Figure 30 were significant at the p < .01 level.

Figure 30 – Proportion of loss/no loss for individuals and business victims.

Table 28 summarises the distribution of losses across crime category, where businesses and individuals reported a loss.[112] It shows that fraud tended towards higher losses than CM reports as the mean and median losses are higher for fraud (also illustrated in Figure 31). The statistical significance of the difference in reported loss between fraud and CM reports was formalised with a Wilcoxon rank sum test, showing a small effect (W = 619739, p-value < .05, r = -0.03). In addition, of all the crime categories considered, reports of *Business Compromise* and *Investment* fraud have the highest mean and median losses, suggesting variation across crime categories.

	n	mean	sd	median	range	skew	kurtosis
Fraud	6,820	3,653.80	18,155.31	344	854,859	28.51	1186.09
Advance-fee	1,132	2,821.50	9,793.93	300	142,999	7.50	73.44
Business Compromise	115	13,813.99	36,629.20	2,750	349,991	6.97	59.17
Card and Banking	443	2,083.15	5,552.58	400	55,322	5.60	39.02
Consumer	3,086	1,495.69	4,506.71	300	67,999	8.73	96.24
Investment	166	22,344.78	29,535.13	10,000	154,950	2.01	4.15
Other	1,164	7,611.72	36,920.11	465	854,859	18.17	387.85

[112] Includes individuals and businesses where loss > £0, n = 7,023.

Retail	465	701.97	2,678.57	70	29,566	6.66	50.67
Services	249	6,835.87	16,370.10	1,330	195,994	7.18	72.29
CM	203	2,599.16	8,276.49	200	74,539	5.95	40.57
Hacking	142	3,545.98	9,728.25	372	74,539	4.95	27.65
Malware, virus & (D)DOS	61	395.08	1,075.18	100	7,884	5.73	35.93
All	7,023	3,623.31	17,946.81	339	854,859	28.68	1206.57
Mixed MO	1,494	2,731.35	20,839.54	354	763,799	32.83	1188.39
Offline Only	1,715	5,444.23	17,320.57	344	349,999	8.33	115.18
Online Only	2,520	2,104.48	7,547.41	300	195,999	11.58	212.82

Table 28 – Distribution of loss by crime group, category and MO group.

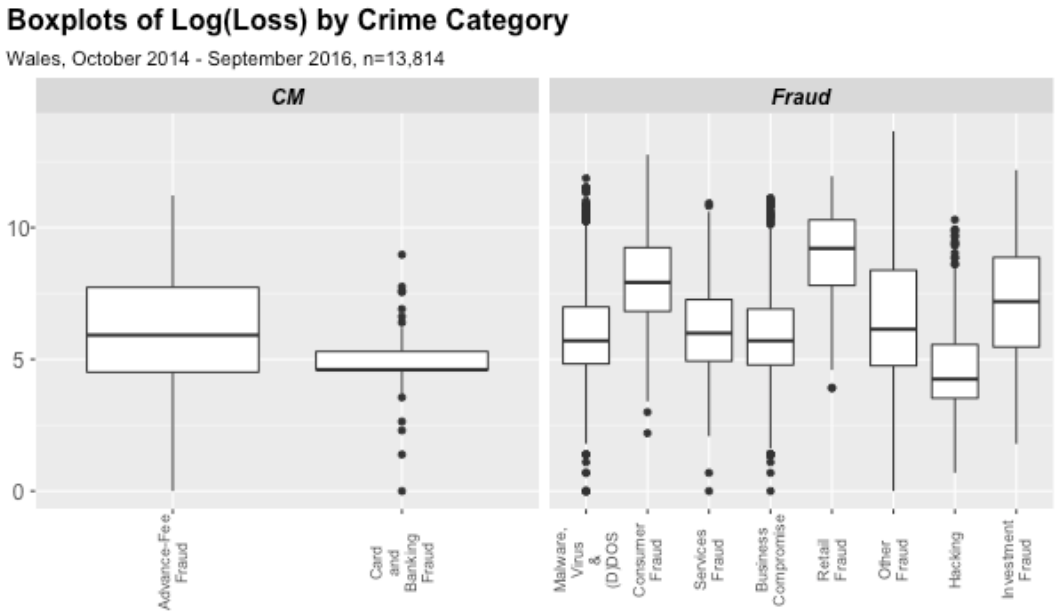

Figure 31 – Boxplot of Log(Loss) by Crime Category.

***The log transformation was applied to allow for a better visualisation, given the high dispersion and number of outliers.**

Given that this data violated multiple assumptions of the more powerful one-way independent ANOVA test, a Kruskal-Wallis test was conducted to test differences in reported loss across

all F&CM categories, resulting in a statistically significant result (χ^2 (9) = 738.79, p < .001).[113] However, given that the direction and magnitude (effect) of this result is not clearly determinable, this relationship was further explored through a chi-square. This showed a significant association between loss and crime categories, with a small effect size (χ^2 (54) = 1298.7, p < .001, *Cramér's V* = 0.18). Once again, the breakdown of this result is best illustrated in Figure 32, by the effect plot of the multinomial logit model *Loss Category ~ Crime Category* (χ^2 (54) = 1146.7, p < .001).[114]

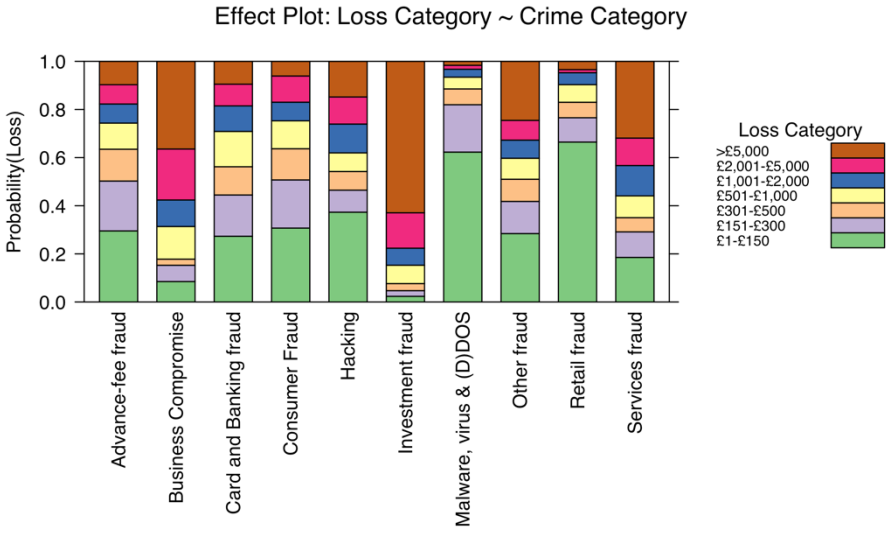

Figure 32 – MLM model *Loss Category ~ Crime Category* effect plot (Model 8).

As shown above, the greatest differences in loss reported are found with respect to *Business Compromise* fraud and *Investment* fraud on the one hand and *Malware, Virus and (D)DOS* and *Retail* fraud on the other. In the case of the first two crime categories, losses tend to be at the higher end of the scale, whereas with respect to the last two categories, reported losses tend to

[113] The lack of normality of the data is evidenced by the skew and kurtosis values across all crime categories in Table 28 and the high dispersion of the loss meant that it did not lend itself to graphical representation without a logarithmic transformation. Furthermore, as illustrated by the different sizes of the boxes in the boxplot above, there is considerable heterogeneity of variance within the loss variable across crime categories. This conclusion was formalised using Levene's test (1960), which tests the null hypothesis that the variances of the group are the same. As the test result was significant (F (9,7013) = 33.83, p < .001), it can be assumed that the variances are significantly different (Field et al, 2012, p.412).

[114] Refer to Annex IV, Part III, section 3.2.2 for Chi-squared standardised residuals and full MLM parameters.

be at the lowest end of the scale. This is confirmed by the odds ratios for each of these possibilities: the odds of a *Business Compromise* fraud report with a loss > £2,0000 are 1.85 times higher than those of a loss <= £2,000 (small effect); the odds of an *Investment* fraud report with a loss > £5,000 are 2.88 times higher than those of a loss <= £5,000 (medium effect); the odds of a *Malware, Virus or (D)DOS* report with a loss between £1-£150 are 2.73 times higher than those of a loss > £150 (small effect); finally, the odds of an *Retail* fraud report with a loss between £1-£150 are 3.92 times higher than those of a loss > £150 (medium effect).

In summary, A significant difference with a medium effect size was found with respect to whether loss or no loss was recorded across crime group and crime category. CM reports and the crime categories *Advance-fee* fraud and *Hacking, Malware, Virus & (D)DOS*, were substantially more likely to be reported without losses. Among those who did report a loss, a statistically significant but substantially small difference was found across crime group, with higher losses for fraud reports. A statistically significant result with a small effect size was also found with respect to losses recorded across crime categories. This difference was driven by *Business Compromise* fraud and *Investment* fraud on one hand and *Malware, Virus and (D)DOS* and *Retail* fraud on the other. In the case of the first two categories, losses tend to be at the higher end of the scale, whereas with respect to the latter, reported losses tend to be at the lowest end of the scale. This analysis suggests that if certain F&CM crimes types were to be prioritised *Business compromise* and *Investment* fraud should take priority. That is despite these categories, as noted in section one, being among the least frequently reported F&CM crime types. However, as discussed below, direct losses provide a limited picture of the overall impact of F&CM on individuals, even where only financial impacts are considered.

3.1.3. Loss by Individual Characteristics

As previously noted, 28.52% of individual reports reported no direct loss. Excluding these, individuals overwhelmingly reported losses at the lower end of the spectrum, although a significant minority reported large losses (Table 29).[115] Losses reported across individual characteristics are considered in greater detail in what follows.

	n	mean	sd	median	3Q	range	skew	kurtosis
Gender								

[115] Table includes cases for loss above £0; n = sample size; sd = standard deviation; 3Q = third quartile.

female	2,719	2,393.55	8,186.45	300	1,063	124,999	7.54	72.24
male	3,094	3,372.55	10,610.88	400	1,917.50	142,999	6.48	53.21
Age								
0-19	204	618.55	1,761.21	200	478.25	21,996	9.27	104.98
20-24	424	915.29	2,650.21	250	605.75	31,998	7.71	73.03
25-29	391	1,128.31	3,795.39	250	678.5	59,998	10.77	150.82
30-34	373	1,259.40	4,257.07	250	600	64,999	10.23	137.24
35-39	385	1,780.78	5,541.29	300	1,000	74,959	8.45	93.3
40-44	401	1,836.09	4,905.76	300	1,400	54,998	6.03	46.44
45-49	397	3,189.98	10,236.63	399	2,150	94,999	6.44	46.56
50-54	381	3,800.56	12,191.46	450	2,000	99,999	5.57	33.8
55-59	356	3,953.49	10,676.38	426.5	2,355	81,999	4.54	22.98
60-64	331	3,997.16	13,073.17	440	2,540.5	124,997	6.61	50.74
65-74	564	4,666.62	13,039.16	499	2,867.25	123,749	5.18	32.1
75-84	298	4,069.36	9,519.81	399.5	2,575	61,549	3.62	14.16
85+	74	7,920.58	15,382.68	725	6,446.75	79,993	2.73	7.72
Ethnicity								
BAME	253	2,708.81	7,809.45	494.00	1512	74,956	5.94	42.31
White	3630	2,727.65	9,079.87	314.00	1480.5	133,499	7.2	65.88

Table 29 - Distribution of loss by individual characteristics.

Loss by Gender

In approximately 48% of reports by male victims (n = 6,036) and 53% of reports by female victims (n = 5,787), no direct financial loss was recorded. A chi-squared test revealed that this was a statistically significant difference but represented a negligible effect (χ^2 (1) = 23.76, p < 0.001, *Cramér*'s V = 0.045).[116] Furthermore, the odds ratio indicated that the odds of a female victim reporting no loss were 1.19 times those of a male victim, i.e., a small difference.

Where a loss was recorded, there were also differences between male and female victims. As Table 29 shows, both mean and median losses were higher for males. The Wilcoxon rank-sum test was used to compare the distribution of financial loss between the two groups and yielded

[116] Chi-squared with Yate's continuity correction.

a statistically significant result but a small effect size, as indicated by Pearson's *r* (W = 3756718, p-value < .01, r = -0.092).[117]

However, given the high dispersion of the loss data, the relationship between loss and gender was also tested using the categorical loss variable. A chi-squared test revealed that the association between the gender and loss categories was a statistically significant one but represented a negligible effect (χ^2 (6) = 40.11, p < .001, *Cramér*'s V = 0.07). Furthermore, the standardised residuals indicated that this difference was driven by reports in the £1-£150 loss category being more likely from female victims, and in the £2,001-£5,000 from male victims (p < .01). As shown in Figure 33, a greater proportion of reports from female victims reported losses in the bottom category of loss. In addition, the proportion of reports from male victims is comparatively high at the top two categories of loss. However, the latter is a visibly smaller difference.

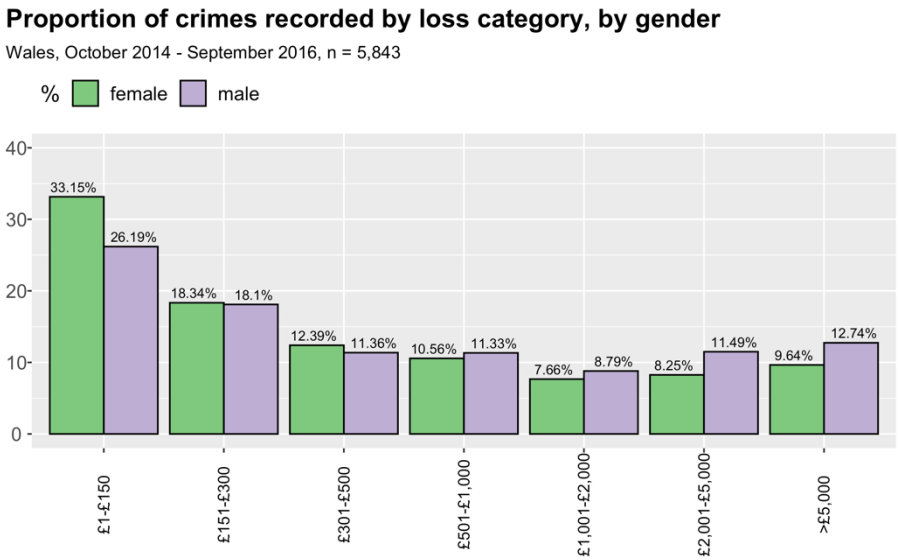

Figure 33 – Proportion of crimes recorded by loss categories, by gender.

Loss by Age

[117] Because r covers the whole range of relationship strengths, from no relationship whatsoever (zero) to a perfect relationship (1, or -1), it indicates how large the relationship between the variables studied (gender and loss) really is - and is independent of how many individuals are in the sample. Cohen (1988, 1992) provided rules of thumb for interpreting these effect sizes, suggesting that an r of |.1| represents a 'small' effect size, |.3| represents a 'medium' effect size and |.5| represents a 'large' effect size. Following the Cohen convention for interpreting effect size, this represents a small effect size as it is just above the 0.1 (+ or -) threshold. As such, while there is a statistically significant difference between the losses experienced by male and female victims, the size of this effect is small.

Some differences were observed with respect whether or not individuals reported a financial loss across age groups. The percentage of reports reporting no loss tended to increase with age category. A chi-squared test revealed that this was a statistically significant relationship with a small effect size (χ^2 (6) = 340.77, p < .001, *Cramér*'s V = 0.19). Nonetheless, this effect is clearly visible in the binomial logit model *No/Loss ~ Age Category* effect plot (χ^2 (6) = 344.1, p < .001).[118] As shown in Figure 34, the probability of reporting no loss tends to increase with age, particularly for the 50+ age groups, for whom the majority of reports are no loss reports. This suggests that factors other than the magnitude of direct financial losses influence the reporting behaviour of older age groups.

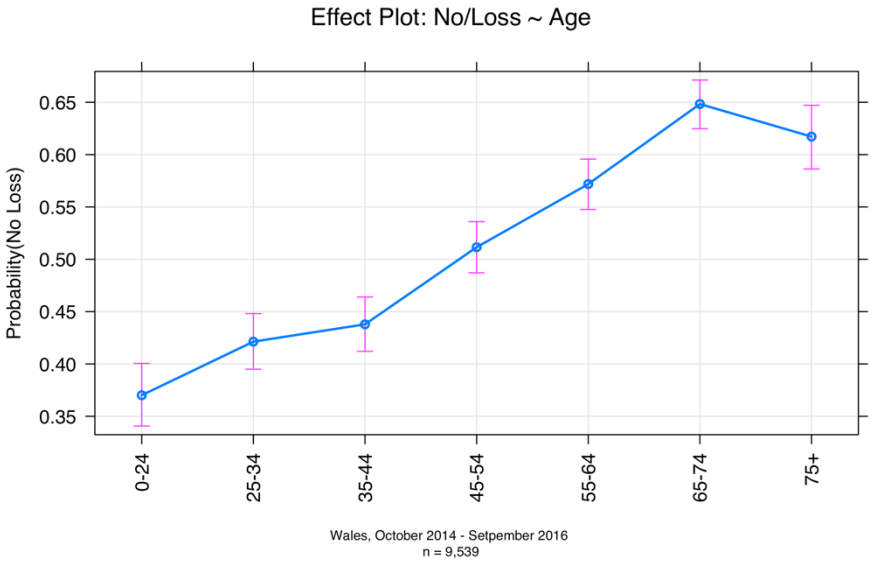

Figure 34 – *No/Loss ~ Age Category* effect plot (Model 9).

While a greater number of older victims report £0 loss, those who report losses tend to report higher losses than younger victims. In fact, Spearman's correlation coefficient identified a statistically significant positive correlation between reported age and loss, with a small effect (rho = 0.19, p < 0.01). [119] As previously, the loss category variable was used to further analysis. Here, a chi-squared test resulted in a statistically significant but small effect size, with respect to the association between loss categories and age categories (χ^2 (72) = 313.75, p < .001,

[118] Refer to Annex V, Part III, section 3.3.2 for Chi-squared standardised residuals and full MLM parameters.

[119] The Spearman Correlation Coefficient (Spearman, 1910) can be used to test relationships of correlation in data which is not normally distributed. It can range in value from −1 to +1. The larger the absolute value of the coefficient, the stronger the relationship between the variables, with a negative number indicating a negative relationship and a positive number a positive relationship. The value obtained here (0.19) therefore indicates a very small positive correlation.

Cramér's V = 0.10). Given the large number of possible combinations in this cross tabulation, it was difficult to get a clear picture of the direction of this effect from the standardised residuals. However, this became clear through interpreting the multinomial logit model *Loss Category ~ Age Category* effect plot (χ^2 (72) = 330.55, p < .001) (Figure 35).[120]

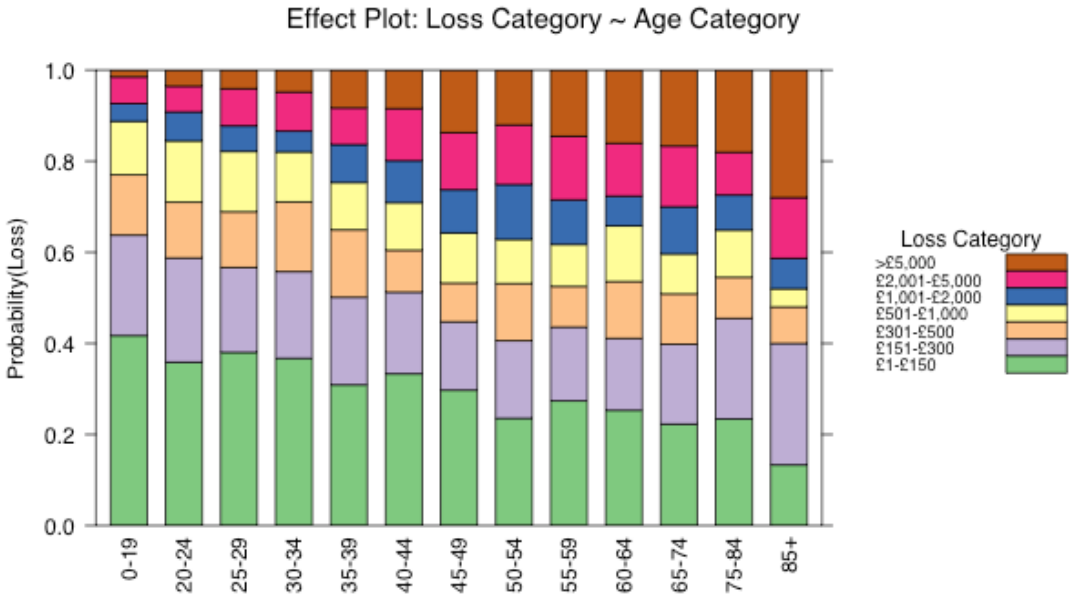

Figure 35 – *Loss Category ~ Age Category* effect plot (Model 10).

As shown, the probability of a report within the lowest category of loss decreases as age increases. Conversely, the probability of a report within the two highest categories of loss tends to increase as age increases. As such, the categorical analysis corroborates and through the effect plot above further illustrates the previously noted weak positive correlation between age and direct loss.

Loss by Ethnicity

With respect to ethnicity, 51.28% of reports from White victims were no loss reports. In contrast, only 35.04% of reports from BAME victims recorded no loss. A chi-squared test confirmed the statistical significance of this difference (χ^2 (1) = 38.58, p < .001). However, the odds ratio indicated that the odds of White victims reporting £0 loss are 1.95 times higher than those of BAME victims, representing a small effect. Furthermore, for those individuals for

[120] As above, refer to Annex V, Part III, section 3.3.2 for Chi-squared standardised residuals and full MLM parameters.

whom ethnicity was known and who reported a loss, the magnitude of reported losses did not vary greatly between White and BAME victims. This is illustrated by the relatively similar measures of central tendency in Table 9.

However, the Wilcoxon rank-sum test for non-parametric data, used to compare the distribution of financial loss between White and BAME victims, yielded a statistically significant result (albeit not at the .01 level), with a small effect size as indicated by Pearson's *r* (W = 500028, p-value < .05, *r* = -0.038).[121] Furthermore, a chi-squared test showed no significant association between ethnicity and loss category (χ^2 (6) = 11.41, p > .05).[122] As such, it was concluded that, based on the available data, there is a lack of persuasive evidence of a difference between the levels of loss reported by White and BAME victims.

3.2. Other Impacts

The thematic analysis (TA) of a sub-sample of reports added nuance to the above insights on the impact of F&CM on individuals and helped answer RQ3(ii). As previously described, a sub-sample of 332 reports (made by 160 individuals) were selected for TA. The themes identified and the number of phrases and reports coded to each theme are summarised in Table 30.[123] As shown, impacts beyond direct losses were common within the TA sub-sample. However, it should be noted that due to the purpose for which crime reports were collected (primarily to identify leads for investigation), it is unlikely that victim impact was systematically recorded. Furthermore, the TA analysis is intended to illustrate the range of impacts captured in crime reports and how they are inter-related, rather than quantify their relative frequency.

---

[121] Because r covers the whole range of relationship strengths, from no relationship whatsoever (zero) to a perfect relationship (1, or -1), it indicates how large the relationship between the variables studied (gender and loss) really is - and is independent of how many individuals are in the sample. Cohen (1988, 1992) provided rules of thumb for interpreting these effect sizes, suggesting that an r of |.1| represents a 'small' effect size, |.3| represents a 'medium' effect size and |.5| represents a 'large' effect size. Following the Cohen convention for interpreting effect size, this represents a small effect size as it is just above the 0.1 (+ or -) threshold. As such, while there is a statistically significant difference between the losses experienced by male and female victims, the size of this effect is small.

[122] As detailed in Annex V, Part III, section 3.3.4.

[123] Please refer to Annex VI for the detailed coding structure; n(victims) = 160, n(crimes) = 332.

Themes	*Definition*	*Coded Phrases*	*Coded Crimes*
Identity, privacy and liberty	The ways in which F&CM crimes impact on the identity, privacy and liberty of victims including four sub-themes: loss of personal identifiable information (PII), identity theft, invasion of private and family life and victim arrest.	44	41
Property loss or damage	Financial losses beyond direct losses, as well as wider financial impacts of F&CM. It includes the sub-themes of indirect losses (e.g. debt and cost of repairs), instances where the (totality) of direct losses are not captured (e.g. they are not known at the time of reporting or multiple losses are recorded separately), impacts on credit scores and situations where losses are devastating, vis-a-vis instances where the relative impact of the loss is small.	32	29
Wellbeing and relationships	Loss or damage to property, tangible or intangible. The types of loss or damage included digital devices being blocked or rendered unusable, loss of access to online accounts and loss or damage to digital files.	62	57
Wider financial impact	The negative impacts of F&CM on victims' wellbeing and relationships with family and friends. It includes victims' experiences of nuisance, distress and anxiety and strained personal relationships.	58	57
	Total	196	184

Table 30 – TA coding summary for impact of F&CM theme.

3.2.1. Identity, Privacy and Liberty

The first theme identified concerned how F&CM can impact on the identity, privacy and liberty of individual victims. This theme brings together four sub-themes including loss of personal identifiable information (PII), identity theft, invasion of private and family life and victim arrest. Each will be discussed in turn.

Often, in the process of defrauding or hacking, offenders obtain victims' PII such as name, date of birth, national insurance numbers etc. This can result in further victimisation as this information can be used to obtain goods and services fraudulently, e.g., through online purchases, subscriptions or credit applications. When this happens, as previous research has suggested, considerable effort to regain control of accounts and identity is then required of victims. Crime 12865 below shows how despite a relatively low direct loss (£114), a combination of F&CM has had a profound impact on the victims' privacy, whose communications were monitored inside her own home. In addition, as illustrated by the victim's personal data requests, the victim has made considerable efforts to rectify the situation, albeit to little effect.

Crime 12865

> "Victim referred by Ofcom. The victim's house, when she moved in, had a disconnected business phone line, and she has found that there were multiple occasions where people have gained unauthorised access to her broadband connection, she found suspicious activities on her iPhone, which was hacked into. The victim reported the access to her BT internet connection in [date], including to Action Fraud. Since then, further hacking has occurred, the victim moved to Sky for her broadband provider, but the hacking has continued, and a brand new desktop computer, with ethernet connection she had bought was hacked and rendered unusable. The suspects gained remote access to the computer, and from there accessed the victim's email account, purchased services from Sky and used the victim's internet service. […] The suspects also attempted to obtain credit from multiple loan companies, which were previously reported, and goods ordered from Amazon and other companies, in the victim's name using the information they obtained from the hacking. The suspects also set up direct debits using the victim's [bank] account, some were successful, […] around 70% were not [successful] but have affected the victim's credit rating. […] The victim has a range of screenshots showing suspicious activities, and unauthorised access to her account. The victim had made DSARs [Data Subject Access Requests] with her internet service providers, [loan company] and other companies whose services were accessed by suspects, providing further evidence of unauthorised activities."

This excerpt illustrates how intrusive persistent targeting can be for victims, including having one's identity used and/or devices or accounts hacked and linking F&CM to the invasion of private and family life. Personal devices and online accounts often contain detailed and very private information about the victims, their families and friends, where they live, what they like doing, personal and employment histories and more. In the excerpt from crime 12865, a large part of the victims' communications were being monitored by criminals, for the purpose of making a financial gain. In other cases, offenders use access to victims' accounts to impersonate them in communications with family, friends or colleagues via direct messages or public posts (e.g. 1055 below). In other instances, the offender might publicly leak private information about the victim (e.g. 6272).

Crime 1055

> "The suspect [victim's ex-partner] has hacked into the victims Facebook account and changed the password so that the victim can no longer access the account. The suspect has post statuses on behalf of the victim and deleted some of his friends from the profile."

Crime 6272

> "The victim feels he has had his mobile phone hacked because personal details which nobody else would know in those conversations were let out via messages through Facebook to his girlfriend who also had her account hacked. […] When the victim said

> he was going to the police the suspect deleted the messages that were sent in the hacking."

Finally, in one extreme case outlined in crime 14261 below, the victim became inadvertently implicated in criminal activity, resulting in their arrest. This situation can arise particularly where fraud victims are manipulated into laundering money. While we return to this case in chapter six, here the focus is on how, having suffered a financial loss, the victim goes on to (temporarily) lose their liberty. Being initially treated by the CJS as an offender rather than a victim, this may be seen as example of secondary victimisation (see chapter two). In crime 14261 below, it appears that money laundering (ML) charges were not pursued against the victim. However, cases reported in the media demonstrate that victims of fraud can be convicted of ML offences and/or have their bank accounts frozen and/or find themselves being refused services such as opening bank accounts or obtaining credit (BBC, 2016; Munbodh, 2019). This is particularly trying for young people who have been targeted by offenders who operate around schools and on social media (Keyworth, 2018). As such, victim involvement in ML can lead to severe secondary victimisation and other consequences and is therefore a key area for prevention interventions.

Crime 14261

> [The] victim [1] has applied for a £9000 loan online, and has then been contacted via phone by a company called "[X]". […] Shortly after this, money started arriving in her account from different sources, none of which were named as [X]. […] This incident has only come to light, as one of the other victims [victim 2], whose money was transferred into this victim's [1] account for wiring to India via Western Union, [victim 2] has reported the matter to action fraud, who located this victim [1] as the suspect account and informed Dyfed-Powys police. The police have arrested this victim [1] on suspicion of fraud, and have interviewed her, at which point, it has become clear that she is herself a victim, […].

While only one example of an arrest was found within the sample, the circumstances of several others suggested that other victims may also have been used as a 'money mules'. These included similar circumstances where 'loans' or returns on 'investments' were overpaid to the victims, as well as situations where refunds were requested on over-payments for goods and services. These examples strongly suggest connection to organised ML operations. However, further research is necessary to fully substantiate and understand the implications of this hypothesis.

3.2.2. Wider Financial Impact

The wider financial impact theme captured several ways in which recorded direct losses are imperfect measures of overall loss. There were instances where individuals were unable to confirm the level of direct losses at the time of reporting and others where the incident description mentioned indirect costs such as repairs. In the case of victims who experience a series of related crimes, their overall direct loss is not captured. In addition, to establish the impact of F&CM victimisation on a given individual it is important to consider the wider financial impact of the crime including where it leads to devastating financial loss as in crime 16847 below, to victims accruing debt or being unable to obtain future credit (e.g., CR7 below). The value of the financial loss recorded says little about each of these impacts and, as further discussed in chapter six, overall financial impact can only be understood with reference to the victim's own circumstances.

Crime 16847

> "About 4 years ago, I wanted to unify two pension funds. After [completing a] survey, online, I was contacted by a financial advisor. […] I proceeded to transfer my two pensions into pension trust [REF], the total investment was £78000ish. […]"

As noted above, the reported direct loss recorded in Crime 12865 was £114. Post-linkage, it became possible to identify a total direct loss of £813, over the six related reports made by this victim. Unsurprisingly and as will be further discussed in chapter five, for repeat victims, the total direct losses across all incidents were typically much higher than those for each individual incident. Even where total losses are calculated however, these do not capture the indirect losses such as damaged computers, the costs of changing internet providers or the financial detriment of a decreased credit rating. Additionally, some individuals go into debt to meet the demands of fraudsters and, in extreme situations, suffer devastating financial losses such as losing their entire pension savings as in the above excerpt.

As such, direct losses are not, on their own, sufficient to assess the financial impact of F&CM. As further examined in chapter six, were indirect loss and total loss across a series of related crime reports considered, it is likely that crime categories leading to property damage or with a high rate of repeats would become more prominent with respect to their financial impact on individuals. Furthermore, it is important for practitioners to be able to distinguish situations where losses are devastating or leave the victim temporarily unable to make ends meet, vis-a-vis instances where the relative impact of the loss is small.

3.2.3. Property Loss or Damage

Property loss or damage also emerged as an impact theme and included damage to computers or other devices and/or the loss or damage to intangible property such as online accounts and data stored on physical devices, cloud or web applications. As will be discussed in the next chapter, often F&CM offenders establish remote control of the victims' devices. Across a wide variety of crime categories including the most prominently reported categories of *Consumer* and *Advance-fee fraud*, there were examples of offenders rendering devices unusable through malware such as crypto-locks. As demonstrated below, this is sometimes done to extort the victim (e.g., 5116) and other times as retaliation when the victim does not cooperate with the offender's wishes (e.g., 11140).

Crime 5116

> "The victim was contacted by the suspect, claiming that there was a problem with their computer that they could fix. The suspects gained remote access to the computer and asked the victim to pay £234 for their "service". The victim gave their card details. The suspects have proceeded to take £1,234 from their account and have now locked their computer until the victim pays an additional £500 to unlock it. […]"

Crime 11140

> "[…] [The] suspect was purporting to be from Windows support. Suspect gave a security licence number and asked the victim to go to his pc. Suspect said that the victim PC had some security breaches and showed some alleged proof of this. […] Suspect said that the victim PC was about to crash, which it did and then suspect said that the victim would need to take out PC security with them for $149. Victim rang Geek Squad as he wasn't sure about it and they said that it was a hoax. Victim contacted the suspect back and said that he would not proceed with the purchase. Suspect terminated the call and locked down the victims PC so that he could not get access."

As well as loosing access to physical devices, victims may also be locked out of their online accounts (e.g., social media, payment or online marketplaces). Like situations where accounts and services are set up in the victim's name by fraudsters, re-gaining control of these accounts will likely require considerable time and effort. As it will be discussed further in chapter six, in some situations, this is despite the individual themselves having had no opportunity to stop the fraud/hack e.g., where their details were compromised in data breaches. Furthermore, while the kind of property loss/damage discussed here requires hacking to occur (i.e., the offender gains unauthorised access to a computer system, through social engineering or more technical means), as discussed in the next chapter, F&CM and online/offline MOs often go hand in hand

and cannot meaningfully be separated. Given the prominence of mixed MOs, this theme cuts across instances of both fraud and CM. Furthermore, as with financial impact, the impact of loss/damage to property is relative to the individual's circumstances. The loss of this very file for instance, may result in a previously inspired portion of writing being lost. However, the multiple paranoid backups which any researcher of online crime keeps, would considerably limit the loss. Such precautions are not widespread, however, and the loss of work and personal files can be irreparable. Furthermore, offenders may seek to extort victims for the restoration of access to files and accounts. Interestingly, of all the cases which reported devices being locked, none mentioned a victim yielding to any subsequent extortion. This suggests that either extortion is rarely successful, or alternatively, that where it was most effective, victims did not report the crime.

3.2.4. Wellbeing and relationships

The knowledge that personal information is being maliciously accessed will inevitably cause victims distress and anxiety, particularly where offenders persist in targeting the same individual over again. Reports of persistent contact by the offenders suggest that this type of victimisation is, at the very least, a nuisance, even if no financial loss is experienced. However, some victims indicated being distressed by the repeated contacts (e.g., 14084). Furthermore, in some cases the nuisance is aggravated by threats of violence as illustrated in crime 10531.

Crime 14084

> "[Victim] has been getting contacted repeatedly by all different companies cold calling her, the victim advised that on one call they had used sexual language towards her, the victim has advised that she is disabled and has suffered from 2 major strokes and that these calls are becoming too much for her […]."

Crime 10531

> "[Asset Management Company X] contacted victim saying shares are still active from a previous fraud with [Asset Management Company Y]. If victim pays £1800 up front for legal fees so he can come back with us (…). Suspect threatened to send someone round to gang rape victim if victim didn't pay up, victim contacted local police about this as he was concerned, they said they don't think anyone will come."

As discussed in the next chapter, MOs often include a "honeymoon" period where fraudsters build a relationship of trust with victims, followed by a change in the emotional register of the interaction, where fraudsters themselves express distress or behave in a threatening manner to manipulate/intimidate victims. Given the reference to a previous fraud, crime 10531 above

implies a long-term relationship and explicitly illustrates the threatening turn with the suspect threatening to "send someone round to gang rape" the victim. The experience of manipulative and threatening tactics is inevitably upsetting for victims. This will be especially acute in the case of romance fraud, where victims are emotionally invested in a relationship which is revealed to be based on deceit and turns abusive.

A 'threatening turn' can also lead to experiences of fear**.** In 10531, however, the expression of "concern" appears somewhat euphemistic given the seriousness of the threat. It also appears that the victim was directed to make a report via AF, with no further action recorded after this report, suggesting that the seriousness of the threat was toned down through the victims' interaction with the local police and AF. However, it is worth considering whether a threat of rape in a context other than F&CM victimisation would be similarly dismissed.

As well as emotional distress, F&CM victimisation can also result in strained relationships with friends and family for victims, as illustrated in the excerpts from a repeat victim below.

Crimes 15228 / 15852

Report 1:

"The victim is vulnerable due to learning difficulties has been befriended by men on Facebook and has been duped into sending large amounts of money to them in Nigeria and Pakistan. […] The victim being on low income and residing with her mother, has borrowed from her family and requested large amounts of money in order to send to these males, unaware of the implications of befriending person/s unknown due to her vulnerabilities. […]"

Report 2:

"(…) [The Police] spent several hours and several visits explaining to [XXX] this is a scam, and she still refuses to believe it's a scam. I visited her on Monday and spent an hour explaining again it was a scam, but as soon as I left she went to the bank and transferred the scammer a further £210 by Western Union. We reported this to the police again, and [PCXXX] visited [XXX] this afternoon. She explained again that this is a scam and to stop sending them money, but [XXX] still thinks she is getting a 6 million pound inheritance. [PCXXX] is completing a referral to social services."

The first excerpt above is from the second in a series of three reports over a period of 10 days, made by family members on behalf of a victim who was being repeatedly targeted by fraudsters. Across the three reports, the total direct loss reported was £6,800. Furthermore, the first report in the series mentions previous similar instances of victimisation, not captured within this sample. As noted above, the victim has limited financial means and borrowed money from her mother to meet the demands of fraudsters, which will inevitably lead to

tensions within the home. In addition, the frustration of the reporting family member vis-à-vis the victims' continued engagement with the fraudsters, is clear in the second excerpt. This illustrates how the focus is on the victim's rather than the offender's actions and the strain this victimisation experience created between the victim and her family. Furthermore, the mention of a referral to social services suggests the possibility that the victim may increasingly come under institutional surveillance and potentially lose some autonomy – a cruel irony considering that none of these reports were disseminated for investigation and thus the apprehension of the offenders is but a remote possibility.

Across many cases such as the ones mentioned above, it was implied that repeat targeting by offenders caused victims considerable nuisance. In other cases, threats and abuse from offenders left victims distressed and/or even in fear of physical violence. In such circumstances, there is a risk that the victim's distress will not be taken seriously, given the prevalence of online or remote forms of interaction between victim and offenders and the prioritisation of personal and violent crime. However, given the erosion of the online/offline and remote/face-to-face dichotomies discussed in the next chapter, any assumption that there is no objective threat, even if the victim subjectively believes there is, may be misplaced. Furthermore, de-valuing the victim's subjective experience is not compatible with the Victims' Code, which requires that all victims be treated with dignity. Lack of empathy with victims on the part of CJS representatives constitutes a form of secondary victimisation. Finally, there were instances where being victimised resulted in deteriorating relationships between victims and their family and friends, especially in the case of so-called 'chronic victims'. As will be discussed in chapter six, however, support from family and friends is an important aspect of increasing resilience to F&CM. As such, in some cases, it is suggested that there may be a role for support services in engaging with the family and friends closest to the victim and challenge any misconceptions about F&CM victimisation which may be contributing to the deterioration of victims' personal relationships. In addition, where necessary, victim support may be able to refer the victim and others to mediation services.

3.3. Impact Across Crime Categories

3.3.1. Impact of Fraud Categories

As illustrated in Figure 36, the losses reported by individual victims of *Investment* fraud were generally higher than those reported by victims of other fraud types. The highest median loss

was for cases of *Investment* fraud (median loss £9,851), while the lowest was for cases of *Consumer* fraud (median loss £300). However, substantially more cases of *Consumer* fraud with losses were reported by individuals within this sample, so that the total losses reported by all individuals were greater for *Consumer* than *Investment* fraud (respectively £4,286,460 and £3,329,824). A Kruskal-Wallis test was conducted to test differences in reported loss across all Fraud categories, resulting in a statistically significant result (χ^2 (5) = 278.68, p < .001).

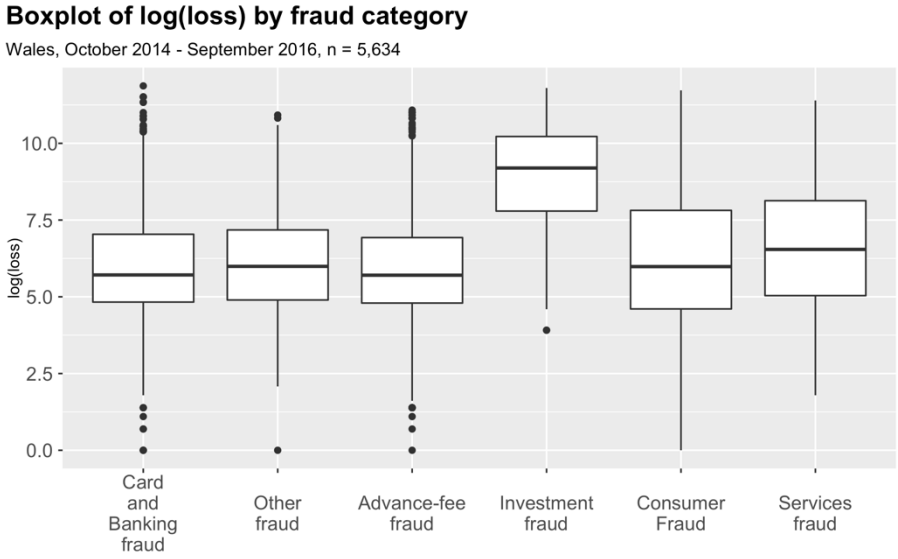

Figure 36 – Boxplot of Log(Loss) by Fraud Type for individual victims.

***The log transformation was applied to allow for a better visualisation, given the level of dispersion and the number of outliers.**

Furthermore, while some statistically significant differences were found with respect to the losses reported across gender, ethnicity and age, these all had small substantial effects. The statistical significance of the difference in reported loss for males and females was formalised with a Wilcoxon rank sum test, showing a small effect (W = 3519596, p-value < .01, r = -0.09). While a similar test also found a statistically significant difference in reported fraud losses across White/BAME ethnicity, the effect size was negligible (W = 479178, p-value < .05, r = -0.03). Finally, with respect to age, as previously tested, the Spearman's correlation coefficient identified a positive correlation between reported age and loss, but this represented a small effect (rho = 0.19, p < 0.01).

In addition, a summary of the impacts coded for each fraud category through the thematic analysis highlights that some were more common in relation to specific crime categories. As shown in Table 31, impacts within the theme of identity, privacy and liberty were observed

predominantly with respect to *Services* fraud, whereas property loss or damage was more common amidst cases of *Consumer* fraud. Furthermore, there was evidence of all fraud types having an impact on wellbeing and relationships, as well as wider financial impact. Nonetheless, impacts on wellbeing and relationships were most common among cases of *Consumer* and *Advance-fee* fraud and wider financial impacts were most common with *Consumer* fraud. These themes were explored in detail in the previous section.

	A : Identity, privacy and liberty	**B : Property indirectly lost or damaged**	**C : Wellbeing and relationships**	**D : Wider Financial impact**
Advance fee	1	0	17	6
Card and banking	10	1	4	4
Consumer	6	12	22	22
Investment	0	0	8	4
Other	0	1	13	4
Services	21	0	3	2

Table 31 – TA coding summary for impact theme by fraud category (phrases coded).

3.3.2. Impact of Computer Misuse Categories

As shown by the last row of Table 32, the typical level of direct financial loss was found to be much greater for victims of *Hacking* than those of *Malware, Virus & (D)DOS*. In addition, for victims of *Hacking* there were also significant variations in the typical level of loss across victim gender and age. The table also shows highly divergent median loss values for reports of Hacking across age and gender, in contrast to comparable median loss values for *Malware, Virus & (D)DOS*. Given that only one report of CM with a loss was made by a BAME victim, no such comparison was possible with respect to ethnicity.

	Hacking			**Malware, Virus & (D)DOS**		
	n	mean	median	n	mean	median
Age						
0-24	6	1893	214	5	198	100
25-34	13	542	145	4	186	100
35-44	23	1112	269	9	1043	100
45-54	25	951	130	6	417	100
55-64	19	3303	1899	15	314	150

	Hacking			Malware, Virus & (D)DOS		
65-74	7	1535	499	5	146	100
75+	7	5005	3210	4	361	172
Ethnicity						
BAME	1	3755	3755	0	n/a	n/a
White	80	1888.78	329	38	457.24	100
Gender						
Female	64	2088.45	225	28	528.71	100
Male	67	3926.27	700	31	238.42	100
All victims	131	3028.40	349	59	376.19	100

Table 32 – Distribution of loss for CM categories.

In addition, a summary of the impacts coded for each CM category through the thematic analysis suggests that *Hacking* has a wider variety of impacts than the *Malware, Virus & (D)DOS*. As shown in Table 33 however, few CM cases were coded thematically as having impacts other than direct financial loss. Given the close links between online/offline MOs shown in section four below and the prioritisation of fraud as the main offence in many cases, this may simply result from recording practices whereby higher impact cases tend to be recorded as fraud rather than CM, even if CM offences are also involved.

	A : Identity, privacy and liberty	*B : Property loss or damage*	*C : Wellbeing and relationships*	*D : Wider Financial impact*
Hacking	6	7	2	13
Malware, Virus & DDOS	7	1	3	0

Table 33 – TA coding summary for impact theme by CM category (phrases coded).

The following excerpts illustrate the wide range of impacts of CM crimes on victims. Crime 644, categorised as Hacking, provides an example of an adverse impact on the victims privacy and personal information at risk, with suspects having access to her online banking, driving license, email and Skype accounts. In the example of crime 9621, malware damaged the victim's device. The next excerpt (crime 10939) describes the victim being repeatedly targeted, which she connects with experiences of bullying on social media, which while not explicit, was interpreted as having a detrimental impact on the victim's wellbeing. Furthermore, it should be noted that victims were not explicitly asked, at the time of data collection, about the impact of the crime on their wellbeing – although this can reasonably be assumed based on any of the

excerpts below. Finally, in the previously mentioned crime 12865, demonstrates the wider financial impact which fraud, in that case linked to hacking, can have on victims – as well as the privacy risks and the time and effort victims must dedicate to rectify situations. These excerpts show that the impact of CM on victims goes far beyond direct financial losses. For a full discussion of each of the impact themes identified however, please refer to the previous section.

Crime 664

> "The victim has received a call purporting to be from Windows support/Microsoft and saying the computer was running slowly and they could fix it and asked the victim to log onto the website to allow access so they could fix it. The victim allowed access and entered her credit card details on the screen while speaking to the suspects at the same time as they were on the computer. […] Driving licence given as well. The victim's email address was hacked into at the same time as well as her skype account."

Crime 9621

> "The victim was using her iPad [for] browsing online last night when a message took over the screen saying that she was going to be investigated by Interpol. The message was advising that she had been viewing things illegally online and that if she was found guilty of this, she would face 3-7 years in prison or faces a fine of £100 - £250." […]

Crime 10939

> "I had rent payments set-up by direct debit to [XXX] Housing Association allegedly go missing []… I believe that all my accounts have been hacked Hotmail account, Facebook, phone. I had also noted an account taken out for a TalkTalk account, on [date] a pack was sent out, I rang to cancel. [I also received] unwanted invites/contacts on my Facebook account invited in by others [account names] [including] nasty obscene comments reported personal comments-ageist."

4. Victim Profiles

Drawing from the insights in previous sections of this chapter, this section brings together both quantitative and qualitative insights to construct, to the extent that it is possible, a summary of the typical victim of fraud and of CM, taking into account victim crime categories, victim characteristics and the typical impact of these crimes on victims.

4.1. The Typical Victim of Fraud

As well as looking at differences between profiles of fraud and CM victims, the typical victim profile for each crime category was also explored. Table 34 summarises the typical victim profile for each fraud category in this study, with some small variations in age, ethnicity, gender and the levels of loss reported. As previously noted, the probability of reporting a *Consumer* fraud drops considerably for the 75+ victims, while the probability of reporting an *Advance-fee* fraud increases linearly with age, from age 45 onwards. To the extent that some differences were found across ethnicity and gender, these were driven by reports of *Advance-fee* fraud being predominantly from white females, while the reports of *Investment* fraud were predominantly from males (of any ethnicity). With respect to direct losses, *Investment* fraud stands out as the crime type with the second greatest proportion of cases with a loss (67.66%) and the highest median loss (£9,851). With respect to *Card and Banking* fraud, while the proportion of cases reporting a direct loss is somewhat greater (70.5%), this is likely due to individuals being referred to their banks for reporting in the first instance. Finally, a wide variety of other impacts were identified via the thematic analysis with respect to all types of fraud and Table 34 identifies the most commonly coded theme for each fraud type.

	Age	*Ethnicity & Gender*	*WIMD & Net access*	*% Loss*	*Median Loss*	*Common other impacts*
Advance-fee	45+	White Female	Any	41.50	£400	Wellbeing and relationships
Card and Banking	Any	Any	Any	70.51	£397	Identity, privacy and liberty
Consumer	< 75	Any	Any	54.35	£302.5	Wellbeing and relationships; Wider financial impacts
Investment	Any	Any Male	Any	67.66	£9,851	Wellbeing and relationships

Other	Any	Any	Any	51.09	£300	Wellbeing and relationships
Services	Any	Any	Any	57.91	£695	Identity, privacy and liberty

Table 34 – The typically recorded victim of fraud.

4.2. The Typical Victim of Computer Misuse

Table 35 summarises the typical victim profile for each CM category. Overall, while victims of CM were typically younger than fraud victims, no substantial difference was found between victims of *Hacking* and *Malware, Virus & (D)DOS* with respect to the demographic characteristics of age, ethnicity or gender. As such, compared to fraud victims, the profiles of CM victims were less distinct. However, the typical direct loss incurred by victims varied significantly across gender and age, for *Hacking* victims. Finally, while cases of CM presented less evidence of impacts beyond direct financial loss than those of fraud, it should be noted that there will be cases where a main offence of fraud is recorded but they nonetheless involve a CM offence within their MO (e.g., in the case of Computer Software Fraud, classed in this study within *Consumer* fraud).

	Age	*Ethnicity & Gender*	*WIMD & Net Access*	*% Loss*	*Median Loss*	*Common other impacts*
Hacking	< 65	Any	Any	20.25	£225 (females) £700 (males)	Wider Financial impact
Malware, virus & (D)DOS	< 65	Any	Any	18.79	£100	Identity, privacy and liberty

Table 35 – The typically recorded victim of CM.

5. Conclusion

This chapter has focused on exploring the volume, impact and victim characteristics associated with F&CM victimisation and discussing the implications of these findings for policy and practice. In doing so, it has answered research questions one to three and sub-questions, thus contributing towards meeting the first aim of this thesis. It has also examined reporting patterns, against the backdrop of wider demands on the police and other CJS agencies, as well as local demographic characteristics. It started by demonstrating the volatility of AF data to external events, such as the AF call centre crisis in the summer of 2015. As such, sharp changes in reporting volumes must be interpreted with caution. Where events attract considerable media attention, for example high-profile data breaches or COVID19, these may also impact on reporting behaviour and practices, creating challenges but also opportunities to anticipate and optimise victim response. At the same time, although F&CM reports represent a small proportion overall crime in Wales, the recording rate of fraud found was higher than most other property crimes and increased visibly between the first and second years of the sample. As such, despite its demonstrable under-reporting, fraud remained among the top property crimes reported to law enforcement in Wales. As noted, a proportion of CM incidents will be registered as fraud due to the 'principle crime' rule. Nonetheless, ensuring victims of fraud are provided with an adequate response is therefore not just about meeting individual victims' needs, but vital to continued public trust in the CJS.

Furthermore, this chapter has raised questions about which victim groups may be over and under-represented within F&CM reports in Wales, highlighting key areas for further research. With respect to fraud, it suggests that while younger groups suffer the highest proportion of victimisation, it is older groups who tend to report being victimised. However, while older individuals are over-represented in the sample of reports, this is driven by fraud reports. At the same time, the relatively large number of males in the oldest categories (75+) may indeed reflect a higher likelihood of F&CM victimisation for the oldest males. As such, further research is needed to examine the interaction effect of age and gender with respect to F&CM victimisation, vis-à-vis reporting behaviour. Nonetheless, fraud prevention campaigns would do well to target older males. At the same time, to develop a better picture of the scale and nature of fraud, these results suggest that campaigns to raise awareness of the importance of reporting may be better targeted at younger individuals, among which under-reporting appears more acute.

In addition, no differences were found with respect to gender and, subject to considerable caveats given the level of missing values in the sample, the proportion of reports from BAME individuals broadly reflected the proportion of the BAME population in Wales, as estimated in the last census. That said, this discussion has raised new questions with respect to the experiences of race and gender and how their may intersect with F&CM victimisation in Wales. Finally, while no significant differences were found with respect to overall levels of deprivation and internet access in areas where F&CM were recorded, future research might compare the local characteristics of areas with high levels of F&CM to reporting of other crimes. Nonetheless, this analysis demonstrates that far from 'typical', victims of fraud known to the CJS are overwhelmingly older, victims of CM overwhelmingly young and both are primarily Caucasian. Following Grabosky and colleagues (1998; 2001), that F&CM victims have somewhat different profiles than victims of other crimes, does not necessarily mean that their victimisation cannot be understood through an RAT lens. However, as summarised below, the case for these victim 'profiles' was relatively weak. Furthermore, as the next chapter will show, 'the victim' is often not a singular, human, agent.

Alongside volume and patterns of reported victimisation, this chapter considered the impact of F&CM on victims. Firstly, it corroborated previous findings (Elkin, 2020), showing that direct financial losses experienced by victims were concentrated at the lower end of the spectrum, with a small number of victims reporting high losses. While on average business losses were higher, the most typical losses for individual and business victims were similar. At the same time, the highest losses were found to be associated with the least commonly reported crime types including *Business Compromise* and *Investment* fraud. As such, high-volume categories of F&CM are not necessarily the ones with the greatest impact. Reflecting previous research (summarised in Button & Cross, 2017), thematic analysis of a sub-sample of incident descriptions identified four key themes characterising the impact of F&CM on individuals, beyond direct losses. The first theme brought together different ways in which F&CM can impact on the identity, privacy and liberty of the victim including through loss of personal identifiable information, identity theft, invasion of private and family life and ultimately the victim being arrested. The first three are of course intimately connected and frequently re-occurred within the sample. They are also of great relevance to the 'protect' strand of policing (see chapter one) as they often result in repeat victimisation. As such, on reporting, victims would benefit from guidance on what can happen to their lost information and what steps to

take to mitigate the risk of future targeting. Individuals should also be made aware of offenders' common MO of using unwitting victims as 'money mules'.

While the impact of F&CM on victims has been clearly illustrated, this chapter has also shown that the data collected when a crime is recorded is not optimised to establish the relative impact of the crime victims. The key issues affecting the quality of crime data are identified in the literature (e.g. Hope, 2007; Levi & Burrows, 2008) and include misalignment between rules of inclusion/exclusion within an administrative (in turn linked to purposes of data collection) and the information which is needed for analysis. At the time of data collection, some limited information on the victim's own self-assessment crime impact and their own vulnerability was collected by AF. However, this information was not passed onto the forces responsible for the victim-response. Since then, local forces have begun to receive information about how the victim scores the impact of the crime across several dimensions including impact on health, finances and confidence. As such, future research using AF data will be able to provide further insights on the impact of F&CM on individuals. Nonetheless, in line with the discussion in chapter one, the information that is collected from the victim when the crime is first recorded is considerably oriented towards 'Pursue' rather than 'Protect' aims. As such, more can be done to optimise the information collected on F&CM impact, to enable a victim-focused response.

Finally, the results of the above analysis were brought together to develop 'typical victim' profiles. The initial aim of this exercise was to provide an informed starting point to ensure the effective targeting of prevention advice. These were not meant to be rigid as inevitably, each victim will have their own subjective experience and personal circumstances to contend with, often eroded by the averaging effects of statistical analysis. In addition, victim profiles may change over time and therefore patterns of victimisation should be continuously monitored. Having analysed the sampled data however, the limitations of these 'victim profiles' are considerable. Firstly, given the high levels of under-reporting, they are indicative of patterns of F&CM recording, but not necessarily of victimisation. Secondly, with the exception of age, no demographic factors were substantially associated with specific F&CM categories. While many were statistically significant, all the associations found had relatively small effects. In addition, the impact of crime on victims will vary depending on their personal circumstances. As such, the case for targeting specific groups for prevention advice based on profiles from reported crimes is weak. Assessing the relative impact of F&CM on victims and the likelihood

of repeat victimisation of specific victim groups, may be better ways to prioritise support and target prevention initiatives.

CHAPTER 5: Crime Mechanisms and Repeat Victimisation

Firstly, section one of this chapter adds to previous research describing the 'anatomy' of F&CM crimes (Whitty, 2015a), in the context of the previous theoretical discussion on 'hybrid' crimes in a digital society. It addresses RQ4 on the characteristics of the criminal Modus Operandi, with a particular focus on online/offline dynamics (RQ4i-iii), before turning to the broader features of these crimes (RQ4iv). Secondly, as discussed in chapter two, little is known about the profiles of repeat victims, or the mechanisms of F&CM repeat victimisation. Section two of this chapter addresses this research gap. To do so, F&CM reports from individual victims pertaining to three Welsh police forces (Dyfed/Powys, Gwent and South Wales) were linked to identify reports made by the same victim.[124] Thus, this chapter addresses RQ5 on the extent of repeat victimisation (section 2.1), RQ6 on the characteristics of repeat victims (section 2.2), RQ7 on the impact and RQ8 on the time-course of repeat victimisation (section 2.3), as well as RQ9, which focused on the mechanisms of repeat victimisation (section 2.5). Before presenting the results and discussion however, the relevant research questions will be re-stated in full, and the methods used in this chapter summarised.

Research Questions

RQ4: What online/offline dynamics enabled F&CM in Wales, over the reference period?

i. Was there an association between the online/offline Modus Operandi (MO) and victim characteristics?
ii. What online/offline dynamics characterised each of the crime categories considered?
iii. To what extent were online/offline elements driving these crimes?
iv. What other the key MO features can be identified? (qualitative)

RQ5: What was the extent and nature of individual F&CM repeat victimisation (RV) in Wales?

i. What is the extent of RV within the sampled data?

[124] As noted in the methodology section, reports from North Wales were excluded from the repeat victim analysis on the basis that the large proportion of missing values within linkage variables skewed the results of the linkage. This high proportion of missing values resulted from the extra processing which the North Wales data underwent between collection by Action Fraud and supply for the purposes of this research. A combination of exact and probabilistic linkage techniques was used to identify crimes reported by the same individual, see methodology, section 4.2.

ii. Did the distribution of RV vary across crime categories?

RQ6: What were the characteristics of repeat victims?

i. What were the demographic characteristics of repeat-victims and how did these differ from one-time victims?
ii. Did RV vary with respect to the local area's socio-economic profile and level of internet access?
iii. Which crime categories and victim characteristics were best suited to predicting individual RV?

RQ7: What was the impact of RV?

i. Was there an association between RV and the financial loss suffered by victims?
ii. What other RV impacts can be identified from F&CM crime reports?

RQ8: What was the characteristic time-course of RV?

i. What was the overall/typical time-course of RV?
ii. Did the distribution of time-course vary across crime group/category?

RQ9: What were the mechanisms through which RV happened? (qualitative)

Methods Summary

Similarly to the analysis presented in the previous chapter, to answer research questions RQ4 to RQ8 and sub-questions, a mix of bi-variate and multi-variate analysis was carried out on a sample of Action Fraud crime reports, made by victims within the Wales, between 1st October 2014 and 30th September 2016 (the reference period). RQ4 was answered using the full sample n = 17,049 cases, (of which n = 11,844 were identified as pertaining to individual victims). As with chapter four, bivariate relationships were tested using the appropriate statistical tests and measures of statistical significance and effect size are provided throughout. Annex III includes a list of all dataset variables including classification (e.g., numeric, categorical etc), along with variable descriptions. Statistical significance is measured through p-values, whereas effect size was interpreted with reference to the measures and guidelines in chapter three, Table 10 (see section 4.1.2). Effect plots of generalised linear models (GLMs) were also produced where traditional bivariate analyses was inconclusive with respect to the size and/or direction of the effect, particularly for chi-squared tests on larger than 2x2 contingency tables.

As discussed in the methodology, the analysis pertaining to repeat victimisation (i.e., RQ5 to RQ8) was limited to the reports made by individual victims within three out of the four police forces (Dyfed/Powys, Gwent and the South Wales), a total of n = 10,001. were linked using a combination of deterministic and probabilistic data linkage, using the R package *RecordLinkage*. This method allowed the author to identify reports made by the same victim within the reference period. The quality of the linkage was tested using two commonly used linkage quality metrics, precision and recall (or sensitivity), based on the clerical review of a sample of 100 pairs of matches. Although both precision and recall were estimated at 100%, the linkage method was optimised to minimise false-positive matches and thus may have yielded false-negatives (missed matches) which were not captured in the reviewed sub-sample. Following the data linkage, bivariate statistical analysis and GLMs were used to explore patterns of repeat victimisation.

Finally, thematic analysis of a sub-sample of incident descriptions (332 incidents reported by 160 victims) was undertaken to answer RQ9. As with chapter four, TA was conducted in six stages, adapted from Braun and Clarke (2006, 2012, 2013).

1. Recorded Modus Operandi Features

This section addresses the fourth research question (RQ4), by identifying the criminal tactics/mechanisms which enable F&CM, with a particular focus on the online/offline dynamics. The key features of the Modus Operandi (MO) of the reports of F&CM sampled were explored both quantitatively and qualitatively. The nature of the online/offline dichotomy was explored primarily through the quantitative coding of crime reports. In addition, the thematic analysis (TA) of a sub-sample of reports added nuance to the quantitative insights and allowed for a broader exploration of crime enablers and offender tactics. In line with Powell et a. (2018) and the discussion in chapter one, this section highlights the inadequacy of the online/offline dichotomy in relation to F&CM victimisation. It also highlights how Gibson's (1986) concept of technological affordances can help understand crime mechanisms in the digital society. The results of this analysis and its implications for theory and practice are presented in what follows.

1.1. The Online/Offline Dichotomy

As previously discussed, the widespread use of the term 'cybercrime' rests on the distinction between 'online' and 'offline' crimes, based on their *Modus Operandi* (MO). To the extent that cybercrime is a policy priority, what constitutes cybercrime will impact on the availability of police resources and wider investments. However, this dichotomy is increasingly being challenged (Furnell & Dowling, 2019, Powell et al., 2018). As such, to explore the prevalence of online/offline elements and their inter-relation, each case was (quantitatively) coded according to whether significant online or offline elements were present, into the categorical variable 'MO group' (see methodology). The analysis that follows demonstrates that in practice, determining what constitutes 'cybercrime' is not straightforward. As illustrated in the graph below (Figure 37), a significant proportion of reported cases of F&CM contained mixed online and offline elements, most acutely for business victims.

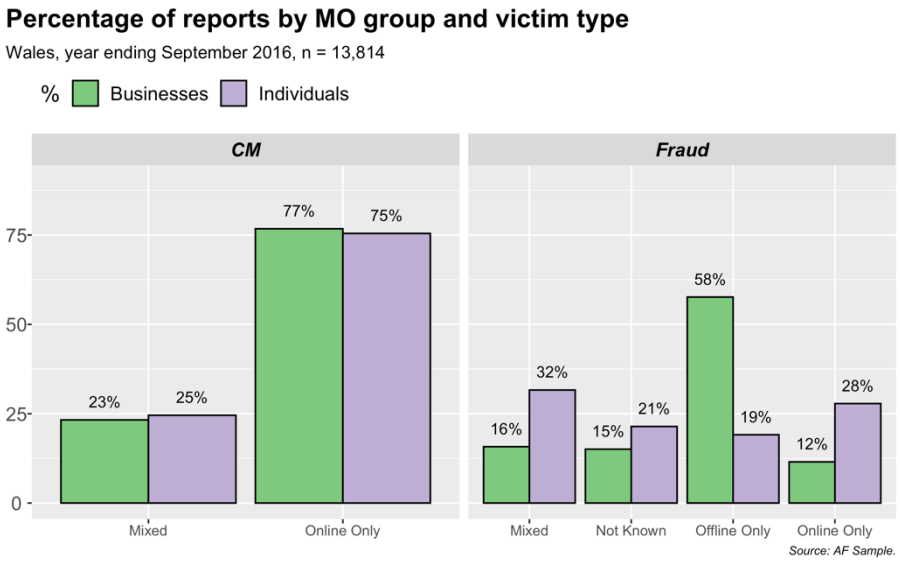

Figure 37 – Percentage of reports by MO group and victim type.

It was not possible to determine MO Group for a large proportion of cases (19.68% of individual and 14.42% of business reports), which is a considerable limitation. In future research, the number of unknowns may be reduced by taking into account Action Fraud variables concerning the first mode of contact between victim and offender (including email, web forum, chat room or similar, visit to a website, phone call, text message or similar, letter or fax, among others) and the type of enabler in the case of fraud (e.g., email, postal service, in person etc.). However, these variables were not supplied to the local forces and thus could not be considered in this study. Nonetheless, assuming the missing values are randomly distributed

across MO group, the predominance of mixed MO raises questions about the often-used dichotomy between online/offline crime. This section will thus further examine MO Group (online/offline/mixed MO) in relation to crime group (Fraud/CM), trends over time and associated individual victims' characteristics.

1.1.1. Crime Group & Crime Categories

The extent to which crimes recorded across crime group (Fraud and CM) were identified as containing online, offline or mixed elements (Figure 37) and is further summarised in Table 36, including observed frequency (n), percentage and standardised residuals.

	CM			**Fraud**			
	Mixed	**Offline**	**Online**	**Mixed**	**Offline**	**Online**	**Not Known**
Individuals							
n	236	0	725	3442	2080	3030	2331
%	24.56	0	75.44	31.63	19.11	27.84	21.42
Businesses							
n	20	0	66	297	1086	217	284
%	23.26	0	76.74	15.76	57.64	11.52	15.07
Overall							
n	256	0	791	3739	3166	3247	2615
%	24.45	0	75.55	29.29	24.80	25.73	20.48
St. Res	-9.13	-24.16	31.45	9.13	24.16	-31.45	NA

Table 36 – Reports by MO and crime group (businesses and individuals).

The high level of mixed fraud observed (30%) is not surprising, as fraud MOs have been found to straddle the on/offline divide (e.g., Button, Lewis, Tapley, 2012; Gini, Card Noel, Pozzoli, 2017). The difference between the frequency of MO group categories across F&CM cases was confirmed as significant with chi-squared test, with a medium effect size (χ^2 (2) = 1088.3, p < .001, *Cramér's* V = 0.29). Unsurprisingly, the standardized residuals in Table 16 indicate that this difference was driven by fraud reports being significantly more likely to present Mixed or Offline only MOs, whereas CM cases were significantly more likely to present an online-only MOs (p < .001).[125]

[125] Refer to Annex V, Part IV, section 1.1.1 for chi-squared calculation in full.

Nonetheless, a substantial proportion of CM cases (24.45%) also had mixed elements, which lends support to the hypothesis that the on/offline dichotomy is also blurred in the case of CM victimisation. A more nuanced analysis is possible by considering the patterns found with respect to online/offline/mixed coding in reports from individual victims across specific crime categories – albeit with considerable caveats given the high proportion of 'not knowns' (Figure 38). Despite the limitations imposed by the missing values, a greater proportion of *Hacking* cases appear to have a Mixed MO than *Malware/Virus & (D)DOS*. In addition, *Consumer* fraud stands out among fraud categories, for the high proportion of mixed or online-only MOs.

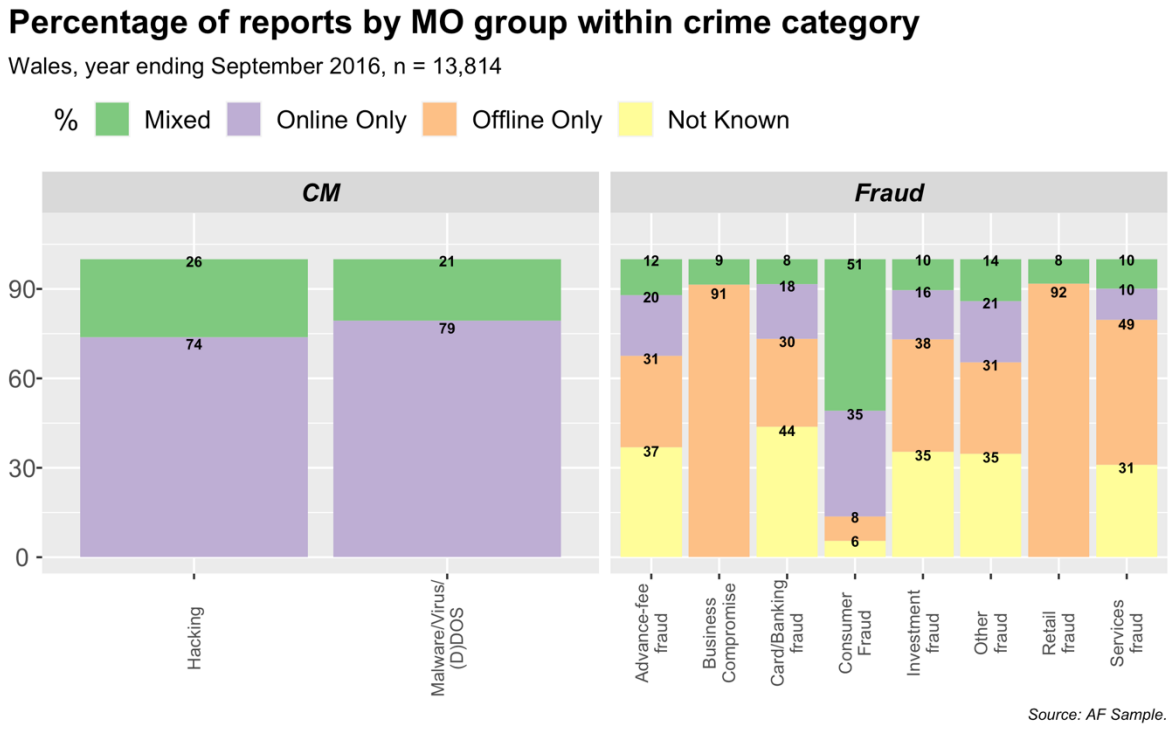

Figure 38 – Percentage of victim type by MO group and crime category.

All cases in categories *Malware, Virus & (D)DOS* and *Hacking* were, by definition, coded as 'online'. Nonetheless, over 20% of cases in both categories had mixed MOs, suggesting an on/offline interaction. As such, over 1/5 of CM cases reported by individuals presented offline elements. Additionally, most fraud types (except *Retail* fraud) had some online elements (ranging from 20% for *Services* fraud, to 86% of *Consumer* fraud, calculated by adding Online and Mixed). As such, over ¼ of most fraud types presented online elements. Imperfect as they are, these results suggest that the online/offline dichotomy is indeed blurred for a considerable proportion of F&CM reports.

It is also striking that *Consumer* fraud presents a strikingly different MO pattern to the remaining fraud types. With *Consumer* fraud, 50.83% of crimes reported display mixed MOs and 35.43% online-only, resulting in an overwhelming 86.26% of *Consumer* fraud cases containing at least some online element. This may be explained by the high levels of online shopping taking place in the UK. In contrast over 37.75% of *Investment*, 48.67% of *Services* fraud and the overwhelming majority of *Business Compromise* and *Retail* frauds were classed as Offline-only, an indication that these crime types may be yet to digitise.

1.1.2. Change Over Time

The proportion of online, offline and mixed cases changed in different ways over the reference period. A chi-squared test showed a statistically significant difference in the number of online/offline/mixed reports by individuals over each quarter of the reference period (excluding the first quarter of year one), with a medium effect size (χ^2 (12) = 64.78, p < .001, *Cramér's* V = 0.26).[126] While the standardised residuals provided some indication of what drives this difference, given the number of categories (seven quarters multiplied by the three levels within the variable MO group), the results are not easy to interpret. Furthermore, such a test does not consider the ordered nature of *Quarter*. In contrast, the multinomial logit model *MO Group ~ Quarter* (χ^2 (12) = 65.43, $p < 0.001$) allows for trends to be easily visualised and interpreted via the effect plot (Figure 39). Furthermore, using Helmert contrasts allows for a quantification of the ordered effect over time.[127]

[126] As noted in the methodology, the first quarter of the first year of data was removed from the longitudinal analysis as it unduly skewed the data.

[127] Refer to Annex V, Part IV, section 1.3.2 for full model parameters.

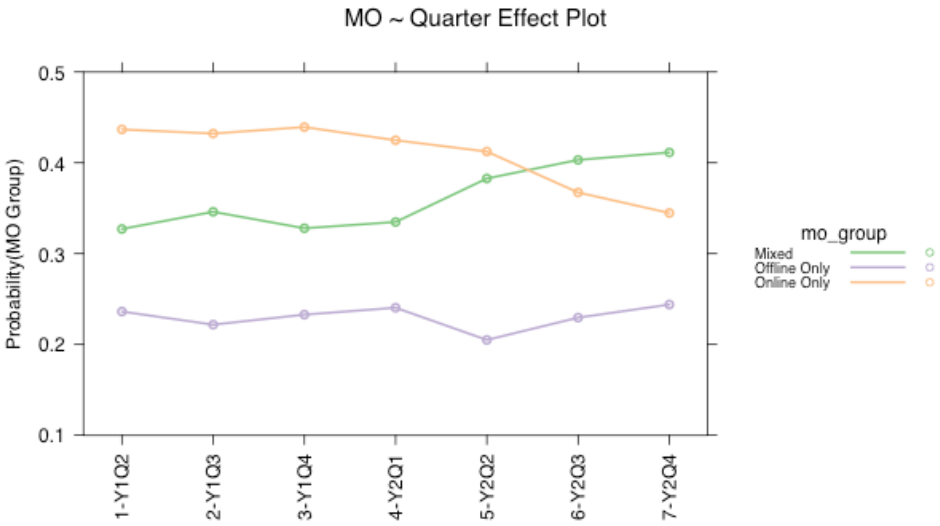

Figure 39 – Effect display of MLM model *MO Group ~ Quarter* (Model 11).

Interpreting the effect plot, while there was no change throughout Q2-Q4 of year 1,[128] there is a clear positive trend with respect to the Mixed MO group in the second year of the sample (from 4 – Y2Q1 onwards). There is also a corresponding downward trend with respect to Online only cases. In addition, there does not appear to be any change with respect to Offline-only MO over the reference period. Once again, this may be explained by the increased integration of digital technologies into everyday life on one hand, leading to 'online' crimes seamlessly integrating 'offline' life. On the other, certain crime categories still overwhelmingly remain in the 'analogue' camp, keeping the offline-only MOs relatively constant.

1.1.3. Individual Characteristics

Age

A series of chi-squared tests revealed that there were statistically significant differences across age groups with respect to whether they were coded for any online/offline elements and both (each representing a non-mutually-exclusive, binary true/false category, i.e. online and offline can be both 'true' for a given case). Based on *Cramér*'s V, these differences amounted to a medium effect for cases coded for online elements (χ^2 (12) = 486.99, $p < 0.001$, *Cramér*'s V = 0.23), and offline elements (χ^2 (12) = 508.56, $p < 0.001$, *Cramér*'s V = 0.23), and to a small

[128] As noted in the methodology, due to the effect of the rollout of AF resulting in a low number of cases, the first quarter of year 1 was excluded from this analysis.

effect size where there were mixed elements (χ^2 (12) = 188.22, $p < 0.001$, *Cramér*'s V = 0.14). Breaking down these results further using standardized residuals creates difficulties of interpretation given the large number of age categories. However, by interpreting the results through a GLM effect plot, using Helmert contrast coding to account for the ordered nature of the age category variable (Figure 40), differences between age groups become clearly interpretable.

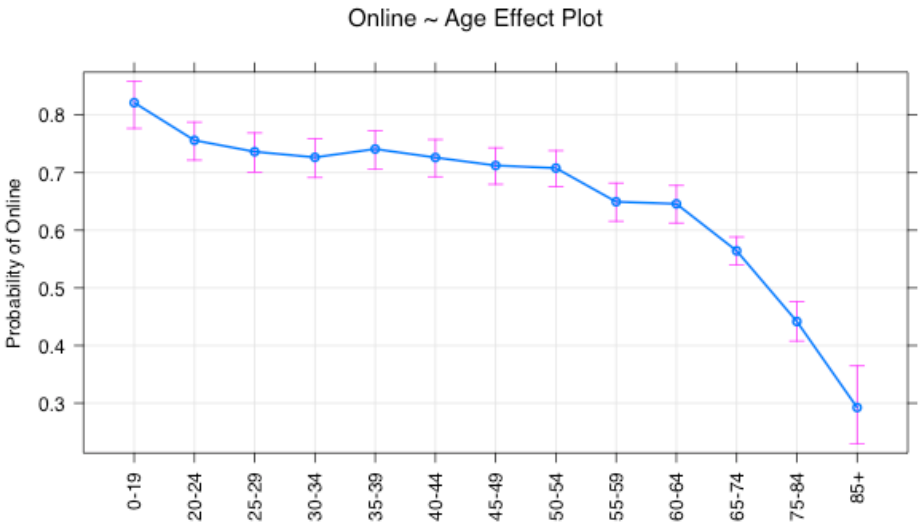

Figure 40 – Effect display of GLM model *Online MO ~ Age* (Model 12).

The result of the binomial logit GLM Model 12, *Online MO ~ Age* above is quite revealing – not only is there a significant ordered relationship between age category and cases with online elements (χ^2 (12) = 477.12, $p < .001$), but the effect display also demonstrates a downward trend across the age categories, which becomes more accentuated for the 60+ age groups. As such, despite the large numbers of individuals in the older age categories reporting to Action Fraud overall, it is the younger groups who are predominantly reporting cases with online elements. The same analysis in relation to cases coded as having an offline element is just as revealing – albeit of the opposite trend. While the ordered relationship in the binomial logit model *Offline ~ Age* is also statistically significant (χ^2 (12) = 517.63, $p < .001$), the chi-squared value indicates that the magnitude of that relationship or the effect size is larger than that of Model 12.[129] In addition, the effect display (Figure 41) shows that the probability of offline

[129] Refer to Annex V, Part IV, section 1.4.1 for full model parameters.

elements increases with age, with a particularly sharp increase for the 60+ age groups – although it remains constant between the ages of 30-49.[130]

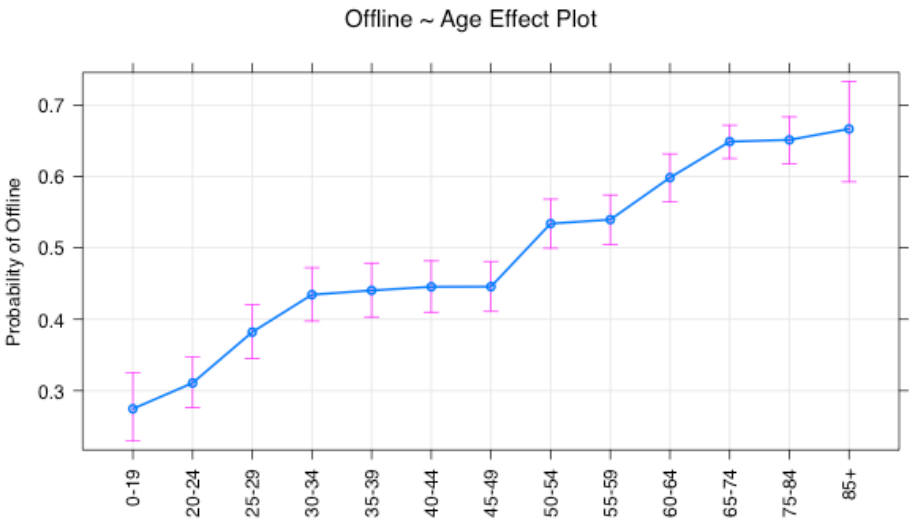

Figure 41 – Effect display of GLM model *Offline ~ Age* (Model 13).

The online/offline pattern by age group can be further examined by modelling the probability of the overall MO Group variable (whether the incident contained online-only, offline-only or mixed elements) across age groups. The effect display of the multinomial logit model *MO Group ~ Age Category* (χ^2 (24) = 1082.4, $p < .001$) (Figure 42), shows that the probability of an online-only MO tends to decrease and offline-only increase (albeit more slowly) with age, to a point of conversion somewhere between 60-74 years. Once again, it is from the age category 60+ that the two groups start to diverge more significantly, with a sharp increase in reported offline-only MOs and a sharp decrease in online-only MOs.[131]

[130] Op. cite 47.

[131] Refer to Annex V, Part IV, section 1.4.1 for full model parameters.

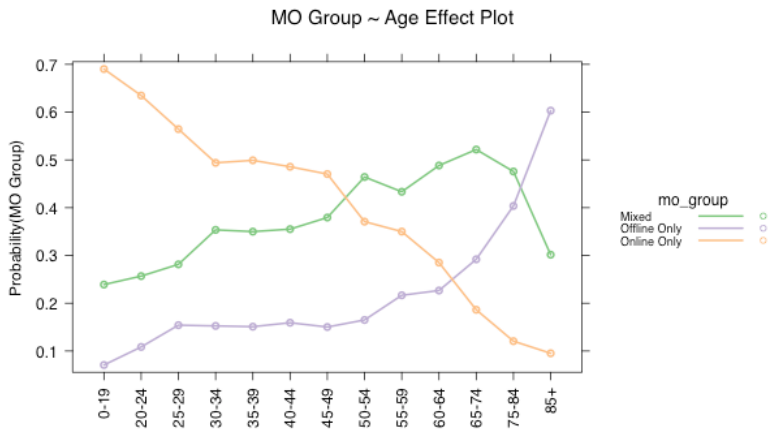

Figure 42 – Effect display of MLM model *MO Group ~ Age* (Model 14).

However, the probability of an online-only report is greater than that of other MO types for all age groups up to 45-49. At the same time, mixed MO reports increase linearly with age, with a sharp decrease from 65-74 onwards. The probability of a mixed MO report is also consistently higher than that of an offline only report for all but the oldest age group. This suggests a large role for the online elements for most age groups, either on its own (when reporting victims are between 0-49 years old) or mixed with offline elements (for victims between 50-74 years old). It is only within reports from victims 75+ that offline-only MOs become more predominant. It was only by simultaneously coding for both on and offline elements as recommended by van Wilsem (2011), that this pattern could be identified.

Ethnicity

Statistical differences between White/BAME ethnic groups across the binary categories of online (χ^2 (1) = 4.07, $p < .05$), offline (χ^2 (1) = 5.52, $p < .05$) or mixed MOs (χ^2 (1) = 1.20, $p > .05$) were tested with chi-squared tests.[132] These were not significant at the $p < .01$ level, or at all, in the case of mixed MO. Based on the odds ratio, BAME victims were approximately 1.27 times more likely to report a case with online elements than their 'White' counterparts (n = 7777), while 'White' victims were approximately 1.29 times more likely to report a case with offline elements than BAME victims (n = 7730). As these odds ratios are all under 1.55, they are considered negligible. Furthermore, while the differences between ethnic groups and the combined *MO group* variable (online-only, offline-only or mixed) were statistically significant,

[132] Yate's continuity correction applied.

their substantial effect was also negligible (χ^2 (2) = 9.97, $p < .01$, *Cramér*'s V = 0.04). As such, it is concluded that no differences of practical relevance were found with respect to online/offline MOs across ethnic groups, within respect to individual victim reports.

Gender

A chi-squared analysis revealed that there was no significant statistical difference between males and females with respect to cases with any offline (χ^2 (1) = 16.08, $p > .05$) or online elements (χ^2 (1) = 0.45, $p > .05$), whereas there was a significant difference with respect to those coded for mixed elements (χ^2 (1) = 10.78, $p > .01$).[133] Based on the odds ratio, females are approximately 1.14 times more likely to report a case with mixed elements (n = 11582), which constitutes a negligible effect. Furthermore, while the differences between male/female victims across the overall MO group (online only, offline only or mixed) were statistically significant, their substantial effect was also negligible (χ^2 (2) = 19.42, $p < .01$, *Cramér*'s V = 0.06). As with ethnicity therefore, it is concluded that no differences of practical relevance were found with respect to online/offline MOs across gender.

1.2. Enablers and Offender Tactics

While the previous subsection explored the online/offline dichotomy quantitatively, this section turns to a broader qualitative exploration of the MO features of the crime reports sampled. As described in the methodology chapter, a sub-sample of 332 reports (made by 160 individuals) were selected for TA. The sample was then thematically analysed to identify the range of enablers and offender tactics which could be identified from crime reports. The themes identified and the number of reports coded to each theme are summarised in Table 37.[134]

[133] Op cite. 45.

[134] Please refer to Annex VI, for the detailed coding structure in including definitions for each theme.

*Themes**	*Sub-Themes*	*Coded Phrases*	*Coded Crimes*
1. Enablers	1. Online/offline and remote/in person dynamics	33	33
	2. Legal enablers	218	153
	3. Criminal enablers	30	26
2. Offender Tactics	4. Victim manipulation	277	157
	5. Repeat targeting	68	66
	Total	626	435

Table 37 –TA coding summary for MO features.

1.2.1. Online/Offline, Remote/In person Dynamics

In relation to CM, the most common way in which on/offline elements combined were cases where a 'cold call' to the victim led to suspects obtaining remote (online) access to victims' computers. This type of MO was typically associated with cases of *Consumer* fraud and, to be more specific, Computer Software Service Fraud (see crime 5116 below). In addition, there were also cases of suspects obtaining personal information from victims through cold calls and then using this information to obtain unauthorised access to their online accounts, including shopping and internet banking.

Crime 5116

> "The victim was contacted by the suspect, claiming that there was a problem with their computer that they could fix. The suspects gained remote access to the computer and asked the victim to pay £234 for their "service". The victim gave their card details. The suspects have proceeded to take £1,234 from their account, and have now locked their computer until the victim pays an additional £500 to unlock it. The victim has refused to pay any more money."

Conversely, another typical on/offline combination occurred where the victim searched/applied for rogue services online (e.g., loans), thus providing suspects with personal information which is used to further contact the victim and/or commit fraud. Of these, as has been noted in the previous chapter, loan fraud can have a high relative impact on victims. Furthermore, some less typical ways in which online/offline elements combined, included where multiple members of the same household were targeted by hackers, where hacking followed from

information obtained in the course of a burglary or where victims physically travel somewhere with the intention of finalising an online purchase (at which point the fraud transpires).

Alongside the online/offline dynamics, in some situations there is both remote and in-person contact between victim and offender. Alternatively, the offender implicitly or explicitly indicates that they know the victims' physical location. In the first scenario, a common situation was one where the fraudsters cold call the victim on the pretext of carrying out some work in the house and then actually visit and interact with the victim face-to-face. In the second, the suggestion that the offender knows where the victim lives may be implicit through threats of physical violence on one hand, and through demonstrations of local knowledge on the other. In the case below, the suspect booked a local taxi to take the victim to the bank, so they could make a cash withdrawal to send the fraudster.

Crime 12895

> "[The] victim received a phone call to his landline from a male stating he was from Santander and attempts had been made to hack into his account. Victim, who is elderly, got into a conversation with this male and the male then told the victim to withdraw £2500 from his Santander account then call him back. The victim did as instructed and called back that same day. Victim was then told to send £600 to two persons in India via MoneyGram, he was given instructions over the phone on how to fill out the MoneyGram form. [The offender] even arranged for a taxi to pick up the victim from his home address and take him to the post office to send the money. […]"

1.2.2. Legal Enablers

Legal enablers refer to legitimate services, practices and technologies which are exploited by offenders in the commission of F&CM. Several such legitimate activity was identified through the qualitative analysis as enabling F&CM. These included offenders' use of advertising, call divert and domain registration services, mimicking legitimate organisations, as illustrated in the excerpt from crime 7606 below. Offenders also leveraged legitimate social media platforms and online marketplaces to find, establish first contact and defraud victims.

Crime 7696

> "Victim received an email claiming to be from PayPal saying that a summary of a payment to a mark brown and gave an address. The suspect email address was service@intl.paypal.com and slobooptiupdates@netcabo.pt. The email then gives a link saying if you did not authorise this transaction click on this link to cancel it. The victim has clicked on the link which took the victim to an identical PayPal website and filled out some details. Victim had to give username and password for PayPal, victims address, mother's maiden name and bank details. Victim has now realised this is a scam."

Finally, two key legal mechanisms which enabled F&CM were bank payment services and alternative Money Service Businesses (MSBs). Both were further enabled by identity verification systems which assume information such as date of birth is confidential, when it is often made public through data leaks or can be accessed online. Legal enablers can thus be understood as affordances (Gibson, 1986, Chemero, 2003), or properties of the technological environment, which suspects are capable of re-constructing to victimise others.

1.2.3. Criminal Enablers

The criminal enablers theme includes actions and technologies used by FCM offenders, which are in themselves illegal (to create, possess and/or use). Like the previous theme, they can also be viewed as *affordances* and sources of *embedded vulnerability*, but in this case, their use is criminally sanctioned. They included unauthorised access to information and systems, the use of malware and ransomware to extort victims (e.g., crime 3071), the use of spoof websites and spoof phone numbers to mimic those of legitimate organisations or which cannot be connected when the victim calls back (e.g., crime 3890) and criminal reliance on "stolen" personal information (i.e., "identity theft") to fraudulently obtain goods and services.

Crime 3071

> "Received email that I attempted to open, but could not. File name (ransom;win32crowti.a) unknown to me it was a virus in a 'zip' file. This virus has encrypted all the files on my computer. I took the computer in to Pembrokeshire Computer Centre and they were unable to remove the encrypted off the files. A message came up with if I pay 500 dollars, I would be given the code to remove the encryption. I have not paid this."

Case 3890

> "The victim reported a lender loan fraud previously and lost money to it. Since then, she has received numerous calls from a mobile number from a male with an Indian accent, who asks her if she is having difficulty paying her loan. The victim asks if he is calling from the last place she lost money and the suspect hangs up. When the victim calls the number back it says it does not exist."

Finally, in the case of *Consumer* fraud, fraudulent adverts and stolen goods also played a key role within criminal MOs. The most common cases were of fraudulent adverts for vehicles (e.g., 9648), electronics and vehicles.

> "I saw a car that I liked advertised on gumtree. I spoke to the person selling it on the phone and email. They said that the car would be delivered to me and the payment was to go through eBay, I had 7 days to decide if I wanted to keep the car, eBay would hold the money until then. The car was not delivered [on] the day it was supposed to be or ever. I checked my bank account my money was gone the person did not reply to my 18 phone calls [then] I then realised it was a fake and the person somehow had pretended to be eBay payment dept."

1.2.4. Victim Manipulation

Victim manipulation by suspects was a strong overarching theme for cases of fraud and many cases of CM. This theme was sub-divided into four stages leading to a 'successful' victimisation: 1) the suspect establishes a pretext to contact the victim, 2) they build a relationship of trust with the victim, 3) they use one or several persuasion techniques and 4) the victim is manipulated into some kind of 'action'. These findings echo previous research (e.g., Button, Nicholls, Kerr, & Owen, 2014; Cross, Dragiewicz, & Richards, 2018) and are explained in turn below.

The first stage refers to the pretext or subterfuge used by the offender to establish first contact with the victim. The variety of pretexts identified are captured in the diagram in Figure 43.[135] As illustrated by the size of each square, the most common pretexts were computer faults, refunds and compensation, loan offers, security concerns, fraud recovery and romance. Others included sale of shares and investments, services offenders allegedly rendered (e.g., "fixing" victims' computers), energy efficiency house works and telephone 'preference' services to (ironically) stop nuisance calls.

[135] Refer to Annex VI section 2 for full NVivo codebook. Tree diagram (Figure 43) re-drawn in R, see Annex 5, Part V, section 2.

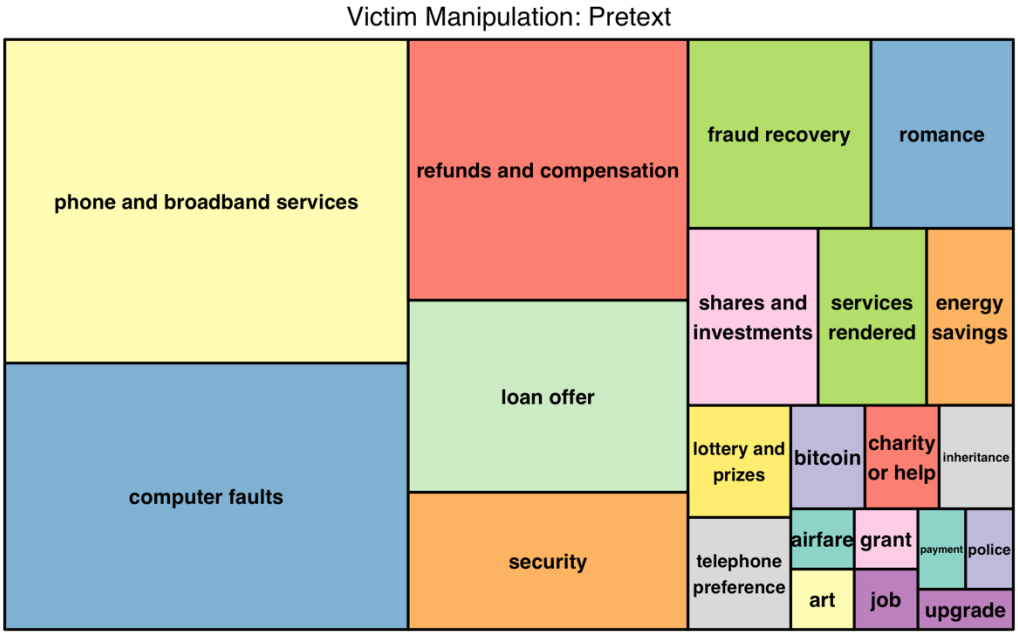

Figure 43 – Tree diagram of *Pretext* sub-theme.

Once a pretext was established, offenders proceeded to build relationships of trust with victims. This included projecting an image of legitimacy and developing relationships over time. To communicate legitimacy, offenders sought to demonstrate prior knowledge about the victim, especially when contacting them under the pretext of representing a legitimate company, which the victim has reason to speak to. This also suggests that a "cold call" may not be so "cold" after all – in some cases, the offender may be contacting the victim precisely because they have some prior knowledge that will enable a pretext to work. While it is not possible ascertain the provenance of this information, it is possible that this is linked to data breaches (e.g., 11689), the so-called "suckers' lists", or offenders conducting some form of open-source intelligence on their victims.

Crime 11689

> "The victim has received a call purporting to be from TalkTalk and [the caller] knew all the information about the victim's account. The suspect talked the victim into allowing him access to the computer. The suspect then said the victim was entitled to money back. The victim's email account has been hacked and all the TalkTalk information gained from there according to TalkTalk."

Legitimacy is also projected by providing the victim with the illusion of choice or a sense that what the offender is promising has "no strings attached". For example, the offenders may give the victim time to think about a particular "offer", offer multiple "payment" methods or even,

in one case, the option to pay by instalments. With respect to *Advance-fee* frauds based on fake loan offers for example, victims were often told that they could either pay the advance-fee or provide the fraudsters with the details of a guarantor. Finally, an image of respectability is also projected by alleging considerable wealth or by faking professionalism or a 'respectable' occupation. The former may be expressed by calls being transferred to "managers", the latter was a feature of romance fraud, where fraudsters claimed to be professionals e.g., an architect or engineer.

Alongside legitimacy, the offender often builds their relationship with the victim over time, sometimes years, before the fraud is uncovered, as illustrated in crime 15181 below. As is discussed further in the next section, in this example relationships built over years appeared may be associated with victim vulnerabilities such as ill-health and disability, suggesting that such individuals are preyed on. However, shorter term relationships were also commonly established between offenders and victims.

Crime 15181

> "Letter sent claiming my father had won the jackpot on World Lotto. He's 87 years old, receiving chemotherapy for prostate cancer, is diabetic and has other medical ailments so is an easy target. These details came to my attention today, he's also dealt with companies such as [X] based in Belgium, [Y] based in France, [Z] also based in France, and possibly other companies who appear to have scammed him. We will be requesting bank statements to ascertain the level of costs involved as he's been dealing with some of these companies for over 2 years and will update this report when received. We have documents and correspondence from these companies with addresses, payments etc if required. He's sent 3 payments by cheque to the World Lotto based in Australia and I believe when the bank statements are received the total scam amount will run into hundreds of pounds, possibly thousands."

Once first contact and legitimacy were established, further tactics of manipulation employed by the offender included the creation of a sense of urgency. For example, fraudsters may frame the situation as a "good opportunity" which much be seized straight away. In some cases, fraudsters also appealed to victims' empathy and beliefs e.g., by expressing distress and/or pleading for help out of a difficult situation; or appealing to a shared faith. Often however, a common tactic of manipulation was for the offender to urge the victim into action by becoming aggressive and threatening. As previously highlighted, some offenders threated victims with physical violence. Crime 10490 however, highlights a more common type of threat, that of legal or criminal liability.

Crime 10490

> "After scanning my computer, he said that I had to subscribe to either an all in one 4 year package at £324 or a home platinum lifetime package at £415 if I wanted to continue using my computer with Microsoft which by this time I was starting to get annoyed and accused him of being a scammer but he said he would not tolerate such abuse and assured me he was employed by Microsoft and started threatening to sue me for abuse."

The manipulation tactics used by the offender lead the victim to perform actions essential to the successful completion of the crime, after which the offender often terminates all contact with the victim – although, as will be seen in the next sub-section, this can be followed by renewed contact under a new pretext, which is nonetheless a continuation of the previous narrative (e.g., fraud recovery or fraudsters claiming to be the police). As illustrated in Figure 44, the types of actions which the victims sampled were persuaded to carry out included providing the offender with personal information, or entering this information via the web, following technical instructions given by the offender thereby providing them with remote access to their computer, calling the suspect back, travel or journey somewhere at the request of the offender in order to withdraw money, make payments to the offender, act as a 'money mule' for the offender, clicking malicious links and recruiting other victims into an 'investment' opportunity.

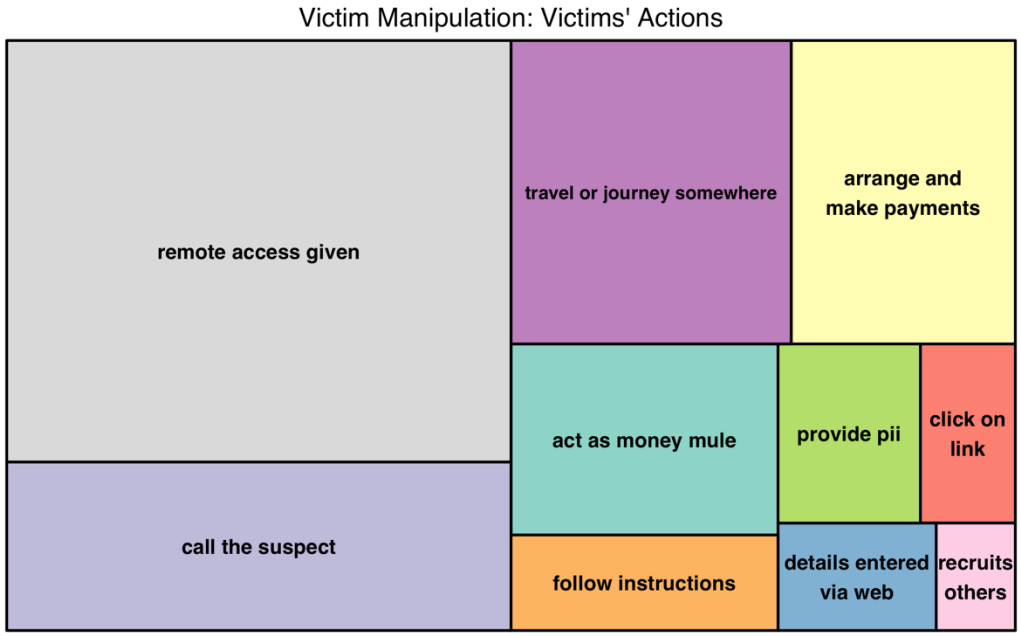

Figure 44 – Tree diagram of *Victim' Actions* sub-theme.

1.2.5. Repeat Targeting

Another tactic deployed by offenders which emerged from the analysis of MOs was the repeat targeting of the same individuals. Repeat targeting was made evident firstly, by the persistent contact offenders made with the same victim and secondly, by cases where there was evidence that the individual had previously been victimised in similar ways. For example, crime 119 below is the last case in a series of three and crime 10815 the sixth in as many reports. Both provide examples of the kind of persistent contact, which was prevalent throughout the sample and which, can cause nuisance if not distress to the victims.

Crime 119

> "The victim is reporting that she was contacted by the same suspect that cheated her and purporting to be from Microsoft. The suspect has phoned her five times today. The victim also made a report with Action Fraud her [about the] previous [victimisations]."

Crime 10815

> "The victim has been receiving multiple telephone calls from a company called [X]. The suspect company are looking to help fix a fault with the victim's machine. The victim has fallen victim to this in the past so knows not to give the suspect access to his machine. The victim has however been contacted on multiple occasions by this company. No money has been lost [on this occasion]."

In both of the above cases however, the repeat targeting has resulted in the victim becoming wise to the tactics employed by the offenders and thereby resisting further attempts of victimisation. In this respect, the presence of repeat reports may represent repeat targeting of the same individual, but 'boost' guardianship on the part of the victim, rather than 'boosting' vulnerability to victimisation. This runs contrary to the hypothesis discussed in chapter two, that repeat victimisation may 'boost' the likelihood of further RV, particular if offenders keep the so-called 'sucker's lists' of individuals who have previously become fraud victims.

At the same time, evidence of repeat victimisation was often present within a single report. As is explored in greater detail in Annex VII, the application of crime recording rules can lead to different instances in a series of victimisations being recorded as one. As such, repeat reporting does not equal repeat victimisation in more ways than one. Given the lack of research with respect to repeat F&CM victimisation and its strategic importance for law enforcement, the extent, key features and the above-mentioned nuances of repeat victimisation are the focus of the next section.

1.3. Towards 'Hybrid' Crimes

This analysis in this section demonstrates that extricating online from offline F&CM crimes and vice-versa poses real challenges and lends support to the hypothesis set out in chapter one that these crime types should be understood as on/offline 'hybrids' (Caneppele & Aebi, 2019). Despite caveats regarding a high proportion of missing values, over 1/5 of the reported CM over the reference period presented significant offline elements within its MO. Likewise, in all but one of the fraud types analysed, ¼ of cases contained online elements. With respect to *Consumer* fraud in particular, an overwhelming 86% of cases contained an online element. In addition, a positive trend was observed with respect to the number of cases reported by individuals which contained mixed (online and offline) elements from the first quarter of the second year sampled onwards. As such, not only are mixed elements prevalent within both crime types, but they appear to also be increasing – at least in relation to individual victims. With the growth of Internet of Things devices, current developments in bio-engineering and wearable technology, the blurring of the online/offline dichotomy is expected to continue. For CJS agencies, this points towards the need to move away from strict segregation of expertise between tech-oriented practitioners and the rest. Importantly for victims, prevention advice and interventions that over-emphasize this false dichotomy run the risk of alienating individuals who disengage based on a false perception that online crimes do not affect them. That said, while no difference was found with respect to MO group across either gender or ethnicity, the probability of reporting a crime with an online element decreased with age, while conversely, the probability of reporting a crime with an offline element increased with age. As such, it is suggested F&CM prevention materials and advice be developed for specific age groups.

The qualitative analysis adds nuance and dimensionality to the above. It shows that the ways in which online and offline elements combine, often include offenders cold calling victims and manipulating them into providing remote access to their devices or, conversely, victims seeking services and submitting their details online, which are thereafter used by offenders to contact the victim via phone and proceed to de-fraud them. In addition, there were instances of a hack following a burglary and of several individuals being targeted by hackers within the same household. As such, the TA highlights the mechanisms of the online/offline interaction, but also suggests the ways in which cases where a CM offence has occurred may be subsumed under cases where fraud is recorded as the main offence. Alongside this, the qualitative analysis revealed four more key dimensions which characterize the MO of F&CM crimes. These were

the role of legal enablers, the role of criminal enablers, the range of manipulation tactics used by offenders and the repeat targeting of victims.

Legal enablers refer to legitimate services, actions and technologies which are exploited by offenders in the commission of F&CM. A wide range of legal enablers were identified in this analysis including how the offender first established contact with the victim (phone, social media, email etc.), the use of bogus advertising, as well as the abuse of payment services and of identity verification systems. The last two factors are examined further in chapter six in relation to victim vulnerability. However, their predominance within this sample suggests that further research is necessary with respect to whether these are adequately regulated. Criminal enablers on the other hand, are actions and technologies used by offenders in the commission of F&CM, which are in themselves illegal. Among these are the use of stolen information, the leveraging of data breaches, the deployment of malware to extort victims and the sale of fake goods and services. Both legal and criminal enablers can be understood as affordances (Gibson, 1986, Chemero, 2003), properties of the environment, which suspects are capable of re-constructing to victimise others. Viewed through this prism, the answer to the last the key questions posed by a restorative justice approach noted in chapter one (who has the responsibility/ability to repair the harms caused by crime?), leads to the recognition that those who design and manage the relevant services and technologies have a role and must take responsibility for addressing the harms which result from F&CM victimisation. These enablers can also be viewed through a vulnerability theory lens (Fineman 2008, 2017) and conceptualised as sources of *embedded vulnerability,* as discussed in chapter two. As such, enablers are discussed in greater detail in chapter six, within the proposed vulnerability framework.

This analysis also revealed the importance of the victim manipulation tactics used by offenders in the commission of fraud as well as the repeat targeting of F&CM victims. Adapting Whitty's (2015a) term, the "anatomy" of victim manipulation followed four stages: 1) the suspect establishes a pretext to engage with the victim, 2) the offender builds a relationship of trust with the victim, 3) the offender uses one or several persuasion techniques and 4) the victim is manipulated into action. While it is true that the victim 'acts' in this process, it should be stressed that in all the cases reviewed the victim acted in good faith and thus victim-blaming narratives are inappropriate. Of course, there will be instances where a stark contrast between the 'innocence' of the victim and the culpability of the offender may be questioned and, in

some circumstances, it may be possible, desirable or even essential to empathise with the offender and their circumstances, in the pursuit of justice. However, this should not be incompatible with understanding victims, first and foremost, as having experienced harm as a result of having their rights violated by offenders.

Finally, the final theme with respect to MO characteristics was the targeting of previous victims, which was clear in the references to persistent contact from the offender and the evidence of victims' experiences of prior victimisation. As noted in chapter two, repeat victims are considered a policy priority (in theory, if not in practice). However, the TA revealed some of the challenges and nuances of measuring repeat victimisation within crime reports and making assumptions as to whether a repeat victim is necessarily a more vulnerable victim. Firstly, given the low legal thresholds for both F&CM offences, making repeat reports may be a 'flag' for increased guardianship on the part of the victim. Secondly, depending on crime category, multiple instances of victimisation may be recorded as a single crime. Given the lack of research with respect to F&CM repeat victimisation and its strategic importance for law enforcement, the extent, key features and the above-mentioned nuances of repeat victimisation are the focus of the next section.

2. Repeat Victimisation

This section addresses RQ5 to RQ9, which focused on the extent of individual repeat victimisation (section 2.1); the characteristics of repeat victims (section 2.2), the impact (section 2.3) and time-course of repeat victimisation (section 2.4), as well as the mechanisms of repeat victimisation (section 2.5). These questions, the analysis and discussion that follows, draw from the literature identified in chapter two (e.g., Farrell, 1992; Farrell, Tseloni, & Pease, 2005; Sidebottom, 2012). As previously noted, the analysis presented below was limited to n = 10,001 incidents reported by individual victims within three Welsh forces (Dyved/Powys, Gwent and South Wales). Ultimately, this section addresses the research gap with respect to F&CM repeat victimisation, also identified in chapter two. In addition, the final section 2.6, provides a brief insight into levels of repeat business victimisation, in so far as these could be discerned from the data sampled for this thesis.

2.1. Extent of Repeat Victimisation

2.1.1. Overall volume

Of the total (n = 10,001) incidents reported by individuals in the three Welsh police forces analysed in this chapter, 350 individual victims were identified who, between them, reported 787 crimes. This indicates that around 8% of crimes reported by individual victims (and recorded as crimes) were instances of repeat victimisation (RV) (Figure 45).

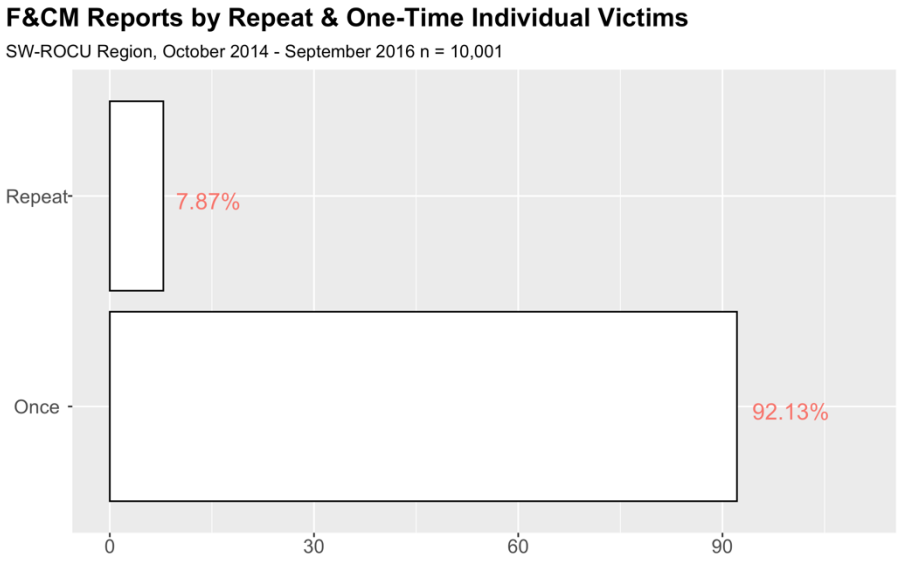

Figure 45 – Percentage of reports attributed to repeat & one-time individual victims.

Victims who reported two or more crimes (i.e., repeat victims) made up approximately 4% of all individual victims who reported F&CM. As noted above, these victims reported approximately 8% of all crimes within the reference period. This does not represent as large a proportion of known crime found in previous research. As previously noted, early estimates suggested 14% of the population were repeat victims and they reported 70.9% of the incidents recorded on the then British Crime Survey (Farrell, 1992, p. 92). Furthermore, Whitty (2019) estimated that 45% of fraud victims were repeat victims over their lifetime. However, this sample is restricted to recorded crime and a two-year period. In addition, given that only about 15% of all F&CM crime reported in Wales within the reference period was actioned in some way (Correia 2019), 8% of repeat victimisation within crime reports is very significant.

Furthermore, as illustrated in Tables 38 and 39, the extent of repeat victimisation varied across the two crime groups considered, with a greater proportion of repeat victims among those who reported Computer Misuse (CM) crimes.[136]

N reports	*N records*	*Incident proportion*	*N victims**	*Victim proportion*
1	8527	92.72	8527	96.53
2	533	5.8	267	3.02
3	88	0.96	29	0.33
4	23	0.25	6	0.07
5	5	0.05	1	0.01
6	21	0.23	4	0.04
Σ(n>1)	670	7.29	8527	3.47
TOTAL	9,197	100	8,833	100

Table 38 – Fraud records per number of total reports linked as a series.

N Reports	*N records*	*Incident proportion*	*N victims**	*Victim proportion*
1	687	85.45	687	93.99
2	59	7.34	30	4.04

[136] Tables include % incidents and victim proportion. *Approximate estimate based on N incidents / N reports.

N Reports	*N records*	*Incident proportion*	*N victims**	*Victim proportion*
3	20	2.49	7	0.91
4	9	1.12	2	0.31
5	20	2.49	4	0.55
6	9	1.12	2	0.21
Σ(n>1)	117	14.56	44	6.02
TOTAL	804	100	731	100

Table 39 – CM records per number of total reports linked as a series.

As shown in the highlighted cells above, approximately 3% of fraud victims are estimated to have reported 7% of recorded frauds. For CM, 6% of victims reported 15% of crimes. This difference was significant as confirmed by a Chi-squared test (χ^2 (1) = 52.86, $p < 0.01$). In addition, the odds ratio indicates that the odds of a CM victim being a repeat victim are 2.17 times higher than those of a Fraud victim, a small effect size. As it will be discussed however, this is most likely due to differences in recording practices when comparing F&CM.

Alongside the above, this data indicates that there is a significant difference between the number of repeats, versus one-time crime reports, across the three Welsh forces considered (χ^2 (2) = 16.26, $p < 0.01$). However, the effect size based on *Cramér's V* (0.04) is negligible. Nonetheless, the standardised residuals (Table 40) indicate that this difference is driven by reports in Dyfed/Powys being significantly more likely to be made by repeat than one-time victims and conversely, those reported in South Wales were significantly more likely to be made by one-time victims ($p < 0.01$).[137] As such, RV appears to be somewhat more prevalent in Dyfed/Powys and less prevalent in the South Wales force area. As hypothesised in the discussion section, this may be explained by differences in the local characteristics of these areas.

[137] ** indicates statistical significance at $p < 0.01$.

Force	*Victim Type*	*N*	*St. Residuals*
Dyfed/Powys	Once	2210	-3.60**
	Repeat	234	3.60**
Gwent	Once	2200	-0.57
	Repeat	195	0.57
South Wales	Once	4804	3.58**
	Repeat	358	-3.58**

Table 40 – Repeat and one-time reports by force, with standardised residuals.

2.1.2. Crime Categories

As discussed above, a statistically significant difference with a small effect was found across crime group with RV more likely among CM than fraud cases. In addition, differences in the extent of RV across specific crime categories were also found to be statistically significant (χ^2 (7) = 126.45, $p < 0.01$). The small effect (*Cramér's* V = 0.11) appears to be driven by a greater probability of repeat reports of *Advance-fee* fraud and *Hacking*, while reports of *Consumer* and *Other* fraud are more likely to come from one-time victims, as shown by the standardised residuals in Table 41 ($p < 0.01$).[138]

[138] ** indicates statistical significance at $p < 0.01$.

F&CM Category	*Victim Type*	*N*	*Prop of Type*	*St. Residuals*
Advance-fee fraud	Once	1907	0.21	-2.95**
	Repeat	198	0.25	2.95**
Card/Banking fraud	Once	445	0.05	2.43
	Repeat	23	0.03	-2.43
Consumer fraud	Once	4279	0.46	2.85**
	Repeat	324	0.41	-2.85**
Hacking	Once	439	0.05	-9.76**
	Repeat	102	0.13	9.76**
Investment fraud	Once	174	0.02	-1.76
	Repeat	22	0.03	1.76
Malware, Virus & (D)DOS	Once	248	0.03	1.32
	Repeat	15	0.02	-1.32
Other fraud	Once	1480	0.16	4.19**
	Repeat	82	0.1	-4.19**
Services fraud	Once	242	0.03	-0.07
	Repeat	21	0.03	0.07

Table 41 – Repeat and one-time reports by crime category, with standardised residuals.

The next aspect analysed concerned the sequence of crimes repeatedly reported by victims. Table 42 provides a matrix for the observed sequences, including the count for each combination of consecutive crimes reported by individual victims, along with row percentages and standardised residuals. Given the small numbers in some of the combinations, CM categories were combined and thus no distinction can be made between CM crime categories. In addition, *Other* and *Services fraud* were combined, as were *Card/Banking* and *Investment Fraud*.

	Advance-fee	*Card/Bank & Investment*	*Consumer*	*Hacking*	*Other*
Advance-fee Fraud	66 58.93% 7.54**	7 6.25% 0.13	23 20.54% -2.9**	3 2.68% -3.8**	13 11.61% -0.9
Card/Bank & Investment Fraud	8 33.33% 0.93	9 37.50% 6.34**	2 8.33% -2.32	1 4.17% -1.59	4 16.67% 0.23
Consumer Fraud	21 11.73% -3.36**	6 3.35% -1.42	125 69.83% 7.13**	15 8.38% -3	12 6.70% -2.83**
CM	3 4.35% -3.33**	1 1.45% -1.53	6 8.70% -3.89**	57 82.61% 12.73**	2 2.90% -2.58
Services & Other	7 13.21% -1.61	3 5.66% -0.09	7 13.21% -2.87**	2 3.77% -2.43	34 64.15% 9.3**

Table 42 – Change matrix of consecutive reports, including, count, row percentage and standardised residuals.

A statistically significant difference with a medium to large effect was found between the crime categories likely to follow each other, as confirmed with a chi-squared test (χ^2 (7) = 511.2, p < 0.01, *Cramér's* V = 0.54).[139] Looking across the highlighted diagonal in Table 42, it becomes apparent that the repeat crime is significantly more likely to be of the same category as the crime that preceded it (p < .01). Where a significant difference was found between the other possible combinations of crime categories for consecutive reports, as the negative residuals indicate, these are negative associations.

[139] As noted in the methodology, using Pearson's chi-square test assumes that the expected frequency for each of the contingency cells is no lower than 5. As the contingency table in the technical annex indicates (see section 2.1.5), the minimum expected frequency was 1.43 and there were 5 contingency cells (or 20% of the category combinations) where the expected frequency was below 5. However, with a larger contingency table such as this one, having up to 20% of expected frequencies below 5 is acceptable, given that no expected frequencies are below 1 (Field et al., 2012, p. 818). The result of this is loss of statistical power – i.e. the test may fail to detect a genuine effect. Using Fisher's exact test was considered, however we were unable to access enough computer power to compute the calculation. As such, it was decided to use the chi-square test in this case.

2.1.3. Summary & Discussion

The above analysis shows that around 8% of F&CM crimes reported by individual victims were made by repeat victims, which totalled approximately 4% of all victims captured in this sample. This varied between the two crime groups with 3% of fraud victims estimated to have reported 7% of recorded frauds and 6% of CM victims estimated to have reported 15% of the CM crimes. As such, this analysis suggests that a not insignificant proportion of victims who report F&CM are repeat victims. These results lend strength to the argument that overall, crime volumes could be reduced by targeting prevention activity at repeat victims.

At the same time, the estimated level of RV found within reported crime in this study is lower than the 16% previously identified through the CSEW (ONS, 2016b) or the 45% of RV found by Whitty (2019) in relation to online fraud. This difference will be, in large part, due to the different methodologies – particularly the fact that this study is restricted to victimisation which was reported to the police. However, the degree of RV identified within reported F&CM is also likely to be an underestimate, for four main reasons. Firstly, the limitations of the data linkage methodology may have conditioned the number of repeats that could be identified (see section 4.2.5 of methodology). Secondly, because the sample analysed is limited to a two-year period, the sample is both left and right-censored. In other words, both earlier and later reports may be repeats of reports that are out of the reference period covered and thus not be identified as such. In the study carry out by Whitty (2019) for example, respondents were asked about RV throughout their lifespan. Thirdly, as shown in section 2.5 below, the nature of F&CM means that victimisation is not easily compartmentalised into discrete events. In the case of fraud in particular, as was highlighted in the previous section, the nature of the offenders' manipulation is such that the individual may be victimised several times before becoming aware of the fraud. Linked to this is that, arguably, Home Office Counting Rules (HOCR) determine that in some circumstances of fraud, several instances of victimisation are recorded as one crime. In order to better understand the levels of RV, it is suggested that recording practices should be improved so that the identification of repeat victims may become less ambiguous. For example, a field might record an estimate of how many distinct payments were made by the victim to the offender, in relation to the fraud crime being recorded. Since this data was collected, some improvements have already been made. Now, the new AF system automatically identifies whether or not a victim has previously reported a F&CM crime. While a welcome advance, this provides limited information to officers and analysts about the degree of RV. As has been

shown in this chapter, two instances of the same victim reporting are relatively common, but these will raise less concerns than victims who have reported three or more cases.

The key differences identified across crime group and crime categories should also inform the planning and delivery of crime prevention. As noted above, RV figures were considerably higher for victims of CM. In addition, certain crime categories including *Advance-fee Fraud* and *Hacking* were associated with a higher likelihood of repeat victimisation and, where victims are victimised repeatedly, this tends to be within the same general crime category. Awareness campaigns and prevention advice should emphasize these features of F&CM victimisation so that victims may guard against further victimisation. At the same time, previous research has noted that it is important that individuals understand that crime categories such as *Advance fee* and *Investment* frauds have varied MOs. As with insisting on an online/offline dichotomy, being too prescriptive about how RV typically operates can also lead to complacency on the part of CJS agencies and potential (repeat) victims.

A significant difference was found between the number of repeat versus one-time crime reports across the three Welsh forces, but the effect size was negligible. To the extent that a difference was found, this was driven by a higher likelihood of RV in Dyfed/Powys and a conversely lower likelihood of RV in South Wales. The demographic differences found between the two areas in chapter four may explain this negligible difference as reports from Dyfed/Powys were more likely to be from areas of low or low-medium deprivation, while reports from South Wales tended to come from areas of High or Medium-High deprivation. This suggests that, in line with previous CSEW insights regarding all victims of F&CM, repeat victimisation may also be greater among more well-off groups. Given the limitations of the deprivation measured used (see section 3.1.4 of the methodology) and the observed effect size of this difference, however, further research is required to test this hypothesis with confidence. In addition, it was noted in chapter four that victims in Dyfed/Powys were somewhat older and, as it is shown in the next section, there is an association between older age and RV. As such, the presence of older victims may explain the greater proportion of RV in Dyfed/Powys.

Despite all its limitations, this analysis demonstrates that identifying RV has the potential to help target limited victim-support and prevention resources towards areas where the demand is greater. While the extent of RV observed in this dataset is not of the same order of magnitude found within other types of crime (violent crime and domestic violence in particular), identifying and targeting prevention measures at repeat victims would still help reduce a

significant proportion of the crimes reported. This is particularly important in a context where, as discussed in chapter one, only a small minority of F&CM crimes reported are currently actioned in some way by the NFIB and/or local police forces. Considering and identifying differences in levels of RV across England and Wales, may also enable better allocation of police and victim support resources. Furthermore, it would enable strategic resource allocation within each force, towards crime types where re-victimisation is more common and/or victim groups who are most vulnerable to further victimisation (more on this below).

2.2. Repeat Victims' Characteristics

2.2.1. Individual Characteristics

This section considers the characteristics of repeat victims and, following previous research (e.g. Ignatans & Pease, 2015, 2016), whether they differ significantly from one-time victims (RQ6). As shown in Figure 46, more incidents reported by male victims were repeats when compared to incidents reported by female victims. However, a chi-squared test ($\chi^2(1) = 14.05$ $p < 0.01$, *Cramér's V* = 0.03) indicated that while this is a statistically significant difference, the effect size is negligible. This is further illustrated by the odds ratio, with the odds of an incident reported by a male victim being a repeat only 1.33 times higher than those of report by a female victim.

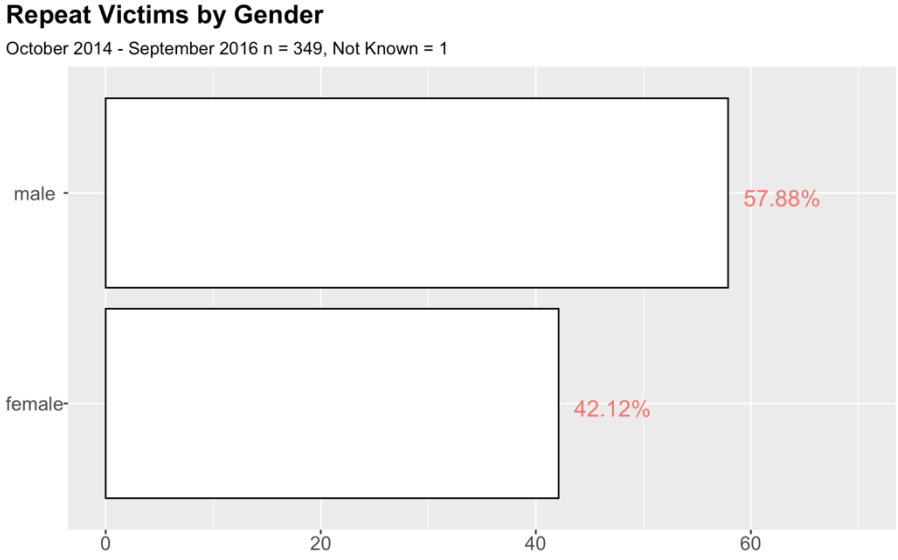

Figure 46 – Percent of Repeat Victims by Gender.

No statistically significant difference was found between one-time and repeat victims with regards to ethnicity (χ^2 (1) = 0.067, p > 0.5). However, due to the low number in non-White categories, the ethnicity variable was combined into a binary BAME/White to enable statistical analysis. Furthermore, a large number of missing values remained within the recoded ethnicity variable (n = 6,605; NA = 3,379). As such, this result should be interpreted with caution and further research is needed to better understand any differences in RV between ethnic groups.

Considering age however, the typical individual identified as a repeat victim was older than those to whom only one incident could be attributed. This is visible on the age histograms of repeat and non-repeat victims as there are fewer reports from younger victims in the repeat victim group (Figure 47). Both the mean and the median age at the time of reporting are higher for repeat than one-time victims (Table 43). Furthermore, the significance of the difference between the mean age between these groups was confirmed with the Wilcoxon rank-sum test (W = 2598423, p < .001).

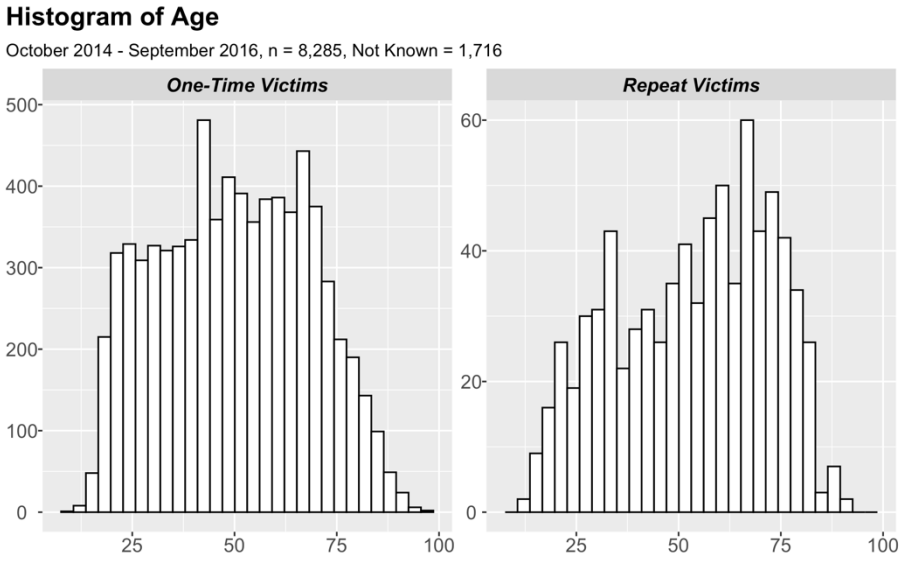

Figure 47 – Histogram of Age: Repeat v One-Time Victims.

	One-Time Victims	*Repeat Victims*
Min.	9	12
1st Qu.	34	37
Median	50	57
Mean	49.91	53.6
3rd Qu.	65	69

Max.	97	92
NA's	1716	0

Table 43 **– Distribution of age at the time of reporting for one-time and repeat victims.**

It is possible that the linkage methodology introduced a bias towards linking for older victims. However, date of birth (DOB) was a key component of the linkage method and proxy reports made on behalf of older victims (e.g., by family and friends) were more common for older victims. If anything, this should have led to increased inaccuracies or missing values of DOB provided for older victims. As such, these findings are indicative of a statistical association between RV and older age, suggesting that among recorded crime, older individuals are more vulnerable to RV. However, as is discussed further in chapter six, embodied characteristics such as age cannot be considered in isolation to determine the relative vulnerability of victims. It was also considered whether there may be an interaction effect between age and gender, however, as shown by effect plot of the binomial logit model *Repeat Victim ~ Age*Gender* (χ^2 (1) = 0.77, $p > .05$) (Figure 48), while the probability of RV is slightly greater for males, it increases with age for both male and females and, for older victims, the overlapping confidence bands indicate that the effect is less clear for older groups.[140]

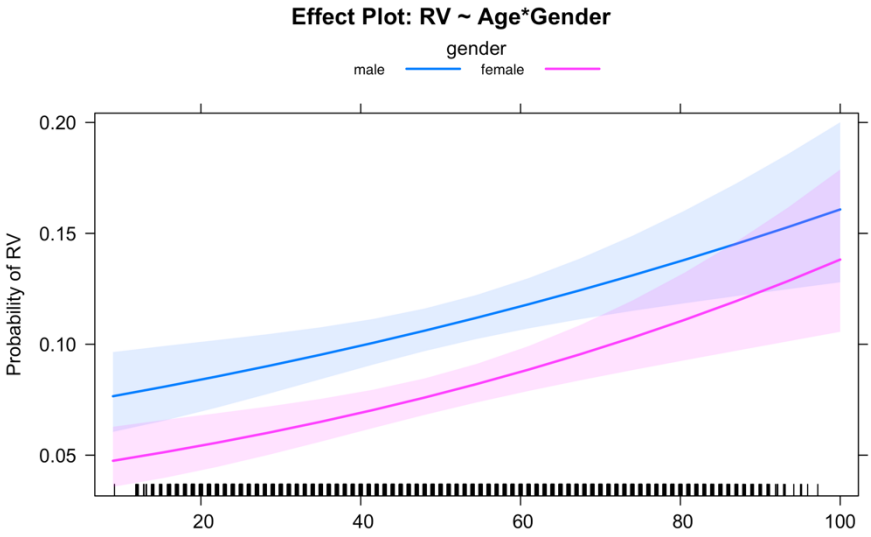

Figure 48 – Effect display of GLM model *Repeat Victim ~ Age*Gender* (Model 15).

[140] Refer to Annex V, Part IV, section 2.3.3 for full model parameters.

Finally, it was hypothesized that cases flagged as having been reported by a "proxy" on behalf of the victim may be associated with greater vulnerability to victimisation and therefore with repeat victims. This hypothesis was tested based on anecdotal evidence from practitioners that often friends and family reported on behalf of especially vulnerable individuals. However, the data shows the opposite effect – a greater proportion of one-time victims were flagged for a proxy report, although the effect size was negligible ($\chi^2(1) = 13.58$, $p < .01$, *Cramér's V* = 0.04). This raises the possibility that practitioners' experience is indicative that proxy reports are associated with wider conceptions of vulnerability, beyond vulnerability *to re-victimisation*.

2.2.2. Local Factors

In addition, the data was also analysed with respect to whether repeat victimisation was associated with geographic areas with better internet access, based on internet access data from Ofcom, and the level of socio-economic deprivation, based on the Welsh Index for Multiple Deprivation. The first provides an indication of internet access at the Local Authority (LA) level (Table 44), the second a measure of deprivation at the Lower Super Output Area (LSOA) level (illustrated in Figure 49).[141]

Internet Access	*High*	*Medium*	*Low*
One-time	6419	1771	1024
	4.39**	-4.87**	-0.28
Repeat	489	208	90
	-4.39**	4.87**	0.28

Table 44 – Reports by one-time and repeat victims by internet access, with standardised residuals.

With respect to Internet access, the picture that emerges is unclear. While a significant difference was found between repeat and one-time victims with respect to the level of internet access in the local area ($\chi^2(2) = 25.06$, $p < 0.01$, *Cramér's* V = 0.04).[142] The odds of a repeat victim in an area with medium or high internet access are 0.08/0.12 times higher than those of a one-time victim respectively. These results therefore suggest the effect size is negligible.

[141] The LSOA is a geographical unit used in official statistics in England and Wales.

[142] **indicates significance at the $p < 0.01$ level.

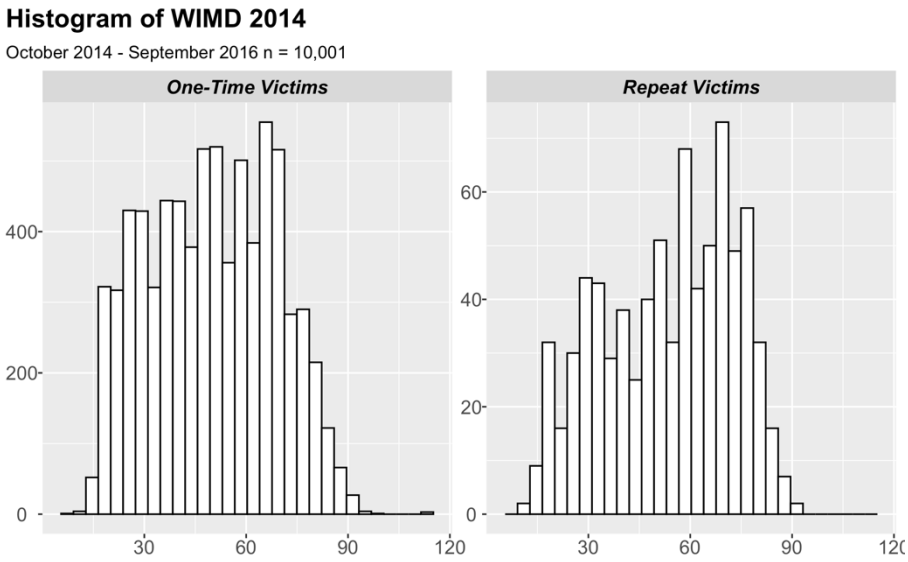

Figure 49 – Histogram of WIMD Score: Repeat v One-Time Victims.

The median WIMD ranking of repeat victims' LSOA was 918 (more deprived), compared to 936 for one-time victims (less deprived). However, the histograms of the distribution of WIMD ranks for repeat and one-time victims show more reports from one-time victims at the lower end of the WIMD rankings (meaning more deprived), suggesting that RV are generally in wealthier LSOAs (Figure 49). However, a Wilcoxon rank sum test failed to show a statistically significant difference between these distributions ($W = 3542036$, p-value > 0.05).

2.2.3. Summary & Discussion

This analysis suggests that males are marginally more likely to be repeat victims and that the likelihood of RV increases with age, while ethnicity and proxy reports had no effect on the probability of repeat reports. While this is considerably different to the typical repeat victim profile for other crime types such as violent crime and domestic violence, it is in line with the profile of F&CM victims discussed in chapter four – more males and older victims report being victimised, and more report RV. As such, this analysis suggests that similarly to other crime types (Ignatans & Pease, 2015, 2016), the characteristics that distinguish repeat from one-time victims, are similar to those that distinguish victims from non-victims of F&CM.

However, no significant interaction effects were observed between age and gender, as may have been expected from the analysis in the previous chapter. Given the limitations of the present linkage method however, this is an area for further enquiry. Likewise, no significant association was found between repeat reporting and the socio-economic characteristics of the victims' local area, as measured by the WIMD, or levels of local internet access. However,

there were considerable limitations to the analysis of these two environmental factors considered as the measures did not capture granular differences at the individual level. As such, further research is also necessary to understand the impact of socio-economic factors and levels of internet access on RV.

2.3. Impact

2.3.1. Financial Impact

Approximately 71% of reports from one-time victims versus 67% of reports from repeat victims reported a loss, with no significant difference between the two ($\chi^2(1) = 3.26$, $p > .05$). However, this analysis is somewhat limited by the high proportion of missing values for the variable loss for unique reports and repeat reports (61% and 84% missing loss values respectively). Table 45 provides a summary of loss where this was reported. However, it should not be assumed that missing values represented no loss and recording practices should be improved so that no loss is always explicitly recorded.

	n	*Min.*	*1st Qu.*	*Median*	*Mean*	*3rd Qu.*	*Max.*
Unique Reports	4,567	1	120	328	5,940	1,400	5,000,000
Repeat Reports	338	1	150	431	3,202	2,500	92,960
Repeat Victims Total Loss	210	1	241	637	5,153	4,450	130,460

Table 45 - Distribution of loss for one-time and repeat victims.

The descriptive statistics indicate that for both one-time and repeat victims, there is considerable variability in terms of the loss reported and thus the median value of loss reported is the most typical loss experienced. While the average loss is higher for one-time reports, the median loss by incident for one-time victims (£328) is lower than that for repeat victims (£431). When the total loss over all reports made by repeat victims is computed, the total median loss for repeat victims is even higher (£637). As such, this data indicates that while on average the losses associated with one-time reports are higher, the average is distorted by a few very large losses and the typical losses experienced by repeat victims are higher. This is illustrated by the greater concentration of losses towards the right-hand side of the x-axis when comparing one-time and repeat victims in Figure 50 below.

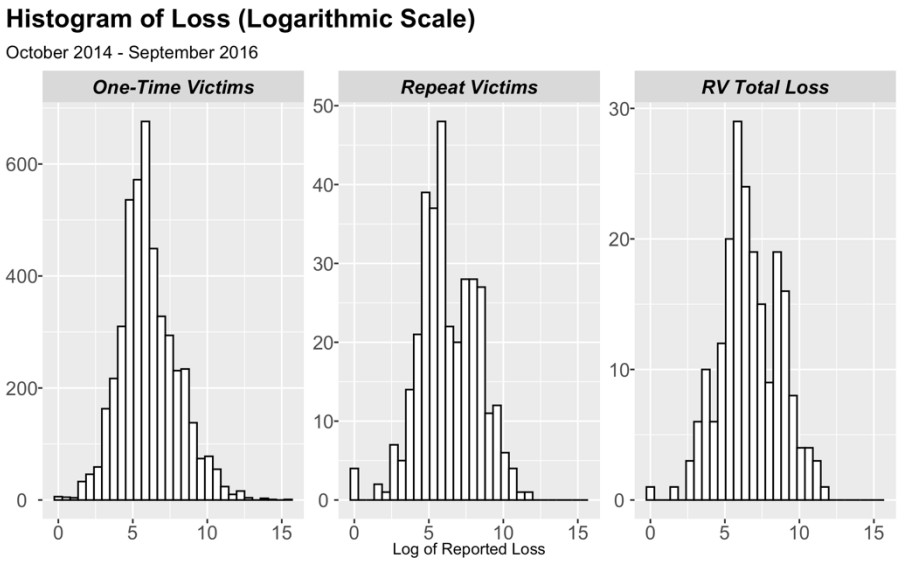

Figure 50 – Histogram of log(loss): one-time, repeat victims and total loss across series of repeat reports.

This conclusion is supported by the results of a Wilcoxon rank sum test, confirming that there is a significant difference between the distribution of the loss reported by one-time and repeat-victims ($W = 707824$, $p < .05$, $r = -0.04$). This suggests a medium effect size, where higher losses are associated with RV. As such, while one-time victim reports contain a greater number of extreme values which influence the measures of central tendency, on the whole repeat victims are more likely to report higher losses – even where losses are considered for repeat reports individually, rather than taking the total losses in a series of repeats. In addition, Figure 50 also illustrates a greater concentration of higher losses where total losses across series of repeat reports is taken into account.

2.3.2. Other Impacts

As noted in the methodology, an equal number of repeat and one-time victims were randomly selected for TA (160 victims in total). Section 3.2 of chapter four explored the impacts of F&CM beyond direct financial loss and this sub-section should be read in the context of that previous discussion. Nonetheless, a summary of the impacts coded for the TA samples of one-time and repeat victims are shown in Table 46 below.

	Identity, privacy and liberty	*Wider Financial impact*	*Property loss or damage*	*Wellbeing and relationships*
One-time victims	10	2	4	11
Repeat victims	34	56	28	51

Total codes	44	58	32	62

Table 46 – Crime impacts by one-time/repeat victim category, TA coding summary.

It is striking that impacts beyond financial loss were predominantly coded within the RV sub-sample. As such, this analysis suggests that as well as typically suffering higher direct financial losses, repeat victims also report a wider range of other impacts with considerably greater frequency. The relevance of this finding is that it appears that the qualitative themes identified in chapter four were derived primarily from accounts of RV. This further illustrates that understanding the impact of victimisation across the full series of repeat reports and across a wide variety of possible impacts, has the potential to considerably change the assessment of the impact F&CM victimisation has on individuals. In part, this may be explained by the impacts of the RV mechanisms used by offenders, discussed in section five below.

2.3.3. Summary & Discussion

This analysis shows that while on average the losses associated with one-time reports are higher, this is distorted by a few very large losses and the typical losses experienced by repeat victims are higher. In addition, it appears that the qualitative themes identified in chapter four were found primarily from accounts of RV, suggesting that for repeat victims, not only are losses typically greater, but also that RV has a greater and wider impact on their lives including each of the themes discussed in the previous chapter, i.e., their identity, privacy and liberty, wider financial impacts beyond direct losses, property loss or damage and their wellbeing and relationships.

These findings have clear implications for a response focused on reducing harm to victims, as well as the provision of a victim response. Firstly, preventing RV is of strategic importance where CJS interventions aim at reducing harms to victims, caused by experiences of F&CM. Secondly, where prioritising of limited victim support services is concerned, repeat victimisation may indeed be considered a ‘flag’ that individuals may be coping with relatively greater harms post-victimisation. Furthermore, an aim of victim support is to help victims overcome the negative impacts of victimisation, and so support should be informed by the ways in which the experience of repeat victims is different to that of one-time victims.

2.4. Time-Course

2.4.1. Overall Time-Course

As discussed in chapter two, previous literature highlights the importance of the time-course of RV and its implications for crime prevention activity. As such, this section investigates the time-course of F&CM RV based on recorded crime and its implications for crime prevention activities. The first aspect investigated was the distribution of the inter-report time – i.e., the distribution of the time elapsed between consecutive incidents. As the sample spanned two years, a small number of cases linked across a period longer than one year would have skewed the analysis towards longer periods between events, particularly towards the end of the reference period. As such, the time-course analysis provided below is limited to consecutive reports within 12 months, excluding a minority of cases where the time difference was greater than 366 days (n = 31)[143]. In any case, given the cross-sectional nature of this study, any period chosen suffers from both left and right-censoring, as further discussed below.

As shown in Figure 51, this was concentrated at the lower end of the scale and the graph gives the appearance of an exponential decrease in the number of incidents as the time difference between them increases. The distribution shown in Figure 51 is in line with previous research into repeat network attacks (Soumyo Darshan Moitra & Suresh L. Konda, 2004). In addition, 15.5% of all linked (repeat) incidents were reported on the same day (n = 122).

[143] The year was assumed to have a maximum of 366 days given that 2016 was a leap year. In addition, the time course analysis only counts the time difference between reports made by the same individual. As such, the first case of each series of reports by the same individual does not count, which results in NA = 350 out of the 787 linked incidents.

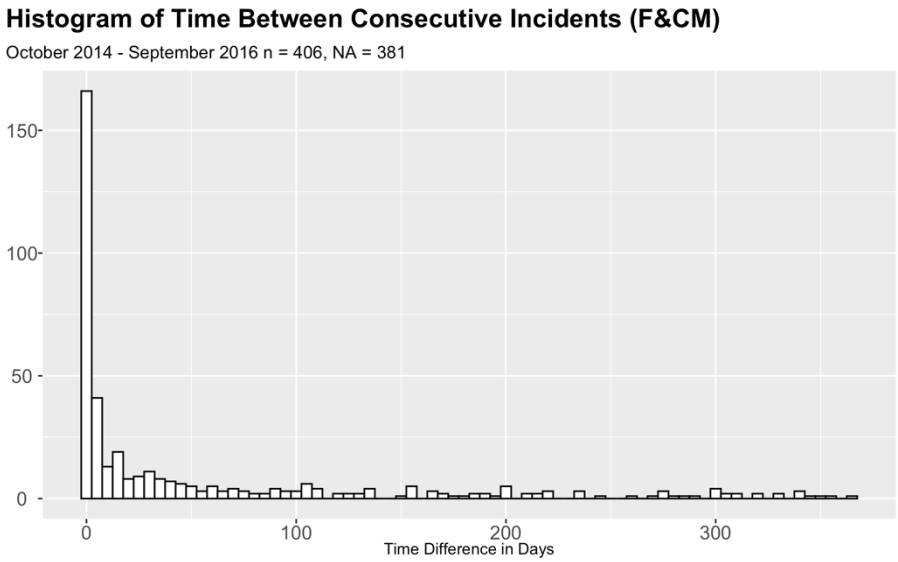

Figure 51 – Histogram of time difference (in days) between consecutive incidents.

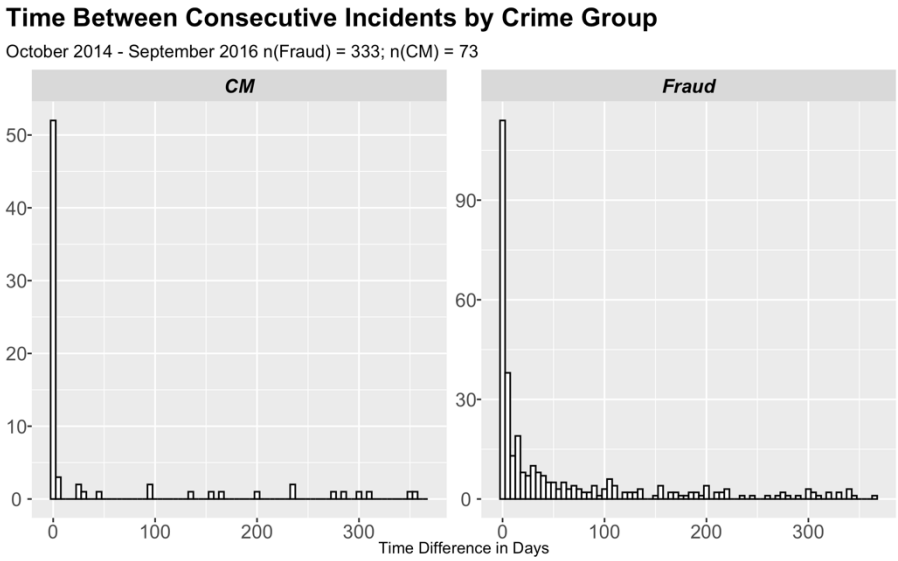

Figure 52 – Histogram of time difference (in days) between consecutive incidents, by crime group.

This reflects the application of HOCR, which can result in multiple reports being made when the rules determine they are discrete crime events, regardless of whether they are reported on the same day and/or are part of the same continuum of victimisation (e.g., where multiple online accounts are hacked in a short space of time). In this respect, HMCR favour a principle of one crime per incident with respect to CM and one crime per victim, even where there are multiple incidents, with respect to Fraud. The effects of these rules are visible by disaggregating the time-difference data by crime group, with many more CM consecutive reports made on the same day (Figure 52). In line with previous research therefore (Shorrock, McManus, & Kirby,

2020), these results indicate that crime recording practices have a considerable impact on the identification and measurement of RV.

The exponential nature of this distribution of time differences (made starker by the number of same day reports) means that the median is a better representation of a typical time difference between reports than the mean. The overall mean difference found between reports was 83 days and the median 12 days (excluding same day reports, the mean was 115 days and the median 40 days). In addition, the mean difference between the first and last report by individual repeat victims was 137 days and the median 49 days (excluding same day reports).

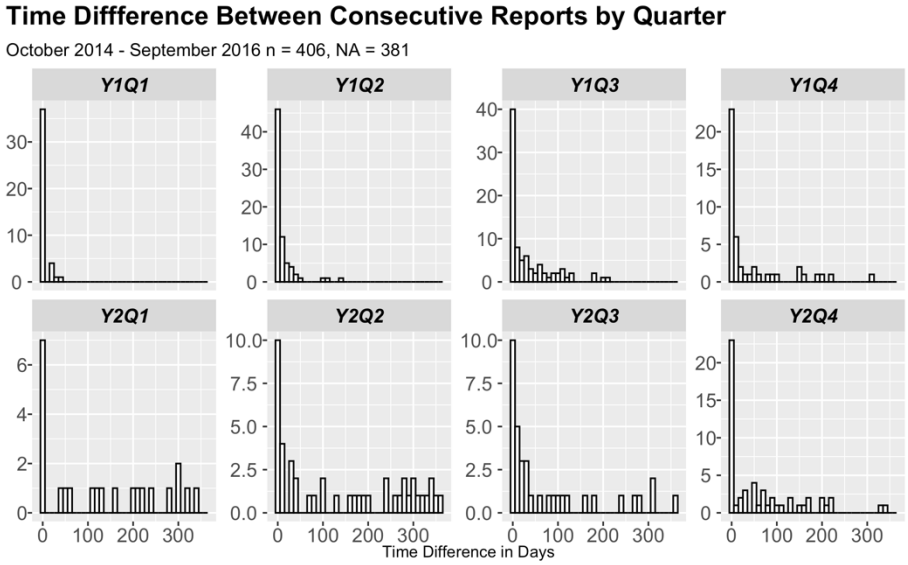

Figure 53 – Histogram of time difference (in days) between consecutive incidents, by quarter.

Furthermore, this tendency for a higher concentration of consecutive reports within the lower range of time differences seems to hold over the reference period, divided into quarters. However, as Figure 53 shows, the data becomes considerably more dispersed in year two. This increased dispersion is also observable in the mean and median time differences over time (Table 47).

year	*quarter*	*n*	*mean(diff)*	*median(diff)*	*max(diff)*
2014-2015	Q1	43	4.02	0	45
	Q2	73	12.16	2	136
	Q3	85	34.48	7	208
	Q4	46	43.43	5	306
2015-2016	Q1	23	134.22	122	338
	Q2	45	142.71	97	363
	Q3	36	81.61	25.5	357
	Q4	55	67.33	30	338

Table 47 – Time difference (in days) between consecutive incidents.

As the time difference was measured in relation to a previously reported incident, this increased dispersion effect is most likely caused by the left-censoring and right-censoring of the data. For the earlier quarters, there is a shorter period available within which the previous event could have occurred. As such, this left-censoring results in less repeats being identified, as well as smaller mean and median differences within the first year sampled. At the same time, the right-censoring of the data means that crime reports towards the end of the reference period may be the first in a series, but only the first instance is captured in this sample, which is therefore not identified as a repeat. As such, larger time differences will be increasingly captured towards the later quarters.

Additionally, the previously discussed crises in the AF service between the first and second years of the reference period can be expected to have had a considerable impact on the number of repeat reports recorded. The limited availability of the reporting service may have resulted in less repeat victims completing reports in Q4 of year 1 and Q1 of year 2. Thus, this may have exacerbated extreme time difference values throughout the second year of the reference period, especially in quarters one and two, explaining the particularly high mean and medium time-difference values in these quarters.

2.4.2. Number of Repeats

There is mixed evidence with respect to the relationship between the number of RV reports and the time-difference between reports.

nreports	*N*	*Mean time diff*	*Median time diff*
2	296	93 days	35 days
3	72	77 days	45 days
4	24	79 days	83 days
5	20	17 days	28 days
6	25	39 days	28 days

Table 48 – Time difference between consecutive reports by number of reports made.

Table 48 above gives the appearance of a general decrease in the mean time-difference between reports, particularly where the number of repeat reports is greater than 4, but there is no clear trend. A Kruskal-Wallis rank sum test confirmed that there was a statistically significant difference between the mean time difference grouped by number of reports made ($X_2(5) = 1369.8$ $p < 0.01$). However, using the R function *pairwise.wilcox.test* to calculate pairwise comparisons between group levels with corrections for multiple testing, it was concluded that only where nreports = 5 is the mean time-difference significantly different from the nreports groups 2 to 4 ($p < 0.05$). More research is required to fully understand the impact the number of repeat victimisations has on the time-course of repeat victimisation.

2.4.3. Summary & Discussion

In line with previous research (e.g. Soumyo Darshan Moitra & Suresh L. Konda, 2004; Sagovsky & Johnson, 2007) this analysis of the time-course of repeat victimisation indicates that crime prevention activities will be most effective within a month of first victimisation. However, the scope for intervention is reduced when considering the time-course of repeats as 16% of these were recorded on the same day. Reflecting the HMIC's (2015) findings and as corroborated by Shorrock and colleagues (2020) in the context of domestic violence and repeat safeguarding referrals respectively, recording practices have a considerable impact on the identification and measurement of RV. In the case of F&CM they may lead to an under-estimate of the time-course of RV, as separate crimes recorded on the same day have not necessarily taken place on the day of recording. In addition, the measurement of RV will be deeply affected by any changes in the availability of the recording services. Finally, no clear pattern emerged with respect to whether the time-course of victimisation varies with the number of repeat victimisations recorded.

2.5. Mechanisms

To explore MO and mechanisms of RV the thematic analysis of MO characteristics was compared between the one-time and repeat victims' sub-samples, as summarised in Table 49. While it is unsurprising that the majority of the coding for the MO theme of repeat targeting came from the sub-sample of repeat victims, it is striking that the themes *Legal Enablers* and *Victim Manipulation* were also more prevalent within the repeat victims' sample.

	Criminal Enablers	*Legal Enablers*	*On/offline & Remote/In Person*	*Repeat Targeting*	*Victim Manipulation*
One-time					
Phrases coded	11	84	15	20	111
Crimes coded	10	56	15	19	58
Repeat					
Phrases coded	19	134	18	48	166
Crimes coded	16	97	18	47	99
Total					
Phrases coded	30	218	33	68	277
Crimes coded	26	153	33	66	157

Table 49 – TA coding summary for MO characteristics, by one-time/repeat victim category.

One possible explanation for this is that the use of legal enablers lends the offenders additional credibility to continue to operate. In addition, it is logical that victim manipulation techniques become more important where the offender sustains a relationship with the victim over time, enabling RV. Further qualitative TA was employed to explore the RV process in its own right. This analysis adds to the previous quantitative insights as it goes beyond describing the characteristics of RV, by focusing on the mechanisms through which RV takes place. The themes summarised in Table 50 are examined in turn below.

Themes	*Description*	*Coded Phrases*	*Coded Crimes*
Narrative Continued	Captures the continuation of narrative across multiple instances of repeat victimisation. This involves the offenders developing a more or less complex 'story' which expands or evolves from the initial 'pretext' of their first contact with victims.	36	36
Subtle Nuance	Instances of RV were found to be linked by similar MOs characteristics including crime type (e.g. multiple Advance-fee fraud or multiple Consumer frauds), modes of contact (e.g. phone or social media platform) and suspects (e.g. where the victim states that they recognise the offender's voice from previous fraudulent phone calls). However, these similarities are sufficiently subtle that victims are manipulated into continued engagement with the offender.	111	96
Existing Vulnerabilities	How victims' a priori vulnerabilities, including financial hardship or cognitive capacity to identify deceit, were in some cases exploited repeatedly by suspects.	38	35
	Total	185	167

Table 50 - TA coding summary for repeat victimisation mechanisms.

2.5.1. Narrative Continued

The first key theme which emerged from the TA subsample is the extent to which there is a continuation of narrative across repeat victimisations. This involves the offenders developing a more or less complex 'story' which expands or evolves from the initial 'pretext' of their first contact with victims. For example, repeat victims of *Investment* fraud may initially see some returns on their investment, then be continuously asked to pay fees to release their funds until they realise that they have been defrauded. They may subsequently be targeted by offenders claiming they will recover previous losses. Similar 'recovery' fraud situations are also frequent following *Advance-fee* fraud as illustrated in the excerpts from a repeat victim below.

Crimes 6866 / 6888

Report 1:

"The victim has received a cold call from the suspects who claimed if the victim has paid 399GBP they would send out a surveyor to see if the victim was entitled to a boiler. The victim has gone to the bank and paid the money. Since then the victim has not received the surveyor to their door and the victim's daughter has since realised and contacted the suspects and they claim they are not a scam and that they are going to send a surveyor out. The victim has since tried to call back and the suspects have taken their phone lines."

Report 2:

"The victim has paid upfront fees to get a free boiler from the government and not received any service. The victim then received a call from the suspects claiming they know the victim has been a victim of fraud and they can get the money back for the victim. This is a fraud recovery fraud phone call but at this stage has not been asked for any money."

As noted, one way in which offenders extended their contact with victims included the request for further payments. For example, where 'extra' or 'hidden' fees suddenly appear in the administration of a 'loan' or, in the context of dating fraud, where the offender creates new excuses for needing for financial 'help'. Further payments were also requested in relation to new 'investment opportunities' or further 'repairs' to victims' devices. Of course, as previously discussed, the ability to continue to build on their narrative requires that the offender successfully develops a relationship of trust with the victim (see section 1.2 above). In such circumstances, the more engagement the victim has with the offender, the more likely they are to continue to successfully defraud the victim, suggesting that RV may indeed 'boost' vulnerability to further victimisation. In many cases, reports within the sample were only made once the victim became aware of the fraud and, as such, there is little CJS agencies could have done to prevent specific individuals from being repeatedly victimised. However, making victims aware of the prevalence of continued narratives such as the 'recovery' fraud tactics is key to preventing RV.

2.5.2. Subtle Nuance

Linked to the above and in line with the quantitative analysis, instances of RV were found through thematic analysis to be linked by similar MOs including the same broad crime type (e.g., multiple *Advance-fee* fraud or multiple *Consumer* frauds), modes of contact (e.g., phone or social media platform) and suspects (e.g., where the victim states that they recognise the offender's voice from previous fraudulent phone calls). However, unlike the previous theme, there was no continuation of narrative as such.

Crimes 227 / 883 / 884

Report 1:

"Victim received a phone call from Indian male claiming to be from TalkTalk saying line not working correctly, asking for access to computer. Victim gave access to his computer and suspects set up an online banking account for him. Suspect said would take £15 but took £115. Suspects then contacted victim again and victim said he wanted it refunding, said to do this would pay a cheque into his account and he would have to

transfer the remaining £360 via MoneyGram. Victim did not do this and spoke to TalkTalk who advised it was not a genuine call from them."

Report 2:

"The victim was contacted originally by the suspect who accessed his computer and set up his internet banking for him. Since then, he has completely wiped his computer. The suspects have then reopened his online banking and have taken a further £710 from the victim. The suspect has been calling ever since [date] but no access has been granted again."

Report 3:

"The suspect rang again purporting to be from Lloyds bank. The victim believes this is the same suspect whom he gave access to his PC in [date]."

In the above example, while they have not used a continuous narrative, the victim believes they are being contacted by the same suspect. Furthermore, there are similarities and subtle variation across the three reports. Firstly, a call under the pretext of slow internet connection; secondly unauthorised access to victim's online banking; thirdly a call under the pretext of calling from the bank. This variation would not be captured in a quantitative analysis, as all three instances shared the same crime category. In various cases of fraud however, subsequent crimes were sufficiently different that the victim was manipulated into continued engagement with the offender. Furthermore, with respect to CM, often hackers obtained control of victims' personal email or account recovery settings and hacked multiple accounts in quick succession. As such, the fact that more often than not subsequent F&CM victimisations are similar to previous victimisations, should not be mistaken for victim complacency or lack of common sense. In addition, these cases suggests that more could have been done to secure the victims' devices/accounts, thus preventing further victimisation.

2.5.3. Existing Vulnerabilities

Finally, in a small number of cases of repeat victimisation analysed, it was clear that victims' vulnerabilities which predated the experience of victimisation, including financial hardship or cognitive capacity to identify deceit, were in some cases exploited repeatedly by suspects. While not fully explained, the presence of pre-existing 'vulnerability' is noted in the excerpt that follows. As explored in chapter 2, it is likely that these were likely embodied vulnerabilities, particularly as the victim was over 75 years old. At the same time, as further explored in chapter 6, this case also demonstrate the importance of structural vulnerability factors in creating the risk of victimisation, namely the technological affordances which enable

rogue services to advertise on search engines and the abuse of Alternative Money Services to extract money without a trace.

Crimes 4111 / 11790 / 12694

Report 1:

"The victim searched online for a BT support number and dialled to speak to a suspect. The victim was instructed to turn the computer on and given instructions on allowing the suspect remote access to the machine, the suspect claimed to have discovered a number of problems which required attention. Victim was asked to pay for a protection service which cost £216 and given instructions to make a bank transfer. […]"

Report 2:

"[Civilian staff officer reports on behalf of victim who] received a phone call from someone saying they were from the Ministry of Justice and she was due to get £5600 plus bank over charges and to get this the victim had to pay upfront of £200.00, victim had to get vouchers of value of £200.00 Pay-Safe vouchers on [date], [on another date] £895.00, [on another date] £1480.00 […]; there were 11 pay-safe vouchers in total – the suspects are now looking for 10,000 off the victim for Income Tax."

Report 3:

"IP [Intended Person or victim] has transferred approximately £39,500 to various bank accounts believing that they were associated with the Ministry of Defence in relation to PPI claims. The IP is considered a vulnerable adult, which is why DPP are dealing."

Most cases coded under this theme were also the cases where the victim may be described as a 'chronic victim', defined for the purposes of this study as having been victimised four times or more. As such, in the case of 'chronic victims', this analysis lends support to the suggestion that RV is indeed a 'flag' for vulnerabilities which pre-date the first instance of victimisation.

2.5.4. Summary & Discussion

Through thematic analysis, it emerged that the themes Legal Enablers and Victim Manipulation were more prevalent within the repeat victims than the one-time victims sub-samples. Hand in hand with manipulation, two themes that emerged from cases of RV included the continuous/common narrative thread between reports in a series and, even where there was no continuation of narrative as such, some links between subsequent victimisations. This analysis therefore suggests support for the 'boost' theory of RV.

For fraud offences, with the exception of 'recovery' type fraud, many of the cases of RV are only recorded at the point that the victim has become aware of the fraud, making it difficult for CJS agencies to provide advice that might prevent RV. Similarly to cases of *Hacking*, often individuals only report once multiple online accounts have already been hacked. As such, while

a strong case can be made for targeting prevention advice at one-time victims, there is a role for awareness raising around typical offender tactics among the public, so they can safeguard themselves and others.

With respect to fraud cases, individuals often report several related losses at once, but while these may have taken place over a relatively long period of time, crime counting rules result in one incident being recorded. As anticipated in chapter two, therefore, the qualitative analysis in this section confirms that demarcation between instances of fraud victimisation is not easily captured in recorded crime, which in turn is likely to contribute to the under-estimation of RV. Furthermore, where separate records are made, consecutive incidents are often of the same general type, but the narratives employed by offenders are deliberately nuanced, in order to keep the victim engaged.

Finally, the analysis in this section has suggested that in the case of 'chronic' victims, RV may also be a 'flag' for vulnerabilities which predated the victimisation experience. In order to adequately respond to the needs of such victims, it is imperative that CJS agencies are able to identify these especially vulnerable victims in the first place and are then equipped to refer them onto further support, be it from social services, victim support services or other organisations.

2.6. Business Repeat Victimisation

While it was not possible to develop a detailed linkage methodology to identify repeat business victims in the same way that this was done for individuals (see methodology), a rough estimation of the levels of business RV can be gauged from the variables repeat_h (which provides a count of incidents reported from the same address, based on matching first line of address and postcode) and repeat_biz (which provides a logical TRUE/FALSE for business victims, based on whether more than 1 incident is recorded in repeat_h).

Of the total number of reports attributed to individuals, 10,691 (90.26%) came from unique addresses, while 1,154 (9.74%) were reported from duplicate addresses. This value is close to the overall 8% of reports relating to repeat victims which resulted from the linkage

methodology.[144] Of the total number of business reports, 1,324 (69.39%) came from unique addresses, whereas 584 (30.61%) were repeated and 61 (3.20%) were missing.[145] As such, this data suggests that RV may be considerably more prevalent for businesses than individuals. This was confirmed with a significant chi-squared ($\chi 2(1) = 646.14$, $p < 0.01$, *Cramér's V* = 0.22). Furthermore, the odds ratio indicates that the odds of a business victim reporting from the same address are 4.09 times higher than those of an individual victim, a medium effect size.

As with individual repeat victims however, the majority of reports came from distinct addresses. Also, in line with what was observed for individuals, for reports originating from repeat business addresses, the mode number of reports was two. Overall, the distribution of repeat reports tended towards the lower end of the scale, although it was more dispersed for businesses than individuals.

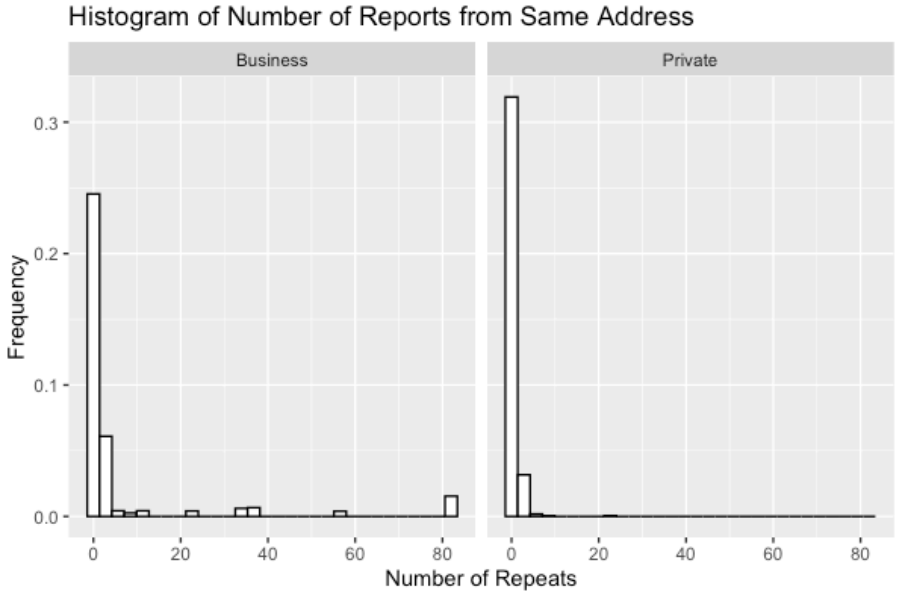

Figure 54 – Histogram of reports from the same address.

While indicative, these results should be considered with caution as the extent of business RV was not calculated following a rigorous linkage method, as with individual RV. On one hand, these business results might overestimate the level of repeat reporting as the calculation will be distorted by multiple businesses being based at the same address (e.g., in business parks).

[144] As expected, this more rudimentary estimate is higher than that found with the linkage method, as different individuals can report from the same address.

[145] While there were no missing values in the original address variable, some missing values resulted from the split of the address variable into line1, line2, postcode etc.

On the other hand, the causes of under-estimation outlined for individuals might also apply to businesses, particularly as, at the time this data was collected, businesses were unable to report 'in bulk' to AF. As a result, businesses would have to report each incident individually and these would be subject to the same, previously discussed limitations.[146] In addition, this data does not permit detailed analysis of the time-course of RV or the characteristics of businesses who repeatedly report F&CM (e.g., business size or sector).

[146] These are also discussed in greater detail in Annex VII.

3. Conclusion

Firstly, this chapter considered the overall features of the *Modus Operandi* (MO) of the F&CM crimes sampled. It has shown that the on/offline dichotomy is increasingly a false one. 'Hybrid' elements were found to be prevalent within both fraud and CM cases and mixed MOs appeared to be increasing. Reflecting the discussion in chapter one (e.g., Powell et al., 2018), these results suggest that focusing on the harms associated with crime in the digital society, where digital technology is increasingly integrated into and inseparable from 'reality', is a more appropriate lens through which to understand and respond to victimisation. With the growth of Internet of Things devices, current developments in bio-engineering and wearable technology, the blurring of the online/offline world is expected to continue and with it online/offline crime. In this context, it is key that law enforcement and other CJS practitioners do not become siloed in specialist 'cyber' units, particularly where their role involves providing victims with appropriate advice and support.

Other MO mechanisms which were identified through TA included the offenders' use of both legal and criminal enablers, their reliance on manipulation tactics and targeting of the same victim repeatedly. Both legal and criminal enablers can be understood as affordances (Gibson, 1986, Chemero, 2003), properties of the environment, which suspects are capable of re-constructing to victimise others. Viewing victimisation through this prism leads to the recognition that those who design and manage the relevant services and technologies have a role and must take responsibility for addressing the harms which result from F&CM victimisation. Enablers can also be viewed through a vulnerability theory lens (Fineman 2008, 2017) and conceptualised as sources of *embedded vulnerability,* as discussed in chapter two. As such, enablers are discussed in greater detail in chapter six, within the proposed vulnerability framework.

In line with previous research (Whitty, 2015a), each of the above-mentioned themes identified highlighted important aspects of the 'anatomy' of F&CM crimes which should inform prevention advice. Victims and support organisations will benefit from understanding the most common F&CM enablers, as well as the manipulation and repeat victimisation tactics commonly used by offenders. Technical and procedural solutions will be well targeted at online/offline, legal and criminal enablers identified in this study. An awareness of common offender tactics is key to improve victims' guardianship. However, important information

around MO characteristics was either not captured or not passed onto local forces. As such, local forces and other organisations responsible for victim support would benefit from utilising the information on MO characteristics, collected at national level, in designing prevention and support activities. In addition, the last theme, raised questions about the measurement of repeat victimisation and its link to increased vulnerability, which was then further explored in section two.

Section two demonstrated that a significant proportion of victims who report F&CM are repeat victims and uncovered patterns of RV relevant to both theory and practice. Along with a forthcoming publication (Correia, forthcoming), it has thus made a significant contribution to an area where existing research is limited (Pease et al., 2018). These results lend strength to the argument that overall, crime volumes can be reduced by targeting prevention activity at those who have already been victimised (Farrell & Pease, 1993). Such activity should, however, be empirically informed by an analysis of what crime types and victims are more prone to RV, a quantitative and qualitative assessment of the impact of repeat victimisation on victims, as well as consideration of the ways in which it has left the victim more vulnerable to further victimisation (e.g. in the form of 'recovery' fraud) or to the wider range of harmful impacts of victimisation (e.g. financial destitution or isolation due to strained relationships with family). Key differences identified across crime group and crime categories should inform the planning and delivery of crime prevention. As with insisting on an online/offline dichotomy, however, being too prescriptive about how RV typically operates can also lead to complacency on the part of CJS agencies, victims and the public. Furthermore, a good understanding of the impacts of victimisation on the victim is vital so that they can be referred onto adequate support services such as social services, debt advice, counselling etc.

A significant difference was found between the number of repeat versus one-time crime reports across the three Welsh forces, but the effect size was negligible. Nonetheless, the potential to analyse AF data across England and Wales to target limited victim-support and prevention resources towards areas where demand by RV victims is greater was demonstrated. Furthermore, the analysis of the time-course of repeat victimisation indicated that crime prevention activities will be most effective within a month of first victimisation. In cases where multiple reports are made on the same day, there may be limited scope for prevention interventions. Nonetheless, there is an opportunity to establish whether appropriate support should be made available to avoid further re-victimisation. This highlights that while the police

recorded crime data collection by AF provides a rich source of data with respect to victims' needs, improving data collection so that repeat victims are more easily identified could aid local forces in the delivery (or facilitation) of a more victim-focused response.

The analysis in this chapter has also highlighted that, in the overwhelming majority of cases analysed qualitatively, themes such as the continuation of the narrative, the similarity of MOs and the relationship built over time are suggestive of a 'boost' effect i.e., being a victim increases vulnerability to further victimisation. Furthermore, for repeat victims, not only are direct losses typically greater, but victimisation has a greater and wider impact on their lives. As such, it is suggested that generally, the impact of F&CM on victims is greater for repeat victims and therefore repeat victims are, on balance, going to be more vulnerable post-victimisation. At the same time, a minority of cases identified as 'chronic victims' were suggestive of repeat victimisation as a 'flag' for a priori states of vulnerability. These are likely to be exacerbated through the experience of victimisation. As such, the qualitative insights presented above suggest that, following Johnson (2008), repeat victimisation can be both a symptom (a 'flag') and a cause of (providing a 'boost' to) F&CM vulnerability. They have also illuminated the relationship between RV and the concept of 'vulnerability'.

Repeat victimisation is a 'complex phenomenon' (Turanovic & Pratt, 2014, p. 47) which can result from a plethora of factors. Furthermore, its measurement was subject to several limitations. Nonetheless, while the extent of repeat victimisation that is captured within AF data has limitations and is not of the same order of magnitude found within other types of crime (violent crime and domestic violence in particular, as discussed in chapter two), identifying and targeting prevention measures at repeat victims, with a view to preventing future victimisation, would still reduce a significant proportion of F&CM crimes reported. More importantly, it is a key - albeit not the only - factor in both *vulnerability to* and *vulnerability post-victimisation*.

Prioritising F&CM RV would therefore increase the provision of a meaningful and victim-centred law enforcement response, in a context where the great majority of F&CM crimes reported to the police are not 'actioned' in any way. The difficulties associated with policing (online) fraud and computer misuse offences have been discussed previously (chapter one), with only 15% of all sampled crimes actioned in some way. In this context, the need to focus on prevention and protecting the most vulnerable from being re-victimised is quite possibly the most effective crime reduction strategy. As such, a strategy for the identification and response

to RV would aid local forces in providing a meaningful law enforcement response, based on the needs of victims. In chapter six, the various aspects of the victim experience identified in this thesis are brought together as a vulnerability framework, which aims to enable a better identification of victim need.

CHAPTER 6: A Vulnerability Framework

Chapter two demonstrated the complexity the concept of vulnerability in policy and practice but highlighted how a vulnerability lens can enable a victim-focused response, i.e., help to identify what harms have been suffered as a result of F&CM, by whom, how to prevent and repair them, and who has the obligation/ability to do so. Drawing on Fineman (2008, 2017) and Nussbaum (2006, 2011), a vulnerability lens shifts the focus of discussion from a narrow focus on the embodied characteristics of victims and situational crime prevention, to a wider focus which encompasses victims' lived experiences, as well as the relational and structural factors which contribute to their vulnerability to F&CM. At the same time, the ways in which current understandings of vulnerability are ill-suited to respond to F&CM victimisation were highlighted. Chapter four captured the characteristics of victims and the impacts of F&CM victimisation. Chapter five explored the phenomenon of repeat victimisation and how it is related to the concept of vulnerability, However, an empirically grounded and comprehensive framework is necessary to bring this analysis together. The vulnerability framework proposed in this chapter will improve understandings of vulnerability and thereby enable better vulnerability assessments for F&CM victims, as required by the Victims' Code. The contours of such a framework began to emerge from the existing literature in chapter two. These were revised and refined in light of the analysis in chapters four, five and additional thematic analysis, and the results brought together into one multi-dimensional vulnerability framework, thus addressing the final research question (RQ10). Before presenting the results and discussion, RQ10 will be re-stated in full, and the methods used in this chapter summarised.

Research Question

RQ10: How was vulnerability constructed within reports of F&CM?

Methods Summary

To answer RQ10, a sub-sample of 332 incidents reported by a random sub-sample of 160 one-off and repeat victims was carried out, applying Braun and Clarke's (2006) Thematic Analysis (TA) technique. This led to the identification of key themes which illustrate how vulnerability is constructed within crime reports.

1. Vulnerability Framework Overview

Drawing on Fineman (2008, 2017) and Chambers (1989), vulnerability in the context of F&CM victimisation refers firstly to the (universal) susceptibility to being harmed as a result of these crimes (*vulnerability to* F&CM); and secondly to the extent to which individuals are or not able to cope with the negative consequences of being victimised (*vulnerability post* F&CM). In other words, it is a state of exposure to F&CM risk and its impacts, and/or a reduced capacity for resilience vis-à-vis the negative consequences of victimisation. This definition highlights that it is both theoretically relevant and operationally useful to distinguish between vulnerability *to victimisation* and *vulnerability post-victimisation*. In addition, the term 'vulnerability' can be understood in contrast to the term 'resilience'. Identifying the ways in which individuals are made more vulnerable, is the first step towards designing a response focused on increasing their resilience. Consequently, from the perspective of a victim-focused response, the framework proposed below may be flipped and used from the viewpoint of increasing resilience rather than reducing vulnerability. In many ways that might be better, as resilience does not have the previously discussed negative connotations of the term 'vulnerability'. Nonetheless, the vulnerability lens was critical for arriving at this point in the discussion.

Vulnerability *to victimisation* refers to the relative risk of becoming a victim of F&CM either once or repeatedly. The risk profiles of individuals more likely to become victims of F&CM, along with the known characteristics of repeat victims, have already been discussed in detail (chapters two and five). Such profiles are often used to generate theory and also to inform the development of targeted crime prevention initiatives. As argued in chapters four and five, however, the case for targeting specific groups for prevention advice based on profiles from reported crimes is weak and crime surveys will be best suited to this task. Vulnerability *post-victimisation* on the other hand, may be described in terms of different levels of resilience to impact, or victims' ability to cope with the impacts of F&CM. This type of vulnerability is often neglected by the CJS, partly because it goes beyond the competence of many of its agencies. However, as discussed in chapter one and further evidenced in chapter four, the impacts of F&CM vary in magnitude and range. Furthermore, as previously discussed, few cases are investigated or make it to the courts. In this context, it is suggested that 'justice' for victims or 'putting the victim first' should include support to cope and recover from victimisation experiences. Models of intervention where the CJS and other state institutions focus on victims' wellbeing are not unheard of, especially in the context of restorative justice.

For such work to be successful however, vulnerability should be recognised in its full complexity, beyond the narrow conceptualisation found in the Victims' Code (see chapter two).

This framework identifies eight vulnerability factors, describes how each factor may be assessed and groups these across three broad vulnerability dimensions. The collection of vulnerability factors presented here is grounded in the data and were arrived at methodically. While these are inevitably open to debate and refinement through future research and further empirical testing, this framework nonetheless provides a starting point for identifying the relative vulnerability of victims and thus designing strategies to both target support where it is most needed and build victim resilience to F&CM.

1.1. Vulnerability Dimensions and Factors

Three broad vulnerability dimensions emerged from the thematic analysis: the *definitional dimension*, the *crime dimension* and finally, the *capabilities dimension*. Within these, eight vulnerability factors were identified (Figure 55). In short, the definitional dimension addresses the question of 'who' is vulnerable to harms associated with F&CM victimisation, the crime dimensions 'how' they are vulnerable and the capabilities dimension 'why' they are vulnerable. Together, these dimensions therefore help establish how to prevent and repair F&CM harms, and who has the obligation/ability to do so (Zehr, 1990, 2015).

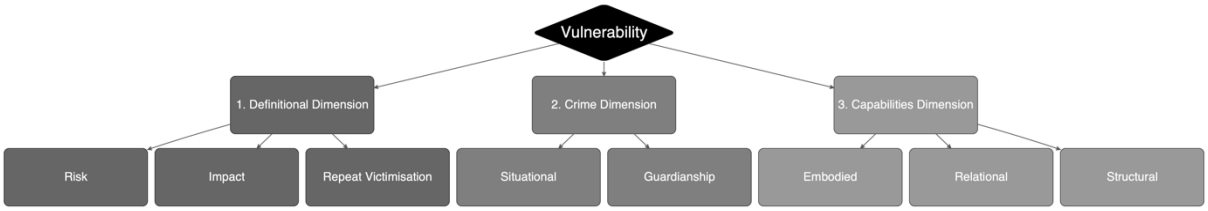

Figure 55 – Vulnerability Framework Diagram

The definitional dimension brings together factors which are directly derived from the definition of vulnerability above: the risk of, or susceptibility to, harm and the impact or magnitude of that harm, with respect to the victim's ability to cope with it. The definitional dimension is, therefore, descriptive. Defining vulnerability at this level will help to tentatively measure relative vulnerability, as risk and impact can be operationalised. However, limiting the analysis to these factors does not illuminate why some are more vulnerable or how their specific vulnerabilities may be addressed. For an in-depth understating of vulnerability, it is necessary to turn to the crime and capabilities dimensions. The crime dimension encapsulates

the circumstances and ways in which the crime was committed, which make an individual susceptible to F&CM (re)victimisation. Drawing on the insights from Routine Activity Theory (RAT) (Cohen and Felson 1979), this dimension illustrates how situational crime prevention can help reduce victims' vulnerability. Finally, the capabilities dimension relates to the wider factors of the victim's life and place in society, which can both make them more susceptible to F&CM (re)victimisation, as well as less able to recover from its impact. Drawing on Sen (1999), Nussbaum (2011) and Fineman (2008), factors within the capabilities dimension are understood as opportunities, or enablers of, coping. These incorporate a strong element of externality to the individual victim (the availability of such opportunities), while also requiring the individual to be ready to use them (Nussbaum's "internal preparedness" (2011, p. 61)).

Understanding vulnerability to F&CM across each of the proposed dimensions brings us closer to identifying why some individuals are more vulnerable and how best to respond to their needs. In doing so, idealised conceptions of the victim (Christie 1986) can be confronted where they are not helpful to victims or practitioners. This chapter describes each of these dimensions and its constituting factors and explores how they influence each other. The analysis is illustrated with excerpts from the data and the coding summarised in Table 51 below.[147]

	Vulnerability Factors	***Coded Phrases***	***Coded Crimes***
1. Definitional Dimension	1. Risk	NA	NA
	2. Impact	196	162
	3. Repeat & Multiple Victimisation	213	149
	Total	409	311
2. Crime Dimension	4. Situational	28	26
	5. Guardianship	84	69
	Total	112	95
3. Capabilities Dimension	6. Embodied	17	16
	7. Relational	31	25
	8. Structural	132	96
	Total	180	137

[147] The number of reports coded for risk is omitted as this is a quantitative concept within this framework. n(victims) = 160, n(incidents) = 332.

Table 51 – TA coding summary for vulnerability themes.

Some of the above vulnerability factors are easier to assess than others. While some can be quantitatively measured, directly or indirectly through proxies, others will require the development of qualitative criteria, akin to legal tests. However, the difficulty of measurement does not make such factors less important. Furthermore, qualitative criteria are not unfamiliar to those involved in criminal justice processes, where qualitative legal tests are regularly applied. In what follows, each of the identified vulnerability factors will be defined and illustrated through excerpts from the data. This will be followed by a proposal of how each factor may be measured or assessed and an exploration of how factors are inter-connected.[148]

1.2. Using This Framework

On one level, this framework articulates the theoretical value of the concept of vulnerability, as capable of bringing together the nuanced aspects of F&CM victimisation and critically engaging with 'ideal' conceptualisations of the victim. At the same time, it was developed to be a useful tool in the assessment of F&CM vulnerability. As an assessment tool, it suggests a variety of methods such as quantitative direct (e.g., population risk) and indirect measurement (e.g., through Likert scales), as well as discursive qualitative methods, for assessing each vulnerability factor as applicable. These different methods correspond to varying depths of assessment and thus the order in which the methods are presented is of relevance.

In the first instance, quantitative measurements are put forward within the definitional dimension, which provide an initial vulnerability score for each victim. These scores will enable practitioners to identify low and high scoring victims. Following this, an assessment of the factors within the crime dimension will help practitioners tailor advice to prevent future victimisation (including the re-victimisation of existing victims). In so far as the aim is to prevent re-victimisation, interventions based on the assessment of the crime dimension will also reduce the overall volume and the impact of F&CM on victims (Farrell & Pease, 1993). Finally, assessing the factors which constitute the capabilities dimension will help practitioners identify what how best to tackle *post-victimisation vulnerability*. Within this dimension, the in-depth assessment of embodied and relational factors aims to identify support which can make

[148] Refer to Annex VI for summary tables including definitions of all themes identified through Thematic Analysis, as well as the Codebook generated through the NVivo software.

individuals more resilient to the impact of F&CM. At the same time, assessing what structural factors make victims more vulnerable to/post victimisation will generate valuable evidence for policy development.

2. Definitional Dimension

The concepts of risk and impact are key definitional elements of 'vulnerability' to/post F&CM. *Vulnerability to* victimisation is understood as synonymous with risk of (re)victimisation and can be quantitatively assessed through victim surveys and, with caveats, through crime reports. Impact includes not just the range of possible negative consequences of F&CM victimisation (see chapter four), but also the extent to which the victim is able to cope and recover from these. The more resilient the victim is to these impacts the less vulnerable they are *post victimisation*. As such, assessing an individual with respect to risk and impact respectively, provides an indication of their relative *vulnerability to* and *post* F&CM victimisation. In addition, as argued in chapter five, repeat victimisation can be both a booster of the individual's vulnerability to victimisation and a vulnerability flag. On one hand, it is an indicator of greater risk (albeit retrospective given that the risk has already materialised), while on the other, being repeatedly victimised can be indicative of vulnerability factors beyond situational crime factors. However, risk, impact and being a repeat victim are descriptive rather than explanatory factors. While they describe relative vulnerability, they cannot explain why a victim is more or less vulnerable.

2.1. Risk of Victimisation

Risk of victimisation may be understood and measured probabilistically, as the odds of an individual being a victim of crime with respect to their characteristics and/or circumstances. Typically, risk of victimisation has been modelled and tested in terms of frequency of victimisation given characteristics of criminological interest such as age, ethnicity and gender, based on national self-report surveys such as the CSEW. Chapter two explored what distinguishes victims of F&CM from non-victims based on the CSEW estimates. Furthermore, risk of re-victimisation was explored in chapter five, by comparing the characteristics of one-time and repeat victims within the crime reports sampled for this thesis. This analysis confirmed that, as with other crime types, the same characteristics which significantly distinguish non-victims from victims, also distinguish one-time from repeat victims.

Furthermore, chapter five showed that age was the most significant characteristic in predicting RV with some differences in the time-course and mechanisms of RV across crime group (Fraud/CM) and specific F&CM categories.

Profiles based on crime surveys will help to identify whether certain groups are being significantly targeted thus are useful to help target F&CM crime prevention materials and campaigns. At the same time, risk profiles provide only a partial picture, as they provide little insight into what drives those differences and the relative impact of F&CM on specific victims. The vulnerability factors within the crime dimension tell us when and how those individuals become more vulnerable, which allows for the design of prevention interventions. Furthermore, risk tends to homogenise the experiences of highly victimised individuals/groups. As crime is unevenly distributed, surveys which are representative of the national population such as the CSEW tend to under-represent the experience of those who suffer disproportionately high criminal victimisation (Hope, 2015b). Similarly, risk (of RV) calculations based on recorded crime, will inevitably under-represent any groups which under-report. For example, differences in profiles of F&CM captured in the CSEW vis-à-vis known population demography and the sampled data, suggest that younger and non-white sub-populations are under-represented in recorded F&CM crime. As more and more factors are controlled for, measures of risk become more nuanced and efforts to target specific sub-populations for prevention advice more effective. However, they still operate at a level far removed from the individual experience and are therefore limited where the aim is to identify and provide support adequate to meet victims' needs. As such, on its own, risk does not explain what drives differences between groups says nothing of the impact of F&CM on victims. Understanding the drivers, however, is key to providing a response which meets the needs of victims. Considering 'why' some are at greater risk to victimisation highlights that risk is mediated by the *crime* and *capabilities* dimensions. As such, while different levels of risk may be observed and measured, understanding (and addressing) those differences will require engagement with all three dimensions of vulnerability. First, however, the impact factor will be explored in more detail.

2.2. Impact of Victimisation

The *impact* or the *harm* caused by a victimisation experience is another factor of the definitional dimension of vulnerability. The scale and range of impacts F&CM have been discussed throughout this thesis. In chapter four, it was demonstrated that financial losses

varied widely between victims, with many reporting no losses and, for those who did, most losses being concentrated at the lower end of the spectrum (median of £350 for individuals). However, it was noted that there were some demographic differences with older individuals and males reporting higher losses. There were also some noteworthy caveats regarding reported loss, as amounts were found to not always have been recorded in a way that was appropriate for quantitative analysis and victims were only asked to report direct losses, known at the time of reporting. Furthermore, in chapter five demonstrated that RV results in higher financial losses. The data sampled for this study did not enable a quantitative assessment of the impact of F&CM victimisation across a wider range of impacts. Nonetheless, the themes identified through TA in chapter four corroborated previous research showing that the impacts of F&CM beyond direct losses are varied. As such, assessments of vulnerability necessitate the consideration of a wider range of impact factors.

Furthermore, the impacts of F&CM victimisation are linked to the other vulnerability dimensions in this framework. Firstly, negative impacts can exacerbate vulnerability factors within the capabilities dimension. For example, as discussed in section 4.3 below, individuals who are "desperate" for loans may be more susceptible to *Advance-fee* fraud. As such, financial precarity can both drive and worsen the impact of financial losses caused by F&CM. Similarly, capability factors can also contribute towards increasing the impact of the crime on victims' wellbeing and/or make them more vulnerable to further victimisation. The excerpts below illustrates the link between embodied and structural factors, with respect to vulnerability to online fraud. Here, the victim's repeated victimisation is connected to their learning difficulties and the impact of the crime to their economic precarity. It also shows the importance of the relational dimension as support from family members, as previously discussed, can be both essential to identifying a victim in the first place, but also strained by victimisation experiences. Furthermore, in this case the supportive role of various institutions is highlighted, including the police and social services.

Crimes 15228 / 15852

Report 1:

"The victim is vulnerable due to learning difficulties has been befriended by men on Facebook and has been duped into sending large amounts of money to them in Nigeria and Pakistan. At the time, she thought that there was nothing wrong in doing this thinking they were brother's of the same faith. The victim being on low income and residing with her mother, has borrowed from her family and requested large amounts of

money in order to send to these males, unaware of the implications of befriending person/s unknown due to her vulnerabilities. […]"

Report 2:

"[…] [The Police] spent several hours and several visits explaining to [the victim] this is a scam, and she still refuses to believe it's a scam. I [family member] visited her on Monday and spent an hour explaining again it was a scam, but as soon as I left she went to the bank and transferred the scammer a further £210 by Western Union. We reported this to the police again, [… who] visited this afternoon [… and] explained again that this is a scam and to stop sending them money, but [the victim] still thinks she is getting a 6 million pound inheritance. [Police] is completing a referral to social services."

While it will not be possible to anticipate all impacts, it is straightforward enough to ask the victim (or those reporting on their behalf, referred to as proxies) to indicate what level of impact they have experienced thus far, across the range of areas identified in chapter four. This assessment of victims' experienced impact can be achieved through Likert-scale type questions, with the possibility of allowing individuals to elaborate using free-text, if they wish to do so. Drawing on the impacts identified in chapter four and Nussbaum's notion of "central capabilities", these may include impact on bodily health and integrity, emotions and mental health, play and recreation, relationships with friends and family and control over one's identity and environment. In fact, since this data was collected, the AF/NFIB system has evolved somewhat in this direction. A newly implemented system includes an additional victim impact assessment which individual victims complete either when reporting online or via the AF call centre. As a result, local forces now receive a self-completed (0-5) score on the crime's impact on the victims' confidence, health and finances.

Of course, such an approach is imperfect as it may not capture all types of impact and victims (or their proxies) may not be fully aware of the impact of a crime at the point of reporting. As argued, vulnerability is not concerned with 'impact' as an objective fact, but is relative to the individual's ability to withstand or recover from it. However, at the point of crime reporting the individual's ability to recover might not be fully understood or anticipated. Nonetheless, it is argued that the best judge of impact is always the victim themselves, as individuals automatically make a subjective assessment relative to their circumstances. Furthermore, space can be provided for victims to give an account of the impact of the crime in their own words and the types of impact measured can accordingly be continuously reviewed by academic researchers and practitioners alike. At the same time, given the intersections between impact and other vulnerability dimensions, addressing vulnerability *post victimisation* will require a

more discursive approach to assess "why" the victim is vulnerable, as well as "how much" more vulnerable they are relative to others.

2.3. Repeat and Multiple Victimisation

Research into RV has shown that individuals do not become repeat victims by chance and thus RV is, to some extent, a 'flag' for greater risk of victimisation. In addition, they are more likely to suffer greater impacts, which in turn may increase (or 'boost') their vulnerability to further victimisation. The empirical research in chapter five has demonstrated that RV is associated with older males and that repeat victims typically experience greater financial losses. Furthermore, the qualitative analysis of the impact of F&CM on victims suggested that RV can also be a flag for post-victimisation vulnerability, in so far as evidence of impacts beyond direct financial loss was found predominantly within the repeat victim TA sub-sample. Of particular note, were the mechanisms of repeat victimisation and the degree of impact on so-called 'chronic victims' (four or more reports). In relation to chronic victims, on one hand RV is intimately linked to the crime dimension as the circumstances of the crime itself can lead to victims being victimised over again. At the same time, RV was shown to be a flag for vulnerabilities associated with the capabilities dimension e.g. old age or disability. Thus, in line with Johnson (2008), it is concluded that RV can be both a symptom ('flag') for vulnerabilities which existed before the individual became a victim and a cause (or 'booster') of vulnerability to further victimisation, as well as to the impacts of being victimised.

As also discussed in chapter five, one of the most striking aspects of the process of RV is the continued narrative between multiple incidents. In some cases, the victim realises the fraudulent nature of a subsequent contact, but not always.[149] Furthermore, the nature of the relationship which the offender develops with the victim is key to further victimisation, linking RV to relational vulnerability factors. As such, it follows that (repeat) victimisation can increase an individual's vulnerability to further victimisation. In addition, the qualitative analysis also identified some cases where multiple victimisation – where an individual is the victim of a variety of crime types – may increase vulnerability to/post F&CM victimisation. In

[149] Overall, there were 65 cases of Fraud Recovery in this sample, 74% of which reported a financial loss of, on average, £2060. In addition, 28% of Fraud Recovery cases were linked to repeat victims. For this sub-group, the average loss was £2952.

particular, there were a few instances of businesses reporting fraud following domestic burglaries e.g., suspects attempting to use credit cards in stores following burglaries. In crime 6401 below, it is stated that the victim is considered vulnerable, but no further justification is provided. Based on circumstances where victims were flagged as vulnerable by AF, it is assumed that an embodied factor related to disability or ill health was noted, but not explicitly captured. It is implicit, however, that a burglary and the victim's subsequent vulnerability created the opportunity for this further victimisation. Furthermore, the relationship with the known suspect also increased both the risk and impact of victimisation.

Crime 6401

> "Known suspect, sister of the victim, has been acting on behalf of the victim, who is vulnerable, with initial authority from the victim to deal with an insurance claim for a burglary which occurred in [date]. The insurance claim was for household contents and jewellery. The insurance company settled the claim and split the claim into two separate payments, one for the contents […] and a further payment for the jewellery […]. The suspect had given her bank details to the insurance company instead of her sister's bank details, for the payment to be made into her bank account and retained the money from the insurance payout […]."

As previously shown, the seemingly simple task of measuring RV is not without its challenges. The analysis in this thesis has corroborated previous research and shown that F&CM victimisation is a process rather than an event. Where one 'instance' of victimisation stops, and another begins is not always clear – and in the case of police recorded crime it is mostly designated by administrative rules. As previous noted, these tend to favour the recording of multiple cases of CM where fraud follows the 'one crime per victim' rule. As such, how many crimes are recorded is arguably more reflective of recording rules than the realities of RV. A step in the right direction would be to employ flexible/relational database systems allowing for the following to be distinguished: 1) the victim the report relates to, 2) the totality of the report itself and 3) each 'crime' contained in the report (e.g., how many counts of fraud). Since this data was collected, the AF system has been optimised to automatically create a repeat victim flag, based on whether the victims' details are found elsewhere in the AF/NFIB database. Again, this is a step in the right direction. However, it is important to establish consistent rules with respect to the time-period within which RV is measured (e.g., within the previous year versus all recorded years) and whether one report contains more than one instance of victimisation.

3. Crime Dimension

The crime dimension relates to the circumstances of the crime itself which may render individuals more vulnerable to (further) victimisation. As such, the crime is assumed to constitute a harm in itself. The factors grouped under the crime dimension are inspired by Routine Activity Theory (Cohen and Felson 1979) and relate to the everyday situations or events which (temporarily) increase the victims' vulnerability to victimisation. Such everyday situations arise due to ("risky") activities victims engage in, as well as the level of guardianship, which is exerted, including technical controls, processes and attitudes which prevent F&CM.

In line with previous research, these insights suggest that prevention activity emphasising the role of situational factors, increased guardianship and the potential for repeat victimisation will help reduce vulnerability to F&CM. However, this analysis also suggests that the crime dimension, with the exception to its links to 'chronic' repeat victimisation, says relatively little about vulnerability post victimisation. Furthermore, while factors within the crime dimension of vulnerability are important to explain 'how' victims become vulnerable to F&CM, they are intimately related to structural factors within the capabilities dimension discussed below.

3.1. Situational Factors

Situational factors refer to time and/or spatially constrained situations which make individuals more vulnerable to F&CM. Several ('risky') routine activities were identified as making victims more vulnerable to F&CM victimisation. These included online gambling and gaming, seeking services online (particularly loans), online dating, buying and selling goods online and occupational hazards stemming from professions as diverse as journalism/research and sex work. In addition, there was some evidence for the effect of major events which attract considerable media attention, as these create opportunities which are exploited by offenders to commit F&CM. However, the relative prevalence of these examples in the data was low, with guardianship playing much more significant role within the crime dimension.

Crimes 6769 / 14111

Report 1:

"[I was] first contacted by the bank who advised certain transactions were being made using my bank card. This has happened to a few members in the household. Disputed with the bank to find that someone had also hacked an online [gambling] account registered under my son's name. Disputed this with company as I have checked his bank

> statements and the same has happened to him. […] All bank cards have been changed, however the bank are looking at obtaining the money back because they think my son has taken the money with the account being registered under his details. He has flatly denied this and has decided to take police action because he wants to dispute the use of the account and also someone has been using his details to register on various sites, clear sign of identity theft."
>
> **Report 3:**
>
> "I have been a victim on fraud on numerous occasions. Last year I fell victim to £7000 loss to an online gambling company and the institution weren't able to cover the loss as the account used on the site was in my son's name. He is still fighting till this day to prove he wasn't the user of the account. Today I found that more money was transacted from my credit card to an account with [betting company] online. The account was also in my son's name however the card was used through PayPal to deposit to his account. He has reported the account as compromised and hasn't used the account. He has bank statements to prove this."

There were examples of online gambling and gaming as a risky activity, where accounts were hacked and tampered with (i.e., information on the account changed), as a first step in a series of frauds involving identity theft and/or financial loss. The excerpts above include the first and last of three related reports made over a period of 11 months from mid 2015 onwards, totalling a reported loss of £6,400 (although the above description suggests an even higher loss). Across the set of reports, it transpires that a series of credit accounts were created using the victims' details and fraudulent payments made. The victim attributes these to the hack of their son's online gambling account. There were also several examples of victims who, like in crimes 4692 and 1828 below, provided their details via rogue websites when seeking online services.

Crime 4692

> "Victim has a premium disc for windows 7. Victim lost the key for it and did a search online for a new one. Victim saw a number on the internet which offered aftercare and maintenance. Victim contacted the number. Suspect's asked for access to the victim's computer which the victim gave. Victim can now no longer access his computer."

Crime 1828

> "Victim was cold called by the suspects after looking for loan options online. The victim was told that they had been accepted for an unsecured loan for the full amount of £500. The suspect explained that the victim will be required to make an advanced payment of the first instalment in order to secure the loan. The suspect instructed the victim to purchase £70 in UKASH vouchers and after doing so provide them with the voucher codes. Upon doing so the suspect then made various reasons why the victim should pay further fees before receiving the loan (TAX, PPI, transfer fees) also advising victim could get more money. Victim has contacted UKASH who advised the vouchers have been cashed."

The first excerpt in particular, illustrates a recurring theme where individuals were victimised after looking for a loan and sharing their details with rogue online loan companies. As with online gaming, seeking online services may be classed as a 'risky activity' that makes individuals more vulnerable to F&CM. However, these instances of victimisation also demonstrate the role of lack of guardianship (e.g., entering personal information into an unverified website) and the role of enabling industries as discussed below (e.g., the use of UKASH vouchers as a payment method). In addition, crime 4692 makes it clear that the motivation for engaging in the 'risky' activity of seeking an unsecured loan has its roots in the victim's financial difficulties, a sign of an underlying structural vulnerability. As such, while certain activities may provide the immediate opportunity fraudsters seek, enabling industries may play a role in increasing victims' vulnerability, beyond how 'risky' activities are in themselves.

Alongside risky activities, there was some evidence in the literature of the role that major events, either in the victim's own life or reported in the news**,** can play in increasing victims' vulnerability to F&CM. These may include events as varied as being recently bereaved and having to take on the financial management of new assets or having a specific stake/interest in an event widely publicised by the media which offenders are able to exploit. Within this sample, for instance, there was a high incidence of reports mentioning the UK telecoms company TalkTalk, in the months following their high-profile data breach, made public in late October 2015 (as illustrated in Figure 56).[150] In the context of the current COVID19 pandemic for example, many may find themselves having to engage with more services at a distance, including through digital and analogue means with which they were previously unfamiliar. Such events create opportunities for fraudsters to act – and AF have reported a sharp increase in coronavirus related fraud reports across England and Wales, even before the lockdown

[150] TalkTalk customers were reported to have been affected by data breaches of the company's Indian call centre in December 2014, of Carphone Warehouse in August 2015 and then of the large scale (although by no means sophisticated) cyber attack in October 2015 (Gibbs, 2015). The latter was one of the largest breaches in the UK at the time with the details of 157,000 customers being compromised including bank the account numbers and sort codes of over 15,000 customers – some of which could still be found online via a Google search as late as May 2019 (BBC, 2019b).

started (Action Fraud, 2020b).[151] A cursory review of the communication channels of AF's fraud alerts, the City of London Police (who operate the NFIB) and National Cyber Security Centre, all reveal that their fraud alerts, prevention messaging and even enforcement success communications are overwhelmingly framed by current events e.g. the EasyJet data breach (NCSC, 2020), sporting events (Action Fraud, 2020a), or the COVID crisis (City of London Police, 2020).

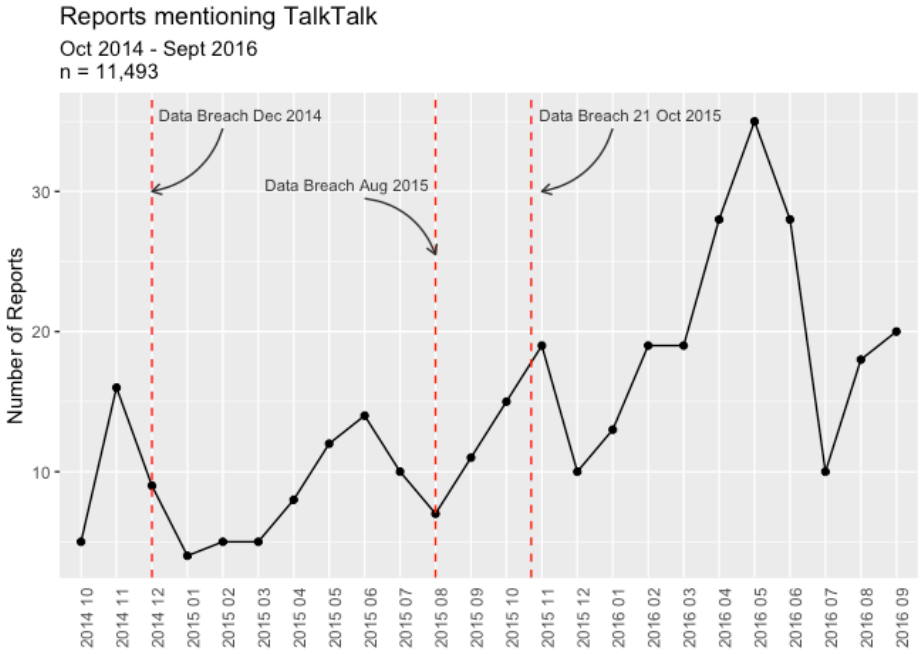

Figure 56 – Reports mentioning telecoms company 'TalkTalk'

As the above discussion demonstrates, law enforcement agencies have developed mechanisms to gather and develop situational intelligence. As was discussed in chapter one, the NFIB's 'Known Fraud' database is designed to find links between recorded incidents for the purposes of investigation. In addition, discussions with practitioners at the NFIB revealed that crime and information reports are analysed to identify trends in the methods and pretexts used by fraudsters and hackers. Situational trends can be explored through a combination of continuous exploratory crime data analysis, combined with keyword searches and coding analysis. Given

[151] Across England and Wales, 20 fraud reports related to COVID-19 were identified in February; in March, there were 46 reports between 1 March and 13 March, and 38 reports in just five days (14 March – 18 March) (Action Fraud, 2020b). In the South Wales region (including Dyfed-Powys, Gwent and the South Wales police force areas), the volume of F&CM reports over the lockdown period (approximately April to June 2020) increased by 69% when compared with the previous 3 months. However, when compared with the same period in 2019, the increase is only 28% (S. Correia, 2020). This shows that while some of the increase may be due to other factors, the COVID situation is likely to have had a large impact.

the current pace of development in data mining techniques, it is expected that such capabilities will continue to improve.

3.2. Guardianship Factors

Guardianship refers to the extent to which specific and effective controls are in place, or specific actions taken, to prevent F&CM. In the way the term is employed in this framework, it includes the control exerted by law enforcement and the CJS more broadly but it also extends to actions by other organisations and victims themselves, to a) frustrate criminal attempts altogether e.g. through cold call blockers, good password hygiene and anti-virus software; b) minimise their impact e.g. cancelling accounts or changing passwords when a hack or social engineering is suspected; as well as c) guardianship attitudes e.g. seeking independent reviews of an investment scheme or independently verifying the fraudsters' credentials. Inadequate guardianship makes individuals more vulnerable to F&CM victimisation and allows hackers and fraudsters to leverage the mechanisms discussed in chapter five, to successfully carry out crime.

The ways in which lack of guardianship amplified victim vulnerability are illustrated by the actions taken by victims in their interactions with criminals and their role in the facilitation of F&CM. In chapter five, it was noted that the typical criminal MO in cases of F&CM involves the offender building rapport with the victim and persuading or manipulating them into taking a wide variety of actions which will help them carry out the fraud. This may include persuading the victim to click a malicious link, call the fraudster back, giving them remote access to a computer, entering personal details in a rogue website, physically journeying somewhere such as a bank or Western Union branch to move or transfer money, or recruiting others into investment "opportunities". These are 'routine activities' in the sense that they are normal, everyday activities, but not exactly in the Cohen and Felson (1979) sense of activities which take place at a certain point in time-space which then converges with a motivated offender and a suitable victim. Rather, it is through the interaction between offender and victim, under the guise of a deceitful pretext, that the need for a given routine activity is created and/or exploited. As such, it may be more appropriate to think of these actions not so much as routine activities but actions which exemplify low guardianship.

Given that the sample of cases analysed related to individuals who were victimised, examples of inadequate guardianship were numerous. Nonetheless, increased guardianship emerged

from the TA as an important factor in stopping RV. Firstly, guardianship attitudes were expressed through the victims' own investigation of the circumstances around the (attempted) crimes. This included attempts to find out more information about the fraudsters by calling them back and engaging them in conversation, tracing suspects' details through online searches (e.g., 8076 below), posting publicly on social media about their experience to solicit information from or warn others (7056), and making subject access requests from legitimate companies (i.e., under the UK's data protection regime), to gather details of their identity being used by fraudsters (12865).

Crime 8076

> "The [victim] then checked the internet about this company and […] when the caller googled it the company came up as the same address but a different name and a number which the caller called and they said that they have never heard of [the suspect]."

Crime 7056

> "Victim was prior victim of dating scam. The victim posted on Facebook a picture of prior dating scam suspect asking if anyone knew them. The victim then received message from suspect purporting to work with the US government with the United Nations. The suspect told victim the suspect was really a major in the US army. The suspect then told victim they would be awarded £250,000 if they paid a Western Union advance fee. Victim is also receiving messages from another suspect purporting to be solicitor requesting Western Union."

Crime 12865

> "The victim had made data subject access requests with her internet service providers, [X] Loans and other companies whose services were accessed by suspects, providing further evidence of unauthorised activities."

The prevalence and extent of victims' own investigations was surprising and suggests that victims are prepared to play active roles in preventing RV. It also suggests an alternative interpretation to Whitty's (2019) finding of greater guardianship among those already victimised – this may follow, rather than precede victimisation. This could be leveraged if victims were given the necessary advice and means to ensure they preserve any (digital) evidence necessary for police investigations. However, attempts at guardianship on the part of the victim can also lead to victims being targeted for further victimisation or even retaliatory action by the criminals. In 12865 above, the act of posting about their experience on social media led to further targeting of the victim. In 166 below, the victim identified the suspect's email address and sent a confrontational email to the hacker of her online account.

Subsequently, a threatening message was displayed on the victim's laptop, before it crashed. In such cases, attempts at guardianship by the victim can potentially increase the victim's vulnerability to/post victimisation. The victim's statement that her laptop was hacked despite her use of anti-virus software also highlights how guardianship is often beyond what 'off-the-shelf' digital security products can offer. This raises questions of how effective guardianship can be against targeted attacks on individuals unless victim vulnerability is construed to include multiple agents, both human and non-human – 'hybrid victims' as theorised by van der Wagen and Pieters (2020).

Crime 166

> "Suspect has hacked into victims laptop ran by Windows 7. The victim uses anti-virus ... The suspect put on the victims screen before crashing; only paying the price of FLTK, you are having one of the most dangerous people on earth. The suspect then closed down the computer. This is more then likely the result of the victim contacting the suspect when her Neteller account was hacked and she could see the email address of the suspect."

Also under the theme of guardianship were actions taken by the victim themselves and a wide network of stakeholders including law enforcement, financial institutions and tech firms, which were intended to prevent (re)victimisation. These include the cancellation of compromised accounts and cards, banks stopping or refusing to process transactions, online marketplaces blocking fraudulent users or advising victims not to continue communicating/transacting with suspects. In 3513 below, the victim was alerted to an ongoing fraud, which had already resulted in financial loss, by staff at the local shop, where the victim went to purchase UKASH vouchers at the request of fraudsters. This case also provides a powerful example of the relational factors discussed elsewhere.

Crime 3513

> "Victim […] received a call from a company claiming to be [local]. It was a female with a South-Walian accent stating she was over-paying for her gas and electricity bills and they could save her around £800 annually. An assessment date was arranged and a male […] attended at her h/a [home address] and conducted an assessment of her boiler. She could not remember what company he said he was from but he did have an ID card but IP [Intended Person] does not remember his details. He came in a private vehicle but [victim] could not remember any make/model. He was white, English. IP had paid £299.99 over the phone to [company name] prior to the assessment. She paid over the phone and gave all bank card details. IP has then been phoned by the following number today – [non local number]. Asian male spoke to IP stating a solicitor would be attending at her h/a today at 12:40hrs to give her a cheque for £3600. He then asked her to go to [local] stores to purchase £200 in UKASH vouchers to give to the solicitor when he

> attended. IP has then tried in [local store] but they did not do UKASH vouchers. (…) She has then been told to attend [x] store, [location] and told her how many miles away she was from her h/a. They told her to get a taxi and get a receipt and they would reimburse her. She has then got a taxi to [x] store, and has cashed £200 in Lloyds bank, to pay for the vouchers. She has then attended [x] and used cash to buy 2x £100 UKASH vouchers. Staff at the store became concerned about why the female needed this amount and have then called [the police]."

There were also instances which suggest that such preventative action is not always adequately taken. As will be seen in the enabling industries section below, a large proportion of victims make payments to fraudsters through services such as UKASH, MoneyGram and Western Union, which are considerably less regulated than the traditional financial industry. However, even high street banks failed to prevent some of the frauds sampled. In another excerpt from 2152 below, the victim (over 75 years old) went into a local bank branch to withdraw a large sum of money with which to pay fraudsters. Since March 2017 however, cases this case would potentially trigger the banking protocol which would prevent the fraud from succeeding (see chapter one). At the same time, as will be discussed below, it is questionable whether such mitigation activity is adequate overall, given the previously discussed role of legal enablers (chapter five).

Crime 2152

> "[The victim] has received a phone call from [number]. And a male has stated that there is a problem with her bank and she needs to take money out and pay it into a different account. As a result of this [the victim] has gone to Barclays bank and withdrawn money, the bank have said £16,000. She has then gone to Natwest bank and paid the money into an account there in the name of [n…] account number [...], sort code […]. The account [the victim] has withdrawn the money from is at Barclays account number […], sort code […]. I have informed her that Action Fraud would look into this incident."

Finally, victims' disbelief regarding being victimised and/or confusion as to what had in fact taken place, emerged as a barrier to effective guardianship. Disbelief and confusion were captured across multiple reports where the victim called AF still thinking/hoping the fraud was legitimate, as exemplified in 12600 below. The wording of this report suggests that the victim was unsure as to whether he had been victimised. In some cases, this was explicitly stated by the AF call handler (e.g., 9723). In other cases, such as the previously mentioned, victims may even refuse to believe they were victimised.

Crime 12600

> "The victim received a call from a firm called [name] (suspect). The suspect asked the victim to invest in 'bit coins', the victim was buying bit coins at £2.30. Originally the victim was asked to invest £1,000 originally in September, the victim agreed and sent the company a cheque for the requested amount. The victim was contacted again by the suspect in October, the suspect claimed that the victims investment was making money and encouraged the victim to invest a further £5,000 in order to reap the full benefits, the victim agreed and sent the suspect another cheque on [date]. The suspect contacted the victim and said that the coins that the victim had bought at £2.30 had now risen to £7.49, by saying this the suspect convinced the victim to invest a further £2,000, again sent by cheque to the suspect. (…) Any time that the victim calls the suspect now he is told that his investments are doing well and everything is in place, the victim has received no returns on his investments whatsoever. The victims bank Barclay's are worried about the amount that the victim has sent and that is why they have asked the victim to call action fraud. The victim states that the suspects are also Barclay's account holder. The victim has funded this investment through his 'standard life fixed bond'."

Crime 9723

> "Euromillions has contacted the victim via letter. Telling the victim that he has won £715k and was asked how he wanted the money, and he told the suspect that he would like it via bank account. Victim then called up and asked why the money wasn't transferred and was asked if he had received a letter from the un with further instructions, was told by letter from 'UN' [United Nations] told that there is a clearance to pay for any funds over $500k of a 1% which would be £7150. This letter included a lot of lawful jargon including referencing major terrorist attacks to back up the legitimacy. Was stamped by 'UN'. Victim called believing that this was still legitimate."

Situations where the victim refuses to believe they were victimised have been highlighted in previous research, as well as news coverage of the impact of fraud (Murray, 2018). As in previously mentioned crime 15852, where victims refuse to improve their guardianship attitudes, this can lead to strained relationships with friends and family and a loss of autonomy and privacy for the victim. In this case, the victim's refusal to believe they were being victimised led to a referral to social services and hence increased state intervention in their lives. In a different scenario, technical controls such as the call blockers distributed by Trading Standards, while installed with the consent of the victim, also introduce an element of surveillance of the victim's communications for the sake of preventing F&CM (see chapter one). As such, an emphasis on increasing guardianship to decrease vulnerability and, conversely increase resilience to F&CM, must be proportionate and carefully consider any negative impacts on victims' wellbeing and autonomy.

Finally, as discussed in chapter one, guardianship has been operationalised across several research studies testing RAT in the context of both F&CM, with mixed results. This may be

the result of a narrow conceptualisation of guardianship e.g., limited to the use of technical controls such as anti-virus to prevent CM. The above discussion suggests that guardianship is best operationalised to include technical controls but also actions to mitigate against F&CM re-victimisation, as well as guardianship attitudes. An assessment of guardianship at each of these levels can be ascertained when victims report an incident, by recording the characteristics of the MO such as methods of contact and payment, asking victims to indicate what measures they have taken to prevent further victimisation and recoding victims' attitudes to and capabilities with respect to guardianship e.g. by using Likert scales to determine how far they agree with a series of statements regarding their guardianship attitudes and proficiency. Since this data was collected, the most up-to-date version of the AF reporting system takes into account the individual's level of proficiency with respect to fraud awareness and digital skills, which is a step in the right direction. In addition, guardianship can be assessed discursively, by engaging the victim in a more in-depth discussion about what steps to take in order to protect themselves from re-victimisation.

4. Capabilities Dimension

Inspired by Sen (1999) and Nussbaum (2006, 2011), the capabilities dimension brings together factors which are independent of the crime itself, but nonetheless adversely impact the victim's ability to recover from the impacts of victimisation and may in fact exacerbate vulnerability to further victimisation. The capability dimension includes *embodied*, *relational* and *structural* factors which, like Fineman's "assets of resilience" (Fineman, 2008, p. 13) or Sen and Nussbaum's "capabilities", create opportunities for individuals to prevent victimisation or withstand the impacts of F&CM. As such, this vulnerability dimension is most useful in understanding "why" some victims are more vulnerable than others – and what is needed to prevent and address the harms of F&CM victimisation.

With the exception of embodied factors, the capabilities dimension is the most neglected in current policy and practice. However, factors within the capabilities dimension not only have a direct effect on the individual's relative vulnerability but, as has already been highlighted, mediate the other dimensions in this framework. As such, it is argued that the CJS, state and non-state agencies should seek to assess and actively address the capabilities dimension of vulnerability. Here, a multi-agency approach is necessary.

4.1. Embodied Factors

Embodied factors include physical characteristics and conditions which, with respect to their own social context, make the individual more susceptible to F&CM victimisation. This may include cognitive states (either permanent, such as having a learning disability or a condition such as dementia, or temporary, such as being under the influence of alcohol) and personal characteristics such as age, gender or ethnicity. As noted by Walklate (2007a), however, there is no reason why these individual characteristics should, in themselves, make individuals more vulnerable. In fact, these may be thought of as indicators for relational and structural factors which imbue them with significance (e.g., ageism rather than age, sexism rather than gender and racism rather than ethnicity). As such, when we consider embodiment as opposed to the individual's characteristics in themselves (as with risk calculations), the focus is on how the subjective experience of those characteristics makes individuals more vulnerable to and post victimisation and, if so, how the subjective experience of those conditions may be changed. This focus is therefore solution oriented and better placed to drive interventions and practices to meet victims' needs.

Several examples of embodiment were identified in the analysis of this data as key to the construction of victim vulnerability within crime reports. These included the victims' age, learning difficulties or cognitive conditions, ill health and disability. In fact, these were the only aspects to be explicitly identified within crime reports as indicators of vulnerability, i.e., the victim was described as "vulnerable" due to age, disability or ill health. With respect to age, the fact that the victims' old age was restated or noted with terms such as "elderly" in the free text incident description, despite age being recorded elsewhere on the crime report, is significant. This emphasis on old age signals its importance to constructions of the vulnerable victim of F&CM. At the same time, the reasons why age may render an individual more or less vulnerable were often not explicitly articulated, with the exception of the excerpts from a repeat victim below.

Crimes 7930 / 8076

Report 1:

"Victim was contacted in respect of his carbon credits by [company] to say that they have sold his credits to the sum of £181,200.00 and request a fee of £25k which is a fixed fee. The victim was also a victim in a fraud case involving the said carbon credits which was investigated by the serious fraud office [ref] no monies have been paid to [company], details from victim are very vague due to his age and vulnerability."

Report 2:

"[The caller's] Granddad got a phone call from a man asking for 25,000 for shares which he sold [on the victim's] behalf and in return for 25,000 he would get 180,000. Keeps calling […] constant[ly] […]. When the caller googled it the company came up as the same address but a different name and a number which the caller called and they said that they have never heard of this man. The letter was signed by Mr. [X]."

The two incidents illustrated above, were made within a week of each other and resulted in no financial loss – although the victim had previously lost money to a similar *Investment* fraud. In this example, it is clear that the call handler attributes the difficulties in understanding the details of the crime to the victims' "age and vulnerability". Given the victims' vulnerability is not justified in any other way, it is implied that vulnerability is primarily due to old age. Difficulties in communicating the circumstances of F&CM to others may result in inadequate provision of prevention advice and support and thus increased vulnerability to and post victimisation. Such difficulties may be associated with a variety of embodied factors including young and old age, cognitive ability or language barriers. In the above case however, a family member intervened to provide support to the victim, illustrating how embodied and relational factors intersect.

The previously noted crime 15218 is one of three reports, as previously noted, by a female victim in her early forties with learning difficulties. The report implicitly suggests that part of the reason why the victim is repeatedly targeted by romance fraudsters is that, because of her cognitive condition, she is unable to identify deception. In this way, the victim's learning difficulties make her more vulnerable to (re)victimisation. This is further highlighted by the fact that all reports were made by a proxy on behalf of the victim who was reluctant to accept that she had been victimised.

Crime 15218

"The victim is vulnerable who has learning difficulties. She has befriended a male on Facebook from Africa and contact has been via e-mail. The male requested she send him £2000. She sent this via Western Union. The money sent forms part of the victim's inheritance. The victim who initially retained the western union receipts has since destroyed them. This has been discovered by the victim's brother after discussing her finances with her and subsequently being reported. This is the second instance since May 2016 of the victim being befriended by unknown males via Facebook and the victim sending monies on their request."

The next excerpt is from crime 15568, the last of three reports with no financial loss However, it is implied that the victim's ill health exacerbates the upset caused by the constant contact

attempts by suspects. In other words, ill health diminishes the victim's ability to overcome the impact of victimisation, leaving her more vulnerable post victimisation. Crime 8661 below is the second of two reports made on the same day and concerning the same situation. Here, the victim's son suggests that his father's medical conditions make him "an easy target" and thus the fragility of ill health leaves the victim more vulnerable to (re)victimisation. Although, the level of financial loss is still being ascertained at the point of reporting, their RV is expected to run to hundreds, maybe thousands of pounds.

Crime 15568

> "Victim called in advising that she has been getting contacted repeatedly by all different companies cold calling her, the victim advised that on one call they had used sexual language towards her, the victim has advised that she is disabled and has suffered from 2 major strokes and that these calls are becoming too much for her, she advised that she was contacted yesterday again claiming to be from BT [British Telecom] and they advised the victim that her broadband is running slow and that 8 other addresses are using her broadband, they then asked the victim if she could open up her laptop, the victim advised that she can't do this as she is partially sighted and asked them to call back when her husband is in. The victim advised that they have called back again today […]."

Crime 8661

> "Letter sent claiming my father had won the jackpot on world lotto. He's 87 years old, receiving chemotherapy for prostate cancer, is diabetic and has other medical ailments so is an easy target. These details came to my attention today, he's also dealt with companies such as [name] based in Belgium, [name] based in France, [name] also based in France, and possibly other companies who appear to have scammed him. We will be requesting bank statements to ascertain the level of costs involved as he's been dealing with some of these companies for over 2 years and will update this report when received. […] The total scam amount will run into hundreds of pounds, possibly thousands."

The above excerpts illustrate the effect of disability and ill health on vulnerability to and post F&CM. This, however, stands in contrast to the account in 15568 where the victim points out that his autism makes him more attentive to patterns which suggest foul play. As such, the focus is not on cognitive states as such, but how these affect risk and impact of victimisation.

Crime 15568

> "[…] I have given them [online betting company] the chance to give me the money played that day back as it did not meet up with their return rate. So in effect defrauding me of several thousand pounds, I have autism and notice patterns in things and I knew something was up as I was getting a bonus round with no bonus, I would send you the game data but they have locked my account so I cannot access any of it, sounds a bit fishy does it not? […]"

The above discussion illustrates the ways in which vulnerability to/ post F&CM victimisation is constructed from embodied characteristics. While the effect of embodiment on vulnerability is not easily measured in a quantitative sense, this does not make it less important. A qualitative test is suggested to assess embodied factors. The test would ask practitioners to consider, in light of the victim's circumstances, any of their embodied characteristics including (but not limited to) age, gender, ethnicity, cognitive ability and health, are likely to result in a reduced ability to increase guardianship against future F&CM attempts, or a reduced ability to seek and access the necessary support in order to recover from the impact of the victimisation experience.

4.2. Relational Factors

Relational factors relate to the way in which relationships and/or dependencies on others can make individuals more vulnerable to F&CM and its impacts – or conversely provide support and be a source of resilience. This includes a wide variety of relationships which the victim has with family and friends. These can be a crucial determinant of F&CM vulnerability.[152]

Crime 1055

> "The suspect is the victim's ex-partner. The suspect has hacked into the victims Facebook account and changed the password so that the victim can no longer access the account. The suspect has post statuses on behalf of the victim and deleted some of his friends from the profile."

With respect to relationships that make victims more vulnerable to/post victimisation, unsurprisingly it emerged that this was the case primarily with respect to victim-offender relationships, but there were also instances of suspects that were known to the victim prior to the incident recorded, or where the victim had been referred to the suspect by a friend (who may have also been victimised). Crime 1055 is the third of five reports made on the same day, relating to an ex-partner who systematically hacked several of the victim's online accounts, starting with his email and ending with their PayPal account. While no financial loss was reported, being targeted by someone previously close to the victim has likely caused considerable upset, reducing their ability to swiftly recover from its impact. In addition, a close

[152] As has been discussed elsewhere, in cases of fraud it is common for the suspect to develop a relationship of trust with the victim over time. However, as such relationship are based on deceit and part of the crime's MO, they are considered under guardianship factors, under the vulnerability dimension.

relation is more likely to be able to gain unauthorised access to the victim's accounts or devices, as they would be in a better position to 'shoulder-surf' login details or simply access stored or guess passwords.

However, the stronger themes concerned relationships supportive of the victim. The sampled data revealed the importance of family, friends and the wider community, in supporting victims to identify that they have been victimised, report the incident to the police and/or adopt measures to improve guardianship. By far, the most important relationships identified were those of family members. In 8661 above, for example, the victim's son reported the crime on their behalf, but also investigated the extent of the financial loss and sought some open-source intelligence about the 'company' who had contacted the victim. In the previously mentioned crime 3513, the victim was alerted to an ongoing fraud by staff at the local shop. The intervention of family, friends and others, can therefore result in further losses being prevented. Of course, as previously mentioned, there will be instances of victims who refused to believe that they were being victimised, even where family and friends sought to support them. As previously discussed, in such circumstances the experience of victimisation may in fact lead to the breakdown of relationships, potentially leaving the victim more vulnerable to further victimisation. Finally, the victims' relationships with CJS agencies and other stakeholder organisations also emerged as key. However, while there are inter-personal aspects to these relationships, given that they represent institutions, they are best addressed with respect to guardianship and structural factors.

A similar qualitative test to the one articulated for embodied factors is suggested to assess relational vulnerability factors. In this case, the test asks whether, in light of the victim's circumstances, there are any relational factors including (but not limited to) the victim's relationship with family and friends, which are likely to result in a reduced ability to increase guardianship against future F&CM attempts, or a reduced ability to seek and access the necessary support in order to recover from the impact of the victimisation experience.

4.3. Structural Factors

Finally, the TA also revealed the importance of structural factors. Structural factors include cultural norms, technological *affordances* or systems of operating which, although unobservable in themselves, can be identified through their effects on victims' vulnerability to/post victimisation. Firstly, the role of the profit and labour-driven economic structure is

implicit in many of the previously discussed cases as contributing towards F&CM vulnerability. Financial difficulties and market pressures were sometimes explicit and more often implicit, in many of the crime accounts sampled.

Secondly, the certain industries create the technological *affordances* necessary for F&CM to be committed and were therefore identified enabling of victim vulnerability. As discussed in chapter one, the concept of *technological affordances* captures how material/technological properties of an environment create possibilities for action, with respect to the abilities of actors (Chemero 2003; Gibson 1986). In this context, it includes procedural and technical mechanisms (beyond victims' direct control) which are exploited by criminals and increase victims' vulnerability to F&CM. The examples of guardianship failures by large organisations such as banks, money services or telecoms companies which have illustrated the crime vulnerability dimension can understood as constituent parts of larger structures which contribute to F&CM vulnerability. Given their prominence and systematic (ab)use by fraudsters, it is argued that insufficient attention has been paid to the role of enabling industries. The role of competitive economic structures and enabling industries are explored in more detail in what follows.

4.3.1. Competitive economic structures

The role of the economic structure in driving victimisation is implicit in several of the previously mentioned cases and especially in instances of *Investment* fraud and *Advance-fee* fraud. In some cases, victims decide to risk savings including pension pots and 'invest' them in attractive 'opportunities' made up by fraudsters, resulting in very high losses. As has been noted in chapter four, despite its relatively low volume, *Investment* fraud had by far the largest mean and median losses within the sample. In 16847, the victim was looking for options online to unify two pension funds. Far from being motivated by personal greed, the victims' actions in this example can be understood in relation to the structure of a profit and labour-driven economy, which requires individuals to 'shop around' for the best possible pension-investment schemes, to ensure their family's and own wellbeing in later life. In this context, individuals rely on multiple pension pots, all of which carry financial risks, to secure financial stability for themselves and their families, when they are no longer able to work. Yet, if defrauded when engaged in this necessary (and often encouraged) activity, this is often framed by both victims and those around them as a personal choice motivated by greed (Button & Cross, 2017).

Crime 16847

> "About 4 years ago, I wanted to unify two pension funds. After [completing a] survey, online, I was contacted by a financial advisor. This advisor referred me to X Management Services. I proceeded to transfer my two pensions into pension trust AU102, the total investment was £78000ish. I have now been informed by another company "Y Management" that X has gone into receivership because another company "Y" had gone into "member voluntary liquidation". Y referred me to thepensionsregulator.gov.uk who then referred me to Action Fraud."

In the totality of the cases of *Investment* fraud in the TA sample, individuals lost money when they thought they were investing in a variety of ways including in carbon credits, shares, fine wine, crypto-currency and art. While, as noted above, victims of fraud are often perceived as greedy, an alternative view would be to understand these risks in the context of an economic structure which encourages fiscal risk taking. As much as taking a risk may be thrilling, it should be noted that society looks kindly on those who 'risk big to win big'. Furthermore, it is just as reasonable to assume that individuals who invest their savings are motivated by the hope of securing financial stability for themselves and their families. It is striking that the behaviour which is rewarded by cultural norms established by market competition, leads to victims being stigmatised as 'greedy'.

In the case of victims who apply for loans with rogue credit providers, this is often in the context of financial strife. There were 24 cases of lender loan *Advance-fee* fraud, representing 7% of the TA sample. In 14261 below, the economic difficulties are made explicit. In other cases, they are implied e.g., where the victim accepts the fraudster's assertion that they have a bad credit rating. However, this can also be deduced by the low amounts requested/offered vis-à-vis the 'advance fee' that victims are willing to pay. Where known, the value of the loans being 'offered' to victims ranged from £500 to £10,000, with an average of £2468.75 and a median of £1,500.00 (n = 16). The average loss to the fraud was £322.54 and median loss £285 (n = 20). As such, the average loss represented approximately 13% of the loan offered/sought. The fact that victims sought relatively low loans and were prepared to pay out a significant proportion up front, suggests financial difficulties.

Crime 14261

> "Victim has applied for a £9000 loan online, and has then been contacted via phone by a company called [X]. The company stated that they would offer the full £9000 loan, at a repayment rate of £295 a month over 3 years. They have then asked that an initial £295 be sent to them to prove that the victim could repay at the rate specified. The victim has complied with this. A couple of days later, the company have asked for more payments, identifying them as "hidden charges" associated with the administering of the loan. As

> victim was desperate for money at the time of applying for the loan, she was unable to send any further money to [X]. Shortly after this, money has started arriving in her account from different sources, none of which were named as [X]. On enquiring with the company, they have assured the victim that these were indeed [X] accounts, and asked the victim to withdraw the money from her account and then send it via a transfer with Western Union to an account holder in India. As victim was desperate for her loan, she believed the company representative and did as she was asked. After some time had passed, and after no loan had materialised, victim confronted [X], and was met with silence, being unable to get in touch with them on any format. --this incident has only come to light, as one of the other victims, whose money was transferred into this victim's account for wiring to India via Western Union, has reported the matter to action fraud, who located this victim as the suspect account and informed Dyfed-Powys police. The police have arrested this victim on suspicion of fraud, and have interviewed her, at which point, it has become clear that she is herself a victim, and her account was being used to defraud others, and it would seem, to further shield Home Equity Loans from suspicion."

The above case illustrates several key points. Firstly, the £295 financial loss recorded in no way captures the severe impact which this experience of victimisation must inevitably have caused. In addition, the reason provided for seeking a loan in the first place is a "desperate" financial situation, illustrating the interaction between impact of crime and structural vulnerability factors such as economic disadvantage. These combine to significantly reduce the victim's resilience to the impact of the crime. However, this insight is easily lost when focusing on CSEW-based typical victim profiles, as victim survey data suggests F&CM victims are generally better off. Finally, this case also demonstrates the key role played by factors within the crime dimension of vulnerability, including low guardianship, as the victim has doubts about the situation but is persuaded by necessity to go along with it.

4.3.2. Enabling industries

Several legitimate practices were previously identified as enabling F&CM in chapter five, including advertising, telecoms (particularly call divert services) and Internet domain registration (particularly the ability to register domain names mimicking legitimate organisations). In addition, there were multiple references to fraudsters operating within legitimate social media platforms and online marketplaces to both find and defraud victims. However, very prominent in both the TA and full samples used in this study was the abuse of payment services by fraudsters including banking payment methods (e.g., using remote card payments, bank transfers and cheques), services such as PayPal, store vouchers (e.g., iTunes vouchers) and overwhelmingly, the abuse of so-called Money Service Businesses or MSBs (e.g., Western Union, MoneyGram and PaySafe). Equally prominent were enabling factors

such as the ability to sign up to (financial) services using digital signatures and (poor) online identity verification systems, both commonly exploited by fraudsters and hackers. These types of services cut across the vast majority of F&CM and thus, given the scale and prominence of their role, they are considered technological affordances which enable F&CM and are examined in turn below.

Payment services

The high prevalence of the (ab)use of payment services in the TA sample led to a broader quantitative exploration of the study sample in full, by searching for cases containing relevant keywords within the incident description.[153] This revealed that at least 34% of all individual F&CM reports mentioned a mix of banking or alternative payment methods being used in the fraud (while they overlapped, banking and alternative methods were each mentioned in approximately 19% of all individual reports). In a great many cases, such payments are authorised by the victims themselves, having been socially engineered into providing fraudsters with their bank details (e.g., 3144, 6018 and 2212 below) and/or making a payment via an alternative payment method (e.g., the previously mentioned crimes 15852 and 1828).

Crime 3144

> "The victim received a popup on his computer screen stating the computer was at risk of collapse due to malicious software. The popup gave a phone number for the suspect which the victim rang. The victim provided the suspect access to the PC. The victim was asked to pay £89.99 by card for Internet security which he did. The victim then spoke their credit card company who require proof the suspect is a fraudster before disputing the payment."

Crime 6018

> "Circle tickets, victim has paid for three tickets which have not been received. Victim's bank have told her she needs to wait 15 days after the event, then they can refund for non-receipt of goods. This can take up to 100 days and they'll investigate."

Crime 2212

> "Customer was contacted several times on [date] from somebody purporting to be from HSBC fraud detection. The caller stated there had been a fraudulent payment debit her

[153] The list of key words was developed based on the TA analysis and included the following for banking payments: "Bank Transfer", "Bank Card", "Credit Card", "Debit Card", "Card Details", "Cheque"; It also included the following for non-banking payments: "Ukash", "Ucash", "Pay Safe", "Pay Safe Card", "Pay-Safe", "PayPal", "Western Union", "MoneyGram", "Itunes Vouchers", "I tune voucher".

> account for £3,700, and in order to return the payment into a holdings account her secure key digits were required. The customer was told to call back the HSBC number for reassurance, she called back and believed the call was genuine, she then provided her secure key digits to the caller. The fraudster made payments totalling a loss of £39,900 - HSBC have refunded as a gesture of good will."

In cases such as the above, it will be difficult to implement automated technical controls to stop fraudulent payments, without adversely impacting legitimate transactions. However, it is also the case that weak authentication measures (more on this below), the immediacy of payment and difficulties tracing/recalling remote payments are designed-in choices, which prioritise the free flow of capital over security. These choices benefit consumers (through the convenience they offer) but ultimately benefit businesses and financial institutions considerably more, as they reduce the likelihood of consumer 'desistance' from purchases. As such, financial institutions may require victims to provide "proof" of fraud before stopping a transaction or attempting to recover money (e.g., 3144), refunds/cancellations can take a considerable time to be processed (e.g., 6018), and often refunds are considered gestures of 'goodwill' on the part of the businesses providing them (e.g., 2212). Crime 2212 also illustrates how attempts at guardianship by the victim (calling back 'the bank') were frustrated by technical systems beyond their control, namely call diverts. As discussed in chapter one (section 2.2.6), some cases such as 2212 may now be covered under the voluntary Authorised Push Payment code (APP Scams Steering Group, 2019b). Nonetheless, the effectiveness and fairness of bank refund policies have been questioned (Hughes, 2018) and many victims of *Card and Banking* fraud are still not compensated for their losses, despite being rendered vulnerable by systems/procedures they have no control over.

Furthermore, victims often interact with the providers of payment services (or their agents) while making payments to fraudsters. Such businesses have the opportunity to identify and stop fraud from taking place – as well as an ethical obligation, where they directly profit from a fraudulent transaction. This has been recognised in the development and roll out of the Banking Protocol since 2017, discussed in chapter one. While the protocol remains optional for banks, victims may slip through the net (Murray, 2018) and it is also not known how many false positives it has led to (i.e. where the protocol is actioned unnecessarily). This initiative has nonetheless been successful at stopping a considerable amount of fraud where banking staff have identified suspicious transactions and called the police. However, bar the actions of conscientious and fraud-aware individuals in the local community as was the case in 3513

above, no such attempts have been made at coordination between MSBs (of which Western Union and MoneyGram are among the largest operating in the UK), to implement similar safeguards to prevent fraudulent activity through their services. That is despite some such service providers having problematic track records with respect to fraud and money laundering.

In 2009, MoneyGram agreed to pay $18 million in consumer redress to settle US Federal Trade Commission charges that, between 2004 and 2008, agents for the company allowed its money transfer system to be used by fraudsters, causing U.S. consumers more than $84 million in losses (US FTC, 2009). In 2017, the Colorado-based Western Union (WU) entered into a Deferred Prosecution Agreement (DPA) with the United States in which it acknowledged that between 2004 and 2012 it broke US law "by (1) wilfully failing to implement and maintain an effective anti-money laundering ("AML") program that was designed to detect, report, and prevent criminals from using Western Union to facilitate their fraud, money laundering, and structuring schemes, and (2) aiding and abetting fraudsters in their unlawful schemes by remaining in business with Agent locations that facilitated the unlawful fraud scheme." (United States of America v. The Western Union Company [2017], Case 1:17-cr-00011-CCC). This included UK-based WU Agents complicit in processing over $72 million in losses to victims through fraudulent transactions. It therefore agreed to forfeit $586 million to compensate victims of the fraud, $153 million of which have begun to be distributed to victims all over the world (US DoJ, 2020).[154] Alongside these quasi-criminal cases, police awareness campaigns and pieces of investigative journalism have highlighted the links between MSBs, fraud and money laundering, including in connection with the financing of drug trade and terrorism (NCA, 2020; Rosca, 2020).

In the two-year period covered by the full quantitative sample in this study (n = 17,049), 429 cases, totalling a direct loss of £833,355, mentioned Western Union payments. This includes a period of just two years out of the thirteen-year period covered by the above-mentioned scheme, within only four of the 43 UK police forces. However, only 1,097 claims were made from the UK under the scheme (WU Remission, 2020). Similarly, 495 cases in the total study sample mentioned MoneyGram payments and reported a total direct loss of £870,223. Finally,

[154] To be eligible for compensation, individuals who made a WU payment within or outside the US between January 1, 2004 and January 19, 2017 (a period of 13 years), and were the victim of fraud, were required to submit a Remission Form and supporting documentation before 31 May 2018, extended to 30 September 2019 via an online remission claim (WU Remission 2020).

PaySafe was mentioned in 178 cases totalling a direct loss of £25,927. This analysis suggests that the current regulatory framework did not effectively protect victims of fraud and highlights how banking payment services and MSBs' systems act as technological affordances which enable offending, thereby rendering victims more vulnerable to F&CM. As such, the continued development and improvement of banking practices and the adequate regulation of MSBs constitutes a timely focus for F&CM crime prevention.

Identity Verification

As was explored in chapter five, in many cases where the victims' identity is used by hackers and fraudsters, the victims' actions play a minimal role. Identity 'theft' is thus often considered a key criminal enabler of fraud (e.g., Home Office 2013). Another way to consider this problem, however, is to focus on how identity verification systems are abused by fraudsters, because of risks taken by legitimate companies on behalf of consumers. As shown in the examples below, the victim has little to gain from the risk being taken on their behalf, while those same organisations benefit directly from passing on the risk to crime victims. As such, crime prevention is best served by focusing on the regulation of these enablers and justice better served through the re-distribution of the risks associated with these practices i.e., by making it easier for individuals whose identity has been compromised to seek compensation from companies who benefit.

In the example of crim 6769, the *Hacking* of an online gambling account led to a series of payment card frauds and the victim's identity being misused. While online gambling can be identified as the risky activity, an alternative is to focus on the gaming platform and the online credit and payment services as crime enablers – these crimes could not have taken place without them and they are one degree closer to the actual crime than the victim's (son's) decision to play online games. Furthermore, in this scenario all the legitimate actors have something to gain from the victimisation experience – the gambling company has profited from the game purchases, the credit company has profited from the charges made to the victim's card (where these have not been refunded), PayPal has benefited from transaction fees. As such, each of these companies has not only created the risk by the inadequacy of their technical controls, but also passed the risk onto the victim and benefited directly from the victimisation itself. As with the previously mentioned examples, the victim has little choice with respect to the technical and legal controls within which these players operate.

For example, the 3-D Secure (3DS) service developed in the early 2000s and known by brand names 'Verified by Visa' and 'MasterCard SecureCode', originally required customers to provide random letters of a static password in addition to the card details, before an on-line purchase was completed. However, this scheme was criticised for being a weak security solution, while shifting liability onto customers (Murdoch & Anderson, 2010). Since then, allegedly to improve customer experience, this password is no longer required to verify a purchase (Brignall, 2014; Curtis, 2014). This was replaced by an algorithm running in the background which, based on factors including the location of the purchase, the device being used or the merchant being paid, determines whether a particular transaction goes through a second layer of authentication (Visa, 2016). An alternative explanation for giving up this security feature however, was that many merchants abandoned 3D-Secure altogether, given the drop in sales which resulted from this second layer of authentication (Adyen, 2014a, 2014b). This was most likely caused by customers forgetting their 3D-Secure password, or having difficulties establishing whether the 'pop-ups' the system used were legitimate or fraudulent (Brignall, 2014; Curtis, 2014).[155] This may be an example of where the cost of compensating customers in the event of fraud was a risk worth taking vis-à-vis sales revenues merchants and financial institutions alike.

[155]Adyen's own research revealed a more complex picture where 3D Secure had a net positive effect on conversion rates in certain countries including an average 3% increase in the UK (Adyen, 2014a). However, this was not the case in other countries such as the US (decrease of over 40%), Germany (decrease of over 20%) and Australia (decrease of over 10%) (Adyen, 2014b). In addition, a twitter search for "verified by visa" is, to this day, guaranteed to result in a stream of negative customer feedback.

5. Conclusion

This chapter has proposed a multi-dimensional framework to assess victims' vulnerability to F&CM. In doing so, it has answered RQ10 and met the third and final aim of this thesis. Drawing on Fineman (2008, 2017) and Chambers (1989), vulnerability in the context of this thesis refers firstly to the (universal) susceptibility to being harmed because of F&CM (*vulnerability to* F&CM); and secondly to the extent to which individuals are or not able to cope with the negative consequences of being victimised (*vulnerability post* F&CM). The framework proposed in this chapter addresses both types of vulnerability. Furthermore, drawing on the previous theoretical and analytical chapters, it has put forward eight vulnerability factors and suggestions of how these may be assessed, grouped into three distinct vulnerability dimensions 1) the *definitional dimension*, 2) the *crime dimension* and 3) the *capabilities dimension*. Assessing vulnerability across these dimensions, it has been argued, is a key step towards identifying and responding to victims' needs, thus increasing their resilience to F&CM and its impacts.

The definitional dimension includes three factors: *risk, impact* and *repeat/multiple victimisation.* Risk provides a quantitative measure of vulnerability to victimisation based on victimisation surveys, while the assessment of impact relates to vulnerability post victimisation and may draw both on survey and crime report data. Measuring risk and impact allows for an initial assessment of the individual's relative vulnerability. In line with Johnson (2008), it was concluded that repeat victimisation can be both a symptom (a 'flag' of greater risk) and a cause ('booster') of vulnerability post victimisation. However, while the data supports the extent to which RV patterns exist, the qualitative analysis revealed that the one-time/repeat distinction is often blurred. Without improvements to the ways in which RV is registered, it will remain under-counted within crime reports. Alongside this, there was some evidence that multiple victimisation (across multiple crime types beyond F&CM) can also increase vulnerability to F&CM. As such, while recognising its contribution to both risk and impact, RV was classed as a descriptive or *definitional* factor in assessing F&CM vulnerability.

However, the statistical measurement of risk can render invisible the experiences of highly victimised individuals and assessments of impact will always be imperfect as they may not be immediately understood or anticipated. Furthermore, risk, impact and levels of repeat victimisation are highly descriptive and mediated by the *crime* and *capability* vulnerability

dimensions. The former draws on Cohen and Felson's (1979) Routine Activity Theory (RAT). The latter draws on the vulnerability theory put forward by Fineman (2008, 2017), as well as Sen (1999) and Nussbaum's (2006, 2011) capabilities approach. An in-depth assessment of vulnerability will need to address these vulnerability dimensions.

The crime vulnerability dimension relates to the circumstances of the crime itself which may render an individual more vulnerable to (further) victimisation and includes *situational factors* and *guardianship factors*. Identifying situational factors is the 'bread and butter' of law enforcement intelligence gathering. Police agencies already have the systems to identify trends in the types of F&CM and associated MOs. In the context of evolving data-mining techniques, these are likely to continue to improve. Guardianship has been operationalised with mixed results in RAT studies of F&CM. However, this analysis suggests that understandings of guardianship should not only include technical controls prior to first victimisation, but also actions to mitigate against F&CM re-victimisation, as well as guardianship attitudes. It would be useful to ask victims when they report an incident, whether they have taken any measures to prevent further victimisation and intervene accordingly. At the same time, in the case of highly vulnerable victims, the adequacy of such measures can be assessed discursively, by engaging the victim in a more in-depth discussion about what steps to take.

Finally, the analysis in this chapter and throughout this thesis shows that an assessment of the capabilities dimension is particularly important to addressing vulnerability post victimisation, as the individual's ability to recover from F&CM has been linked to *embodied*, *relational* and *structural* factors. Embodied factors include physical characteristics and conditions which, with respect to their own social context, make the individual more susceptible to F&CM victimisation. Relational factors relate to the way in which relationships and/or dependencies on others can make individuals more vulnerable to F&CM and its impacts – or conversely provide support and be a source of resilience. To assess each of these factors, a similar qualitative test was suggested whereby, through an in-depth discussion with the victim, practitioners can determine whether embodied or relational factors are likely to result in a reduced ability to increase guardianship against future F&CM attempts, or a reduced ability to seek and access the support necessary to recover from the impact of victimisation.

With respect to structural factors, understanding the ways in which victims' behaviour is shaped by the vulnerability created by the economic 'superstructure', provides an avenue to challenge stigmatising stereotypes. At the same time, it was highlighted that certain services,

in particular payment and identity verification services, are technological *affordances*, i.e., possibilities for action (Chemero 2003, Gibson 1986) which play an overwhelming role in enabling F&CM. Like some other factors in this framework, structural factors are not capable of direct measurement. Furthermore, in most cases, structural factors will not be the focus of intervention for practitioners. However, they are theoretically driven concepts which aid understanding and can direct the focus of policy reformers. As is shown, their effects on victims of F&CM can be demonstrated by their pervasiveness within the crime reports analysed. There is therefore value in practitioners being aware of these and, where appropriate, challenging them when designing and delivering services. In addition, these factors will be of relevance to civil society organisations that campaign on behalf of victims of F&CM and to government agencies developing victim policy.

While each of the above-mentioned vulnerability dimensions/factors are interconnected, distinguishing between them enables a better understanding of vulnerability with respect to F&CM. It also allows for the identification of possible avenues for intervention and response, to aid crime reduction, prevention and achieve justice for victims. In particular, this analysis suggests that the crime dimension is more closely (although not exclusively) linked to vulnerability *to victimisation*, while the capabilities dimension becomes more critical when responding to vulnerability *post-victimisation*. Through a vulnerability lens it becomes possible to identify what harms have been suffered by F&CM victims, how to address them and who is responsible and able to address them by making available the relevant "assets of resilience" (Fineman 2008, p. 13) e.g. law enforcement may provide protection advice, cyber security businesses may secure devices and local authorities may provide social welfare support. Furthermore, it is for the state to monitor differences in access to assets of resilience and address both discriminatory practices and conferring of special privileges on certain groups.

This framework makes visible some dimensions of vulnerability which are currently not adequately addressed, or not addressed at all, by the CJS in relation to victims of F&CM. Many are missing from legal and policy definitions of vulnerability identified in chapter two. In addition, the distinction between vulnerability to victimisation and vulnerability post victimisation enables the mapping of national and local resources and the identification of adequate responses to meet victims' needs. Such an exercise will help in making it clear which organisations within the F&CM 'justice network' (Button, Tapley, et al., 2012) are best placed to address the needs of victims, based on their needs.

THESIS CONCLUSION

This thesis set out to achieve three aims. The first was to identify patterns of fraud and computer misuse (F&CM) reported in Wales. The second, to explore repeat victimisation with respect to these crime types, as well as the characteristics of repeat victims. Finally, it aimed to develop an empirically-grounded theoretical model of vulnerability, optimised to identify and meet the needs of individual victims of F&CM in Wales. The common thread between these aims was that each led to better understandings of F&CM victimisation, contributing to the evidence-base required to inform the development of theory, victim policy and practice. In other words, explore what a victim-focused F&CM response would required from the CJS and the wider justice network. The mantra of putting victims at 'the heart' of the criminal justice process has resulted in many policy initiatives in recent years, including the establishment of a 'Victims Code', which brings together what Hall (2009) has called victims' procedural and service rights. Against this backdrop and despite the difficulties in the investigation and prosecution of F&CM however, this thesis has shown that 'Pursue'-type activity remain the key focus of data collection and activity by criminal justice agencies, at the expense of 'Protect'-type activity i.e., responses focused on preventing (re)victimisation. In addition, to date, although much research has looked at F&CM through a Routine Activity Theory lens, emphasizing situational factors and crime control objectives, relatively little has focused on identifying and addressing the social harms associated with F&CM victimisation (Powell et al. 2018). In this context, the theoretical and empirical insights developed throughout this thesis draw attention to victims and hope to establish parameters within which a victim-focused response is both needed and possible. In this way, this thesis hopes to help move the needle towards the 'Protect' strand of policing and the prioritisation of the 'everyday' victim. It has also sought to shift attention from a traditional retributive justice focus on what laws have been broken, by whom and what punishment they deserve; towards the questions at the heart of a more restorative approach: what harms were suffered, by whom, how to prevent and repair them, and who has the obligation/ability to do so (Zehr, 1990, 2015).

Summary of Results

To meet the above three aims, ten research questions (RQ) were answered throughout this thesis, using a mix of quantitative statistical methods (including data linkage, bivariate statistics

and generalised linear models) and qualitative thematic analysis. The first aim was met by answering research questions one (RQ1) to four (RQ4), the second aim achieved by addressing research questions five (RQ5) to nine (RQ9) and the third and final aim accomplished by answering research question ten (RQ10). Each research question and the relevant results are summarised in what follows.

RQ1: What was the volume of reported F&CM in Wales, over the reference period?

Answering this question included a statistical analysis of the volume of F&CM across victim types and the four police force areas in Wales (Dyfed/Powys, Gwent, North Wales and South Wales), over the reference period (1st October 2014 and the 30th September 2016). The volumes of F&CM recorded in Wales vis-a-vis other crime types were also examined. Over the refence period, n = 17,049 F&CM reports were made within the Welsh forces. Most reports were made in the South Wales Police force area (40.79%), followed by North Wales (22.77%), Gwent (18.46%) and Dyfed/Powys (17.98%). Key insights emerged regarding the relative volume of F&CM vis-à-vis other crime types. This included the observation that while F&CM remains a small proportion of all crime reported in Wales, and despite the considerable under-reporting of fraud, fraud has one of the highest rates of recording among all property crimes targeting individuals. Given this level of reporting and the limited nature of the current response, fraud is an important area for criminal justice and victim policy development in Wales. Other insights included how the Home Office Counting Rules and the design of the recording system may result in the relative under-estimation of CM vis-à-vis fraud, as well as the under-estimation of the levels of repeat victimisation. As discussed below, these are areas where national recording systems could be improved, to generate more accurate data and insights into F&CM victimisation.

RQ2: What were the characteristics of victims who reported F&CM in Wales, over the reference period?

To answer RQ2, victim types and their characteristics were quantitatively examined across crime group (fraud/ CM), F&CM categories (nine fraud and two CM categories) and *Modus Operandi* (MO) group (including online, offline and mixed crimes). The analysis showed that victims of fraud and CM were somewhat distinct, but age was the only characteristic which was consistently shown to have a large effect on the likelihood of crime group, crime category or MO group. With respect to crime group, while younger groups suffered the highest proportion of fraud victimisations, it was the older groups who tended to report being

victimised. Conversely, younger victims tended to under-report both F&CM. At the same time older males (75+) appeared to both experience greater fraud victimisation and report more crimes. However, no clear effects were observed with respect to any of the other demographic and environmental factors considered, suggesting that the case for targeting specific groups with prevention advice, based on profiles developed from reported crimes, is relative weak. Nonetheless, profiles for the 'typical victim' of both fraud and CM were constructed, to the extent that was possible, based on the quantitative and qualitative findings. When compared with the contrasting victim profiles which emerge based on CSEW data, these provide a starting point for understanding reporting behaviour and develop victim policy and practice.

RQ3: What financial and other impacts were reported by individuals and other victims of F&CM in Wales over the reference period?

RQ3 required a quantitative examination of how losses varied across victim types and characteristics, as well as a qualitative thematic analysis of a sub-sample of incident descriptions, to identify and explore impacts beyond direct financial loss. While on average the highest direct financial losses reported were associated with business victims, the most typical losses were not dissimilar between individuals and businesses. In this context, the case for the prioritisation of business over individual victims is harder to justify. Furthermore, the analysis in this thesis also suggests that if certain F&CM crime types were to be prioritised based on the highest typical losses, *Business compromise* and *Investment fraud* should take priority. That is despite these categories being among the least frequently reported crime types within this sample – or indeed in the CSEW.

In line with previous research (summarised in Button & Cross, 2017), the qualitative analysis of incident descriptions showed that direct losses provide a limited picture of the overall impact of F&CM on victims, even where only financial impacts are considered. Four key impact themes were identified. The first theme brought together the different ways in which F&CM can impact on the *identity, privacy and liberty* of the victim and included four sub-themes, namely the loss of personal identifiable information, identity theft, invasion of private and family life and, in extreme cases, victim arrest. The second theme demonstrated the *wider financial impact* beyond direct losses, including indirect losses associated with repairs and financial detriment in the form of debt or worsening credit ratings. The third concerned (tangible and/or intangible) *property loss or damage*, such as to computers or digital files. The final impact theme concerned victims' *wellbeing and relationships*. Across many cases, it was

implied that repeat targeting by offenders caused victims considerable nuisance. In others, threats and abuse from offenders left victims distressed and/or even in fear of physical violence. Finally, there were instances where the experience of being victimised led to deteriorating relationships between the victim and their family and friends.

As such, this thesis corroborated previous research by demonstrating the potentially grave impacts of F&CM on victims in Wales. At the same time, the discussion in chapter two showed that the twin concepts of 'the victim' and 'vulnerability' are directly linked to the 'harms' associated with the risk and experiences of F&CM victimisation. Preventing victimisation and responding to vulnerability therefore, means preventing the risk of harm and supporting victims to cope and recover where that risk materialises. However, the data collected when a crime is recorded nationally by Action Fraud (AF) is not optimised to establish the relative impact of the crime on the victim. At the time this sample was collected, while some limited information was collected by AF on the victim's own self-assessment of the impact of the crime, as well as their self-assessment of vulnerability, this information was not passed onto the Welsh forces within whose jurisdiction the victim-response would fall. To improve the victim response, it is essential that the impact of F&CM on victims is recorded and considered when assessing victim vulnerability, at the earliest possible opportunity.

RQ4: What online/offline dynamics enabled F&CM in Wales over the reference period?

This question considered online/offline dynamics across victim characteristics, crime group and F&CM categories. In addition, a thematic analysis of a sub-sample of incident descriptions led to the identification of broader *Modus Operandi* (MO) features of F&CM. Early in chapter one, it was identified that the online/offline dichotomy might be a false one, which can get in the way of an adequate victim response. This was confirmed empirically by coding each case as to whether it contained online, offline or mixed on/offline elements. Following Caneppele and Aebi (2019), 'hybrid' elements were found to be prevalent within both fraud and CM cases, which were found to have 30% and 25% mixed on/offline elements respectively. Furthermore, mixed MOs increased over the reference period. Thus, in line with the work of Powell et al. (2018), this thesis moved away from a study of "cybercrime" and towards the study of F&CM victimisation, in a context where online and offline elements are anticipated to be increasingly integrated. Nonetheless, these results were limited by the dataset variables available. Future research with AF data would benefit from access to and analysis of variables concerning the first mode of contact between victim and offender (including email, web forum, chat room or

similar, visit to a website, phone call, text message or similar, letter or fax, among others) and the type of enabler in the case of fraud (e.g., email, postal service, in person etc.).

Other MO mechanisms which were identified through TA included the offenders' use of *legal* and *criminal enablers*, their reliance on *manipulation tactics* and targeting of the same victim *repeatedly*. Both legal and criminal enablers can be understood as affordances (Gibson, 1986, Chemero, 2003), properties of the environment, which suspects are capable of re-purposing to victimise others. Viewing victimisation through this prism leads to the recognition that those who design and manage the relevant services and technologies must take responsibility for addressing the harms which result from F&CM victimisation. Enablers can also be viewed through a vulnerability theory lens (Fineman 2008, 2017) and conceptualised as sources of *vulnerability*. Consequently, enablers were integrated into the overall vulnerability framework proposed in this thesis.

RQ5: What was the extent and nature of individual F&CM repeat victimisation (RV) in Wales?

Addressing a considerable gap in the literature (Pease et al., 2018), this thesis has empirically tested the volume and patterns of repeat victimisation within F&CM reported crime in Wales. To do this, a data linkage method including a mix of deterministic and probabilistic linkage was developed, to identify reports made by the same individual victims within the dataset of incidents reported over the reference period, within the three forces within the Southern Wales ROCU region (Gwent, Dyfed/Powys and South Wales). Statistical methods were then used to estimate the overall volume of RV and its distribution across crime group and crime categories.

The analysis confirmed that a significant proportion of victims who report F&CM are repeat victims. This varied between the two crime groups with 3% of fraud victims estimated to have reported 7% of recorded frauds and 6% of CM victims estimated to have reported 15% of recorded CM. As such, this analysis suggests that a not insignificant proportion of victims who report F&CM are repeat victims. These results lend strength to the argument that overall crime volumes can be reduced by targeting prevention activity at those who have already been victimised. Key differences identified across crime groups and crime categories should inform the planning and delivery of crime prevention, as should insights into the time-course of RV.

RQ6: What were the characteristics of repeat individual victims?

To answer RQ6, the demographic characteristics of one time and repeat victims were compared and incidence of RV examined across the socio-economic profile and levels of internet access within victims' local area. This analysis suggested that males are marginally more likely to be repeat victims and that the likelihood of RV increases with age, while ethnicity and proxy reports had no effect on the probability of repeat reports. While this is considerably different to the typical repeat victim profile for other crime types such as violent crime and domestic violence, it is in line with the profile of F&CM victims discussed in chapter four – more males and older victims report being victimised, and more report RV. As such, this analysis suggests that similarly to other crime types (Ignatans & Pease, 2015, 2016), the characteristics that distinguish repeat from one-time victims, are similar to those that distinguish victims from non-victims of F&CM. However, no significant interaction effects were observed between age and gender, as may have been expected from the analysis in the previous chapter. Given the limitations of the present linkage method however, this is an area for further enquiry. Likewise, no significant association was found between repeat reporting and the socio-economic characteristics of the victims' local area, as measured by the WIMD, or levels of local internet access. However, there were considerable limitations to the analysis of these two environmental factors considered as the measures did not capture granular differences at the individual level. As such, further research is also necessary to understand the impact of socio-economic factors and levels of internet access on RV.

RQ7: What was the impact of RV?

To answer RQ7, a mix of quantitative and qualitative methods were used to explore financial and other impacts associated with RV. The analysis showed the typical financial losses experienced by repeat victims were of a higher magnitude than those experienced by one-time victims. In addition, the qualitative themes identified in chapter four were found primarily from accounts relating to repeat victims, suggesting that not only do they experience typically greater losses, but also that RV has more of a wider impact on the lives of repeat victims. These findings have clear implications for a victim-focused response. Firstly, preventing RV is of strategic importance not just to reduce overall volumes of crime, but also where CJS interventions aim to reduce harm caused by F&CM. Secondly, where prioritising of limited victim support services is concerned, high levels of repeat victimisation may indeed be considered a 'flag' that individuals may be dealing with complex vulnerabilities and thus need support coping with harms post-victimisation. That is not to say that all repeat victims are

necessarily more vulnerable. However, in a minority of cases of 'chronic victims', RV was identified as a 'flag' for *a priori* states of vulnerability. A good understanding of the impacts repeat victimisation is vital so that victims can be referred onto adequate support services such as social services, debt advice, counselling etc, and re-victimisation prevented.

RQ8: What was the characteristic time-course of RV?

To answer RQ8, the time-course of RV was statistically examined across crime group and category. In line with previous research (e.g. Soumyo Darshan Moitra & Suresh L. Konda, 2004; Sagovsky & Johnson, 2007) this analysis of the time-course of repeat victimisation indicates that crime prevention activities will be most effective within a month of first victimisation. However, the scope for intervention is reduced when considering the time-course of repeats as 16% of these were recorded on the same day. Reflecting the HMIC's (2015) findings and as corroborated by Shorrock and colleagues (2020) in the context of domestic violence and repeat safeguarding referrals respectively, recording practices have a considerable impact on the identification and measurement of RV. In the case of F&CM they may lead to an under-estimate of the time-course of RV, as separate crimes recorded on the same day have not necessarily taken place on the day of recording. In addition, the measurement of RV will be deeply affected by any changes in the availability of the recording services.

RQ9: What were the mechanisms through which RV happened?

A qualitative analysis of the mechanisms which underpin RV, i.e., what are the typical tactics used by offenders to repeatedly victimise individuals. The themes identified included the *continuation of the narrative*, the *subtle nuance* across consecutive MOs and the role of *existing vulnerabilities* in cases if successful repeat victimisation. In combination, these suggestive of what previous work has described as a 'boost' effect (Pease et al., 2018, p. 258; Tseloni & Pease, 2003) i.e., that being victimised once can, in some circumstances, increases vulnerability to further victimisation. Following Johnson (2008) therefore, and in light of the results of RQ7, the present work suggests that repeat victimisation can be both a 'flag' for *a priori* vulnerabilities to F&CM, particularly in the case of so-called 'chronic victims', and a 'booster' of the risk of re-victimisation.

RQ10: How was vulnerability constructed within reports of F&CM?

Finally, to answer RQ10 and construct a theoretical model of F&CM vulnerability, a qualitative thematic analysis of a sub-sample of incidents was undertaken, to uncovered the ways in which

vulnerability was constructed within crime reports. The analysis sought to integrated the previous qualitative analysis into an overall vulnerability model and resulted in eight key vulnerability factors (or sub-themes) grouped into three distinct dimensions (themes). The dimensions included firstly, the *definitional dimension*; secondly the *crime dimension* and thirdly, the *capabilities dimension*. The definitional dimension was directly derived from the definition of vulnerability established in chapter one and was designed to establish how vulnerable to victimisation someone is relative to others, in terms of risk and impact of victimisation. It is also within this dimension that *repeat/multiple victimisations* are best understood and measured given that, as noted above, they function as both a 'flag' and a 'booster' of F&CM victimisation. The *crime* dimension, drawing on Cohen and Felson's (1979) Routine Activity Theory, relates to the circumstances of the crime itself which may render an individual more vulnerable to (further) victimisation. It includes both *situational factors* and *guardianship factors*. Police forces are already well placed to identify trends in the types of F&CM and associated MOs and assess vulnerability accordingly. Finally, the capabilities dimension is particularly important to addressing vulnerability post victimisation, as the individual's ability to recover from F&CM depends on *embodied*, *relational* and *structural* factors. This dimension draws on the work of Sen (1999), Nussbaum (2006, 2011) and Fineman (2008, 2017) and seeks to make visible the vulnerability factors most neglected in current victim policy and practice.

Research Limitations and Data Quality

As discussed in the methodology chapter, each of the quantitative and qualitative methods used in this thesis had limitations. However, by using a flexible mixed-methods approach, this thesis has produced the best possible evidence using AF data and demonstrated its richness and potential for future research. Nonetheless, as with any research using crime reports, the most considerable limitation of this study relates to the quality of the dataset itself, shaped as it is by the purposes of crime recording as well as reporting behaviour and recording practices. As such, developing an in-depth understanding of the quality of AF data was key throughout the research, analysis and writing stages of this work. In chapter four, the volatility of AF data to external events was evidenced through the sharp fall in reports over a period of crisis within the national reporting centre. This volatility has implications for research and the planning of victim responses. Firstly, the interpretation of any trends in reporting needs to consider inconsistent service provision and the effect of external events. Secondly, events which attract

media attention such as large data breaches should inform the planning of services, to anticipate surges in demand. At the same time, the purpose and rules governing the collection of crime data had considerable implications for the analysis and interpretation of results. However, as highlighted in the above summary of results, reflecting on the quality of the data was, in itself, integral to identifying the policy and practice implications of this research.

Theoretical Contribution

This thesis has made a significant contribution by empirically demonstrating the erosion of the online/offline dichotomy. As noted in the summary of results, mixed on/offline elements were found to be prevalent within both fraud and CM cases and mixed MOs appeared to be increasing. As such, F&CM are increasingly *hybrid crimes* (Caneppele & Aebi, 2019). Reflecting the work of Powell et al. (2018), these results suggest that focusing on the harms associated with crime in the digital society, where technology is increasingly integrated into and inseparable from 'reality', is a more appropriate lens through which to understand and respond to victimisation. Furthermore, the empirical findings corroborate the view expressed by others (van der Wagen & Pieters, 2020) that conceptualisations of 'the victim' as single, human agents, are too narrow to identify and respond to vulnerability in a digital world. These theoretical positions have practical implications as narrow conceptualisations of 'cybercrime' or 'the victim' will lead to ineffectual prevention initiatives and the inadequate distribution of police and support resources.

Furthermore, as also argued by Powell et al. (2018) while cyber-criminology orthodoxy has focused on online fraud and computer misuse, it has done so primarily through limited theoretical perspectives and a crime control lens. However, such perspectives shed limited light on the notion of victim vulnerability and this thesis has demonstrated that the concept of vulnerability is key to understandings of 'the victim' at the micro, meso and macro levels. The micro-level relates to individual victims' experience, the meso-level to institutional labelling, and the macro-level to the socio-cultural recognition of victims' legitimacy. Responses to F&CM, including the dispensation of what Hall (2009) has called victims' procedural and service rights, will most likely be inadequate where these understandings are misaligned. Importantly, victim support services are made available based on assessments of vulnerability which are not consistent across different police force areas and my not be carried out systematically or based on a well-established and tested vulnerability framework. In the absence of such a framework, it is likely that victim response will default to privileging those

who most readily fulfil idealised conceptualisations of 'the victim' (Christie, 1986), an ideal which F&CM victims are unlikely to meet (Cross, 2018).

As such, the vulnerability framework proposed in this thesis is a timely and significant theoretical contribution. It is empirically grounded and addresses F&CM vulnerability at two distinct stages. Firstly, vulnerability *to victimisation* is concerned with risk of (re)victimisisation. Secondly, *vulnerability post-victimisation* is concerned with victims' ability to cope with or recover from the negative impacts of a victimisation experience. This distinction is theoretical, in that it recognises that the concept of vulnerability includes both risk of harm and ability to recover from harm. At the same time, it is useful in practice, as different agencies and stakeholders will be responsible and competent to address one or the other. Crucially, responding to vulnerability *to victimisation* and *post-victimisation* can occur in the absence of sufficient leads for a police investigation or prosecution – the criteria by which most F&CM cases are currently filled with no further actions (Correia 2019).

Implications for Policy & Practice

Despite the volume of F&CM and its impact on victims, it is fair to say that up until recently, these victims (particularly individuals) have been somewhat overlooked in government initiatives. The key reason for this, it is argued, is that reforms around victim's rights have focused on narrow aspects of the overall CJS system – specifically, who constitutes a 'vulnerable victim' and the types of rights to which they are entitled. Firstly, few victims of F&CM will quality as 'vulnerable' given the Victims' Code definition. Secondly, the Code is focused on supporting victims where they become witnesses in criminal trials, something that is unlikely to ever materialise for most F&CM victims. As demonstrated in this thesis, few F&CM reports are investigated and even fewer make it to the courts. As such, it is no surprise that the overwhelming majority of F&CM victims receive little to no response.

For victims to be put at 'the heart' of the criminal justice system, an empirically grounded vulnerability framework that goes beyond the narrowly defined vulnerability dimensions recognised within the Victims' Code, was needed. The framework proposed in this thesis provides a lens through which to systematically consider the circumstances that make individuals more or less *vulnerable to* becoming (repeat) victims, as well as more or less *vulnerable post* victimisation and thereby, more or less able to recover from the impacts of their experience of F&CM victimisation. Furthermore, an attempt was made to sketch how individual factors within each of the identified vulnerability dimensions may be assessed.

Systematically assessing victims' vulnerability is an important step towards identifying an adequate victim response, be it through formal or informal networks. As has been highlighted throughout this thesis, not all victims of F&CM will want or need support. However, it is clear from the case studies examined that some do and that providing this support is key to mitigating the potentially devastating effects of F&CM victimisation. It is recognised that like the term 'victim' the concept of 'vulnerability' may carry stigma and/or be considered an undesirable state. As such, it is important this and any subsequent vulnerability frameworks are used to identify victim needs as a first step. However, subsequent advise and practice should focus on positively enabling victims to become more resilience to F&CM and its impacts.

Furthermore, this work has highlighted flaws in the reporting system including issues of data quality and the lack of a robust system to measure the impact of these crimes on victims, as well as identify vulnerable and repeat victims. Since this data was collected, the reporting system has already improved considerably. Since the data analysed in this thesis was collected for example, local forces have begun to receive information about how the victim scores the impact of the crime across several impact and vulnerability dimensions. As such, future research using AF or local force data will be able to provide further insights on the impact of F&CM on individuals. Nonetheless, the information that is collected from the victim when the crime is first recorded is still considerably oriented towards the 'Pursue' rather than the 'Protect' strand of policing. As such, more can be done to optimise the information collected, to provide local forces with a better picture of victim impact, which can then inform their victim-focused response.

Finally, the proposed vulnerability framework has highlighted the role of the wider F&CM 'justice network' (Button, Tapley, & Lewis, 2012) in identifying and responding to F&CM vulnerability. On one hand, technologies and services provide *affordances* which are enable companies to operate (and profit) but are also exploited by offenders to commit F&CM crimes. In chapter six, enabling industries were identified as increasing *vulnerability to* and *post* victimisation. A vulnerability prism leads to the recognition that those who design and manage the relevant services and technologies have a role and must take responsibility for addressing the harms which result from F&CM victimisation. On the other, given the wide range of vulnerability factors identified within the *capabilities dimension*, it is clear that no one government agency, charity or business will have the ability to respond to victims' heterogenous and sometimes complex needs. As such, initiatives such as the Wales Against

Scams Partnership are needed to continue to work towards a coordinated multi-stakeholder response and ensure victims get the right support, when they need it. The extent to which partner agencies are able to respond to needs, is an area for future research.

In conclusion, this work has taken small steps towards defining what an adequate response to the plight of F&CM victims might look like and what it might require. A vulnerability lens provides a tool to focus on making victims more resilient to F&CM and its impacts. In doing so, it provides an alternative to the traditional 'Just Deserts' approach, focused on investigation, prosecution and ultimately the punishment of those who break the law. Instead, it focuses on addressing harm: what harms were suffered, by whom, how to prevent and repair them, and who has the obligation/ability to do so (Zehr, 1990, 2015). In the context of the current response in England and Wales, this would most certainly be more meaningful for victims.

Areas for Further Research

Having met the three key aims it set out to achieve, this thesis has raised new questions and avenues for research throughout. Overall, four key areas for future research were identified. Recorded crime and survey data can play important roles across each of these. However, collecting data directly from victims and exploring their lived experiences will be essential.

Firstly, future research might explore whether and how experiences of F&CM and responses to victimisation are shaped by victims' gender and race. This question has arisen from the contrasting victim profiles which are observed when crime survey and crime report data are compared and the under-representation of victims from non-White backgrounds. Furthermore, while some work has focused on age, F&CM victimisation has not been studied through a critical gender or race theory lens.

Secondly, while the no significant statistical differences were found with respect to overall levels of deprivation and internet access in areas where F&CM were recorded, socio-economy deprivation was captured within the structural vulnerability theme. Furthermore, the statistical measures used in this thesis related to the victim's locality, rather than their personal circumstances. As such, future research might consider the extent to which risk of victimisation and impact post-victimisation varies with levels of deprivation and internet access, measured at the individual level.

Thirdly, future work is needed to test the proposed vulnerability framework in its entirety. While this thesis has made a major contribution by proposing eight vulnerability factors across

three overall vulnerability dimensions, these are inevitably open to debate and refinement through future research and further empirical testing. In particular, future research might refine this framework by analysing victim experiences in the other UK nations (England, Scotland and Northern Ireland) and seek to establish international comparisons beyond the UK.

In addition, as previously noted, there have been considerable improvements in the AF recording processes since this data was collected. Several of these improvements included better measuring and recording of crime impacts on victims through self-report scales and automated recording of repeat victimisation. Further research might test and demonstrate the extent to which these are working effectively to identify and respond to repeat and vulnerable victims. In addition, there is scope to test the impact of major events (e.g., COVID19 lockdowns) on F&CM victim impact and repeat victimisation metrics.

Finally, more work is necessary to fully understand F&CM victims' experiences of current responses to these crime types and the extent to which current responses across the F&CM 'justice network' are adequate to address vulnerability in an increasingly digital world. Identifying the factors which make victims more *vulnerable to* and *post* F&CM victimisation was a key step. However, ensuring an adequate response to those needs will be the ultimately test of a victim-focused response.

GLOSSARY

Administrative data: data "collected by organisations and agencies expressly for the purpose of conducting administrative tasks and meeting administrative responsibilities for that organisation or agency" (Newschaffer, 2008).

Aggrieved Party: A term often used by law enforcement and Action fraud in lieu of crime 'victim'.

Authorised Push Payment (APP) frauds: where a fraud victim is manipulated into executing or authorising a transfer of funds which turns out to be a fraud because either they were deceived into transferring funds to the wrong person; or they transferred funds to another for purposes which turned out to be illegitimate (APP Scams Steering Group, 2019a)

Computer Misuse: criminal acts under the UK's Computer Misuse Act 1990.

Crime category: a specific sub-category of fraud or computer misuse. In this thesis, a typology which includes nine sub-categories of fraud and two sub-categories of computer misuse is used.

Crime group: whether a crime belongs to one of the two broad crime types covered in this thesis, fraud and computer misuse.

Cyber-dependent crimes: New crimes such as hacking or the spread of malware, arising from the development of Information and Communication Technology (ICT), where ICT is both the means and the target of the crime.

Cyber-enabled crimes: crimes are which (like fraud) pre-date the existence of Information and Communication Technology (ICT) such as computers and the internet but have, by their use, increased in scale or reach.

Cyber-related crimes: crimes which involve online activity, for example where the Internet is used in the planning of crime, but do not fit into the categories of cyber-enabled or cyber-dependent crimes.

Data linkage: the process of matching datasets to produce linked data, generally either via shared identifiers (deterministic matching), or through statistical methods (probabilistic matching), in order to add additional information/variables to a dataset.

Embodied (vulnerabilities): physical characteristics such as being very young or very old, using a wheelchair, gender, or the colour of one's skin which, but because of how they experienced in their particular social and situational contexts, render individuals differentially vulnerable.

Fraud: criminal acts (or omissions) under the UK's Fraud Act 2006.

Identity fraud: A term commonly used to refer to circumstances where an individual's details are appropriated (or false details created) and used fraudulently by an offender for gain or to avoid an obligation (Pascoe et al., 2006).

Identity theft: A term often used to refer to a more permanent appropriation of a victim's identity than identity fraud. It includes circumstances where an offender lives as their double, acquires credit or enters into contracts under the victim's name. Identity theft can be, therefore, considerably more cumbersome for the victim to rectify than a case of identity fraud.

Indirect victimisation: refers to the harms suffered indirectly as a result of criminal acts (or omissions) e.g., by the close relatives or friends of the individuals who are victimised.

Linked data: data that have been crossed referenced or matched with additional data.

Mass marketing scams/frauds: A term used by Button, Lewis and Tapley (2009b) for a group of 'consumer frauds' which generally fall into four categories 1) sale of non-existent goods or services, 2) supplying goods or services of lower quality than paid for, 3) persuading consumers to buy through hard sales techniques and 4) assuming another identity to perpetrate fraud.

Multiple victimisation: where someone is a victim experiences more than one crime of different types (e.g., burglary and fraud) within a given reference period (across crime type victim).

Police recorded crime: data on crimes reported to and reported by the police for the purposes of investigation and the administration of justice.

Repeat victim: see repeat victimisation.

Repeat victimisation: where someone has been the victim fraud and/or computer misuse more than once (within crime type victim), within the sampled 24 months of Action Fraud data.

Secondary victimisation: instances where victims' subjective experience of victimhood and/or their needs are not recognised or properly understood by those around them (e.g., family,

friends or institutions), and consequently the individual experiences further negative outcomes (e.g., distress, anxiety, further victimisation).

Social Engineering: Social engineering is often used in the context of what is known within the financial sector as Authorised Push Payment (APP) frauds, which will include most frauds under the Advance Fee category used in this study. In both of these cases, social engineering techniques will have been used.

Tarian: Welsh word for 'shield'. The code name for the Southern Wales Regional Organised Crime Unit (SW-ROCU).

Unstructured data: data which contains information in a format which is not organised in a standard or pre-defined manner, such as the free-text incident descriptions in Action Fraud data.

Victim: someone who has suffered a harm or "some kind of misfortune" (Walklake, 2007, p. 27). In this thesis, this is limited to harms which result from (another's) criminal act.

Vulnerability: a (universal) susceptibility to being harmed. In this thesis this includes two broad types. Firstly, *vulnerability to* F&CM (considered a harm in itself); and secondly the extent to which individuals are or not able to cope with the negative consequences of being victimised (*vulnerability post* F&CM).

BIBLIOGRAPHY

ACFE. (2016). Report To The Nations On Occupational Fraud and Abuse. In *Global Fraud Study*. Austin, Texas, USA: Association of Certified Fraud Examiners.

Action Fraud. (2018). Economic Crime Victim Care Unit (ECVCU). Retrieved from https://www.actionfraud.police.uk/support-and-prevention-economic-crime-victim-care-unit

Action Fraud. (2020a). Avoid scoring a cyber own goal when streaming Premier League's return [Press release]. Retrieved from https://www.actionfraud.police.uk/news/avoid-scoring-a-cyber-own-goal-when-streaming-premier-leagues-return

Action Fraud. (2020b). Coronavirus-related fraud reports increase by 400% in March [Press release]. Retrieved from https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march

Adyen. (2014a). How 3D Secure can increase conversion rates [Press release]. Retrieved from https://www.adyen.com/blog/how-3d-secure-can-increase-conversion-rates#:~:text=We%20found%20that%20using%203D,an%20average%20of%20almost%208%25.&text=For%20years%2C%20the%20payments%20industry,with%20a%20terrible%20shopper%20experience.

Adyen. (2014b). Optimizing payments to increase revenues. In *8 Best Practices to enhance consumer experience and payment processing*. London: Edgar Dunn & Company.

Aguiar, P., Vala, J., Correia, I., & Pereira, C. (2008). Justice in Our World and in that of Others: Belief in a Just World and Reactions to Victims. *Social Justice Research, 21*(1).

Allaire, J., Xie, Y., McPherson, J., Luraschi, J., Ushey, K., Atkins, A., . . . Iannone, R. (2020). rmarkdown: Dynamic Documents for R. Retrieved from https://github.com/rstudio/rmarkdown

APP Scams Steering Group. (2019a). *Contingent Reimbursement Model Code for Authorised Push Payment Scams*. Retrieved from https://appcrmsteeringgroup.uk/wp-content/uploads/2019/05/CRM-code-LSB-final-280519.pdf

APP Scams Steering Group. (2019b). New voluntary Code on authorised push payment scams launches today [Press release]. Retrieved from https://appcrmsteeringgroup.uk/new-voluntary-code-on-authorised-push-payment-scams-launches-today/

APWG (2020). Phishing Activity Trends Report - 3rd Quarter 2020, APWG.

Bacher, P., Holz, T., Kotter, M., & Wicherski, G. (2008). *Tracking botnets: Using honeynets to learn more about bots*. Retrieved from http://www.honeynet.org/papers/bots/

BBC. (2016). Conned Uxbridge woman convicted in internet dating scam. *BBC News*. Retrieved from https://www.bbc.co.uk/news/uk-england-london-37099195

BBC. (2017). Cyber-flaw affects 745,000 pacemakers. *BBC News Online*. Retrieved from https://www.bbc.co.uk/news/technology-41099867

BBC. (2017a, 13 May 2017). Massive ransomware infection hits computers in 99 countries. Retrieved from http://www.bbc.co.uk/news/technology-39901382

BBC. (2017b, 25 May 2017). Russian postal service 'hit by WannaCry'. Retrieved from http://www.bbc.co.uk/news/technology-40044251

BBC. (2017c, 13 May 2017). Who was hit by the NHS cyber-attack? Retrieved from http://www.bbc.co.uk/news/health-39904851

BBC. (2017d, 10 October 2017). Equifax data hack affected 694,000 UK customers. *BBC News*. Retrieved from http://www.bbc.co.uk/news/business-41575188

BBC. (2019a). Santa hacker speaks to girl via smart camera. *BBC News Online*. Retrieved from https://www.bbc.co.uk/news/technology-50760103

BBC. (2019b, 22 May 2019). TalkTalk data breach customer details found online. *BBC*. Retrieved from https://www.bbc.co.uk/news/business-48351900

Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2017). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? *CyberPsychology, Behavior & Social Networking, 0*(0), null.

Bergoffen, D. (2011). Contesting the Politics of Genocidal Rape: Affirming the Dignity of the Vulnerable Body: Routledge.

Bernardi, F., Chakhaia, L., & Leopold, L. (2016). 'Sing Me a Song with Social Significance': The (Mis)Use of Statistical Significance Testing in European Sociological Research. *European Sociological Review, 33*(1), 1-15.

Berners.Lee, T. (2006). Linked Data. Retrieved from http://www.w3.org/DesignIssues/LinkedData.html

Bies, R. J., & Moag, J. S. (1986). Interactional justice: Communication criteria of fairness. In R. J. Lewichi, B. H. Sheppard, & M. H. Bazerman (Eds.), *Research on negotiation in organizations* (pp. 43-55). Greenwich, CT: JAI Press.

Blackburn, S. (Ed.) (2016) The Oxford Dictionary of Philosophy (3 ed.). Oxford University Press.

Blakeborough, L., & Correia, S. (2018). *The scale and nature of fraud: a review of the evidence*. Retrieved from https://www.gov.uk/government/publications/the-scale-and-nature-of-fraud-a-review-of-the-evidence

Blevins, C., & Mullen, L. (2015). Jane, John … Leslie? A Historical Method for Algorithmic Gender Prediction. *Digital Humanities Quarterly, 9*(3). Retrieved from http://www.digitalhumanities.org/dhq/vol/9/3/000223/000223.html

Böhme, R., & Moore, T. (2012). *How do consumers react to cybercrime?* Paper presented at the eCrime Researchers Summit, Las Croabas, USA.

Bolimos, I. A., & Choo, K.-K. R. (2017). Online fraud offending within an Australian jurisdiction. *Journal of Financial Crime, 24*(2), 277-308.

Bondt, W. D. (2014). Evidence based EU criminal policy making: in search of matching data. *European Journal of Criminal Policy Research, 20*(1), 23-49.

Borg, A., & Sariyar, M. (2020). Record Linkage Functions for Linking and Deduplicating Data Sets (Version 0.4-12). Retrieved from https://cran.r-project.org/web/packages/RecordLinkage/RecordLinkage.pdf

Bowling, B., Parmar, A., & Phillips, C. (2003). Policing ethnic minority communities. In T. Newburn (Ed.), *Handbook of policing* (pp. 528-555). Devon, UK: Willan Publishing.

Bozzaro, C., Boldt, J., & Schweda, M. (2018). Are older people a vulnerable group? Philosophical and bioethical perspectives on ageing and vulnerability. *Bioethics, 32*(4), 233-239.

Braithwaite, J. (2004). Restorative Justice and De-Professionalization. *The Good Society*, 13(1), 28-31.

Brands, J., & van Wilsem, J. (2019). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology*, 1-22. Retrieved from https://journals.sagepub.com/doi/pdf/10.1177/1477370819839619

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101.

Braun, V., & Clarke, V. (2012). Thematic Analysis. In H. Cooper (Ed.), *APA handbook of research methods in psychology* (Vol. 2). Washington DC: American Psychological Association.

Braun, V., & Clarke, V. (2013). Successful Qualitative Research, a practical guide for beginners. London: SAGE Publications.

Brignall, M. (2014). MasterCard and Visa to simplify hated verification systems. *The Guardian*. Retrieved from https://www.theguardian.com/money/2014/nov/13/mastercard-visa-kill-off-verification-systems

Brimicombe, A. J. (2014). Definition of 'repeat victim' and calculation of repeat victim statistics from police recorded crime and incident data. Retrieved from

Brimicombe, A. J. (2016a). Analysing Police-Recorded Data. *Legal Information Management, 16*(02), 71-77.

Brimicombe, A. J. (2016b). Mining Police-Recorded Offence and Incident Data to Inform a Definition of Repeat Domestic Abuse Victimization for Statistical Reporting. *Policing*, paw025.

Brown, B., & Reed Benedict, W. (2002). Perceptions of the police: Past findings, methodological issues, conceptual issues and policy implications. *Policing: An International Journal of Police Strategies & Management, 25*(3), 543-580.

Brunton-Smith, I. (2017). Fear 2.0 Worry about cybercrime in England and Wales. In M. Lee & G. Mythen (Eds.), *The Routledge International Handbook on Fear of Crime*. London: Routledge.

Bryman, A. (2012). *Social Research Methods*. Oxford: Oxford University Press.

Buetow, S. (2010). Thematic Analysis and Its Reconceptualization as 'Saliency Analysis'. *Journal of Health Services Research & Policy, 15*(2), 123-125.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/14616696.2020.1804973?needAccess=true

Burnes, D., Deliema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports, 17*, 101058.

Busby, J. S., Green, B., and Hutchison, D. (2017). "Analysis of Affordance, Time, and Adaptation in the Assessment of Industrial Control System Cybersecurity Risk." *Risk Analysis* 37(7): 1298-1314.

Bushway, S. D., Sweeten, G., & Wilson, D. B. (2005). Size matters: Standard errors in the application of null hypothesis significance testing in criminology and criminal justice. *Journal of Experimental Criminology, 2*(1), 1-22.

Butler, J. (2006). Precarious Life: The Power of Mourning and Violence. London: Verso.

Button, M., & Cross, C. (2017). *Cyber Frauds, Scams and their Victims*: Taylor & Francis.

Button, M., Lewis, C., & Tapley, J. (2009a). *A better deal for fraud victims: Research into victims' needs and experiences*. Retrieved from London: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118468/better-deal-for-fraud-victims.pdf

Button, M., Lewis, C., & Tapley, J. (2009b). *Fraud typologies and victims of fraud Literature review*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118469/fraud-typologies.pdf

Button, M., Lewis, C., & Tapley, J. (2012). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36-54.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36-54.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391–408.

Button, M., Tapley, J., & Lewis, C. (2012). The 'fraud justice network' and the infra-structure of support for individual fraud victims in England and Wales. *Criminology & Criminal Justice, 13*(1), 37-61.

Calder, J. (1996). Statistical Techniques. In R. Sapsford & V. Jupp (Eds.), *Data Collection and Analysis* (pp. 225-261). London: Sage Publications.

Calder, J., & Sapsford, R. (1996). Multivariate Analysis. In R. Sapsford & V. Jupp (Eds.), *Data Collection and Analysis* (pp. 262-281). London: Sage Publications.

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. *Psychological Bulletin, 56*, 81-105.

Caneppele, S., & Aebi, M. F. (2019). Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *Policing: A Journal of Policy and Practice, 13*(1), 66-79.

Carrabine, E., Iganski, P., South, N., Lee, M., Plummer, K., & Turton, J. (2004). *Criminology: A Sociological Introduction*. London, UNITED KINGDOM: Routledge.

Castells, M. (1996). *The Rise of the Network Society* (Vol. 1). Oxford: Blackwell.

Castells, M. (2000). Toward a Sociology of the Network Society. *Contemporary Sociology, 29*(5), 693-699.

Castells, M. (2010). *The Rise of The Network Society* (2 ed.). Chichester, West Sussex: Wiley Blackwell.

Chakraborti, N., & Garland, J. (2012). Reconceptualizing hate crime victimization through the lens of vulnerability and 'difference'. *Theoretical Criminology, 16*(4), 499-514.

Chambers, R. (1983). Rural Development: Putting the Last First. London: Longman.

Chambers, R. (1989). Editorial Introduction: Vulnerability, Coping and Policy. *IDS Bulletin, 20*(2), 1-7.

Charmaz, K. (2006). Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis: SAGE Publications.

Chemero, A. (2003). An outline of a theory of affordances. *Ecological Psychology,* 15, 181-195.

Christen, P., & Goiser, K. (2007). Quality and Complexity Measures for Data Linkage and Deduplication. In F. J. Guillet & H. J. Hamilton (Eds.), *Quality Measures in Data Mining* (pp. 127-151). Berlin: Springer.

Christen, P. (2012). *Data Matching, Concepts and Techniques for Record Linkage, Entity Resolution, and Duplicate Detection*. Berlin: Springer.

Christie, N. (1986). The Ideal Victim. In E. A. Fattah (Ed.), *From Crimw Policy to Victim Policy*. Simon Fraser University: Macmillan.

Cifas. (2017). *Fraudscape*. Retrieved from https://www.cifas.org.uk/insight/reports-trends/fraudscape-report-2017

City of London Police. (2020). Man sentenced for making and selling fake COVID-19 treatment kits [Press release]. Retrieved from https://www.cityoflondon.police.uk/news/city-of-london/news/2020/template3/pipcu/man-sentenced-for-making-and-selling-fake-covid-19-treatment-kits/

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd. ed.). New York: Lawrence Erlbaum Associates.

Cohen, J. (1992). A power primer. *Pychological Bulletin, 112*(1), 155-159. Retrieved from http://www.bwgriffin.com/workshop/Sampling%20A%20Cohen%20tables.pdf

Cohen, J. (1994). The earth is round ($p < .05$). *American Psychologist, 49*(12), 997-1003.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*(4), 588-608. Retrieved from http://www.jstor.org/stable/2094589

College of Policing. (2015). *Estimating demand on the police service*. Retrieved from https://www.college.police.uk/About/Pages/Demand-Analysis-Report.aspx

Commissioner of Police. (2015). *National Lead Force: First Quarter Performance Report*. (Pol 36/15). London: Police: Economic Crime Board Retrieved from http://democracy.cityoflondon.gov.uk/documents/s53101/Pol_36-15_Q1_ECB%20_Performance_Report_June_2015%20vfinal.pdf

Commissioner of Police. (2016). *National Lead Force: Q4 Performance Report*. (Pol 30-16). Commissioner of Police

Cooke, E., Jahanian, F., & McPherson, D. (2005). *The Zombie roundup: understanding, detecting, and disrupting botnets*. Paper presented at the Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop, Cambridge, MA.

Corera, G. (2017, 19 December 2017). Cyber-attack: US and UK blame North Korea for WannaCry. *BBC News*. Retrieved from https://www.bbc.com/news/world-us-canada-42407488

Corera, G. (2020). Smart camera and baby monitor warning given by UK's cyber-defender. *BBC News Online*. Retrieved from https://www.bbc.co.uk/news/technology-51706631

Correia, I., & Vala, J. (2003). When Will a Victim Be Secondarily Victimized? The Effect of Observer's Belief in a Just World, Victim's Innocence and Persistence of Suffering. *Social Justice Research, 16*(4), 379-400.

Correia, S. (2019). Responding to victimisation in a digital world: a case study of fraud and computer. *Crime Science, 8*(4).

Correia, S. (2020). *Computer crimes and fraud during the Covid19 pandemic: key observations from England & Wales.* Paper presented at the International Conference on Cyberlaw, Cybercrime & Cybersecurity, New Delhi [virtual].

Correia, S. (forthcoming). *Patterns of online repeat victimisation and implications for crime prevention*. Paper presented at the The Symposium on Electronic Crime Research (eCrime 2020), Boston [virtual conference].

Creswell, J. W. (2010). Mapping the developing landscape of mixed methods research. In A. Tashakkori & C. Teddlie (Eds.), *SAGE handbook of mixed methods in social & behavioral research* (2 ed.).

Cross, C. (2013). *'Nobody's holding a gun to your head...': Examining current discourses surrounding victims of online fraud.* Paper presented at the ustice and Social Democracy: Proceedings of the 2nd International Conference, Queensland University of Technology, Australia.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology, 21*(2), 187-204.

Cross, C. (2016). 'They're Very Lonely': Understanding the Fraud Victimisation of Seniors. *International Journal for Crime, Justice and Social Democracy, 5*(4), 60-75.

Cross, C. (2018). “They thought I was a bloody fool”: The Challenge of Gaining Legitimate Victim Status for Online Fraud Victims. In M. Duggan (Ed.), *Revisiting the 'Ideal Victim': Developments in Critical Victimology*: Policy Press.

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding Romance Fraud: Insights From Domestic Violence Research. *The British Journal of Criminology, 58*(6), 1303-1322.

Cross, C., Richards, K., & Smith, R. (2016). *Improving responses to online fraud victims: An examination of reporting and support*. Retrieved from https://eprints.qut.edu.au/98346/1/29-1314-FinalReport.pdf

Cross, C., Smith, R., & Richards, K. (2014). Challenges of responding to online fraud victimisation in Australia. *Trends and Issues in Crime and Criminal Justice, 474*, 1-6.

Curtis, S. (2014). Mastercard and Visa to kill off password authentication. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/technology/news/11228300/Mastercard-and-Visa-to-kill-off-password-authentication.html

DCMS. (2020). *Cyber Security Breaches Survey 2020*. Retrieved from https://www.gov.uk/government/publications/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

Deem, D., & Lande, E. S. (2018). Transnational Scam Predators and Older Adult Victims: Contributing Characteristics of Chronic Victims and Developing an Effective Response. *DOJ Journal of Federal Law and Practice, 66*(117). Retrieved from https://static1.squarespace.com/static/59ab97acf43b556d9260a671/t/5c2418f04fa51a5c3eba22e9/1545869553816/lande+us+attorney+bulletin+article.pdf

Deliema, M., Shadel, D., & Pak, K. (2019). Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors. *Journal of Consumer Research, 46*(5), 904-914.

Delor, F., & Hubert, M. (2000). Revisiting the concept of 'vulnerability'. *Social Science & Medicine, 50*(11), 1557-1570.

Denzin, N. K. (1978). The research act: A theoretical introduction to sociological methods. New York: Praeger.

Eastbourne Herald. (2016). Vulnerable residents offered call blockers to tackle phone scams. Retrieved from https://www.eastbourneherald.co.uk/news/vulnerable-residents-offered-call-blockers-to-tackle-phone-scams-1-7303909

Elkin, M. (2020). *Nature of fraud and computer misuse in England and Wales: year ending March 2019*. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019

ESRC. (2015). ESRC Framework for Research Ethics. In. Swindon, UK: Economic and Social Research Council.

Farrall, S. D., Jackson, J., & Gray, E. (2009). *Social Order and the Fear of Crime in Contemporary Times*. Oxford: Oxford University Press.

Farrell, G. (1992). Multiple Victimisation: Its Extent and Significance. *International Review of Victimology, 2*(2), 85-102.

Farrell, G. (1995). Preventing Repeat Victimization. *Crime and Justice, 19*, 469-534.

Farrell, G., & Birks, D. (2018). Did cybercrime cause the crime drop? *Crime Science, 7*(1), 8.

Farrell, G., & Pease, K. (1993). One Bitten, Twice Bitten: Reapeat Victimisation and its Implications for Crime Prevention. London: Home Office Police Research Group.

Farrell, G., Tseloni, A., & Pease, K. (2005). Repeat Victimization in the ICVS and the NCVS. *Crime Prevention and Community Safety, 7*(3), 7-18.

Fattah, E. A. (1991). Understanding criminal victimization: An introduction to theoretical victimology. Scarborough, Ontario, Canada: Prentice Hall.

Fayard, A.-L., & Weeks, J. (2014). Affordances for practice. *Information and Organization, 24*(4), 236-249.

Fellegi, I. P., & Sunter, A. B. (1969). A Theory for Record Linkage. *Journal of the American Statistical Association 64*(328), 1183-1210.

Ferraro, K. F. (1995). *Fear of Crime: Interpreting Victimization Risk*. Albany: State University of New York Press.

FFA UK. (2017a). *Fraud The Facts*. Retrieved from https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/fraud_the_facts.pdf

Field, A. (2009). *Discovering Statistics Using SPSS*. London: SAGE Publications.

Field, A., Miles, J., & Field, Z. (2012). *Discovering Statistics Using R*: SAGE Publications.

Fildes, J. (2010, 23 September 2010). Stuxnet worm 'targeted high-value Iranian assets'. *BBC News*. Retrieved from http://www.bbc.co.uk/news/technology-11388018

Fineman, M. A. (2008). The Vulnerable Subject: Anchoring Equality in the Human Condition. *Yale Journal of Law & Feminism, 20*(1).

Fineman, M. A. (2012). "Elderly" as Vulnerable: Rethinking the Nature of Individual and Societal Responsibility. *The Elder Law Journal, 20*.

Fineman, M. A. (2017). Vulnerability and Inevitable Inequality. *Oslo Law Review, 4*, 133-149. Retrieved from https://ssrn.com/abstract=3087441

Fisher, R. A. (1922). On the interpretation of chi square from contingency tables, and the calculation of P. *Journal of the Royal Statistical Society, 85*, 87–94.

Flatley, J. (2013). The measurement of fraud and cyber-crime and their implications for crime statistics. Retrieved from

Fohring, S. (2018). What's in a word? Victims on 'victim'. *International Review of Victimology, 24*(2), 151-164.

Fox, J. (1987). Effect Displays for Generalized Linear Models. *Sociological Methodology, 17*, 347-361.

Fox, J. (2003). Effect Displays in R for Generalised Linear Models. *Journal of Statistical Software, 8*(15).

Fox, J., & Weisberg, S. (2011). *An R Companion to Applied Regression* (2nd ed.). London: Sage Publications.

Fox, K. A., Nobles, M. R., & Piquero, A. R. (2009). Gender, crime victimization and fear of crime. *Security Journal, 22*(1), 24-39.

Franceschi-Bicchierai, L. (2016). Hackers Make the First-Ever Ransomware for Smart Thermostats. *Motherboard*. Retrieved from https://www.vice.com/en_us/article/aekj9j/internet-of-things-ransomware-smart-thermostat

Fruhlinger, J. (2017). What is Stuxnet, who created it and how does it work. Retrieved from https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html

Furnell, S., & Dowling, S. (2019). Cyber crime: a portrait of the landscape. *Journal of Criminological Research, Policy and Practice, 5*(1), 13-26.

Ganzini, L., McFarland, B. H., & Bloom, J. D. (1990). Victims of fraud: Comparing victims of white collar and violent crime. *Bulletin of the American Academy of Psychiatry & the Law, 18*(1), 55-63.

Garland, D. (2001). The culture of control : crime and social order in contemporary society. Oxford: Oxford University Press.

Gaver, W. W. (1996). Situating Action II: Affordances for Interaction: The Social Is Material for Design. *Ecological Psychology, 8*(2), 111-129.

Genn, H. (1988). Multiple victimisation. In M. Maguire & J. Pointing (Eds.), *Victims of Crime: A New Deal?* Milton Keynes: Open University Press.

Gibbs, S. (2015, 23 Oct 2015). TalkTalk criticised for poor security and handling of hack attack. *The Guardian,*. Retrieved from https://www.theguardian.com/technology/2015/oct/23/talktalk-criticised-for-poor-security-and-handling-of-hack-attack

Gibson, J. J. (1986). *The ecological approach to visual perception*. London: Lawrence Erlbaum Associates.

Goodin, D. (2018). Hack causes pacemakers to deliver life-threatening shocks. *Ars Technica*. Retrieved from https://arstechnica.com/information-technology/2018/08/lack-of-encryption-makes-hacks-on-life-saving-pacemakers-shockingly-easy/

Gordon, S., & Ford, R. (2002). Cyberterrorism? *Computers & Security, 21*(7), 636-647.

Grabosky, P. N., & Smith, R. G. (1998). *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*. New Brunswick: Transaction Publishers / The Federation Press.

Grabosky, P. N., Smith, R. G., & Dempsey, G. (2001). *Electronic Theft: Unlawful Acquisition in Cyberspace*: Cambridge University Press.

Grannis, S. J., Overhage, J. M., & McDonald, C. J. (2002). *Analysis of identifier performance using a deterministic linkage algorithm.* Paper presented at the AMIA Symposium.

Grear, A. (2010). Redirecting Human Rights: Facing the Challenge of Corporate Legal Humanity. UK: Palgrave Macmillan.

Green, S. (2007). Crime, victimisation and vulnerability. In S. Walklate (Ed.), *Handbook on victims and victimology* (pp. 91-117). Cullompton, Devon, England: Willan Publishing.

Greenberg, J. (1993) The social side of fairness: Interpersonal and informational classes of organizational justice. In, *Series in applied psychology. Justice in the workplace: Approaching fairness in human resource management.* (pp. 79-103): Lawrence Erlbaum Associates, Inc.

Grundy, E. (2006). Ageing and vulnerable elderly people: European perspectives. *Ageing & Society, 26*(1), 105-134.

Hall, M. (2009). Victims of crime: Policy and practice in criminal justice. Cullompton, England: Willan.

Hand, D. J. (2018). Statistical challenges of administrative and transaction data. *Journal of the Royal Statistical Society*(181), 555-605.

Harron, K., Goldstein, H., & Dibben, C. (2015). Introduction. In K. Harron, H. Goldstein, & C. Dibben (Eds.), *Methodological Developments in Data Linkage*. New York: John Wiley & Sons.

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of Crime Online? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization. *Journal of Contemporary Criminal Justice, 29*(4), 475-497.

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30*(May), 1-19.

Hindelang, M., Gottfredson, M. R., & Garofalo, J. (1978). Victims of Personal Crime: an Empirical Foundation for a Theory of Personal Victimisation. Cambridge, Mass.: Ballinger.

HMIC. (2015). Increasingly Everyone's Business: A Progress Report on the Police Response to Domestic Abuse. Retrieved from London:

Holder, R. L. (2016). Untangling the Meanings of Justice: A Longitudinal Mixed Methods Study. *Journal of Mixed Methods Research, 12*(2), 204-220.

Holt, T. J., & Bossler, A. M. (2013). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior, 35*(1), 20-40.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2018). Assessing the Macro-Level Correlates of Malware Infections Using a Routine Activities Framework. *International Journal of Offender Therapy and Comparative Criminology, 62*(6), 1720-1741.

Home Office. (2020a). *Home Office Counting Rules For Recorded Crime: Crime recording General Rules*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/913721/count-general-sep-2020.pdf

Home Office. (2020b). *Home Office Counting Rules For Recorded Crime: Fraud & Computer Misuse*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/881505/count-fraud-apr2-2020.pdf

Hope, T. (2007). Theory and method: the social epidemiology of crime victims. In S. Walklate (Ed.), *Handbook on victims and victimology* (pp. 62-90). Cullompton, Devon, England: Willan Publishing.

Hope, T. (2015b). We need a different crime survey. Retrieved from https://www.crimeandjustice.org.uk/resources/we-need-different-crime-survey

Hope, T., & Norris, P. A. (2013). Heterogeneity in the Frequency Distribution of Crime Victimization. *Journal of Quantitative Criminology, 29*(4), 543-578.

Howell, D. C. (2013). *Statistical methods for psychology* (8th ed.). Belmont, California: Wadsworth Cengage Learning.

Hughes, K. (2018, 5 October 2018). Scam victims face postcode lottery over support as thefts top £500m so far this year;FOI probe shows help varies dramatically across the country despite repeat targeting. *The Independent*.

Hutchby, I. (2001). Technologies, Texts and Affordances. *Sociology, 35*(2), 441-456.

Hutcheson, G. D. (2011). Categorical Explanatory Variables. *Journal of Modelling in Management, 6*(2), 225–236.

Hutcheson, G. D. (2018). Generalized Linear Models: A Course Overview. In *Methods@Manchester Summer School*. Machester: The University of Manchester.

Hutchings, A., & Hayes, H. (2009). Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the 'Net'? *Current Issues in Criminal Justice, 20*(3), 433-452.

Ianelli, N., & Hackworth, A. (2005). *Botnets as a vehicle for online crime*. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_51249.pdf

Ignatans, D., & Pease, K. (2015). Distributive Justice and the Crime Drop. In M. A. Andresen & G. Farrell (Eds.), *The Criminal Act: The Role and Influence of Routine Activity Theory* (pp. 77–87). London: Palgrave Macmillan.

Ignatans, D., & Pease, K. (2016). Taking Crime Seriously: Playing the Weighting Game. *Policing: A Journal of Policy and Practice, 10*(3), 184-193.

Israel, M., & Hay, I. (2012). Research Ethics in Criminology. In G. David, K. Susanne, & F. M. Steven (Eds.), *The SAGE Handbook of Criminological Research Methods* (pp. 500-516): SAGE Publications Ltd.

Jackson, A. (2012). *2011 Census: First Results for Ethnicity, National Identity, and Religion for Wales*. Retrieved from Cardiff: https://gov.wales/sites/default/files/statistics-and-research/2018-12/121217sb1262012en.pdf

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of elder abuse & neglect, 26*(2), 107-122.

Janoff-Bulman, R. (1995). The aftermath of victimization: Rebuilding shattered assumptions. In C. R. Figley (Ed.), *Trauma and its wake: The study and treatment of post-traumatic stress disorder* (pp. 15–35). New York: Brunner and Mazel.

Jarvis, L., & Macdonald, S. (2015). What Is Cyberterrorism? Findings From a Survey of Researchers. *Terrorism and Political Violence, 27*(4), 657-678.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher, 33*(7), 14-26.

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a Definition of Mixed Methods Research. *Journal of Mixed Methods Research, 1*(2), 112-133.

Johnson, S. D. (2008). Repeat Burglary Victimisation: A Tale of Two Theories. *Journal of Experimental Criminology & Public Policy, 4*(3), 215–240.

Jones, L. (2014). Welsh Index of Multiple Deprivation 2014: A guide to analysing deprivation in rural areas - Revised. Cardiff: StatsWales

Jordan, T. (2008). Hacking : digital media and technological determinism / Tim Jordan. Cambridge: Cambridge : Polity, 2008.

Karagiannopoulos, V., Sugiura, L., & Kirby, A. (2019). *The Portsmouth Cybercrime Awareness Clinic Project: Key Findings and Recommendations*. Retrieved from Portsmouth: https://www.port.ac.uk/research/research-projects/cybercrime-awareness-clinic

KAS. (2012). *2011 Census: Usual resident population by single year of age and sex, Wales*. Retrieved from: https://statswales.gov.wales/Catalogue/Census/2011/UsualResidentPopulation-by-FiveYearAgeBand-Gender

Keane, C. (1995). Victimization and Fear: Assessing the Role of the Offender and the Offence. *Canadian Journal of Criminology, 37*, 431-455.

Kerr, J., Owen, R., Nicholls, C. M., & Button, M. (2013). Research on Sentencing Online Fraud Offences. In. London: Sentencing Council.

Keyworth, M. (2018, 28 April 2018). I was a teenage 'money mule'. *BBC News*. Retrieved from https://www.bbc.co.uk/news/business-43897614

Killias, M. (1990). Vulnerability: Towards a Better Understanding of a Key Variable in the Genesis of Fear of Crime. *Violence and Victims, 5*(2), 97-108. Retrieved from https://search.proquest.com/docview/208553839?accountid=14680

Kirby, P. (2006). Vulnerability and Violence: The Impact of Globalisation. London: Pluto Press.

Krebs, J. H. (2018). *Online contracting and the supply of digital content to consumers.* (Ph.D). Swansea University, Swansea. Retrieved from https://cronfa.swan.ac.uk/Record/cronfa38915

Kruskal, W. H., & Wallis, W. A. (1952). Use of ranks in one-criterion variance analysis. *Journal of the American Statistical Association, 47*, 583-621.

Kuhl, L. (1998). The criminal law protection of the Communities' financial interests against fraud: Part 1. *Criminal Law Review*, 259-269. Retrieved from http://login.westlaw.co.uk/maf/wluk/ext/app/document?sp=at02c29b2902-55123&crumb-action=reset&docguid=IA84BD511E72111DA9D198AF4F85CA028

Larsen, K. R., & Monarchi, D. E. (2004). A mathematical approach to categorization and labeling of qualitative data: The latent categorization method. *Sociological Methodology, 34*(1), 349 – 392.

Laughlin, A. (2019). Kids' karaoke machines and smart toys from Mattel and Vtech among those found to have security flaws. Retrieved from https://www.which.co.uk/news/2019/12/kids-karaoke-machines-and-smart-toys-from-mattel-and-vtech-among-those-found-to-have-security-flaws-in-a-which-investigation/

Laurie, G., & Stevens, L. A. (2014). The Administrative Data Research Centre Scotland: A Scoping Report on the Legal & Ethical Issues Arising from Access & Linkage of Administrative Data. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2487971

Law Commission. (2002). Fraud - Report on a reference under section 3(1)(e) of the Law Commissions Act 1965. Retrieved from London:

Lee, P. M. (2012). *Bayesian Statistics : An Introduction*. New York, UNITED KINGDOM: John Wiley & Sons, Incorporated.

Lerner, M. J. (1980). Belief in a Just World: A Fundamental Delusion. New York: Plenum.

Lerner, M. J., & Simmons, C. H. (1966). The observer's reaction to the "innocent victim": Compassion or rejection? *Journal of Personality and Social Psychology, 4*(2), 203–210.

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3), 263-280.

Levene, H. (1960). Robust Tests for Equality of Variance. In I. Olkin (Ed.), *Contributions to Probability and Statistics: Essays in Honor of Harold Hotelling* (pp. 278-292): Stanford University.

Levenshtein, V. I. (1966). Binary codes capable of correcting deletions, insertions, and reversals. *Soviet Physics Doklady, 10*(8), 707–710.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and issues. *Crime, Law and Social Change, 67*(1), 3-20.

Levi, M., & Burrows, J. (2008). Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey. *British Journal of Criminology, 48*(3), 293-318.

Loseman, A., & van den Bos, K. (2012). A Self-Regulation Hypothesis of Coping with an Unjust World: Ego-Depletion and Self-Affirmation as Underlying Aspects of Blaming of Innocent Victims. *Social Justice Research, 25*(1), 1-13.

MacDonald, Z. (2001). Revisiting the Dark Figure: A Microeconometric Analysis of the Under-reporting of Property Crime and Its Implications. *The British Journal of Criminology, 41*(1), 127-149.

Mann, H. B., & Whitney, D. R. (1947). On a test of whether one of two random variables is stochastically larger than the other. *Annals of Mathematical Statistics, 18*(1), 50-60.

Matthews, R. (2014). *Realist Criminology*. Basingstoke: Palgrave Macmillan.

McAfee. (2020). What is Stuxnet? Retrieved from https://www.mcafee.com/enterprise/en-gb/security-awareness/ransomware/what-is-stuxnet.html

McGuire, M. (2007). *Hypercrime: the new geometry of harm* (1st ed. ed.). Milton Park, Abingdon, Oxon: Routledge-Cavendish.

McGuire, M., & Dowling, S. (2013). *Cyber crime: a review of the evidence*. Retrieved from https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

Mendelsohn, B. (1956). Une nouvelle branche de la science bio-psycho-sociale —la victimologie. *Revue Internationale de Criminologie et de Police Technique, 10*, 95–109.

Mendelsohn, B. (1976). Victimology and contemporary society's trends. *Victimology, 1*(1), 8-28.

Merleau-Ponty, M. (2012). *Phenomenology of Perception*. Florence, UK: Taylor & Francis Group.

Moitra, S. D., & Konda, S. L. (2004). An Empirical Investigation of Network Attacks on Computer Systems. *Computers and Security, 23*(1), 43-51.

MOJ. (2015). Code of Practice for Victims of Crime. In. London: Ministry of Justice.

MOJ. (2018). Victims Strategy. In. London: Ministry of Justice.

Moore, T., Clayton, R., & Anderson, R. (2009). The Economics of Online Crime. *Journal of Economic Perspectives, 23*(3), 3-20.

Morse, J. (1991). Approaches to qualitative-quantitative methodological triangulation. *Nursing Research, 40*, 120-123.

Mullen, L. (2016). Predict Gender from Names Using Historical Data In: CRAN.

Munbodh, E. (2019, 7 Oct 2019). 'I was a 15-year-old money mule after criminals hired me at the school gate'. *The Mirror*. Retrieved from https://www.mirror.co.uk/money/i-15-year-old-money-20531741

Munro, V. E., & Scoular, J. (2012). Abusing Vulnerability? Contemporary Law and Policy Responses to Sex Work in the UK. *Feminist Legal Studies, 20*(3), 189–206.

Murdoch, S. J., & Anderson, R. (2010). Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication. In R. Sion (Ed.), *Financial Cryptography and Data Security* (Vol. 6052, pp. 336-342). Berlin, Heidelberg: Springer.

Murray, A. (2018, 24 February 2018). Banks' branch security protocols under fire as criminals force widow, 81, to withdraw £136,500. *The Daily Telegraph,* pp. 1-2.

NCA. (2020). Multi-agency action targets city money laundering [Press release]. Retrieved from https://nationalcrimeagency.gov.uk/news/multi-agency-action-targets-city-money-laundering

NCSC. (2020). NCSC statement: EasyJet cyber incident [Press release]. Retrieved from https://www.ncsc.gov.uk/news/easyjet-incident

Newcombe, H. B., Kennedy, J., Axford, S., & James, A. (1959). Automatic linkage of vital records. *Science, 130*(3381), 954-959.

Newgard, C. (2006). Validation of probabilistic linkage to match de-identified ambulance records to a state trauma registry. *Academic Emergency Medicine, 13*(1), 69– 75.

Newschaffer, C. (Ed.) (2008) Encyclopedia of Epidemiology. Sage Publications, Inc.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology, 5*(1), 773–793.

Niche Techonology. (2019). Who We Serve. Retrieved from https://nicherms.com/who-we-serve/

Norman, D. A. (1999). Affordance, conventions, and design. *Interaction,s* 6(3), 38-43.

NTS. (2018). Successful project blocks over 100,000 nuisance calls [Press release]. Retrieved from https://www.nationaltradingstandards.uk/news/successful-project-blocks-over-100000-nuisance-calls/

NTS. (2019). Free call blockers for victims of scam and nuisance phone calls. Retrieved from https://www.nationaltradingstandards.uk/news/free-call-blockers-for-victims-of-scam-and-nuisance-phone-calls/

Nussbaum, M. C. (2006). *Frontiers of Justice*. Cambridge, MA: Harvard University Press.

Nussbaum, M. C. (2011). *Creating Capabilities*. Cambridge, Massachusetts: Harvard University Press.

Odell, M. K. (1956). The profit in records management. *Systems Mgazine, 20*.

Ofcom. (2017a). *About this data: Fixed local and unitary authority*. Retrieved from: https://www.ofcom.org.uk/__data/assets/pdf_file/0032/97565/About-this-data-fixed-local-and-unitary-authority-2016.pdf

Ofcom. (2017b). *Fixed local authority 2016*. Retrieved from: https://www.ofcom.org.uk/research-and-data/multi-sector-research/infrastructure-research/connected-nations-2016/downloads

OFT. (2006). Research on impact of mass marketed scams / A summary of research into the impact of scams on UK consumers (OFT883). Retrieved from

ONS. (2016a). ONS Postcode Directory User Guide. In. Newport, Wales, UK: ONS Geography.

ONS. (2016b). Overview of fraud statistics: year ending Mar 2016. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudstatistics/yearendingmarch2016

ONS. (2017a). *Crime in England & Wales, year ending September 2016 - Additional experimental tables on fraud*. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables

ONS. (2017b). *Crime in England and Wales: Experimental tables - Year ending September 2016*. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables

ONS. (2017c). *Household Crime Prevalence: CSEW Open Data Table - Year ending March 2016*. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/householdcrimeprevalencecsewopendatatable

ONS. (2018). *Estimates of the population for the UK, England and Wales, Scotland and Northern Ireland; Mid-2012 to Mid-2016*. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/datasets/populationestimatesforukenglandandwalesscotlandandnorthernireland

ONS. (2019). *Local Authority District to Community Safety Partnerships to Police Force Areas (December 2016) Lookup in England and Wales*. Retrieved from: https://geoportal.statistics.gov.uk/datasets/local-authority-district-to-community-safety-partnerships-to-police-force-areas-december-2016-lookup-in-england-and-wales

ONS. (2020a). *Crime in England and Wales: Annual Trend and Demographic Tables - Year Ending March 2020*. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesannualtrendanddemographictables

ONS. (2020b). *Crime in England and Wales: Appendix Tables - Year Ending March 2020*. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables

ONS. (2020c). *Crime in England and Wales: Other related tables - Year Ending March 2020*. Retrieved from:

https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesotherrelatedtables

ONS. (2020d). Significance testing for proportion of adults who were victims of fraud and computer misuse by personal and household characteristics, year ending March 2019 CSEW. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/adhocs/11219significancetestingforproportionofadultswhowerevictimsoffraudandcomputermisusebypersonalandhouseholdcharacteristicsyearendingmarch2019csew

ONS. (2020e). User guide to crime statistics for England and Wales. In (pp. 1-138). Titchfield: Office for National Statistics.

Out-Law.com. (2015). Action Fraud 'turmoil' leaves litigation the only option for fraud victims, says expert. Retrieved from https://www.out-law.com/en/articles/2015/july/action-fraud-turmoil-leaves-litigation-the-only-option-for-fraud-victims-says-expert/

Owen, J. (2015). Concentrix: US firm brought in by City of London police to run Action Fraud helpline despite concerns. *The Independent*. Retrieved from https://www.independent.co.uk/news/uk/home-news/concentrix-us-firm-brought-in-by-city-of-london-police-to-run-action-fraud-helpline-despite-concerns-a6701771.html

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice, 43*(4), 626-642.

Palm, R. I. (1990). Natural hazards: an integrative framework for research and planning. London: The Johns Hopkins University Press.

Pascoe, T., Owen, K., Keats, G., & Gill, M. (2006). *Identity Fraud: What about the Victim?* Retrieved from

Pearson, K. (1990). On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. *Philosophical Magazine, 50*(5), 157-175.

Pease, K., Ignatans, D., & Batty, L. (2018). Whatever happened to repeat victimisation? *Crime Prevention and Community Safety, 20*(4), 256-267.

Peaston, S. (2019). Fraudscape. In. London: Cifas.

Peroni, L., & Timmer, A. (2013). Vulnerable groups: The promise of an emerging concept in European Human Rights Convention law. *International Journal of Constitutional Law, 11*(4), 1056 - 1085. Retrieved from https://academic.oup.com/icon/article-lookup/doi/10.1093/icon/mot042

Polvi, N., Looman, T., Humphries, C., & Pease, K. (1990). Repeat Break-and-Enter Victimization: Time Course and Crime Prevention Opportunity. *Journal of Police Science and Administration, 17*(1), 8-11.

Polvi, N., Looman, T., Humphries, C., & Pease, K. (1991). The Time Course of Repeat Burglary Victimization. *The British Journal of Criminology, 31*(4), 411-414.

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital Criminology, Crime and Justice in Digital Society*. London: Routledge.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Pullen, P. J. (2019). Nail in the MLAT Coffin: Examining Alternative Solutions to the Current Mutual Legal Assistance Treaty Regime in International Cross-Border Data Sharing. *North Carolina Journal of International Law, 44*(4).

Quach, K. (2020). Researchers trick Tesla into massively breaking the speed limit by sticking a 2-inch piece of electrical tape on a sign. *The Register*. Retrieved from https://www.theregister.co.uk/2020/02/20/tesla_ai_tricked_85_mph/

Ranapurwala, S. I., Berg, M. T., & Casteel, C. (2016). Reporting Crime Victimizations to the Police and the Incidence of Future Victimizations: A Longitudinal Study. *PLOS ONE, 11*(7), e0160072.

Randa, R. (2013). The influence of the cyber-social environment on fear of victimization: Cyberbullying and school. *Security Journal, 26*(4), 331-348.

Rea, L. M., & Parker, R. A. (2014). *Designing and conducting survey research: a comprehensive guide, fourth edition* (4th ed. ed.). San Francisco, CA: San Francisco, CA: Wiley.

Reicher, S. (2000). Against methodolatry: some comments on Elliott, Fischer, and Rennie. *British Journal of Clinical Psychology, 39*(1), 1-6.

Reiss, A. J. (1980). Victim proneness in repeat victimisation by type of crime. Retrieved from Washington:

Reyns Bradford, W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime, 22*(4), 396-411.

Reyns, B. W., & Henson, B. (2015). The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory. *International Journal of Offender Therapy and Comparative Criminology, 60*(10), 1119-1139.

Rhysider, J. (2020). EPISODE 72: BANGLADESH BANK HEIST. In. Darknet Diaries.

Riek, M., Abramova, S., & Böhme, R. (2017). *Analyzing Persistent Impact of Cybercrime on the Societal Level: Evidence for Individual Security Behavior*. Paper presented at the Thirty Eighth International Conference on Information Systems, South Korea.

Rosca, M. (2020). Money laundering on the high street. *Politico*. Retrieved from https://www.politico.eu/article/money-laundering-britain-high-street-foreign-exchange-shops/

Rosenthal, R. (1991). *Meta-nalytic procedures for social research* (2 ed.). Newbury Park, CA: Sage.

Ross, M., Grossman, I., & Schryer, E. (2014). Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimised by consumer fraud. *Perspectives of Psychological Science, 9*(4), 427-442.

Rountree, P. W. (1998). A Reexamination of the Crime-Fear Linkage. *Journal of Research in Crime and Delinquency, 35*(3), 341-372.

Roux, G. (2018). Perception of Police Unfairness Amongst Stigmatized Groups: The Impact of Ethnicity, Islamic Affiliation and Neighbourhood. In S. Roché & M. Hough (Eds.), *Minority Youth and Social Integration*. Cham.: Springer.

Sagovsky, A., & Johnson, S. D. (2007). When does repeat burglary victimisation occur? *Australian and New Zealand Journal of Criminology, 40*(1), 1-26.

Şahin, E., Cakmak, M., Doğar, M. R., Uğur, E., & Üçoluk, G. (2007). To afford or not to afford: A new formalization of affordances toward affordance-based robot control. *Adaptive Behavior*, 15(4), 447-472.

Sampson, A., & Phillips, C. (1991). *Reducing Repeat Racial Victimisation on an East London Estate*. Retrieved from London: http://library.college.police.uk/docs/hopolicers/fcdps67.pdf

Sariyar, M., & Borg, A. (2010). The RecordLinkage Package: Detecting Errors in Data. *The R Journal, 2*(2), 61-67. Retrieved from https://journal.r-project.org/archive/2010-2/RJournal_2010-2_Sariyar+Borg.pdf

Schiebe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., & Cartensen, L. (2014). Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic and Applied Social Psychology, 36*(3), 272-279.

Scholes, A. (2018). *The scale and drivers of attrition in reported fraud and cyber crime*. Retrieved from London: https://www.gov.uk/government/publications/the-scale-and-drivers-of-attrition-in-reported-fraud-and-cyber-crime

Schroder-Butterfill, E., & Marianti, R. (2006). A framework for understanding old-age vulnerabilities. *Ageing & Society, 26*(1), 9-35.

Schuilenburg, M. (2017). The Securitization of Society: Crime, Risk, and Social Order (2nd eds ed.): NYU Press.

Sen, A. (1999). *Development as Freedom*. Oxford: Oxford University Press.

Shorrock, S., McManus, M. A., & Kirby, S. (2020). Profile of repeat victimisation within multi-agency referrals. *International Review of Victimology, online first*, 1-12.

Sidebottom, A. (2012). Repeat Burglary Victimization in Malawi and the Influence of Housing Type and Area-Level Influence. *Security Journal, 25*(3), 265–281.

Siegel, S., & Castellan, N. J. (1988). *Nonparametric statistics for the behavioral sciences* (2 ed.). New York: MacGraw-Hill.

Simon, J. (2006). Governing through crime how the war on crime transformed American democracy and created a culture of fear. New York: Oxford University Press.

Skidmore, M., Goldstraw-White, J., & Gill, M. (2020a). Understanding the police response to fraud: the challenges in configuring a response to a low-priority crime on the rise. *Public Money & Management, 40*(5), 369-379.

Skidmore, M., Goldstraw-White, J., & Gill, M. (2020b). Vulnerability as a driver of the police response to fraud. *Journal of Criminological Research, Policy and Practice,* 6(1), 49-64.

Skogan, W. G. (1987). The Impact of Victimization on Fear. *Crime and Delinquency, 33*, 135-154.

Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber Criminals on Trial*. Cambridge: Cambridge University Press.

Spalek, B. (1999). Exploring the impact of financial crime: A study looking into the effects of the Maxwell scandal upon Mawell pensioners. *International Review of Victimology, 6*(3), 213-230.

Spalek, B. (2006). *Crime Victims: Theory, Policy and Practice*. Basingstoke, Hampshire: Palgrave Macmillan.

Sparks, R. (1981). Multiple Victimisation: Evidence, Theory and Future Research. *Journal of Criminal Law and Criminology, 72*(2), 762-778. Retrieved from https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=6239&context=jclc

Sparks, R. (2020). Crime and justice research: The current landscape and future possibilities. *Criminology & Criminal Justice, 20*(4), 471-482.

Sparks, R., Genn, H., & Dodd, D. (1977). *Surveying Victims*. London: Wiley.

Spearman, C. (1910). Correlation calculated with faulty data. *British Journal of Psychology, 3*, 271-295.

Stabek, A., Watters, P., & Layton, R. (2010). The Seven Scam Types: Mapping the Terrain of Cybercrime. 41-51.

StatsWales. (2014a). *WIMD 2014*. Retrieved from: https://statswales.gov.wales/Catalogue/Community-Safety-and-Social-Inclusion/Welsh-Index-of-Multiple-Deprivation/Archive/WIMD-2014

StatsWales. (2014b). WIMD 2014: Report. In *Welsh Index of Multiple Deprivation (WIMD) 2014 - Revised*. Cardiff: Welsh Government.

Stripe, N. (2020). *Crime in England and Wales: Police Force Area data tables*. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/policeforceareadatatables

Strobl, R. (2010). Becoming a victim. In S. G. Shoham, P. Knepper, & M. Kett (Eds.), *International Handbook of Victimology* (pp. 3–25). Boca Raton, F.L.: Taylor and Francis,.

Sussex PCC. (2017, 21 November 2017). Victim speaks out as Sussex Police reveal rise in romance fraud. Retrieved from https://www.sussex-pcc.gov.uk/about/news/victim-speaks-out-as-sussex-police-reveal-rise-in-romance-fraud/

Sussex Police. (2018). Operation Signature. Retrieved from https://sussex.police.uk/advice/protect-yourself-and-others/fraud/operation-signature/

SWP. (2019). *Response to Freedom of Information Request 1157/19*. (Freedom of Information Request 1157/19). Bridgend: South Wales Police

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly, 33*(5), 890-911.

Teddlie, C., & Tashakkori, A. (2009). Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioral sciences. California: Thousand Oaks.

Thibaut, J., & Walker, L. (1975). *Procedural justice: A psychological analysis* Hillsdale, NJ: Wiley.

Titus, R. M., & Gover, A. R. (2001). Personal fraud: the victims and the scams. In **G. Farrell** & **K. Pease** (Eds.), *Repeat Victimisation: Crime Prevention Studies* (Vol. 12, pp. 133-151): Criminal Justice Press.

Trickett, A., Osborn, D., Seymour, J., & Pease, K. (1992). What is Different About High Crime Areas? *British Journal of Criminology, 32*(1), 81–89.

Tseloni, A., & Pease, K. (2003). Repeat Personal Victimization. 'Boosts' or 'Flags'? *The British Journal of Criminology, 43*(1), 196-212.

Tseloni, A., & Pease, K. (2004). Repeat Personal Victimization: Random Effects, Event Dependence and Unexplained Heterogeneity. *The British Journal of Criminology, 44*(6), 931-945.

Turanovic, J. J., & Pratt, T. C. (2014). 'Can't stop, won't stop': Self-control, risky lifestyles, and repeat victimiza tion. *Journal of Quantitative Criminology, 30*(1), 29-56.

Turner, B. S. (2006). *Vulnerability and Human Rights* (T. Cushman Ed.). University Park, Pennsylvania: The Pennsylvania State University Press.

UK Finance. (2018). Financial services industry commits to new code of practice to support victims of financial abuse [Press release]. Retrieved from https://www.ukfinance.org.uk/financial-services-industry-commits-new-code-practice-support-victims-financial-abuse

UK Finance. (2020a). Bank branch staff and police team up to stop £19 million of fraud in first half of 2020 [Press release]. Retrieved from https://www.ukfinance.org.uk/press/press-releases/bank-branch-staff-and-police-team-stop-%C2%A319-million-fraud-first-half-2020

UK Finance. (2020b). *Fraud - The Facts 2020*. Retrieved from https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-11-June.pdf

UKSA. (2014). Statistics on Crime in England and Wales. In *Assessment of compliance with the Code of Practice for Official Statistics*. Newport: UK Statistics Authority.

UN. (1985). Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power. In: United Nations.

US DoJ. (2020). Department of Justice Begins First Distribution of Funds Recovered Through Asset Forfeiture to Compensate Victims of Western Union Fraud Scheme [Press release]. Retrieved from https://www.justice.gov/opa/pr/department-justice-begins-first-distribution-funds-recovered-through-asset-forfeiture

US FTC. (2009). MoneyGram to Pay $18 Million to Settle FTC Charges That it Allowed its Money Transfer System To Be Used for Fraud [Press release]. Retrieved from https://www.ftc.gov/news-events/press-releases/2009/10/moneygram-pay-18-million-settle-ftc-charges-it-allowed-its-money

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences, 15*(3), 398-405.

van der Wagen, W., & Pieters, W. (2015). From Cybercrime to Cyborg Crime: Botnets as Hybrid Criminal Actor-Networks. *British Journal of Criminology, 55*(3), 578-595.

van der Wagen, W., & Pieters, W. (2020). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology, 17*(4), 480-497.

van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*(2), 115-127.

Victim Support. (2015a). *Listening and supporting: Annual Report and Accounts 2014/15*. Retrieved from https://www.victimsupport.org.uk/sites/default/files/Trustees%27%20Annual%20Report%202014-2015.pdf

Victim Support. (2015b). Victim Support figures show fraudsters targeting older people [Press release]. Retrieved from https://www.victimsupport.org.uk/about-us/news/victim-support-figures-show-fraudsters-targeting-older-people#sthash.MTmMIsvs.dpuf

Virtanen, S. M. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology and Law, 24*(3), 323-338.

Visa. (2016). Visa upgrades Verified by Visa for a new age of -ecommerce [Press release]. Retrieved from https://www.finextra.com/pressarticle/66181/visa-upgrades-verified-by-visa-for-a-new-age-of--ecommerce

von Hentig, H. (1948). The criminal and his victim: Studies in the sociobiology of crime. New Haven: Yale University Press.

Walby, S., Towers, J., & Francis, B. (2016). Is Violent Crime Increasing or Decreasing? A New Methodology to Measure Repeat Attacks Making Visible the Significance of Gender and Domestic Relations. *British Journal of Criminology, 56*(6), 1203–1234. Retrieved from http://bjc.oxfordjournals.org/content/early/2016/01/31/bjc.azv131.abstractN2

Walklake, S. (2007). *Imagining the Victim of Crime*. Maidenhead, England: Open University Press.

Walklake, S. (2011). Reframing criminal victimization: Finding a place for vulnerability and resilience. *Theoretical Criminology, 15*(2), 179–194.

Walklate, S. (2007a). *Handbook on victims and victimology*. Cullompton, Devon, England: Willan Publishing.

Walklate, S. (2007b). *Imagining the Victim of Crime*. Maidenhead, England: Open University Press.

Walklate, S. (2011). Reframing criminal victimization: Finding a place for vulnerability and resilience. *Theoretical Criminology, 15*(2), 179–194.

Wall, D. S. (1999). Cybercrimes: New Wine, No Bottles? In P. Davies, P. Francis, & V. Jupp (Eds.), *Invisible Crimes: Their Victims and their Regulation* (pp. 105-139). London: Macmillan.

Wall, D. S. (2001). *Crime and the internet*. London: Routledge.

Wall, D. S. (2007). Cybercrime: the transformation of crime in the information age. Cambridge: Polity.

Webb, E. J., Campbell, D. T., Schwartz, R. D., & Sechrest, L. (1966). *Unobtrusive measures: Nonreactive research in the social sciences*. Chicago: Rand Mcnally.

Webster, F. (2006). *Theories of the Information Society* (Vol. 3rd ed). London: Routledge.

Weedon, C. (1987). Feminist practice and postructuralist theory. Oxford: Blackwell.

Wemmers, J. (2010). The Meaning of Justice for Victims. In S. G. Shoham, P. Knepper, & M. Kett (Eds.), *International Handbook of Victimology*. London: Taylor & Francis Group.

(2018, 10 December 2018). *Inside the TalkTalk Hack 1-3* [Retrieved from https://podcasts.apple.com/gb/podcast/cybercrime-investigations/id1428801405

Whitty, M. T. (2015a). Anatomy of the online dating romance scam. *Security Journal, 28*(4), 443-455.

Whitty, M. T. (2015b). Mass-marketing fraud: a growing concern. *IEEE Security and Privacy, 13*(4), 84-87.

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 277-292.

Wickham, H., Averick, M., Bryan, J., Chang, W., McGowan, L., François, R., . . . Yutani, H. (2019). Welcome to the tidyverse. *Journal of Open Source Software, 4*(43), 1686.

Wilcoxon, F. (1945). Individual Comparisons by Ranking Methods. *Biometrics, 1*(6), 80-83. Retrieved from https://sci2s.ugr.es/keel/pdf/algorithm/articulo/wilcoxon1945.pdf

Willenborg, L., & de Waal, T. (2012). *Elements of Statistical Disclosure Control*: Springer New York.

Williams, M. L. (2016). Guardians Upon High : An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *British Journal of Criminology, 56*(1), 21-48.

Willig, C. (1999). Beyond Appearances: A Critical Realist Approach to Social Constructionist Work in Psychology. In D. Nightingale & J. Cromby (Eds.), *Psychology and Social Constructionism: A Critical Analysis of Theory and Practice*. Buckingham: Oxford University Press.

Winkler, W. E. (2015). Probabilistic linkage. In K. Harron, H. Goldstein, & C. Dibben (Eds.), *Methodological Developments in Data Linkage* (pp. 24-55). New York: John Wiley & Sons.

Wisner, B. (1993). Disaster vulnerability: scale, power and daily life. *Geojournal, 30*(32), 127-140.

Woods, A. K. (2015). Data Beyond Borders Mutual Legal Assistance in the Internet Age. Retrieved from Washington DC:

WU Remission. (2020). Map. Retrieved from http://www.westernunionremission.com/map.aspx

Xie, Y., Allaire, J., & Grolemund, G. (2018). *R Markdown: The Definitive Guide*. Boca Raton, Florida: Chapman and Hall/CRC.

Yar, M. (2006). *Cybercrime and Society* (1st ed. ed.). London: SAGE Publications.

Yar, M. (2013). *Cybercrime and Society* (2nd ed. ed.). London: SAGE Publications.

Yates, F. (1934). Contingency tables involving small numbers and the χ 2 test *Journal of the Royal Statistical Society, 1*(2), 217–235.

Yu, S. (2014). Fear of cyber crime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology, 8*(1).

Zehr, H. (1990). *Changing lenses: a new focus for crime and justice*. Scottdale, Pa: Herald Press.

Zehr, H. (2015). *The Little Book of Restorative Justice*. New York: Good Books.