Understanding the Journeys of Online Crime Victims Through Law Enforcement in Britain

Angela Heeler
Royal Holloway, University of London, UK

mcva139@live.rhul.ac.uk

Abstract: Many rely on digital technology and online services to conduct their lives and businesses. However, digital technology has broadened online crime (the term here denotes cybercrime and fraud), enabling transnational offending. Reported fraud and computer misuse offences continuously rise in the UK despite being under-reported, and total recorded crime falling. The situation for those falling victim to online crime is bleak; victims approach different organisations for help and advice and rarely receive the assistance they need. This paper concerns the journeys taken by victims of online crime when approaching Britain's law enforcement. Adopting an exploratory methodology, the research maps organisations, processes and connections between organisations supporting victims. The mapping process and the resulting data displays illustrate the journeys that online crime victims take and how law enforcement supports victims. Snowball sampling was used to recruit 46 participants involved with victims of online crime (23 in British law enforcement). Through semi-structured interviews and analysing official documents and reports, the research uncovered the roles and connections between specialist law enforcement units supporting online crime victims. The research found broken systems in law enforcement–Action Fraud, a lack of access to data across forces/regions and a lack of knowledge. There is under-reporting of online crime, and victims take different journeys through law enforcement depending on whether they are victims of cyber-dependent or cyber-enabled crimes. While Action Fraud's reporting systems are outdated and victims rarely report online crimes, this has in part led to resources being allocated to the most reported (rather than most prevalent) crimes. Victims take different journeys through law enforcement, even as victims of the same events. Victims of fraud (and other cyber-enabled crimes) rarely receive assistance, whereas victims of cyber-dependent crimes are always contacted. Team Cyber is a law enforcement structure dedicated to tackling cyber-dependent crime, which is not replicated for fraud.

Keywords: Online crime, Victims, Cybercrime, Fraud, UK Policing, Crime reporting

1. Introduction

Many people and organisations rely on digital technology and online services to conduct their lives and businesses (Ball, 1984). However, the internet's ubiquity enabled traditional crime to migrate online alongside a parallel rise in online crime and transnational offending (Anderson, et al., 2013). UK recorded fraud and computer misuse offences continue to rise despite being under-reported and total *recorded* crime falling (ONS, 2024). The true scale of online crime is unknown, with the National Crime Agency (*NCA*) suggesting only 2–10% of cybercrime is reported (UK Parliament, 2023). The term *online crime* in this paper denotes cybercrime and fraud committed online. A *victim* refers to a person or business that suffered a cybercrime, fraud or an incident with an online element. Cybercrime is not a "victimless crime" (Goucher, 2010).

The overall research question aims to understand the support landscape for victims of online crime. This paper explores the journeys online crime victims take through law enforcement in Britain. Unintentionally, law enforcement participants in my study were from police forces in Great Britain (England, Scotland and Wales), hence Britain's law enforcement. Participants described victims being failed, taking different journeys and reporting to Action Fraud without receiving any feedback.

No participants were pre-chosen to interview, instead, participants were sought online. Participants included law enforcement (serving and ex-officers, seconded officers and staff), service providers, support organisations and victims. My study engaged with 46 participants in 43 semi-structured interviews to discover their roles in advising individuals and businesses about cybersecurity and/or supporting victims of online crime. This paper mostly concerns the 23 law enforcement participants who discussed victims and law enforcement's internal processes and systems, and the issues surrounding Action Fraud. Data displays (including social networks) were built to assist in explaining this exploratory research.

Online crime scholarship often consists of systematic reviews since gaining access to the `hard-to-reach' law enforcement population is difficult, e.g. (Akdemir, et al., 2020). Hutton (2017) found a "fundamental lack of law enforcement data". These findings explore this gap. Moreover, the paper contributes by demonstrating the vastly different journeys travelled by cybercrime and online fraud victims.

2. Background and Related Work

Related work unpacks this paper's title into three parts: online crime, victims and law enforcement.

2.1 Online Crime

First, online crime (fraud and cybercrime) is defined. To be guilty of *fraud* under UK law, one person intends to make an unlawful gain or another an unlawful loss (GOV.UK, 2006). Fraud can be offline or online, but only fraud with an online/digital element is explored here. Scholars find the term *cybercrime* difficult to define, e.g. Yar (2006), since cybercrime refers to "diverse […] illegal and illicit activities". However, defining cybercrime establishes boundaries for what constitutes illegal activities in cyberspace, aiding law enforcement, policymakers and the judicial system's response to cybercrime.

Law enforcement participants divided online crime into cyber-dependent and cyber-enabled, describing digital devices as increasing cyber-enabled crime scale but mandatory in cyber-dependent crimes. However, crimes can have elements of both, e.g. mandate fraud (cyber-enabled) committed after credentials gathered during hacking (cyber-dependent). Distinguishing cyber-dependent and cyber-enabled is popular with academics and law enforcement, but irrelevant for victims and criminals.

2.2 Victims

Ball (1984) saw cybercrime victims as companies lacking controls. Now, victims are individuals and companies suffering from many types of cybercrime.

2.2.1 Cybercrime reporting

Victims report to different organisations depending on the crime, e.g. cybercrime/fraud to Action Fraud, deepfake child indecent images to the IWF (2024). Victims often report hoping for financial loss reimbursement (Skidmore, et al., 2018). Scholarship states online crimes are under-reported, e.g. cybercrime (Saunders, 2017) and Wood et al. (2022) believe only "a small fraction" of fraud is reported.

The plethora of reasons why cybercrime is under-reported include victims:

- Not knowing how/where to report, e.g. (Yar, 2006).
- Unaware that a crime had occurred, and they were a victim (Goodman, 1997).
- Feeling the incident is part of modern-day life, and they can remedy/resolve the situation themselves (Wall, 2007).
- Believing law enforcement is incapable of solving online crimes, criminals will not be prosecuted, and fraud is not a law enforcement priority (Wall, 2007).
- Not wanting to be labelled as a `victim' or the loss too small to report, e.g. (Goucher, 2010).

Businesses rarely report cybercrime to prevent damaging the company's reputation or negatively impact business (Goucher, 2010), cause further business disruption (Saunders, 2017), and unwillingness to break the employer's trust by exposing employees suspected of committing crimes (Hrncir & Metts, 2011). In summary, online (and other) crime is difficult to quantify and is under-reported for multiple reasons.

2.3 Law Enforcement

There are 45 territorial police forces across England, Wales, Scotland and Northern Ireland (known as *local forces*). Nine Regional Organised Crime Units ROCUs cover England and Wales, tackling serious organised crime (HMICFRS, 2021). Nationally, law enforcement enters into public-private partnerships to address and prevent crime (e.g. National Cyber Security Centre (*NCSC*)), other law enforcement bodies (e.g. NCA) (Levi, et al., 2016).

2.3.1 Action Fraud

The Home Office, as the lead government department for policing, funds Action Fraud (Action Fraud, 2014). Action Fraud is run by the City of London Police (*COLP*), and is the UK's 24/7 reporting centre for fraud and cybercrime, however, Scotland does not use Action Fraud. Individuals report to Action Fraud from England, Wales and Northern Ireland (Action Fraud, 2014), yet Action Fraud does not investigate fraud. Action Fraud's systems and processes are often criticised, e.g. the media (Martin, 2024) and law enforcement's inspectorate (HMICFRS, 2019). Action Fraud reporting has been described as "could be much improved" (Correia, 2019), call handlers having a "limited level of cyber knowledge" (Nouh, et al., 2019) and the resulting data "imperfect" (Levi, et al., 2016).

A Home Office Counting Rules (*HOCR*) code added to a victim's report classifies the crime type (Home Office, 2021). Codes can be inaccurate as Action Fraud reporting was designed for fraud, not cybercrime (Nouh, et al., 2019).

3. Methodology

This qualitative research constructs its narrative from the "lived experiences" of participants (Creswell, 2007), captured during semi-structured interviews.

3.1 Study Design

The study had three parts: building the network, interviewing participants, and collecting and analysing the data. Snowball sampling recruited adults in Great Britain whose work concerned victims of online crime or who were victims of online crime.

The research focused on contacts meeting the selection criteria who formed a connected network of interview participants (Tracy, 2013). The selection criteria were people who have experienced business crime, (current or ex-)law enforcement officers dealing with online crime, and people working as service providers or in organisations supporting/advising people who have experienced online crime. Issues with recruiting participants included knowing who was in the `hidden' population of those supporting victims and gaining access to the `hard-to-reach' law enforcement population, since the researcher had no law enforcement affiliation. Browne (2005) suggests that difficult-to-access populations may be "wary" of interacting with those not working in this population. Tracy (2013) recommends snowball sampling (existing participants recommending contacts suitable for the study) for reaching `hard-to-reach' and/or `hidden' populations. Contacts made use of weak and strong ties in their social network to recommend business acquaintances (weak) and colleagues (strong) to participate (Granovetter, 1983). A disadvantage of snowball sampling is that participants could be part of the same echo chamber (Tracy, 2013). However, my study's participants worked in three different sectors: business, support organisations and law enforcement.

This exploratory study takes a grounded theoretical approach to understanding and interpreting the data, using the participants' data to explore and narrate the victim support landscape and map the processes and connections between organisations.

3.2 Data Collection

The plan to make contacts in person was thwarted by the COVID-19 pandemic, which necessitated seeking contacts online. Online participant recruitment was sluggish until a College of Police employee emailed and recommended three law enforcement personnel, opening law enforcement's door. Hutton (2017) declares that independent access to policing is unusual since access is normally only granted to serving officers.

Participant recruitment achieved 98 contacts, resulting in 43 interviews. Almost all interviews were conducted online (due to the pandemic) in the participant's work setting. Participants answered open-ended questions about handling online crime. No knowledge of these processes was known, and so questions evolved from high-level questions at the outset to deeper questions in later interviews. Pseudonymising participant information protected participant anonymity. Contacts were allocated a unique identifier, e.g. L-U12, consisting of letters representing the participant's category (e.g. L- Law enforcement) and the chronological interview number. Interviews were recorded and transcribed.

Table 1: Participants

Participant identifier: L- Law enforcement	National, Regional, Force	Rank
L-S13	National	Senior
L-U12, L-W30	National	Middle
L-O27, L-U28	National	Low
L-S25	Regional	Senior
L-W31	Regional	Middle
L-H26	Regional	Low
L-O22, L-F32	Force	Staff
L-R15, L-R35	Force	Senior
L-X36	Force	Middle
L-X43	Force	Low

Participant identifier: P- Service provider S- Support organisation
S-B16
P-W18

Table 1 shows the participants quoted in this paper.

3.3 Data Analysis

The interviews were thematically analysed manually according to Braun & Clarke's (2006) methodology and coded using Saldaña's (2009) methodology. Coding was simultaneous, resulting in 303 codes and 18 themes.

During interviews, participants described the structure of their organisation, the role they played, and their part in the support landscape. The landscape described was complex, and so data displays were created from the thematic data and grey documents (e.g. UK government reports). Data displays included building maps and three social networks (of the recruitment process, the organisations and internal law enforcement) (see Heeler, 2024). The data displays incorporated the data and visualised the structures and patterns within the landscapes and networks (Miles & Huberman, 1994).

4. Research Findings

Three findings of concern (victim's journey, under-reporting and broken systems) are now discussed.

The victim's journey in **Figure 1** was determined from the interviews, and participants knew individuals and businesses were being failed, e.g. L-W31 said:

> *"I think we sadly erm fail them [victims] quite a lot [...] Policing is a long way behind the curve."*

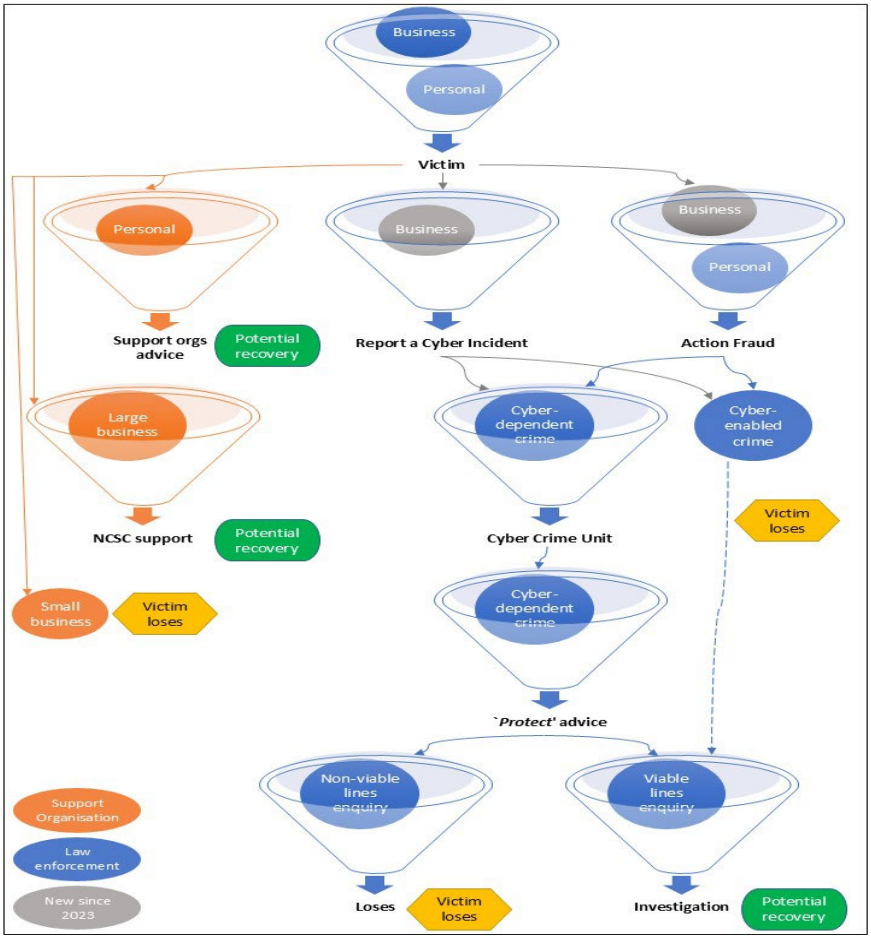

Figure 1: Victim's journey

Figure 1 depicts the victim's journey as a series of funnels through which victims pass and are either caught by another funnel or drop out, and the victim's journey terminates at the "Victim loses" hexagons. The victim's journey can be compared to playing a pinball machine with the same or different results happening with each ball (cyber event). The victim's journey begins with individuals or businesses discovering they are victims, reporting the incident and being caught by specific funnels depending on how the crime is labelled, supported or investigated. Victims may start with similar events, but the journey and outcome may vary or be the same depending on how the crime is handled. **Figure 1**'s funnels are now described.

L-W30 and L-W31 explained that the victim's journey only starts when people understand they have become victims of online crime. From **Figure 1**, the victim's journey splits into seeking support and reporting the incident. Personal victims (individuals) can seek support from victim support organisations (e.g. Age UK) or banks. Large businesses may be supported by the NCSC/NCA. The small business journey terminates when the small businesses is not supported by support organisations or the NCSC/NCA. Support organisations are outside the scope of this paper. Since 2023, organisations have used a new reporting portal called `Report a Cyber Incident' that allows law enforcement and NCSC to triage and task NCSC, National Fraud Investigation Bureau (*NFIB*), NCA or local/regional forces (NCSC, 2020). Previously, organisations decided where to report and relied on the receiving organisation to disseminate the report correctly. L-F32 said organisations wanted no publicity after online crime, such as data breaches. Personal victims report cybercrime and fraud to Action Fraud either online or by telephone.

Figure 1 then shows how the victim's journey splits along two pathways depending on the reported crime being classified as cyber-dependent or cyber-enabled. The cyber-enabled victim's journey mostly terminates here, as cyber-enabled crimes are rarely reviewed or investigated, whereas cyber-dependent crime reports are reviewed and victims receive advice. Crimes with viable lines of enquiry are investigated and occasionally prosecuted. Although L-X43 revealed,

"We only investigate a very, very, very small percentage

of those that are actually being reported to Action Fraud."

Crimes without viable lines of enquiry are not investigated, and the journey terminates. The pathways are explored further.

4.1 Cyber-Dependent Versus Cyber-Enabled Pathways

Crimes reported to Action Fraud are sent to NFIB for processing (not investigating).

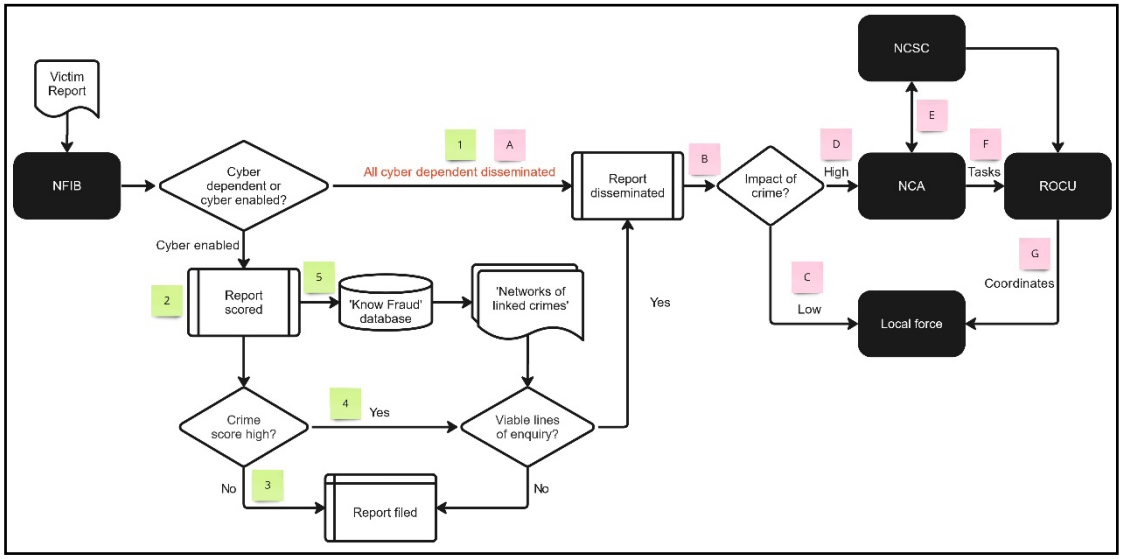

Figure 2: NFIB's treatment of cyber-dependent and cyber-enabled reports

Figure 2 was determined from NFIB employee L-O27's description and Action Fraud (2013) User Guide. The steps for processing Action Fraud (2013) reports are described using the numbered Post-it note captions in **Figure 2**:

1. Any cybercrime reported to Action Fraud will automatically be disseminated for investigation.
2. NFIB's systems automatically score each fraud report. L-O22 criticised the crude scoring mechanism.
3. Fraud reports are filed without review or investigation where the automated score is below a pre-determined threshold. Although L-H26 said,

"I don't know what the thresholds [are for] fraud [sigh]."

4. (Human) assessors triage fraud reports scoring above the threshold. Reports with viable lines of enquiry will either be disseminated to COLP's economic crime team or the force closest to the suspect or the victim. COLP is the National Lead Force for fraud (UK Parliament, 2023).

5. All fraud reports feed into NFIB's `Know Fraud' system, together with industry and public sector fraud data. Nightly `Know Fraud' creates "networks of linked crimes" which are reviewed to identify suspects and disseminated (Action Fraud, 2013).

My study's participants disputed that these processes were followed. First, official force procedures vary, e.g. Surrey Police (2017) contact centre could report to Action Fraud on the victim's behalf, despite Action Fraud (2013) User Guide stating only victims can report. Second, L-X43 said victim reports could be classified incorrectly as,

> *"understanding what a cyber-dependent or cyber-enabled crime is, is still for some people really complicated."*

And the threshold for disseminating cyber-enabled reports was not a fixed value. L-O27 explained that teams determined dissemination criteria based on evidence of viable lines of enquiry (e.g. identifying potential suspects) and the loss value.

Figure 2's lettered Post-it note captions describe how cybercrime reports are disseminated and coordinated by the agencies in Team Cyber according to the report's priority. L-S13 described Team Cyber UK as a connected network classifying and handling cybercrime (not fraud) incidents at different levels (nationally, regionally and locally) according to the incident's severity. L-O27 explained, "almost all" cases are low-impact and sent to local forces.

4.2 Under-Reporting

Another area of concern in the victim's journey is that, as L-U12 said, "a very very small fraction" of business crimes were reported. S-B16 believed low-value scams (e.g. £40 skirt ordered online but never received) were commonplace during the pandemic and) not routinely reported. L-X43 felt that other crimes, e.g. sexual and domestic offences and modern slavery, were also very under-reported.

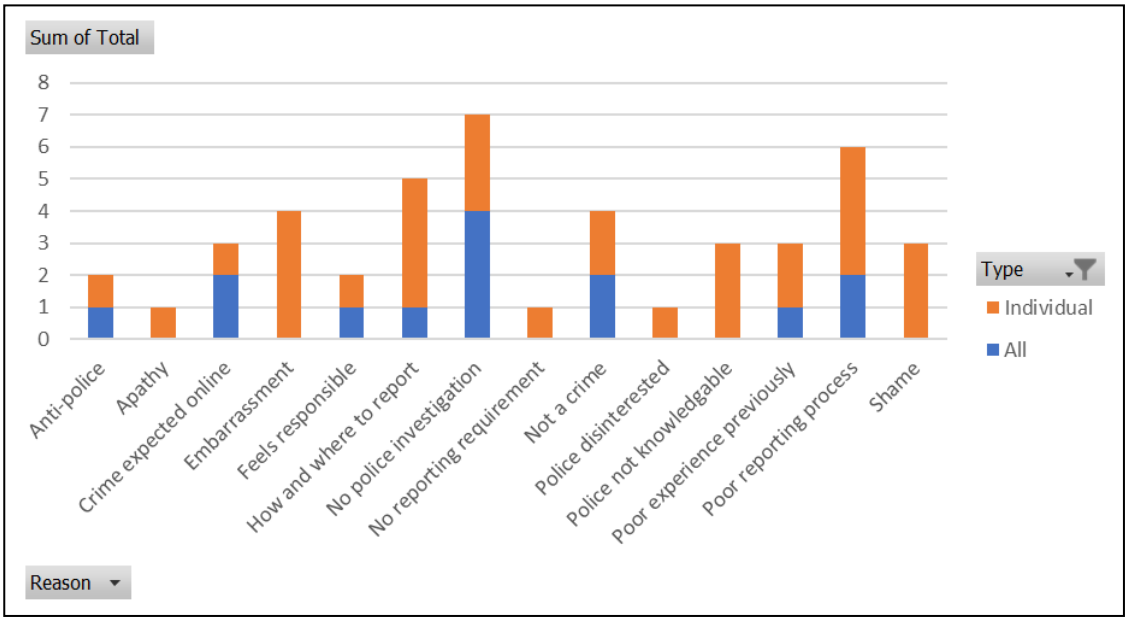

Figure 3: Reasons why few individuals report online crime

When asked why so few individuals and businesses reported cybercrime and fraud, 27 participants gave 108 reasons that are summarised into 14 categories for individuals shown in **Figure 3**. Under-reporting reasons were based on the participant's interactions with victims and the public. The most popular reasons were law enforcement not investigating, the poor reporting experience and not knowing where/how to report. L-S25 said under-reporting led to law enforcement being unaware of which crimes are happening, not assisting victims adequately, and targeting the wrong issues. L-X36 and L-O27 explained that under-reporting means the scale of the problem is unknown, and intelligence information to prevent future attacks is lost. For the victim, under-reporting can affect investigations as funding streams are based on reported crime numbers.

4.3 Broken Systems

Two examples of broken systems are Action Fraud and crime recording systems. Action Fraud was a popular topic discussed by 37 participants, with many making derogatory comments, including law enforcement. The main issue was that the public expects Action Fraud to investigate fraud, rather than being purely a reporting portal. The following quotes summarise participants' views:

> *"I think the problem with Action Fraud is the name, Action Fraud, they don't action fraud, they report-they record fraud." (L-O22)*

> *"Action Fraud is the national cybercrime reporting process because that makes sense, doesn't it?" (L-S25)*

Contrary to Action Fraud's tagline as "the *UK's* national reporting centre for *fraud and cybercrime"* (Action Fraud, 2014), L-U28 explained Scottish victims report by calling `101' instead of Action Fraud, describing this as "politics and stuff". Also, P-W18 mentioned cybercrime, e.g. cyberstalking is reported by calling `101' or the victim's local police force (POLICE.UK, 2021). P-W18 thought reporting confusion enhanced a person's "whether it's worth reporting" indecision.

Participants described victims experiencing difficulties completing reports online and explaining their incidents to Action Fraud's call handlers. L-R35 explained local forces needed one consistent system for all forces, saying:

> *"Are the 43 police forces that we have at the moment, are they fit for purpose? {[...]} Personally, I'm a bit of a radicalist [sic], I think we just need to sweep away the old [systems] and bring in the new."*

L-R15 mentioned a disconnect between forces using different systems: Athena (case management), COMPACT (missing persons), Merlin (vulnerable adults) and NICHE (records management). L-R35 said that because of the different ways forces record and count crimes and the different systems, "fraud is an absolute nightmare" to analyse regionally across forces.

5. Discussion

There is no single victim's journey; individuals/business victims may take different journeys for the same crimes, and journeys differ for cybercrime versus fraud. Journeys blur for business victims as their employees, as individuals, can also be victims.

5.1 Victim's Journey

The victim's journey begins with reporting cybercrime and fraud to Action Fraud. Participants and scholars criticised Action Fraud similarly; maybe as Button (2021) suggests, law enforcement uses Action Fraud to redirect their investigation inadequacies. First, the name `Action Fraud' implies action will be taken upon reporting, but this is a reporting portal only. Button et al. (2020) suggested renaming to `National Fraud and Cybercrime Reporting Centre'. Second, victims are confused about reporting fraud and cybercrime to Action Fraud, yet cyberstalking–also a cybercrime–is reported locally (POLICE.UK, 2021). Third, individuals report to Action Fraud while businesses report to NCSC (NCSC, 2020). Also, HOCR codes are missing for recent crime types, e.g. ransomware (McGuire & Dowling, 2013). The new reporting system for individuals may add new codes, but the launch has been delayed again until 2025 (Martin, 2024). Vastly less crime is reported to Action Fraud than England and Wales Crime Survey estimates; only 7% of frauds and 4% of computer misuse crimes were reported to Action Fraud in 2023–2024 (ONS, 2024). Consistently, scholars say businesses do not report crimes considered insignificant or `business as usual' (*BAU*) (e.g. McGuire & Dowling, 2013). This tallies with my study's top under-reporting reasons as returning to BAU, reputational damage and lack of law enforcement knowledge/investigation. Frauds may be numerous and impact business operations, but businesses continue despite this.

Law enforcement is funded based on reported crimes, so under-reporting can lead to underfunding and under-resourcing of investigations, resulting in reduced crime knowledge (Goodman, 1997). Correia (2019) suggested that poor-quality crime reports and under-reporting led to inaccurate crime analysis. Law enforcement uses crime analysis and knowledge to create protective/preventative advice (Bidgoli & Grossklags, 2016). Therefore, under-reporting could reduce law enforcement's ability to prevent individuals/businesses from becoming victims. Under-reporting could be improved by publicising and explaining any new reporting system, providing feedback and advice to those reporting, and publicising successful investigations to improve public perception.

5.2 The Journey Divides

The victim's journey is divided according to whether a cyber-dependent or cyber-enabled crime has been reported. Potentially, cybercrime is reported, but not categorised as cybercrime, since cybercrime has no agreed-upon definition. Cyber-dependent crime victims will be contacted and their cases investigated at some level. Cyber-enabled crime reports are scored and added to a fraud database. Unless the reports are high-scoring or the local force chooses to review all fraud reports, reports are filed, and the victims receive no further contact. Hence, labelling a victim's report as cyber-dependent/cyber-enabled is crucial to the victim's journey. Law enforcement's structure for cyber-dependent crimes helps victims along their journey and hinders cyber-enabled crime victims. The boundary between cyber-dependent and cyber-enabled crimes is blurred, and crimes can have elements of both (Gordon & Ford, 2006). If a chain of events started with an account compromise leading to identity theft, fraud, stalking, harassment or any/all of these events, the victim's journey becomes complicated. Also, the cyber-dependent victim's journey would change if Team Cyber's funding is not renewed after the fixed funding period ends. Levi et al. (2016) suggest law enforcement partnerships investigate cyber-enabled crimes to reduce the investigatory load and counteract declining fraud resourcing in law enforcement. Wood et al. (2022) suggested merging law enforcement's fraud and cyber capabilities, making the dependent-enabled split irrelevant. Another suggestion could be simplifying some cybercrime to traditional crimes and tackling them using existing processes, e.g. ransomware could be handled by specialists in blackmail.

5.3 The Systems

Different systems in law enforcement are seen as broken, and participants discussed this openly, e.g. Action Fraud and the difficulties local and regional forces have in sharing data. HMICFRS regularly inspects law enforcement, finding the same broken systems at each inspection, e.g. HMICFRS (2021) ROCUs inspection found the same funding model issue as their 2015 inspection. HMICFRS (2019) assessed law enforcement's response to fraud and found no national fraud strategy, information lacking about fraud reporting, unclear roles and responsibilities, poor service for victims (unless vulnerable), and 96% of frauds disseminated from NFIB not investigated. My study showed there was a strategy and law enforcement understood their role, but that the volume of fraud was greater than their investigatory capacity.

6. Conclusion

The views of the `hard-to-reach' population of Britain's law enforcement on the journeys of victims of online crime were unpacked. When individuals and organisations discover an online crime, they need to know whom to approach for cybersecurity help and advice. Generally, individuals tend to seek reimbursement for their loss, and businesses want to return to BAU. The empirical contributions of this paper add to existing cybercrime and fraud scholarship.

This paper showed that victims rarely report online crimes and need encouragement to report because policymakers allocate funds to the highest-impact crimes that are reported, without knowing if these are the most prevalent crimes. Increased reporting could fund more cybercrime investigations and prevent further crime. A victim's journey is analogous to decision funnels through which victims pass to the available support channels. The journey's events can be complicated. There is no single journey for victims; victims of similar crimes will not travel the same journey, and victims of cybercrime and fraud travel vastly different journeys. Cyber-dependent crime reports will be reviewed, and victims advised, whereas cyber-enabled crime victims may report and never receive any feedback. Hence, the crime type label affects the outcome and the recovery.

Victims rarely receive the help and support they need. Participants described the effort being made by law enforcement and support organisations to improve the situation for victims.

The novel aspects of this paper are threefold. First, empirical data from this `hard-to-reach' law enforcement population is rarely collected, so documenting from the perspective of Britain's law enforcement enhances the cybercrime and fraud communities' knowledge. Second, the different journeys cyber-dependent and cyber-enabled crime victims take through law enforcement are not visible from outside law enforcement. Scholars and the media have mapped part of the journey (e.g. through Action Fraud), but this paper's contribution was to understand, map and document the entire cyber-dependent/cyber-enabled crime victims' journeys through law enforcement. Third, complementing existing scholarship, Action Fraud is still a broken system of which academics and participants were fully aware. The replacement reporting system has been repeatedly delayed, with a new planned launch in 2025. This paper showed a bleak outlook for victims, which can be improved.

Future work could include examining the journeys victims take through banks and banking processes, as fraud appears a major issue for banks.

Acknowledgements

Many thanks to the participants who gave their time and energy discussing their working lives during the global COVID-19 pandemic. This was a time when the borders of your world seemed to be the front door and the energy to engage in new activities, such as being interviewed, felt depleted. This research thrived because of the depth of the participants' input. Thanks also to the anonymous reviewers for their insights and recommendations.

Ethics declaration : Full ethical approval was granted on 27/04/2020 with the Research Ethics Committee Project ID 2081. No **AI** tools were used to create this paper.

References

Action Fraud, (2013) Action Fraud & NFIB: User Guide, s.l.: s.n.

Action Fraud, (2014) Action Fraud, National Fraud & Cyber Crime Reporting Centre. s.l.:s.n.

Akdemir, N., Sungur, B. & Başaranel, B., (2020) Examining the challenges of policing economic cybercrime in the UK. Güvenlik Bilimleri Dergisi, Volume Özel Sayı, p. 113–134.

Anderson, R. et al., (2013) Measuring the Cost of Cybercrime. In: The Economics of Information Security and Privacy. Berlin: Springer, p. 265–300.

Anon., n.d. Fraud Act 2006, s. 1, s.l.: s.n.

Ball, L. D., (1984) Testimony before the Subcommittee on Small Business Crime Prevention Act. SIGSAC, Volume 3, p. 11–13.

Bidgoli, M. & Grossklags, J., (2016) End User Cybercrime Reporting: What We Know and What We Can Do to Improve It. Vancouver, IEEE, p. 1–6.

Braun, V. & Clarke, V., (2006) Using thematic analysis in psychology. Qualitative Research in Psychology, Volume 3, p. 77–101.

Browne, K., (2005) Snowball sampling: using social networks to research non-heterosexual women. International Journal of Social Research Methodology, Volume 8, p. 47–60.

Button, M., (2021) Hiding behind the Veil of Action Fraud. Policing: A Journal of Policy and Practice, Volume 15, p. 1758–1772.

Button, M. et al., (2020) Victims of computer misuse: Executive summary.

Correia, S. G., (2019) Responding to victimisation in a digital world: a case study of fraud and computer misuse reported in Wales. Crime Science, Volume 8, p. 4.

Creswell, J. W., (2007) Qualitative Inquiry and Research Design: Choosing Among Five Approaches. Second ed. California: SAGE Publications.

Goodman, M. D., (1997) Why the police don't care about computer crime. Harvard Journal of Law and Technology, Volume 10, p. 465–494.

Gordon, S. & Ford, R., (2006) On the definition and classification of cybercrime. Journal in Computer Virology, Volume 2, p. 13–20.

Goucher, W., (2010) Being a cybercrime victim. Computer Fraud & Security, Volume 2010, p. 16–18.

Granovetter, M., (1983) The Strength of Weak Ties: A Network Theory Revisited. Sociological Theory, Volume 1, p. 201–233.

Heeler, A. E., (2024) Applying Social Networks to Snowball Sampling of a 'Hard-to-Reach' Population and to Illustrate Qualitative Findings. SNAMS, IEEE, p. 219–226.

HMICFRS, (2019) Fraud: Time to Choose, s.l.: s.n.

HMICFRS, (2021) Regional Organised Crime Units: An inspection of the effectiveness of the Regional Organised Crime Units, s.l.: s.n.

Home Office, (2021) Counting Rules for Fraud, s.l.: s.n.

Hrncir, T. & Metts, S., (2011) Why small businesses fall victim to fraud: size and trust issues. Boca Raton, USA, p. 48–57.

Hutton, S. K., (2017) Organized Crime: An ethnographic study of the monitoring and disrupting of those designated as high-level `organized criminals' within the Metropolitan Police. Open University.

IWF, (2024) Report Online Child Sexual Abuse Images. s.l.:s.n.

Levi, M. et al., (2016) The Implications of Economic Cybercrime for Policing.

Martin, A., (2024) Replacement for Action Fraud, UK's cybercrime reporting service. s.l.:s.n.

McGuire, M. & Dowling, S., (2013) Cyber crime: A review of the evidence. Home Office, Volume 75, p. 1–35.

Miles, M. B. & Huberman, A. M., (1994) Qualitative Data Analysis: An Expanded Sourcebook. Second ed. California: Sage Publications.

NCSC, (2020) Report A Cyber Incident, s.l.: s.n.

Nouh, M., Nurse, J. R. C., Webb, H. & Goldsmith, M., (2019) Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement. San Diego, USA.

ONS, (2024) Crime in England and Wales: year ending March 2024, s.l.: s.n.

POLICE.UK, (2021) Welcome to Police.uk. s.l.:s.n.
Saldaña, J., (2009) The Coding Manual for Qualitative Researchers. London: SAGE.
Saunders, J., (2017) Tackling cybercrime - the UK response. Journal of Cyber Policy, Volume 2, p. 4–15.
Skidmore, M. et al., (2018) The Police Foundation: More than just a number. Computer Fraud & Security, Volume 2018, p. 4–4.
Surrey Police, (2017) Recording and Investigating Allegations of Fraud Procedure, s.l.: s.n.
Tracy, S. J., (2013) Qualitative research methods: Collecting evidence, crafting analysis, communicating impact. U.K.: Wiley-Blackwell.
UK Parliament, (2023) Written evidence submitted by His Majesty's Government, s.l.: s.n.
Wall, D. S., (2007) Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace. Police Practice and Research, Volume 8, p. 183–205.
Wood, H., Keatinge, T., Ditcham, K. & Janjeva, A., (2022) The Silent Threat: The Impact of Fraud on UK National Security. London: RUSI.
Yar, M., (2006) Cybercrime and Society. London: SAGE.