Behind the screen: Perceptions and experiences of online fraud victimisation

> "I think we consider [online fraud] background noise and something that happens to vulnerable people, [and] you don't consider yourself vulnerable."
> — In-person, focus group 8

Freya Smith, Manon Roberts, Sophie Davis, Amber Evans (Crest Advisory)
Alex Murray (Institute for Crime and Justice Policy Research [ICPR])

May 2024

Crest Advisory

Crest Advisory are experts in justice, policing, and public safety. Through our three practices – Crest Insights, Crest Consulting, and Crest Inquiries, we identify and help solve complex problems arising from crime, vulnerability and other social harms. We're subject matter experts, and many of us have previously worked at the organisations and in the sectors we now service. We bring expertise, real-world experience and a powerful sense of purpose to our mission – to make communities safer.

Crest Insights

Crest Insights is the think tank for the whole of the criminal justice system. Our mission is to do the hard thinking which drives policy reform and makes communities safer.

About the Institute for Crime and Justice Policy Research (ICPR), Birkbeck, University of London

The overarching aims of ICPR's work are to produce and disseminate knowledge about justice, and thereby to inform public and political debate, and to contribute to improvements in policy and practice. All ICPR's research is informed by concerns with justice, fairness and human rights. The audiences for ICPR's research include policy-makers, academics, civil society organisations, justice practitioners, and the wider public.

Crest Advisory (UK) Ltd is a company registered in England and Wales (08181317)
2 Bath Place, Rivington Street, London, EC2A 3DR
www.crestadvisory.com

Contents

Acknowledgements

We would like to thank the Dawes Trust, the generous funders of this research project, for their support.

We would also like to thank Dr Bina Bhardwa and Professor Jessica Jacobson of the Institute for Crime and Justice Policy Research (ICPR), Dr Michael Skidmore of the Police Foundation, and Jon Clements, Beth Mooney and Madeline Rolfe of Crest Advisory for reviewing and providing feedback on the report.

Finally, we would like to express particular gratitude to the participants who shared their views and experiences on online fraud.

Glossary

Action Fraud: The national reporting centre for fraud and cyber-crime in England, Wales and Northern Ireland.

Advance fee fraud: When an offender targets an individual to make an advanced or upfront payment for goods, services or financial gains that do not materialise.

Bank card and cheque fraud: When an offender steals an individual's cards/chequebook to take money from their account.

Consumer and retail fraud: When individuals, businesses, or organisations intentionally mislead consumers through false information and misrepresentation to obtain money, goods, services, or personal information from consumers.

Fraud: To act dishonestly with the intent to make a gain for oneself or cause a loss to another. The Fraud Act 2006 encompasses three primary categories of fraud offences: false representation, failing to disclose information, abuse of position.

Identity fraud: When the offender deliberately obtains and uses an individual's personal information, usually for financial gain. Also known as identity theft.

Online fraud: Online fraud refers to any fraudulent activity or deception that occurs through digital means to obtain financial and personal information.

Romance fraud: A type of fraud in which the offender dupes the victim into believing they are in a relationship with the offender to gain their trust and financially exploit them. Also known as a romance scam or dating scam.

Small and medium enterprises (SMEs): Encompass micro-enterprises (employing less than 10 individuals and having an annual revenue under £2 million), small businesses (employing fewer than 50 people and having an annual revenue below £10 million), and medium-sized enterprises (employing fewer than 250 people and having an annual revenue under £50 million).

The Crime Survey for England and Wales: A nationally representative sample conducted in England and Wales to understand and measure the extent of crime experienced by individuals or households on a yearly basis, including crimes that have not been reported.

Victim: Within this report, ‘victim’ is defined as an individual who has responded through the use of the internet to a fraudulent attempt which has led to financial loss (as well as potential other impacts).

Executive summary

Fraud is now the most commonly experienced crime in the UK, making up over 40 per cent of all recorded crime.[1] Instances of fraud have risen substantially over the last decade, from 510,403 offences recorded in the year ending 2013 to 1.16 million offences recorded in the year ending 2023,[2] with online fraud contributing significantly to the increase (the Crime Survey for England and Wales estimates that over 60 per cent of cyber incidents take place online). Yet our understanding of online fraud in particular — its typology, scale and impact — is limited.

Crest Advisory, in partnership with the Police Foundation and Birkbeck, University of London (Institute for Crime and Justice Policy Research), and with funding from the Dawes Trust, is carrying out a large research project into tackling online fraud.

The first part of our project focuses on developing a better understanding of the impact of online fraud on victims and the wider public. In September 2023, Crest published findings from large-scale online surveys of the public and small and medium enterprises (SMEs)[3] which explored public perceptions and experiences of online fraud. This report presents the findings from interviews with 20 victims and 12 focus groups (with 96 members of the public) to build on the survey findings and deepen our insight and knowledge of online fraud victimisation and its impact. It addresses a key gap as most existing studies do not distinguish between online and offline fraud victimisation, in part because many fraudulent activities combine offline and online elements. Key findings from the interviews and focus groups are set out below.

1.

Experiences of online fraud were ubiquitous and seen as ‘part of everyday life’.

Building on the findings of our surveys — which found that victimisation among both the general public and businesses was higher than commonly reported — focus group conversations centred around the pervasiveness of online fraud, with participants describing online fraud as ‘part of everyday life’. Being on the receiving end of online fraudulent attempts was seen as normal and expected. The interview and focus group findings also corroborate findings from our survey on the significant underreporting of online fraud, particularly to the police or Action Fraud. Underreporting rates were associated with study participants’ lack of confidence in the police’s capacity to

[1] Crime in England and Wales: Appendix tables - year ending September 2023. Office for National Statistics

[2] Office for National Statistics Dataset Crime in England and Wales: Appendix tables. *Year ending December 2023 edition of this data set*, Appendix table A4a

[3] Evans, A., Reynoso-Serna, F., Smith, F., Brown, E., & Davis, S. (2023). Online fraud: what does the public think?. Crest Advisory.

effectively investigate online fraud — also echoing our survey results — and their lack of awareness of Action Fraud. As long as victims do not feel empowered or motivated to report online fraud when it does happen, the information and statistics available to enforcement and research agencies will continue to not adequately represent the scale of the issue, further impeding agencies and financial organisations' ability to address online fraud.

2.

Word-of-mouth, and first-hand experiences, were relied on as the main source of knowledge about online fraud. No study participants mentioned official sources such as government campaigns as a source of information.

Study participants stated that prior to their victimisation, their knowledge of online fraud had been mainly acquired via word-of-mouth — in most cases, information shared by friends and family. Post-victimisation, some victims often felt compelled to share their experiences and the knowledge they had acquired as a result of their victimisation with family and friends. No study participants mentioned awareness of governmental educational campaigns. Peer-to-peer knowledge sharing and awareness raising, with an emphasis on lived experience, was therefore a key, if not the main, source and channel of information on online fraud among study participants.

3.

There was a disconnect between the preconceptions study participants held about online fraud pre-victimisation, and the reality of their experience as victims.

Study participants held a number of assumptions prior to experiencing a fraud attempt, which many said did not align with their subsequent experiences and ultimately made them more vulnerable. Participants assumed that online fraud attempts would be easy to identify. Those who became victims subsequently described the sophistication of online fraud attempts and noted that their preconceptions of what fraud might look like had made it more difficult for them to identify and prevent attempts. This was further exacerbated by preconceived notions that online fraud happened to 'other people', namely the elderly, 'naive' or less technologically advanced. This aligned with our survey results, as did the finding that younger people were more likely to perceive themselves as 'tech-savvy', and therefore less vulnerable. Finally, participants noted that factors which they might not have considered (including temporal characteristics that may affect an individual's cognitive judgements, such as being tired or stressed) had increased their vulnerability.

4.

The emotional impact of being a victim of online fraud was significant and worse than the financial impact, with self-blame featuring consistently across study participants.

Whether victims had suffered minor financial losses or lost tens of thousands, or had been a victim of bank card fraud or romance fraud, the emotional impact of online fraud was commonly cited as the most negative associated outcome, echoing our survey results. Self-blame permeated most study participants' experiences, including among victims of very sophisticated frauds, and was particularly acute among those who considered themselves 'tech-savvy'. However, having a positive interaction or outcome after reporting online fraud (which not all study participants chose to do) reduced the intensity and longevity of participants' anxiety and other negative emotions. Many study participants said that their behaviour changed as a result of becoming a victim, including taking action to become more vigilant online, which reduced vulnerability to future online fraud attempts.

5.

The process of reporting online fraud in some cases contributed to and worsened the effects of victimisation.

Receiving reassuring and prompt responses after reporting online fraud reduced the emotional impact of becoming a victim. On the other hand, having no dedicated point of contact; participants having to make up for a lack of communication from agencies by proactively and repeatedly following up on their case; the difficulty caused by needing to re-explain the situation to a different person each time they got in touch about their case; and a lack of compassionate and empathetic communication, all exacerbated the emotional effects of online fraud victimisation.

Overall, our findings paint a picture of a landscape in which the resource, capacity and capability for addressing online fraud are not commensurate with the scale of the threat, which provides opportunities for offenders to exploit. We drew on the findings above, as well as the findings from our survey, to make recommendations (published separately)[4] to prevent people from being victimised in the first place, to improve the experience of online victims in reporting online fraud when it does happen, and to support victims in the aftermath.

[4] Smith, F., Roberts, M., Davis S., and Murray, A. (2024). Online fraud: Recommendations for victims. Crest Advisory & ICPR.

Introduction

In 2023, the Crime Survey for England and Wales estimated that there were 3.3 million fraud offences,[5] the majority of which took place online (61 per cent of incidents across England and Wales in 2021/22 were estimated to be cyber-related).[6] Analysis by the Victim's Commissioner suggests that almost a quarter of fraud victims are likely to be deeply affected, experiencing high financial loss and emotional strain. Fraud is also significantly underreported, with an estimated 86 percent of fraud offences going unreported to the police or Action Fraud.[7]

Despite this, the full extent and impact of online fraud is not fully understood. This is reflected in a number of myths that surround fraud, including that the elderly are more likely to be victims[8] and that fraud is a low-impact crime.[9] Existing research into fraud victimisation tends not to distinguish between online and offline offences, in part because many fraudulent activities combine offline and online elements. However, the continued rise of online fraud means it is important to understand the specific experiences of online fraud victims (that is, those who have experienced financial loss due to fraudulent activity or deception that occurs through digital means) and to use this to better support victims and inform efforts to prevent and tackle online fraud. This is especially important in the context of future actions associated with the Government's Fraud Strategy (2023),[10] which need to be guided by robust evidence.

Aims and objectives of the research

This report is the second of several publications forming part of a wider major research project into online fraud carried out jointly with the Police Foundation and Institute for Crime and Justice Policy Research (ICPR) at Birkbeck, University of London, and funded by the Dawes Trust. The aims of our research include establishing a better understanding of the nature of online fraud, developing a new classification of online fraud, producing a comprehensive map of policy and practice and assessing future fraud trends.

The first strand focuses on gaining a better understanding of the impact of online fraud victimisation. In September 2023, Crest published findings from two large-scale nationally representative surveys with 3,313 members of the general public and 752 small and medium

[5] Crime in England and Wales: year ending June 2023.
[6] Nature of fraud and computer misuse in England and Wales: year ending March 2022.
[7] As cited by the Home Affairs Committee. (2023). Fraud - Committees
[8] Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., & Chi, M. (2022). The psychology of the internet fraud victimization of older adults: A systematic review. *Frontiers in Psychology, 13*, 912242
[9] Button, M., Lewis, C., & Tapley, J. (2009). Fraud typologies and victims of fraud: literature review. National Fraud Authority.
[10] Home Office. (2023). Fraud Strategy - GOV.UK

enterprises (SMEs) on their experiences of online fraud in England and Wales, focusing on victimisation and impact.[11] Through this research, we found that:

- online fraud victimisation rates may be higher than official figures;
- younger adults had a higher victimisation rate (32 per cent) compared to any other age group; and
- the impact of online fraud goes far beyond the financial.

This report builds on these findings by undertaking qualitative research with victims and the general public to create a more holistic understanding of their perceptions and experiences of online fraud. Recommendations for preventing victimisation and improving the experience of those who do become victims of online fraud were drawn from these two reports and published separately.[12]

Methodology and approach

Between September 2023 and December 2023, Crest Advisory and ICPR (Birkbeck, University of London) interviewed 20 victims of online fraud and conducted 12 focus groups with 96 members of the public.

Interviewees were victims of a wide range of online fraud types — that is, they had responded through the use of the internet to a fraudulent attempt which led to financial loss (see Table 1 in the Annex for a full breakdown of the different online fraud types experienced by the interviewees and see the glossary for definitions). Focus group participants were members of the general public who had not necessarily directly experienced online fraud; although some had.

Interview and focus group discussions centred around participants' understanding, perceptions and experiences of online fraud victimisation, as well as their knowledge and experience of reporting avenues. By conducting both focus groups and interviews we were able to gain a holistic view of the subject matter: focus groups provided a platform for dynamic interactions, revealing both collective and conflicting understandings, while interviews offered a space for personal reflection and depth that may not surface in a group setting.

Further information on our methodology and approach can be found in the Annex.

[11] Evans, A., Reynoso-Serna, F., Smith, F., Brown, E., & Davis, S. (2023). Online fraud: what does the public think?. Crest Advisory.

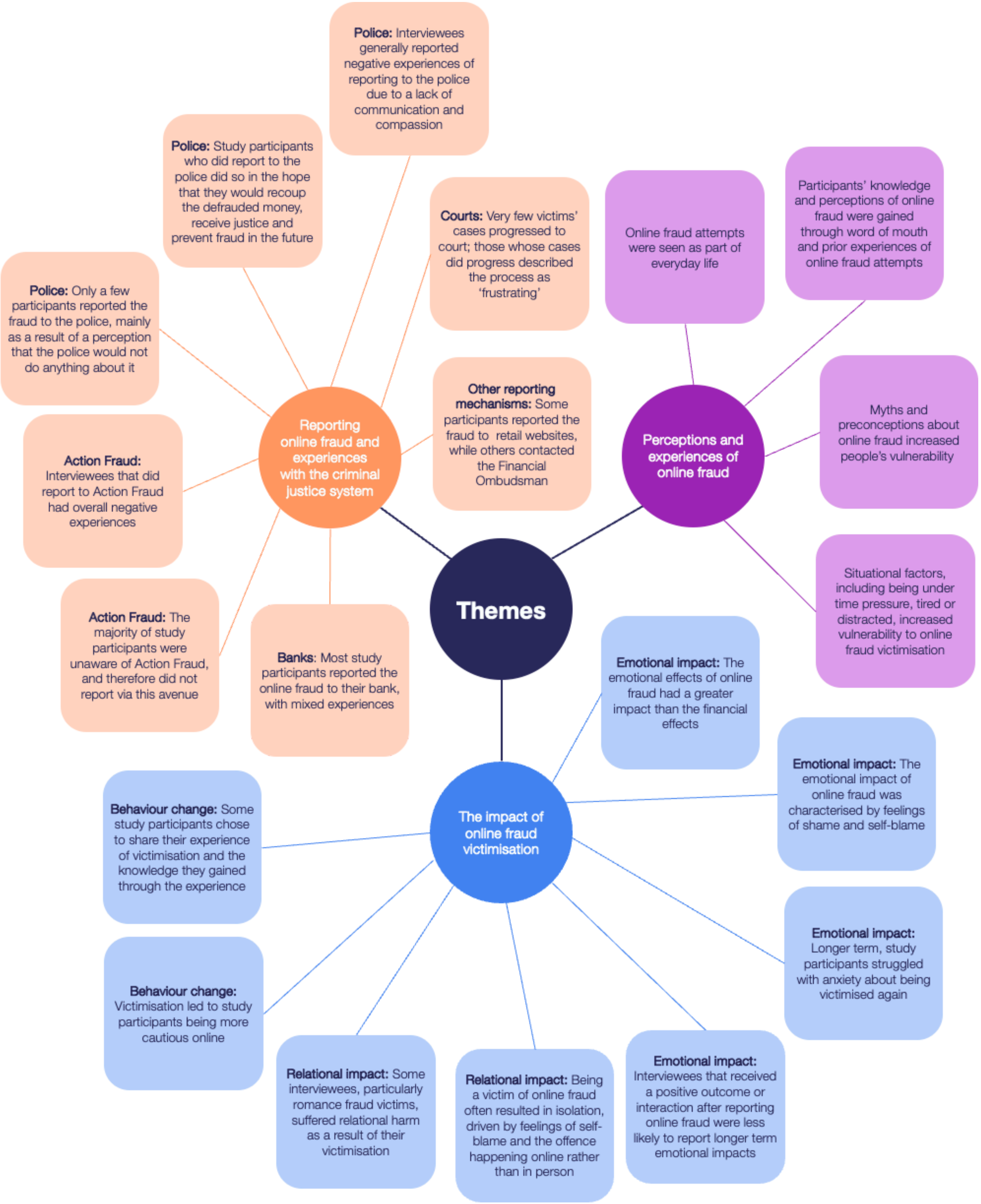
[12] Smith, F., Roberts, M., Davis S., and Murray, A. (2024). Online fraud: Recommendations for victims. Crest Advisory & ICPR.

Results

Analysis of the interviews and focus groups yielded three main themes, also shown in Figure 1, which form the structure of this report:

1. Perceptions and experiences of online fraud
2. The impact of online fraud victimisation
3. Reporting online fraud and experiences with the criminal justice system

Detail on each theme is provided below with relevant quotes. Interview participants (who had all been victims of online fraud prior to taking part) are referred to as 'interviewees' and focus group participants (who had not necessarily experienced direct victimisation of online fraud) are labelled in terms of their focus group location and number (e.g. 'In-person, focus group 4'). 'Study participants' is used to refer to both interviewees and focus group participants, where findings relate to both groups.



Themes

Reporting online fraud and experiences with the criminal justice system

Police: Interviewees generally reported negative experiences of reporting to the police due to a lack of communication and compassion

Police: Study participants who did report to the police did so in the hope that they would recoup the defrauded money, receive justice and prevent fraud in the future

Courts: Very few victims' cases progressed to court; those whose cases did progress described the process as 'frustrating'

Police: Only a few participants reported the fraud to the police, mainly as a result of a perception that the police would not do anything about it

Other reporting mechanisms: Some participants reported the fraud to retail websites, while others contacted the Financial Ombudsman

Action Fraud: Interviewees that did report to Action Fraud had overall negative experiences

Action Fraud: The majority of study participants were unaware of Action Fraud, and therefore did not report via this avenue

Banks: Most study participants reported the online fraud to their bank, with mixed experiences

Perceptions and experiences of online fraud

Online fraud attempts were seen as part of everyday life

Participants' knowledge and perceptions of online fraud were gained through word of mouth and prior experiences of online fraud attempts

Myths and preconceptions about online fraud increased people's vulnerability

Situational factors, including being under time pressure, tired or distracted, increased vulnerability to online fraud victimisation

The impact of online fraud victimisation

Emotional impact: The emotional effects of online fraud had a greater impact than the financial effects

Emotional impact: The emotional impact of online fraud was characterised by feelings of shame and self-blame

Behaviour change: Some study participants chose to share their experience of victimisation and the knowledge they gained through the experience

Emotional impact: Longer term, study participants struggled with anxiety about being victimised again

Behaviour change: Victimisation led to study participants being more cautious online

Relational impact: Some interviewees, particularly romance fraud victims, suffered relational harm as a result of their victimisation

Relational impact: Being a victim of online fraud often resulted in isolation, driven by feelings of self-blame and the offence happening online rather than in person

Emotional impact: Interviewees that received a positive outcome or interaction after reporting online fraud were less likely to report longer term emotional impacts

Figure 1. Thematic map showing the three main themes and associated sub-themes

1. Perceptions and experiences of online fraud

Online fraud attempts were seen as part of everyday life by study participants. However, becoming a victim of online fraud (that is, the attempt being successful) was seen as something that happened to ‘other people’ — namely the elderly, ‘naive’, or less technologically advanced. This was particularly the case among younger study participants, who saw themselves as more ‘tech-savvy’ than older generations, and therefore, less vulnerable to online fraud. Before being victimised, participants thought that fraud attempts would be easy to recognise as fraudulent, which ultimately increased the vulnerability of those who did become victims of online fraud. Participants’ understanding and awareness of online fraud mostly came from word-of-mouth rather than through formal channels or communication campaigns.

Online fraud attempts were seen as part of everyday life

Experiencing online fraud attempts was common within our sample. Focus group conversations often centred around the pervasiveness of online fraud, with participants describing online fraud attempts as ‘part of everyday life’. Being on the receiving end of online fraud attempts was seen as normal and expected, in large part due to day-to-day reliance on the internet:

> “I think it's so widespread. I don't know how it can be clamped down on really, because the internet's like, got a mind of its own hasn't it? [...] I don't know if there's a way to actually regulate it.”
> — In-person, focus group 7

> “I get so many of them [fraudulent emails] that it just becomes background noise. [...] Most of the time mine go [to] spam, so I don't have to deal with it [...] It's nothing new. It's just kind of part of life [...] they’re always there.”
> — In-person, focus group 8

The fact that online fraud happens on/via the internet meant study participants were often cynical about the possibility of any action by agencies to reduce the prevalence of online fraud in their everyday lives:

> “How do you police the internet? Really? How do you police it? It's hard. You have the police in the streets, but the internet, it's a whole entity of itself.”
> — In-person, focus group 7

> “It's that sort of international thing as well, like social media spans every country, everywhere. And so, like, you can't police that in the same way [...] They can't really deal with it.”
> — Online, focus group 2

Participants’ knowledge and perceptions of online fraud were gained through word of mouth and prior experiences of online fraud attempts

When study participants were asked where they gained their knowledge of online fraud, they commonly cited word-of-mouth rather than formal channels such as government campaigns. This often involved family or friends telling them about their experiences of online fraud:

> “I'd heard of it [online fraud]. I hadn't had previous experience before this [...] just family, friends have mentioned different types of fraud, whether it's been online or not.”
> — Interviewee 2

> “A lot of it comes down to people saying, ‘have you heard about this?’. ‘Have you heard about this [AI or robocalls]?’ [...] Definitely through people going through that experience or reading about it themselves, and then we all talk about it.”
> — Online, focus group 4

Experiences of unsuccessful online fraud attempts also informed participants’ understanding of online fraud. This meant that prior to victimisation, many interviewees believed that online fraud attempts were in general not sophisticated or convincing, and that they would therefore consistently be able to identify attempts as fraudulent:

> “I wasn’t expecting quite a lot of what happened. If it had just been a random message from out of the blue from like Nigeria, I think I would have picked up on it, but it was the fact that it was through a portal that is trusted where I was expecting to have an update.”
> — Interviewee 2

Myths and preconceptions about online fraud increased people’s vulnerability

Alongside a preconceived notion that online fraud would be easy to spot, the majority of study participants did not believe themselves to be vulnerable to online fraud prior to victimisation. Online fraud being something that happened to ‘other people’, who may be vulnerable due to factors such as their age or lack of technological skills or knowledge, was a commonly held myth or preconception among study participants.

This finding aligned with our survey findings, in which 50 per cent of respondents thought the elderly were most at risk of online fraud, while 18 per cent of respondents believed those that lacked digital skills were most at risk of online fraud.[13]

> “I never thought I'd get sucked in that kind of thing. Because I always thought fraud is for old people or people who aren't tech-savvy. I never thought I'd be part of it.”
> — Interviewee 3

> “I just, I didn't think that I would get tricked by it; I didn't think I was naive enough. I thought it was just people that were sort of vulnerable or older, that those were the type of people that would get tricked by scams and stuff.”
> — Interviewee 8

> “I always thought it was something that happened to other people who didn't know how to shop properly online, or fell for people ringing up from other countries and saying, ‘give me your bank account details’, etc, etc. But I never thought for a minute that I would be a victim of online fraud. It was very much something that happened to other people. And I've always been quite careful as well, I've always been very, you know, only going to reputable sites [...] And I've always felt quite safe online until last year.”
> — Interviewee 14

Younger participants in particular were less likely to see themselves as vulnerable to fraud, in part due to perceiving themselves as ‘tech-savvy’, having ‘grown up around computers’. This belief is contradicted by evidence which suggests that younger adults are at high risk of being victimised — for example, our survey found that 18-24 year olds were more likely to be victimised than older adults.[14]

> “I also think that the younger you are, the less likely you are to fall for online scams. Because I only say that because I grew up like Roblox [and] all that kind of stuff. And it used to happen a lot more. So I think people kind of grew up like that, people my age grew up knowing that these types of things happen.”
> — In-person, focus group 2

[13] Evans, A., Reynoso-Serna, F., Smith, F., Brown, E., & Davis, S. (2023). Online fraud: what does the public think?. Crest Advisory.

[14] Evans, A., Reynoso-Serna, F., Smith, F., Brown, E., & Davis, S. (2023). Online fraud: what does the public think?. Crest Advisory.

> “We grew up around computers, you know, all of us. So we're kind of aware, you know, it's the people around us, you know, especially that the elderly [...] they're not very, like, you know, adapted to the whole computing system and how everything works. So it's very easy for, like, hackers and fraudsters to target those people.”
> — In-person, focus group 2

> “What worries me really is that I have elderly people in my family who have been victims. And if they don't have others around who are more knowledgeable on technology, they might, you know, keep getting scammed over and over and over and over again.”
> — In-person, focus group 3

As a result, when interview participants then received more sophisticated fraudulent communications, they were more likely to become a victim. One interviewee, for example, became a victim of advance fee fraud after a fraudster claimed to be their solicitor and told the participant it was time to pay the deposit on the flat they were buying. They made no spelling mistakes (a common tell-tale sign), and were able to answer all their questions. In the end, the interviewee sent £13,000 to the fraudster:

> “They [fraudster claiming to be a solicitor] were really good because I even asked him some questions, and they were answering me, they knew the property, they knew everything about it. They knew that the 13 grand was 10 per cent of the whole thing. I even said to him, ‘What about my help to buy [ISA], the scheme I was doing with the government?’. They answered that question. Yeah. So it was really convincing. [...] There wasn’t spelling mistakes [...] That might have triggered me to think otherwise.”
> — Interviewee 8

> “I think it used to be easier to recognise, because it used to be so laughable that [...] you just had to look at the email address and whatnot, but I have had [...] ones for, you know, your iPhone bill, you know, your Apple account, and it's only because I sat there and thought 'I don't use Apple', but [...] I've had to sit there and mentally go 'have I had an Apple in the past?' because it's so sophisticated.”
> — In-person, focus group 8

Situational factors, including being under time pressure, tired or distracted, increased vulnerability to online fraud victimisation

A few study participants mentioned that situational factors had a role in their online fraud victimisation. For example, time pressure had a role to play in the victimisation of two interviewees:

> “So then I thought, 'Okay, right. I just want to finish this now' and just kind of, you know, wanted to move on to the next thing in my day. So I then put in my main bank details.”
> — Interviewee 2

> “It was the urgency. Yes, it was Black Friday. Yeah. And you think, oh, it's this 24-hour deal. You know, they make it pressured and time sensitive. And I think that feeds into your sense of urgency.”
> — Interviewee 14

Others described being tired and lacking attention/being distracted when they received and responded to a fraudulent communication, which contributed to their victimisation:

> “I didn’t pay attention before I clicked yes to the notification which came on my phone [...] because you’re so distracted by some other things.”
> — Interviewee 19

> “You might just be, I don't know, tired or you know, a moment of weakness and you think, oh, I'll get that, that sounds really good.”
> — Online, focus group 3

2. The impact of online fraud victimisation

The impact of online fraud victimisation was extensive and wide ranging, including emotional, relational and financial impacts. The emotional harms of online fraud were discussed much more frequently and were described as more significant than its financial impacts by study participants, who described feelings of anger, shame and anxiety. These emotions were closely linked to study participants’ feelings of self-blame, which in some cases stopped them from talking about their victimisation with others. This was a common finding across fraud types and scale of financial loss. Becoming a victim of online fraud affected some study participants’ personal relationships, particularly among victims of romance fraud, often as a result of losing trust in others. Interestingly, receiving a prompt and reassuring response when reporting seemed to mitigate the emotional harm, suggesting an important role for reporting authorities. Becoming a victim led to people changing their behaviour and growing more aware and vigilant of online fraud.

2.1 Emotional impact

The emotional effects of online fraud had a greater impact than the financial effects

The most commonly discussed impact of online fraud victimisation was emotional, a finding echoed by our survey results. Most participants rated the emotional effects of online fraud as worse than its financial effects, and described struggling to come to terms with someone '*violating*' them. While this finding should be contextualised by the fact that study participants who were victims had generally suffered low-value frauds, the finding was also true for interviewees who lost more significant sums, making it a consistent finding:

> "That part [the emotional side] is harder than the financial side because it literally played with my emotions and I feel that made me look stupid. It changed me, I still have many insecurities [...] I view [the] emotional parts, [as] harder than the financial parts. Money comes, but, well, you [the fraudster] broke me. You broke me. You should not do what you're doing to anyone. I can pay for whatever, hurt me with work, but don't hurt me emotionally."
> — Interviewee 1

> "So there's that [financial] aspect but it is also violating to think that they were in my emails and stuff and that they tricked me like this [...] It was also the fact that it was obviously a real person talking to me and they were literate, eloquent, they've literally found the answer to my questions and stuff and they were convincing me to pass over my money. And it also just feels really hard to take as well that someone would do that."
> — Interviewee 8

> "The bank account is so personal to you and, like, they've taken your money and you think, 'why have they chosen me?', especially [...] if you don't have that much money either."
> — Online, focus group 4

The emotional impact of online fraud was characterised by feelings of shame and self-blame

Online fraud victims described feeling of shame, embarrassment and anger. This was linked to the preconceived notion that online fraud happened to 'others', resulting in shame and embarrassment that victims 'did not see that [it] was a scam'. These feelings were also apparent among interviewees who had become victim to very sophisticated online frauds:

> “Well [I felt] humiliation, embarrassment, stress, anger, sadness, like, every emotion going really. And then, I suppose, like, once you start telling people, you either get like, 'oh, my God, you okay?' or you get, 'oh, I didn't think that would happen to you'. And then those people you just want to punch in the face — obviously you can't… I think embarrassment and almost shame is probably the biggest. Like my Dad has no idea it happened.”
> — Interviewee 4

> “I also kind of felt a bit ashamed for some reason, like a bit stupid that I’d been duped [...] There's not many times that you can get robbed and blame yourself for it.”
> — Interviewee 8

> “I think the hardest thing was feeling like I was an idiot, and feeling really angry, feeling really angry and feeling really aggrieved.”
> — Interviewee 14

The feelings of shame and embarrassment were particularly heightened for those who saw themselves as ‘tech-savvy’, linking with the notion commonly held among the study participants that only those lacking technological skills become victims of online fraud:

> “I think it's just feeling foolish really is the main thing. You know, I've dealt with computers since whenever.”
> — Interviewee 10

> “I feel a bit ashamed because I'm sort of, I'm a cyber security professional.”
> — Interviewee 19

Longer term, study participants struggled with anxiety about being victimised again

Some study participants struggled with anxiety as a result of online fraud victimisation, which continued into the longer-term. This finding aligned with our survey results, in which the most commonly reported psychological impact of online fraud was anxiety. Study participants’ anxiety was centred around the fear that they may be victimised again:

> “I still panic about that, when I think about [the online fraud victimisation]. I’m scared it will happen again. But I don’t think it will logically, but you do get scared.”
> — Interviewee 3

> "I feel like if someone [has] my bank details, date of birth, and all that sort of stuff, in the future, am I going to be [...] [an] easy target?"
> — In-person, focus group 4

> "It's the sort of devastation of it afterwards, you know, and how it sort of applies to quite a lot of different areas of your life [...] It's security [...] it's how you go forward with your life [...] there's a sort of cynicism. Or we double think everything going forward."
> — Online, focus group 4

> "You could be thinking … I don't know whether I want to buy too many Christmas presents online because I'm scared that it's going to happen. I think it will just kind of always be in the back of your mind. You'll always be a little bit kind of burnt, so to speak [...] You've always got that fear, I guess in the back of your head that, it that, it could happen again."
> — Online, focus group 4

Interviewees who received a positive outcome or interaction after reporting online fraud were less likely to report longer term emotional impacts

Those who received a positive interaction after reporting online fraud were less likely to report longer term emotional impacts. Being able to contact someone quickly, and that person being able to help, put their worry at ease and lowered their anxiety:

> "Just the worry, the dread. I saw the balance and I'm like, 'oh my God', it's just like, 'oh my Lord, what's happened here', you know? So it was only brief, thankfully, because then I spoke to somebody. And like, within like half an hour, they sort of put me to rest a little bit so it kind of was nice. I can't imagine what it'd be like if it'd be any longer than that. Where if I wasn't able to get hold of somebody straight away. So I'm glad I didn't have to go through that."
> — Interviewee 7

This contrasted with the experience of those whose online fraud was not resolved, which was associated with more intense and longer lasting emotional impacts:

> "I was more annoyed at the outcome rather than, than him [the fraudster] doing it [the online fraud] [...] I was even gonna go drive down, to drive down one day and go round and round the roads and see if I can see some shifty character, but no, it's sort of like they beat me, rather than me beat them. That's what annoys me most."
> — Interviewee 10

2.2 Relational impact

Being a victim of online fraud often resulted in isolation, driven by feelings of self-blame and the offence happening online rather than in person

Feelings of shame and embarrassment, as well as a fear that they would be judged or blamed, meant many study participants chose not to tell friends and family about their victimisation, or chose to only tell a select number. As a result, these participants were often left feeling isolated:

> "I didn't go into detail [...] I think it is more the embarrassment, isn't it? That, you know, this happened to you. That you're supposed to be tech savvy."
> — Interviewee 9

> "I suddenly thought, 'who do I tell?'. Because, you know, there's still even now [...] that stigma attached to the fact that you're an idiot. How can you be so stupid, you know, an intelligent woman."
> — Interviewee 11

> "It's that feeling that 'God, I've been done, I've been had'. And how would you actually say that to someone? Yeah. It's very, very difficult to say those words. Because people judge. We still judge. And I judged till it happened to me."
> — In-person, focus group 7

The online setting of the offence heightened feelings of isolation among study participants, who felt they were less likely to receive sympathy compared to if they were the victim of more 'traditional' crimes types:

> "I think the crimes that are committed in person, they can tend to have more witnesses [...] And, you know, I think I'd like to say more people are nicer than not. So I think some of them would come in and ask 'you okay?'. Whereas if you're just say online, by yourself, it's just you. There's no one there like to talk to you or say something to me, you feel alone, I think you feel alone with it [...] So you do kind of feel like it's not worth mentioning."
> — Interviewee 6

> "If you had your house burgled, people would be really sympathetic, wouldn't they, say 'ohh, you know I've lost this, this and this'. But it, it is more of a nebulous sort of thing, isn't it, when it's, it's all online."
> — Online, focus group 1

Some interviewees, particularly romance fraud victims, suffered relational harm as a result of their victimisation

Online fraud victimisation resulted in relational harm (that is, damage to victims' relationships) for some study participants, commonly characterised by reduced trust in others. This was most common among victims of romance fraud, with whom the fraudster built up a relationship and subsequently betrayed:

> "It's made me more cautious. I don't do things I would normally do, I just want to be in my own space. I don't want to interact with anyone and most especially boys. I just want to be left alone [...] it made me detest men."
>
> — Interviewee 1

> "It's made me more suspicious of people [...] there's that wall up now, as protection."
>
> — Interviewee 4

> "It's made me very, very sceptical. I've never been among the most trusting person in the world, I've always been quite not trusting, it's made that worse [...] I can't understand how people can be so horrible to do that [...] so now it's even worse, you know, I'm very, very sort of cynical about the world as a result of it."
>
> — Interviewee 16

Two victims of romance fraud lost friendships due to their decreased trust in others and higher levels of suspicion as a result of becoming a victim:

> "If I find people have lied [...] then that puts walls up. [...] If someone breaks my trust like that, then yeah, I cut them off."
>
> — Interviewee 4

> "I'm sad. It makes me unbelieving, untrusting, every 'un' word you can think of with anybody. And that isn't necessarily a good way to live your life."
>
> – Interviewee 15

2.3 Behaviour change

Victimisation led to study participants being more cautious online

While online fraud victimisation resulted in a wide range of harms among the study participants, and was overall associated with negative impacts, becoming a victim increased study participants' awareness of online fraud and their knowledge of how to avoid becoming a victim in the future:

> “I guess I'm just [...] more aware of messages and emails, and the fact that if they're coming from someone other than the actual company [...] I don't think I really thought about that consciously before.”
> — Interviewee 1

> “I'm kind of grateful for it, because I think it's always good to have experiences that kind of open your eyes to things and make you think about things a bit more carefully. And I think I've always just ignored fraud emails from banks and things that educate you about fraud whereas actually, you know, it's an opportunity to learn about it, think about it more carefully [...] I was trying to turn a negative into a positive that way and, and try and get some learning from it.”
> — Interviewee 2

> “I think generally if you, if you've been caught out by something, you take a closer look next time round. But I think for me it's only after the event has happened that that, you know, then I'm more careful and advise my friends about it.”
> — Online, focus group 3

Behaviour changes to reduce the risk of future victimisation included undertaking extra due diligence when sending money; checking that the website they were buying from was a trusted, legitimate retailer; and increased care with passwords:

> “Yes, I'm a bit more cautious now. I will maybe double or triple triple check when I'm asked to pay in any way that makes me concerned. And I'll try and verify things, ideally using the actual website.”
> — Interviewee 2

> “But based on the experience that I’ve had, and if I did shop with anyone that I was unfamiliar with, I would literally spend a lot more time looking at the website and a little longer looking for little clues really.”
> — Interviewee 14

> “I tend not to order off websites that I've never heard of. And if it's something I've never heard [of] I'll go on to something like Trustpilot to see if anyone else has had any bad experience of them.”
> — Interviewee 20

> “Like someone hacked into my Amazon and like, used my cards on there and things. So now I'm like really careful with passwords.”
> — Online, focus group 2

Some study participants chose to share their experience of victimisation and the knowledge they gained through the experience

Some study participants told friends and family about their experiences with online fraud in the hope that it would educate them and prevent their future victimisation:

> “I told everybody [and] hopefully they use that as experience [...] that's sort of why I wanted to tell people, to share my own experience, to warn people.”
> — Interviewee 7

> “It’s better to talk about it. And in a way, I kind of wanted to make other people aware in case, you know, they ever have something similar happen to them.”
> — Interviewee 8

> “[You should] tell your friends or your family [about] it. Like if you see this scam, like try not to fall for it.”
> — Online, focus group 2

For some study participants, telling friends and family about their experience led to them being blamed for their victimisation, with family and friends criticising victims for responding to the fraudulent communication:

> “I did tell my other half. And he said, ‘well, you've done everything that you can, have you learned from this, you always shop too much anyway’. Which I didn't think was very supportive from him. And [he] said ‘I told you it's dodgy shopping online, I told you’, he said. So maybe I shouldn't have mentioned it to him.”
> — Interviewee 14

> “[It] can make some people feel embarrassed to admit it. Because as soon as you do, somebody would say, ‘oh, how did you fall for that’, you know.”
> — In-person, focus group 4

3. Reporting online fraud and experiences with the criminal justice system

Action Fraud is the national reporting centre for online fraud. However, very few of our study participants reported to Action Fraud, reflecting the fact that most were unaware of its existence. Instead, study participants most commonly reported to banks. Reporting to the police was more common than reporting to Action Fraud, but most study participants did not report online fraud through this avenue, with a lack of trust in the police's capacity to effectively deal with the crime cited as the most common reason. Positive reporting experiences were characterised by quick, proactive and empathetic communication, while negative experiences were characterised by victim blaming and needing to chase for updates.

3.1 Action Fraud

The majority of study participants were unaware of Action Fraud, and therefore did not report via this avenue

The majority of study participants had not heard of Action Fraud, and therefore did not report online fraud via this avenue. At the same time, some interviewees mentioned that it would be beneficial to have a specific body to report fraud to, meaning increased awareness of Action Fraud could have resulted in a greater number of study participants reporting to the agency. When study participants were informed about Action Fraud and the services it offers by the interview/focus group facilitators, responses were generally positive but centred around there needing to be more information available to the general public about how to report online fraud:

> "I think there probably is a body where you can report it, you know, like just solely about online fraud. There probably is a department but I don't know what it is."
> — Interviewee 5

> "I don't know [if I've ever heard of Action Fraud]. Very undercover marketing [from Action Fraud], yeah, opposite of good marketing."
> — Interviewee 8

> "If there was more information on where you could actually go to like, report things and try and get some action taken, you might be more inclined to actually do it. But it's like the unknown. Who do you approach? What do you do when it does happen?"
> — In-person, focus group 7

Interviewees who did report to Action Fraud had overall negative experiences

One interviewee praised Action Fraud for its user-friendly website and proactive communication:

> "[The experience reporting to Action Fraud was] really good. Yeah, I liked it. It was easy. It was online, it was nice and straightforward, and explained everything. That was a nice experience. The website's really intuitive of what it needs to ask me, which is really good, I literally could give them everything and they literally went 'yeah, fantastic thank you.' I think they then contacted sort of the local police. And then they then reached out to me, which is really good."
> — Interviewee 7

However, other interviewees stated that they did not receive sufficient communication from Action Fraud after reporting the offence. Not receiving any update or response about their report left interviewees feeling dissatisfied:

> "I'd also reported him to Action Fraud. But again, I don't really know what they do. From what I can gather, nothing."
> — Interviewee 4

> "I just logged it [to Action Fraud] and never got anything back, just 'thank you for letting us know'."
> — Interviewee 10

> "There was no referral [to the police from Action Fraud], it was just a case of 'we will follow it up, but we can't guarantee that we'll do anything about it'. Nothing was ever resolved in terms of following up, despite the fact that I had given all this information [...] I was chasing [...] there was no other message other than 'we haven't got any information to give you' [...] 'we have too many cases to deal with'."
> — Interviewee 11

3.2 Banks

Most study participants reported the online fraud to their bank, with mixed experiences

Similarly to our survey findings, study participants most commonly reported incidents of online fraud to their bank, especially in cases of bank card fraud where their banking provider would have some administrative involvement in the incident, for example to stop the fraud, to limit future fraudulent transactions, or to determine if they would be reimbursed.

Study participants' experiences with reporting to banks and the outcomes ranged widely. Positive experiences were characterised by receiving a resolution (such as being reimbursed and receiving replacement cards) in a timely manner, the banks taking responsibility for resolving the incident (rather than the participant having to chase), and receiving clear communication around the process:

> "I telephoned the bank and explained that I think my account's been hacked because I haven't made a purchase and this money has been taken out of my account. And the person from the bank on the telephone was very lovely and reassured me that they will cancel my card, they explained if I needed money I could come into the bank. And they said it's gonna take up to five working days and once they've cancelled it we're not going to be able to take any other money, any more transactions out. And they explained that if the money does come out of my account it will be refunded. But thankfully it didn't come to that because they just cancelled the card straight away."
> — Interviewee 6

> "They [the bank] were quite vigilant in the check so I'm happy from that perspective. You know, they did what they needed to do. And like I said from my sort of fall out if you like, I didn't have to do much, which is quite nice."
> — Interviewee 7

In contrast, not being reimbursed, unempathetic communication from bank staff, and lengthy waits for decisions to be made characterised the experiences of interviewees who described being unsatisfied:

> "It took so long, like months and months, months, close to a year […] [I] called them, and then this time someone said to me [...] 'you're not getting your money we've decided'. I just broke down and literally started crying. I didn't realise like how horrible it was going to feel. I think it was his delivery as well. So I was kind of like, 'why didn't you tell me?' and he was like, 'Miss, all I can do is apologise'. I said, 'you haven't apologised'."
> — Interviewee 8

> "I rang them [the bank], gave them the details and they said, 'there's nothing we can do'. So, I said, 'yes, but I can tell you he's scamming'. 'Well, there's nothing we can do, you authorised the payment'. So that was that."
> — Interviewee 10

Negative experiences of reporting incidents of online fraud to banks also included having to continually call the bank and not being given a dedicated contact. This meant interviewees had to call the general number for the bank and repeatedly relay information about their case to different people. Retelling and reliving the incident affected the interviewees emotionally, whilst also delaying the process of getting their money back:

> "But I am very disappointed in how [my bank] handled it. A: that it should take that long to get through and it be that long winded, I just think you need an emergency fraud line [...] B: that they didn't sort it with the first phone call, you know, and it is inconvenient to keep ringing."
> — Interviewee 1

> "I still had to call the general line then [...] they wouldn't just pass me through. They'd be like, 'oh, well, let me have a look'. And then they would say 'I just need to read your notes', which obviously at this point were massive because I rang every week, so they'd go away for ages. Then they come back and go, 'oh God, oh goodness, that's not good'. [...] And I'm like, 'no, anyway, is it alright to talk to that fraud team?' [...] then they pass me over and then I'd have to do like the whole thing again."
> — Interviewee 8

Interviewees also mentioned feeling blamed, judged or treated with suspicion by banking staff in some instances, feeding into broader feelings of shame about making a mistake or being responsible for their victimisation:

> "I went to the bank [and] when I explained you could almost see the women think 'stupid woman'."
> — Interviewee 1

> "I got the impression, especially after this happened the second time, they thought I was culpable. [...] I think that it was that suspicion."
> — Interviewee 16

3.3 Police

Only a few participants reported the fraud to the police, mainly as a result of a perception that the police would not do anything about it

In contrast to high levels of reporting to banks, most study participants had not reported their online fraud to the police or even considered doing so. Our survey results found that, of those that did not report online fraud, 14 per cent did not due to not having confidence in the police. Building on this, several study participants believed that the police were already overburdened with 'more serious crime'. Participants also held the perception that the police did not have the resources to tackle online fraud — particularly more sophisticated online fraud offences which would require comparatively more resource to investigate:

> “I'd rather report it myself to a non-police agency. I don't feel comfortable, I don't have a lot of trust in the police. I don't feel that many things that get reported to the police get resolved, and I think often you are spending a long time filling out paperwork, but not actually getting the outcome that you want, because the police don't have the resources to do much, you know [...] So I would rather report it to a non-police agency. i.e. the banks or somewhere else, you know, to get it resolved.”
> — Interviewee 2

> “The reason I think I didn't go to the police [was] because I thought it was too sophisticated for them to actually do. It probably wasn't, on reflection, easy.”
> — Interviewee 16

> “Sometimes it's not worth it. We feel there's no point to report it because [...] then they turn around and say now, ‘it's not serious enough’ or you know, [they’re] not gonna deal with it.”
> — In-person, focus group 3

> “I feel like if you did [report] what was the point because no one's gonna do anything about it.”
> — In-person, focus group 6

Study participants who did report to the police did so in the hope that they would recoup the defrauded money, receive justice and prevent fraud in the future

Of the few study participants who reported their online fraud to the police, the majority did so with the motivation of receiving the defrauded money back, to achieve a sense of justice through prosecution of the perpetrator, and to prevent future instances of fraud:

> “I was hoping to [catch] the person and that I get my money back and the person be prosecuted. And I was hoping maybe the police could use the account, the account that I usually chat with the person, his Instagram account, and track him.”
> — Interviewee 1

> “I went the legal route. I was like, 'he can't do this to somebody else'. Like, that's just, that's not on.”
> — Interviewee 4

> "I think it's a kind of two-pronged thing for me [why I reported]. Number one, you want the money back [...] But I think the hardest thing was feeling like I was an idiot, and feeling really angry, feeling really angry and feeling really aggrieved. And I think that's why I went to pursue all of the lines of inquiry and did it myself."
> — Interviewee 14

> "I could have afforded to lose the 50 pounds, but I wanted to report it so that it doesn't happen again to somebody else, because nobody reports anything."
> — In-person, focus group 5

Interviewees generally reported negative experiences of reporting to the police due to a lack of communication and compassion

The interviewees that did report online fraud to the police described their interactions as lacking in communication and compassion. This included not being proactively contacted with updates of the progress of the case (and, therefore, the victim having to contact them), poor explanations of decisions, and never meeting the investigating officer:

> "I would email every couple of weeks. All I would get told was 'we're looking into it', or 'we've got to phone this place' or whatever. And I just kind of lost it and was like 'ok, who do I need to phone' [...] So we wrote an email to my MP, and [...] it kind of got pushed up [...] I mean, no wonder I have no faith in them [the police]."
> — Interviewee 4

> "They [the police] were just awful. That nobody knew what was, what was happening, who was doing what [...] So what I did is I actually did a lot of the legwork myself [...] I had a picture of the person who tried to use my cards and everything, I literally handed on a platter to the police. They [the police] did nothing."
> — Interviewee 7

> "I spoke to the police after, saying 'this is what happened'. Then they referred me to the cyber division for the police force and I just filled out a long form. And then I think two weeks pass and it says, 'sorry, there's nothing we can do' [...] Yeah, it is a bit of a kick in the nuts [...] You know, I followed the process, went to the bank and the cyber division, and they all say there's nothing else you can do. But obviously, I still see that person on social media still, you know, advertising, selling fake stuff clearly."
> — Interviewee 9

Where communication did occur, it was often coupled with a lack of compassion from the investigating officers, which made the interviewees feel ‘more stupid’ and ‘insignificant’:

> “Some of the police, the way they spoke to me also broke me, I already felt like a fool so they were already making me feel more stupid, more foolish and dumb. Maybe the manner of approach and the way they spoke to me could have helped at least, even if they couldn't help me get the money back, it would help me emotionally by the way they spoke to me.”
> — Interviewee 1

> “I think that the whole police investigation is lack of action, lack of care, I never met the DC that I was dealing with. I felt like there was no… There was no compassion. I felt like I was a pain in her arse and like my case was just insignificant to her. I emailed the police officer and was like, 'I don't know how much longer I can carry on'. And she just ignored it, like it was insignificant. She was just like, 'oh, don't worry, we've got him'. At this point, I couldn't give a fuck, excuse my English [...] I feel like with them, you're just a number, you're just another case that they've got to get through. They don't care who you are. They don't care how it affects you.”
> — Interviewee 4

3.4 Courts

Very few victims’ cases progressed to court; those whose cases did progress described the process as ‘frustrating’

The cases of only three interviewees progressed to court out of the entire study sample, two of which resulted in a conviction. Of the three interviewees whose cases went to trial, two were involved in the court process. Both described their experiences as ‘frustrating’ and ‘stressful’, in part because they received little guidance on what the process would entail:

> “The whole court process, whether it was civil or criminal was, I think, some of the most stressful times and frustrating times I've ever dealt with [...] I think the realisation that you've been conned out of a load of money is like the worst, and then having to deal with the police and the court systems is definitely next on the list.”
> — Interviewee 4

> “I'd done my victim impact statement in court, and then obviously claimed for compensation. And she wasn't very helpful. Like for someone that's never done it before, she's like, 'receipts of everything'. And I'm like, 'well, what do you mean by everything?'. And she's like 'well just everything.' I'm sorry, shall I put my car tyres on there? I had to get new car tyres after he [the offender] borrowed my car. Like, like, do I put my milk and bread on there? Because I ate after he [the offender] stressed me out?”
> — Interviewee 4

One interviewee was not asked to attend court but said that if they had been asked, they would not have attended. This was due to their perception that it would be too stressful and their previous experience of a court process:

> “I wouldn't have gone [if I'd been asked to attend court], it's not far, it's about an hour and a half from us, but it's just too stressful. I've been in a court proceeding before and I would never want to go through it again.”
> — Interviewee 18

3.5 Other reporting mechanisms

Some participants reported the fraud to retail websites, while others contacted the Financial Ombudsman

Some victims of retail fraud reported the offence directly to the retail company/website via which the fraud took place, with mixed results:

> “I sent an email [...] and said, 'your site, your website, your name, your colours are being used to defraud'. And that again got me annoyed [...] they wrote back and said, 'oh, yes, you have to be careful'. And I thought 'that's your answer is it? ‘you have to be careful’'. But they are willingly going along with somebody using them. It appears as far as [the company] are concerned, it’s your responsibility.”
> — Interviewee 1

> “I had a look on Vinted as well. And I did report it to them. I discovered that there isn't a telephone number you can ring for Vinted [...] so I reported electronically to Vinted as a message and I think they came back to me like later on in the day just to say that they had removed that person, I think they had confirmed that they thought it was fraudulent.”
> — Interviewee 2

A minority of study participants reported to the Financial Ombudsman in an attempt to recoup the money that was taken from them. For example, one interviewee who was defrauded around

£175,000 to romance fraud went through the Ombudsman after their bank did not refund the stolen money. This was described as a positive experience, as the Ombudsman clearly defined his role and actively listened to the participant:

> “I just felt [the Ombudsman was] fighting for me, like he said his job was to get my money back. That was his own purpose, he sounded lovely [...] I think one of the things that was really good was that he said, 'I want to know, you need to tell me everything. Don't miss anything out'. So there were lots of phone calls about what had happened, you know, over the two, three months. But he was excellent. And then we got, we got the result.”
> — Interviewee 1

It was noted that the onus of identifying the agencies and organisations that exist for online fraud reporting and support, and determining the most suitable agency or organisation for the situation, often falls on victims, who then also need to persevere until they receive an outcome:

> “And I did get amazing action [and] results, because I persevered and didn't let it go. I didn't push it, but persevered. And as a consequence of that the situation was resolved. But you had to be on time with it.”
> — In-person, focus group 7

Conclusion

Myths and misinformation surrounding online fraud, the lack of information on the available reporting structures and support, and a lack of confidence in the capacity of agencies to effectively investigate fraud, affect victims at every stage. This includes underestimating their exposure and vulnerability to suffering online fraud, being reluctant to report an offence once it has been committed due to feelings of shame, and finally confusion about where and how to report and access support. These experiences compound the emotional effects of being a victim of online fraud.

Our findings on online fraud victimisation illustrate a unique experience compared to other crime types. The scale of the problem, and under-prioritisation of fraud over the last decade, has led it to being seen as 'part of everyday life', a situation we would not accept in relation to other crime types. The online element of the crime compounds feelings of isolation that stem from a culture which blames victims for their experiences. The significant rates of underreporting are notable. For those who do decide to report, victims are faced with a multitude of reporting options that do not join up with each other, which is not the case for other crime types.

Overall, our findings paint a picture of a landscape in which the resource, capacity and capability for addressing online fraud are not commensurate with the scale of the threat, which provides opportunities for offenders to exploit.

We drew on our survey, interview and focus group findings to make recommendations that focus on how the experience of victims could be improved, to drive towards a much needed step change in the response to online fraud. These are published in a separate report, alongside this one.[15]

Our conclusions also have implications for the ways in which the policy and practice landscape is set up and how the relevant agencies and organisations interact with each other. These issues will be explored further in the next phase of our project.

[15] Smith, F., Roberts, M., Davis S., and Murray, A. (2024). Online fraud: Recommendations for victims. Crest Advisory & ICPR.

Annex: Methods

Recruitment and procedure

In total, there were 96 focus group participants: 63 who attended the in-person events in two cities in the UK, and 33 people who attended online.

Interviewees had a range of experience of fraud types, including advance fee fraud, romance fraud, bank or card fraud, online shopping fraud, and identity fraud (see Table 1 for a breakdown and the glossary for definitions), and a range of experiences interacting with the criminal justice system.

Table 1. Breakdown of the type of online fraud victimisation experienced by the interviewees

Interviewee	Fraud type
Participant 1	Romance fraud
Participant 2	Online shopping fraud
Participant 3	Romance fraud
Participant 4	Romance fraud
Participant 5	Bank card fraud
Participant 6	Bank card fraud
Participant 7	Bank card fraud
Participant 8	Advance fee fraud
Participant 9	Advance fee fraud
Participant 10	Online shopping fraud
Participant 11	Romance fraud
Participant 12	Identity fraud
Participant 13	Advance fee fraud
Participant 14	Online shopping fraud
Participant 15	Advance fee fraud
Participant 16	Identity fraud
Participant 17	Bank card fraud
Participant 18	Identity fraud
Participant 19	Identity fraud
Participant 20	Bank card fraud

The focus group participants were screened to ensure that they had some experience of using online platforms, such as social media, internet banking, or email. The focus group participants were divided into four groups which Crime Survey for England and Wales data suggests are the demographic groups most likely to become a victim of online fraud:

1. Full-time students aged 18-25
2. People aged 25-65
3. People aged 65 and over
4. People with disabilities aged between 25 and 65

Interviewees and focus group participants were identified through a dedicated recruitment company (Acumen),[16] who ensured that the samples were broadly representative of the general population and of the local population for the in-person focus groups.

Study participants were given a verbal briefing of the research project and interview/focus group process as well as an information sheet to ensure they were able to give their informed consent to take part in the research.

The 20 interviews were conducted online using Microsoft Teams. The 12 focus groups were conducted in-person in two cities in the UK and online using Microsoft Teams (4 in each location). Participants were reimbursed for their time.

Scope and approach

Focus group participants (drawn from the general public) were asked to discuss:

- Their perceptions of online fraud;
- How they viewed the risks to them and wider society;
- How it was different to other types of crime; what it meant to be a victim of online fraud;
- If they knew of any guidance or information about online fraud and how to report it;
- Who should be responsible for tackling online fraud; and
- What they thought of the Government's Fraud Strategy.

The focus groups were not intended to examine individual participants' experiences of fraud; however, many participants did have some experience of being a victim or knew someone close to them who had been a victim of online fraud (such as a family member or friend) and these experiences were discussed in the groups.

The interviews with online fraud victims were conducted to understand victims' experiences of online fraud and the impact this has had on them. The interviews involved discussions around:

[16] Fieldwork Market Research | AcumenFieldwork Agency

- Victims' understanding of online fraud;
- Victims' experiences of online fraud;
- Reporting of online fraud and the criminal justice system process; and
- Recommendations for the future prevention of online fraud.

By conducting both focus groups and interviews we were able to gain a holistic view of the subject matter. Focus groups provided a platform for dynamic interactions, revealing both collective and conflicting understandings, whilst interviews offered a space for personal reflection and depth that may not surface in a group setting.

Analysis

The interview and focus group transcripts were transcribed using transcription software and analysed separately using theoretical thematic analysis, informed by the analytic approach outlined by Braun and Clarke.[17] We applied both inductive and deductive coding, starting with two frameworks based on the discussion questions and adding codes as needed. This allowed us to identify key themes without bias. We then compared and integrated the thematic analysis findings from the interviews and focus groups, enhancing the validity of our results and highlighting both common and unique insights into online fraud experiences.

[17] Braun, V & Clarke V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*, 77-101