The view from the ground

Building a greater understanding of the impact of fraud and how the public view what policymakers should do about it

Richard Hyde
Peter Wilson

Kindly supported by

Nationwide Building Society

FIRST PUBLISHED BY

The Social Market Foundation, September 2023
Third Floor, 5-6 St Matthew Street, London, SW1P 2JT

THE SOCIAL MARKET FOUNDATION

The Foundation's main activity is to commission and publish original papers by independent academics and other experts on key topics in the economic and social fields, with a view to stimulating public discussion on the performance of markets and the social framework within which they operate. The Foundation is a registered charity (1000971) and a company limited by guarantee. It is independent of any political party or group and is funded predominantly through sponsorship of research and public policy debates. The views expressed in this publication are those of the authors, and these do not necessarily reflect the views of the Social Market Foundation.

CONTENTS

ACKNOWLEDGEMENTS

This report would not have been possible without the partnership of Nationwide Building Society and in particular Guy Bilgorri (Lead Policy and Public Affairs Manager) and Sophie Lomax (Policy and Public Affairs Manager) who led on the project from the Nationwide side and were a constant source of help and advice. In addition, SMF would like to thank:

- The experts who participated in the fraud roundtable, in July 2023.
- The 2,670 members of the public that took part in the two surveys: one representative sample of the UK adult population and the second of UK-based fraud victims.
- Adam Drummond and Calum Weir at Opinium for their help in designing the survey, managing it in the field and providing the SMF with the data and various data tables.
- The ten members of the public who gave SMF an hour of their time for semi-structure din-depth interviews on the issue of fraud and to the seven in particular who had been victims of fraud in the preceding three years.
- Zeki Dolen and Richa Kapoor, SMF's Events and Communications Intern and Impact Officer respectively, for their proofreading of drafts of the report, their work on the three diagrams and designing and formatting the final report.

This report could not have been researched, produced and published without the contributions of all those above.

ABOUT THE AUTHORS

Richard Hyde

Richard joined the SMF in August 2019 as Senior Researcher. Before joining he was a Senior Policy Advisor at FSB (Federation of Small Businesses) with responsibility for a diverse range of small business policy issues, including the small business regulatory environment, data and cyber security, crime and civil justice. Prior to FSB, Richard was a Policy Officer at the Law Society of England and Wales. He has also held policy and research roles at Which? and the Small Business Research Centre (SBRC) at Kingston University.

Richard holds an LLM in Law from the University of London and an MA in Global Political Economy from the University of Hull.

Peter Wilson

Peter Wilson is a Senior Researcher in the Education and Skills team at Policy Connect, working with the All-Party Parliamentary Group for Skills, Careers & Employment, the Skills Commission, and the Higher Education Commission.

Peter was with the SMF in February and March 2023 and, although he is no longer involved with the SMF, he contributed in numerous important ways to the development of this report while he was. He carried out extensive desk research into the existing evidence base on fraud and the nature of victimisation, as well as designing much of the two surveys, which this paper focuses upon.

ABOUT THIS REPORT

This report is based on evidence collected from a range of sources. These include:

- An SMF-convened expert roundtable on fraud. Participants included representatives from the financial services industry, digital services providers, the telecoms sector, relevant Government departments and regulators, consumer and business groups and leading academics.
- Two surveys. The first, a nationally representative survey of more than 2,000 UK adults. The second a specific survey of more than 500 British people who were fraud victims in the period 2020 to 2023. Both surveys were in the field between late April and early May 2023.
- In-depth, semi-structured interviews with 10 members of the UK public from a wide range of different earnings cohorts, working in a variety of occupations and spanning the adult age spectrum i.e. participants included people in their twenties through to people in their seventies. Seven interviewees were recent fraud victims and three were not. The latter acted as a small control group and met the criteria of being of average age and on average incomes.
- The primary research was supported by desk research into the existing stock of academic and grey literature on fraud.

FOREWORD FROM THE SPONSOR

By Jim Winters, Director of Economic Crime at Nationwide Building Society

A day rarely passes where we don't hear a tragic story of someone being defrauded or scammed out of their hard-earned money, often their life savings. The interim report, "*Fraudemic: Adding to the evidence base on the scale and impact of fraud on the UK",* published in July, showed that the economic and social cost of fraud in 2021-22 could be as high as £12.8 billion.

The bad news is this trajectory will almost certainly continue if the panoply of organisations involved in the journey doesn't wake up and work together to snuff it out rather than papering over the cracks.

This is why we have worked with SMF as we believe that it is only through strong evidence that we can convince all those involved in the fraud ecosystem to take the steps required to come together. If we all understand the harm that is caused, and the steps that the public are happy for us to take, then we can design the right interventions.

We believe this report is a call to action to work collectively. The criminals may be more fleet of foot than big business on an individual level but we can beat them through a consistent, comprehensive and collaborative approach. Put simply, big tech, social media and telecoms must play their part to help block and prevent crimes from taking place. Fake adverts on social media, spoofed messages and scam calls can and must be cut off at the pass. Currently, financial services continue to bear the brunt of responsibility, if only because we are the last stop in the journey, while law enforcement isn't set up to tackle these crimes. While we will, of course, continue to reimburse those who have their money taken through no fault of their own, it is not a means to an end.

It is very much open season for fraud and scams, despite crooks leaving a trail of breadcrumbs across the platforms they use. It goes unchallenged because there's a significant gap when it comes to sharing data and information between organisations. We are not joining the dots because we are not sharing the responsibility and resolve.

Focussing on individual fraudsters is an exercise in tail-chasing. The only way to starve these networks of oxygen is to tackle the criminal kingpins at their core. It is why Nationwide is calling for the creation of a central 'hub' that brings together multiple industries – from big tech and social media to telecoms and financial services – alongside government and law enforcement. The impact of the collective talent within these sectors would be seismic in stamping out scams.

A hive mind is needed to put in place the barriers and defences that prevent fraud and scams from occurring in the first place. Such an approach can only succeed if it is truly independent, demands collaboration and has the necessary legal framework behind it to enable data sharing.

We are open to helping fund a truly collaborative effort and, subject to a change in legislation by government, could use the money seized from criminals by banks and

building societies to do that. Better that this money is put to positive use than it sitting dormant in an account.

Without such a joined-up approach, we risk the wheels spinning on this issue indefinitely, with alternative remedial options including slowing payments down. Not only would this fail to prevent economic crime from taking place, but it would delay billions of legitimate payments on a daily basis. Consumers deserve better protection but it shouldn't come at the expense of convenience.

We hope this report provides the inspiration to join us and tackle fraud once and for all.

EXECUTIVE SUMMARY

The fraud challenge

- Fraud against individuals in 2021-22 cost the UK around £12.8 billion. Around four in ten crimes committed against the British population are frauds. Polling suggested that perhaps as much as 9% of people in the UK were victims in 2021-22.
- Despite the scale of fraud and the substantial detriment, political debates over crime often ignore the fraud threat. There are many reasons for this, including a lack of a detailed understanding of the fraud problem among decision-makers. Fraud is also a less visible crime than many other types. Failing to recognise the enormity of the fraud issue will help ensure it persists.

The fraud evidence deficit

- There has been a substantial and long-running fraud evidence deficit.
- The evidence deficit has contributed to the under-prioritisation of fraud. At the same time, under-prioritisation has resulted in insufficient interest in building up the evidence base about the true scale and impact of fraud.
- Key contributors to this situation include under-reporting by victims and a limited research effort into understanding the fraud problem.
- However, the scale of fraud is now becoming hard to avoid, even as the evidence deficit continues. Yet, the latter needs to be closed if the fraud epidemic is going to be tackled effectively.

The impact of fraud on victims' economic circumstances

- Part of the evidence deficit involves a lack of understanding about fraud's true impact on victims. In our survey of victims, nearly two-thirds said their economic circumstances were impacted negatively to a "moderate" or "major" degree, by the most recent incident of fraud they suffered.
- Those on lower incomes (i.e. earning £20,000 or less a year) reported more often than respondents in higher income brackets that their direct financial losses as a result of fraud had a "major impact" on their economic situation (43%).
- Pensioners were the most likely to report fraud as having a "major" negative impact on their economic circumstances (38%).
- Female victims (38%) more frequently reported "major" negative impacts on their economic circumstances than men (25%).

The wider impacts of fraud

- For many victims fraud also generates considerable negative second-round effects. These can include detrimental consequences for mental and physical health, victim's relationships and debt levels, among others.
- Victims that most often experienced at least one of the fraud second-round effects were those with annual incomes of £20,000 or below (82%), and those in the £60,001 to £80,000 bracket (82%).
- Victims aged between 18 and 34 were the most likely to report experiencing at least one second-round effect (79%).
- Female victims most often suffered from one or more of the wider impacts as a result of the most recent fraud they were subject to (75%) compared to men (65%).

The reimbursement process can make the impact of fraud victimisation worse

- Among the fraud victims that get their direct financial losses reimbursed, a substantial minority (38%) described the reimbursement process they went through as "somewhat difficult" or "very difficult". More than 1 in 5 (22%) stated that it was "very difficult".
- A difficult reimbursement process amidst dealing with the wider fallout from being the fraud victim can only add to the challenges associated with victimisation. Consequently, consumers that have such an experience are more likely to seek an alternative. Evidence from in-depth interviews with fraud victims illustrated the risk.

Fraud as a collective action problem

- To tackle fraud against individuals that is perpetrated at the current scale and with increasing sophistication, cooperation between the organisations in the "fraud chain", between departments and agencies in the public sphere and between the public and private sectors is needed. However, a number of obstacles hinder this cooperation.
- Among organisations in the "fraud chain", coordinated implementation of counter-fraud measures on the scale needed is hindered by:
    - The considerable costs of investing in the kinds of measures that will be effective.
    - Information barriers that make it difficult for firms in the "fraud chain" to understand, anticipate and deal with incidents of fraud.
- Many of the firms in the "fraud chain" suffer few, if any, costs as a result of the fraud that is propagated across their services. This means there is little incentive to prioritise taking steps to deal with it. The exceptions are firms providing payment services that are required to reimburse defrauded customers.

- The disjointed public sector counter-fraud landscape suffers from similar cost and information obstacles as the entities in the "fraud chain". Further, the departments and agencies that fail to effectively deal with fraud against private individuals rarely bear any of the costs of not doing so either. Consequently, the impetus for effective action is often lacking in the public sector, too.

The public's views on key counter-fraud policy debates

Reimbursement and liability

- The public overwhelmingly say there should be some degree of reimbursement in all fraud victimisation circumstances, but support for reimbursement in full is more conditional. 73% of the UK adult population were in favour of full reimbursement where the victim plays no role in the fraud, but this fell to 43% in cases where the victim enables the fraud. Among victims, full reimbursement support fell from 65% to 48% of respondents where the victim had a role in the fraud.
- Around 6 in 10 of the UK adult population were content to see liability for reimbursement shared across both the "holding" and "receiving" institutions within the payments system, as the Payment Systems Regulator (PSR) currently proposes. Further, 57% would support reimbursement liability placed upon the digital services providers whose services propagate much of the fraud that is committed and 46% believed that telecoms networks should be liable too. While similar proportions of fraud victims supported liability being borne by the "holding" and "receiving" institutions and digital services providers, a greater proportion (53%) were comfortable with telecoms networks also bearing some liability.

Increasing assurance in the payments system

- 70% of UK adults and 73% of fraud victims said they were happy to accept less convenient and slower payment and transfer services, if the corollary was reduced fraud risk.
- When asked about potential future developments resulting in greater assurance over payments and transfers and consequently much lower fraud risk, but also involving greater levels of "friction", 54% of the UK adult population and 64% of fraud victims were in favour.

Data sharing

- Data sharing is central to any effective fight back against fraud. However, the British public is, on balance, slightly more sceptical about policy tilting towards supporting greater data sharing (e.g. among financial institutions) over a focus on privacy and data security. In our nationally representative survey, 38% preferred policy to be more privacy and data security focused, while 31% had a data sharing preference. Notably, however, this reverses somewhat among fraud victims, among whom 40% have a data sharing policy preference while 34% support a privacy and data security stance.

- Among the British public with a view, there was an even split between those preferring a policy that gave law enforcement forces access to the data they need to pursue and disrupt fraudsters (36%) and those who preferred policy to lean more towards privacy and data security (36%). Among fraud victims the plurality favoured policy stances that enabled law enforcement to have the access to the data that they need (44% to 33%).

RECOMMENDATIONS

Reducing the evidence and reporting deficits

- **Recommendation 1**: Help improve politicians' and policymakers' understanding of the fraud threat with a specific multi-year, funded research programme.
- **Recommendation 2**: Reform fraud reporting to close the "reporting gap".

Reflecting the negative impacts of fraud on many victim's economic circumstances

- **Recommendation 3**: Under the auspices of the Consumer Duty, best reimbursement practices should be developed by the regulator, alongside a requirement for relevant financial institutions to systematically integrate access to official victim support services with the reporting and reimbursement of frauds.
- **Recommendation 4**: Develop a robust standard methodology for capturing more definitively the differential impact fraud has on a victim's economic circumstances and the wider psychological and social costs that can accrue.

Recognising the second order impacts of fraud victimisation in the criminal justice response including access to victim support services

- **Recommendation 5**: Toughen the sentencing of convicted fraudsters with reforms to the rules so that they take into account the wider impacts that victimisation has on individuals and also reflect the scale and cost of the current fraud epidemic.
- **Recommendation 6**: Establish an arrangement, similar to the Criminal Injuries Compensation Authority scheme for providing short-term financial support for victims of serious physical crimes, for vulnerable fraud victims.

Reducing the instances of difficult reimbursement processes to minimise unnecessary additional negative impacts from fraud

- **Recommendation 7**: Banks, building societies, credit card providers and other payment services firms that reimburse fraud victims should evaluate their reimbursement offers to ensure they meet high customer services standards, and they are especially sensitive to vulnerable customers who have been fraud victims.

Tackling the collective actions problems bedevilling the response to fraud from both the private and public sectors

- **Recommendation 8**: Start the process of developing a new set of policy proposals, for introduction in 2025, for improving the coordination of the fraud response by solving the collective action problems. These should include the measures proposed in recommendations 10, 11, 12 and 13.
- **Recommendation 9**: Prioritise the fraud threat with new investment in the capacity and capability of the law enforcement and criminal justice system.

Altering the balance of costs and benefits for organisations in the "fraud chain" with incentives to take more effective counter fraud action

- **Recommendation 10**: Continue with the PSR's reimbursement plans to share liability between "holding" and "receiving" institutions and prepare for a second phase, where other organisations in the "fraud chain" are made eligible for some of the costs of reimbursement.

Over-coming first mover disadvantages for financial institutions in the "fraud chain" by requiring more "frictions" in the payments system to help block fraud

- **Recommendation 11**: Introduce more "frictions" into the payments system by placing stronger obligations on financial services firms in the "fraud chain" to lower fraud risks for customers so that there is greater assurance over the legitimacy of payments and transfers, including the provenance of senders and receivers of payments and transfers.

Reducing the information obstacles with a step-change in data sharing along the "fraud chain" and between the public and private sectors

- **Recommendation 12**: Develop a more extensive and deeper data sharing arrangement across the organisations that are part of the "fraud chain" and between the private sector and appropriate parts of the public sector.
- **Recommendation 13**: Set-up a national ID protection service to help reduce the risk of ID related fraud.

CHAPTER ONE – INTRODUCTION

The UK's "fraudemic"

SMF's report, "*Fraudemic: Adding to the evidence base on the scale and impact of fraud on the UK*",[i] developed our understanding of the consequences of fraud.[1] It estimated that in 2021-22, fraud targeted at individuals cost society around £12.8 billion.[2]

The paper also showed that for nearly a third of those who became victims of fraud between 2020 and 2023, the most recent instance they experienced had a "major" impact on their economic situation at the time. Further, it exposed how the impacts of fraud are not confined to direct financial losses for most victims. There are a wider set of negative consequences that accrue, that are much more difficult to quantify.[3] They ranged from mental and physical health issues to debt and relationship problems.

Fraud remains under-prioritised despite its scale and impact

Although there are various estimates of the total cost of fraud to the country,[ii] it is undoubtedly the case that it is the most prevalent crime committed against the population of the UK. Nevertheless, political debates over crime statistics often ignore fraud.[4] There are many reasons for this, including a lack of a detailed understanding among politicians and policymakers (see more on this in Chapter Two). It is also a less visible crime than many others. The impacts are typically widely distributed across a geographically dispersed victim population. In addition, action against it is largely invisible, with little public profile. Consequently, it does not have the same political weight as crime that can be tackled by putting more 'bobbies on the beat'.

Nevertheless, all crime should matter. Just as we ought to investigate more of the thefts that are perpetrated,[5] the same is true of fraud. The latter certainly matters to those who have been victims and who will be future victims. In England and Wales for example, 6.5% of adults were the victim of fraud in the year up to September 2022.[6] An earlier poll of the UK population suggested that between March 2021 and February 2022, perhaps as many as 9% of Britons suffered at the hands of fraudsters.[7]

[i] From here on the report will be referred to as: "Fraudemic".

[ii] The most recent Annual Fraud Indicator (AFI) analysis by Robinson, Tickner, Button and Gee suggests that the total cost of fraud to the UK, including the cost to the public and private sectors as well as that committed against individuals, is in the region of £219 billion. Source: Tim Robinson et al., 'Annual Fraud Indicator 2023', 2023, https://www.crowe.com/uk/insights/annual-fraud-indicator.

The two parts of this report

More evidence on the impact of fraud on the people of the UK

Chapters Two to Five make up the first part of this report. These look in more detail at how the impacts of the frauds committed against individuals are distributed across different demographic groups in the UK population (e.g. age, income, occupation and sex) and help further add to the evidence base on the impact of fraud beyond its direct financial costs. Chapter Five touches upon the issue of the extent to which the reimbursement process could, for some victims, be compounding the challenges they already face when they have suffered from a fraud. The data presented comes from a survey of fraud victims and builds upon the findings presented in "Fraudemic".[iii] The qualitative data that is also described is sourced from in-depth interviews with fraud victims.[iv]

The debate over the best policy response to the fraud epidemic

The second part of the report consists of Chapters Six to Nine. By first identifying the collective action problems that bedevil the response to fraud, these chapters go on to explore some of the most salient issues in the policy debate fraud around frauds perpetrated against individuals. These chapters utilise the evidence gathered from an SMF-convened expert roundtable and the results of polling of both the UK adult population and fraud victims specifically. In addition, it uses qualitative evidence from in-depth interviews with fraud victims to better understand in more detail some of the nuances in the public opinion findings.

[iii] See more on the two survey samples in the "About this report" section.
[iv] See more on the in-depth interviews in the "About this report" section.

CHAPTER TWO – THE FRAUD EVIDENCE DEFICIT

The long-running under-prioritisation of fraud is beginning to be recognised as a mistake

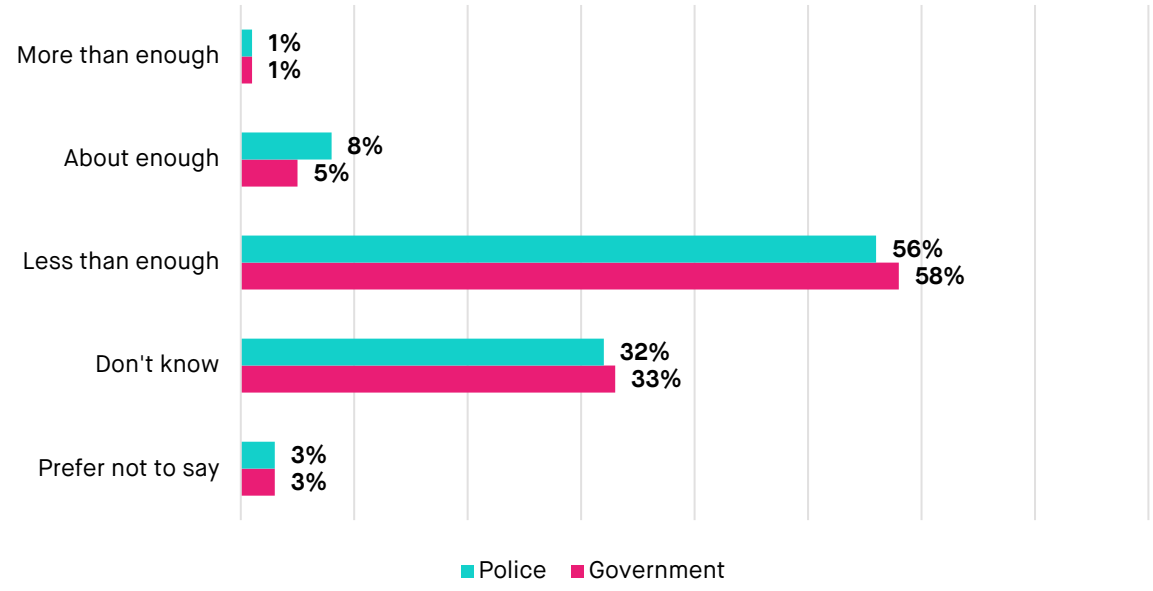
Political and policymaking opinion

The long-standing under-prioritisation of fraud and the consequences of that, is being highlighted more and more. Recent reports from the National Audit Office (NAO),[8] Public Accounts Committee (PAC),[9] the Home Affairs Select Committee[10] and the House of Lords Committee on the Fraud Act 2006 and Digital Fraud are evidence of this.[11] However, as noted in Chapter One, fraud still does not have the salience that other types of crime have, despite its prevalence.

Public opinion

The British public also believe that government and the police are under-prioritising fraud. As Figure 1 illustrates, less than 1 in 10 agree that the government and police are "doing enough" or "more than enough" on fraud.[12]

Figure 1: Public views about the current effort against fraud by the Government and the police, 2022



Source: Electoral Calculus poll of the UK adult public

The new fraud strategy

The recent fraud strategy may herald the beginnings of a shift in perspectives in government. It signalled the development of a number of initiatives which should help against the fraud epidemic if implemented effectively.[v] However, as many pointed out at the time of publication, it fell short of being a strategy with sufficient ambition (and a concomitant resource commitment) to match the scale of the problem (see Annex I for more on the Government's recent fraud strategy).[13] The overall timidity of the strategy helps reinforce suspicions that fraud is still far from being a first tier priority.

The evidence deficit as a constraint on action

There are many reasons behind the continued under-prioritisation of fraud. Some were touched upon in Chapter One. Among them was the knowledge deficit amongst politicians, policymakers, law enforcement and others. That knowledge deficit is, in turn, a consequence of a fraud evidence deficit.[vi]

The fraud evidence deficit is perhaps most obvious in the absence of a truly accurate picture (across a sustained period of time) of the real scale, nature and cost of fraud committed against individuals in the UK. The failure to collect accurate statistics on fraud for many years is emblematic of this evidence deficit (see Box 1 for more on the under-recording challenge). Problems with the evidence base are also reflected in the wide variation in the periodic estimates of the cost of fraud to the UK.[14]

In addition, relatively few efforts have been made to understand and evaluate the non-quantifiable (i.e. psychological and social) costs of fraud.[15] There has also been insufficient criminological research into the characteristics, motivations and methods of fraudsters, including the role of technology and enablers.[16] Nor is much known about why some people fall victim to frauds but others do not.[17] The interconnection of fraud with other serious crimes is also inadequately understood. Equally important is the gap in knowledge about the nature and efficacy of the law enforcement and criminal justice response to fraud. [18] [19] [vii]

[v] In a 2019 review of the police response to fraud, HM Inspectorate of Constabulary (HMICFRS) described the previous 2006 fraud review and 2011 strategy as "forgotten". Source: Alan Doig and Michael Levi, 'Editorial: The Dynamics of the Fight against Fraud and Bribery—Reflections on Core Issues in This PMM Theme', Public Money & Management 40, no. 5 (2020): 343–48, https://doi.org/10.1080/09540962.2020.1752547.

[vi] With regard to economic crime more widely, the Home Office itself has admitted to the existence of an evidence deficit. Source: 'Economic Crime Research Strategy: Home Office Research Priorities', GOV.UK, 2021, https://www.gov.uk/government/publications/economic-crime-research-strategy-home-office-research-priorities/economic-crime-research-strategy-home-office-research-priorities.

[vii] A study published 2010 estimated that a 1% increase in the detection rate charge rate led to a 14% reduction in frauds per 100,000 of the English and Welsh population. There are questions as to whether this relationship still holds and if so, what are the implications of it for what law enforcement could achieve against fraud? Source: [vii] Siddhartha Bandyopadhyay, Samrat Bhattacharya, and Lu Han, 'Determinants of Violent and Property Crimes in England and Wales:

Box 1: Barriers that have resulted in the under-recording of fraud

The recording of fraud crime statistics has been a long running problem. It wasn't until 2016 for example, that the Crime Survey of England and Wales (CSEW) started to capture fraud data, despite it being a crime of significance for some time.[20] [viii] As a result all there was to rely upon was Action Fraud and Police Recorded Crime data, which suffered from the considerable under-reporting of fraud.

Research suggests the reasons for under-reporting include:

- A proportion of fraud is undetected by individuals and their banks. One study showed that 40% of interviewed victims had been unaware of a fraud until contacted by an official organisation.[21]
- A lack of knowledge about Action Fraud;[22] a belief that other authorities such as banks will report incidents; a lack of interest in reporting if the losses are dealt with by the victim's bank or credit card provider, etc;[23] perceptions that a small loss is too trivial to report or not worth the effort;[24] a lack of faith that the authorities will help the victim or get their money back; feelings of embarrassment or shame at being defrauded is also occasionally mentioned[25] [26]; and difficulties identifying and accessing reporting mechanisms due to disability.[ix]
- A view of fraud that it is primarily a civil matter or a victimless crime.[27] [28]

In in-depth interviews with fraud victims, participants revealed the reasons why they did not report their victimisation to the police. They echoed many of the points described in Box 1. For example, one interviewee said:

> *"...what could they [the police] do? They're busy, they're not going to do worry about something simple like that. Or they just give the impression...they say you should 'know better'".*

Another interviewee reflected on the fact that as soon as the credit card company said they were dealing with their defrauding, they felt no need to report it elsewhere:[29]

A Panel Data Analysis', SSRN Scholarly Paper (Rochester, NY, 13 October 2010), https://doi.org/10.2139/ssrn.1691801.

[viii] It should be noted that the ONS does attempt to correct for underreporting by measuring the amount of fraud unreported by the people interviewed in crime surveys.

[ix] The Code of Practice for Victims of Crime sets out what information and other support victims might expect at different stages of the process e.g. from reporting a crime through giving evidence in court to the aftermath. However, there appears to be little guaranteeing vulnerable victims in general and disabled victims in particular, who might have trouble identifying what they need to do if they have been a victim and in accessing reporting mechanisms, access to useful information and the availability of avenues for easily reporting frauds. Source: Ministry of Justice, 'The Code of Practice for Victims of Crime in England and Wales and Supporting Public Information Materials', GOV.UK, 5 September 2023, https://www.gov.uk/government/publications/the-code-of-practice-for-victims-of-crime.

> *"...because...I was made aware of the fraud through a...statement from my credit card company, so the first point of contact really, is to call them...if they hadn't been helpful or hadn't suggested that they would do an investigation, then yeah, the next point of contact would have been to...go to the police. But that was it really, it's just obviously, that you leave it in their hands..."*.

A third described their attempt to report the fraud they experienced as a "tennis match":

> *"...they needed...evidence from the police...the police said, 'no', it's the bank's responsibility...I was just going back and forth between the two...it ended up actually that I didn't get the money back...because they just didn't believe me...and I couldn't get the help from the police..."*.

Reporting fraud was one of the topics touched upon in the SMF-convened expert roundtable that helps inform this report. A contributor argued that a key reason behind it is the nature of the process i.e. having to report a potentially traumatic incident multiple times to different entities. They suggested that a "one-stop-shop" or "single window" would likely increase reporting levels:

> *"...being able to tell somebody once...provide all the information once, and if somebody then wanted to follow up...that would [be]...better...If you've ever had to register a death...there is a tell us once service...and that involves...a lot of sensitive data...It must be possible"*.

A strong evidence base is needed on which to build a more effective response to fraud

The under-prioritisation has meant a lack of interest in building up the fraud evidence base. A vicious circle has been created where evidential neglect has then enabled fraud to stay a relatively low priority.

Therefore, building out the evidence base is important to improving the response to fraud. Without understanding the problem, it is very difficult to devise and implement effective strategies and allocate appropriate resources to it.[30] Therefore, a priority should be to change this situation.[31]

Implications for politicians and policymakers

Politicians and policymakers who are serious about tackling fraud need to urgently build a more extensive and detailed picture of the many facets of the fraud problem. They should support more efforts to research fraud more extensively and improve current reporting levels.

Recommendation 1: Help improve politicians' and policymakers' understanding of the fraud threat with a specific multi-year, funded research programme

To help close the knowledge gaps that exist about the fraud threat and in particular its extent and impact on victims and the economy, the motivations and characteristics of fraudsters and their criminal operations and the efficacy of law enforcement and criminal justice response, as part of the Home Office's existing commitment to tackling the economic crime evidence deficit a specific and extensive programme of research on fraud should be commissioned. It should be co-funded by the industries that have a substantial role in the "fraud chain". It should be a rolling programme of research, which not only produces an accurate and detailed picture of the fraud threat and its consequences for people and the economy, but also aims to identify best counter-fraud policy and practices from the UK and around the world and develop performance benchmarks against which progress can be measured.

Recommendation 2: Reform fraud reporting to minimise the "reporting gap"

The reporting of fraud is a vital source of knowledge about the fraud threat. It is particularly important for law enforcement. To help close the "reporting gap" victims should only have to report fraud once. This will dramatically reduce the problem of victim reporting attrition, provide law enforcement and policymakers with the most comprehensive picture of fraud victimisation, and consequently ensure that the fraud response across the public and private sector can be built upon an accurate understanding of the situation.

To implement this, all organisations whose customers report a fraud to it should be obligated, in-turn, to report that fraud to Action Fraud (and in time its replacement) in a timely manner. Action fraud should then follow-up with each victim directly. Further, if a victim reports the fraud to Action Fraud, the latter should pass those details onto the relevant financial institution with the latter required to reach out proactively to the defrauded customer if they have not already done so (e.g. where the fraud was reported separately to them).

In addition, if relevant financial institutions are to become more prominent parts of the reporting landscape, the regulator and Action Fraud should work together with appropriate financial services providers to ensure the reporting needs of vulnerable victims in particular, are suitably catered for.

Over time, if the broader data sharing challenge is overcome sufficiently effectively (see Recommendation 12 in this report) the "reporting gap" will likely largely fall away as such reporting will be a routine part of more extensive and deeper data sharing arrangements.

CHAPTER THREE – THE IMPACT OF FRAUD ON VICTIMS' ECONOMIC CIRCUMSTANCES

A significant part of the fraud evidence deficit is around the impact on victims. A fuller understanding of the latter will strengthen the argument for investing in a better response to fraud because the consequences of victimisation can be significant for many but are often hard to quantify. Building on the report "Fraudemic", this chapter outlines more detailed findings about which parts of the population suffer the most negative impact on their economic circumstances, as a result of fraud .

The impact of fraud on the economic circumstances of victims

The real impact of fraud is dependent on a victim's economic circumstances

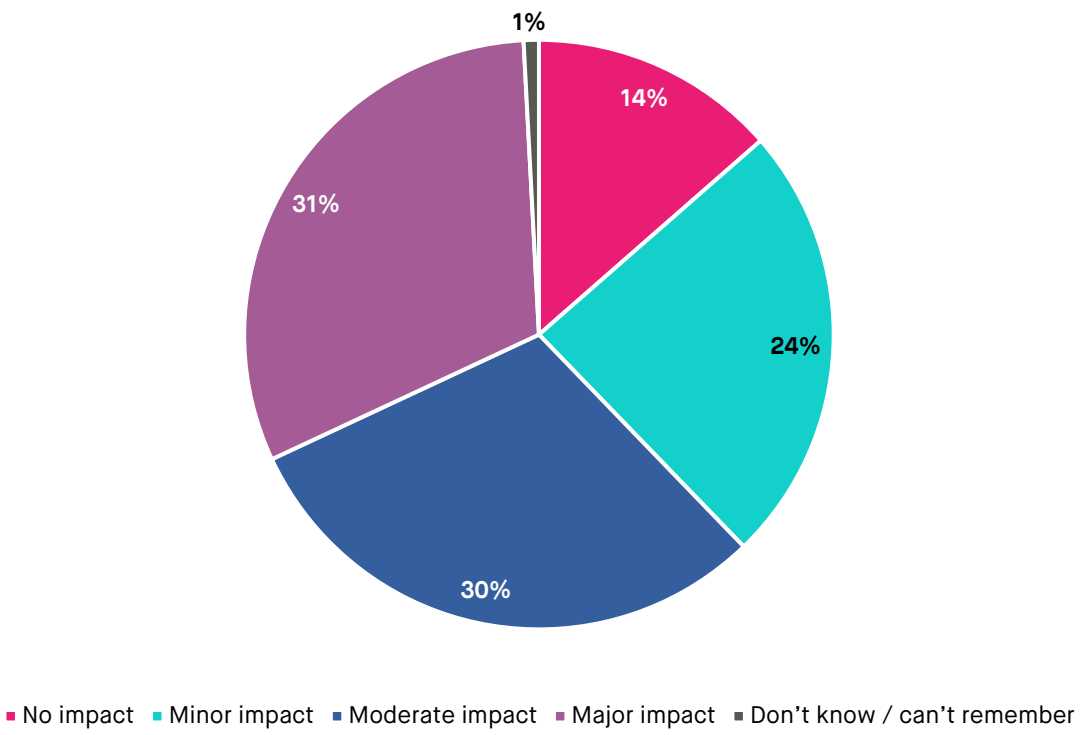
In some instances, the direct financial loss from being a victim of fraud can cause substantial financial problems, e.g. where the fraud has resulted in a victim losing their pension or home.[32] In such examples, the impact on the economic circumstances of the victim are clear to any observer. Nevertheless, most losses suffered by victims are not that large.[33]

That said, as "Fraudemic" showed, the average direct financial loss from frauds committed between 2020 and 2023 was just under £3,000 – a not inconsequential sum.[34] However, to understand the real impact on a victim's economic situation, such losses need to be seen in relative terms. A small direct financial loss for someone on a low income and who struggles with cash flow can be much more significant to them, than a nominally larger loss for someone who is well off.[35]

Most fraud victims experience moderate or major negative impacts to their economic situation

Most fraud victims suffered at least some negative impact, with only 14% experiencing no consequences for their economic situation (see Figure 2).

Figure 2: The severity of the impact of fraud victimisation on an individual's economic situation, 2020-2023



Source: Opinium survey of fraud victims

Figure 2 shows that, overall, nearly two-thirds said their economic circumstances were impacted negatively to either a "moderate" or "major" degree by the most recent fraud they experienced. More specifically, 30% suffered a "moderate" and 31% a "major" impact on their economic circumstances.

One of the victims interviewed in-depth for this report described how, as a middle-aged individual on an average income, they lost a sizeable amount of money from a pot of savings due to an investment fraud:

> *"It didn't completely drain my account. But…I had probably £500 left from…an account that was for a rainy day… for instance, you know, if the boiler goes or something else that you're not expecting to happen…that's a big dent…it did have a financial impact on me".*

The big impact on the interviewee's financial circumstances came not from the overall amount lost but because they lost the majority of a pot of savings that was supposed to be there when needed. The fraud resulted in the loss of a degree of economic security the savings had provided.

The severity of the economic impact of fraud on victims in different income groups

Figure 3 shows that the relative impact on a fraud victim's economic situation varies across income cohorts. Those on lower incomes, i.e. earning £20,000 or less a year, reported most often that the direct financial losses they experienced from the most recent fraud suffered had a "major impact" on their economic situation (43%).

Figure 3: Severity of the economic impact of being a victim of fraud among people in different income groups, 2020 – 2023

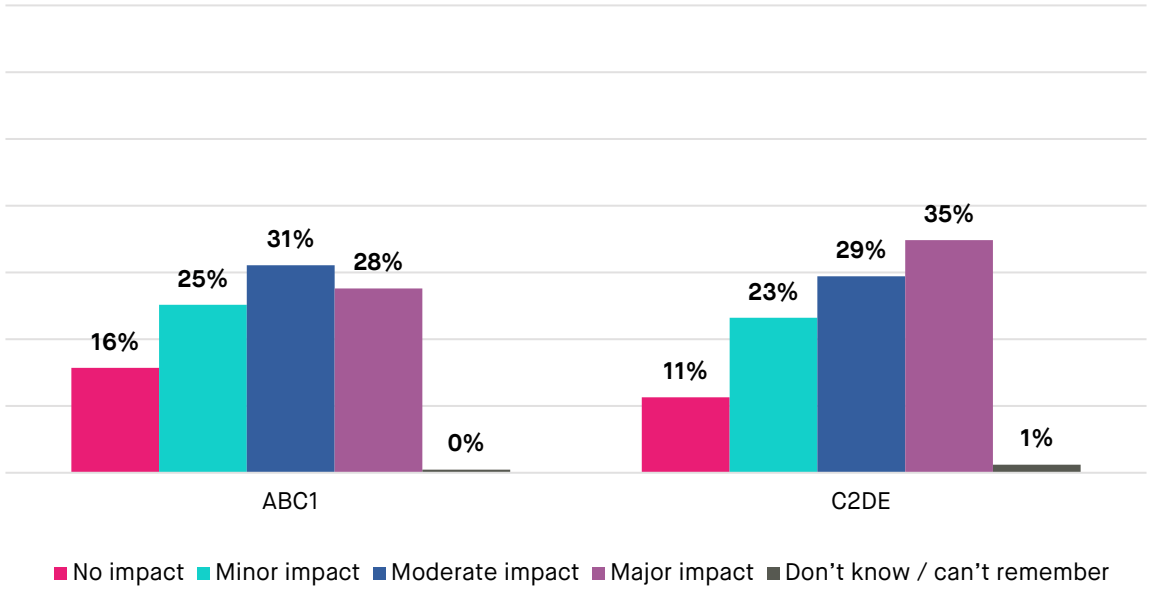
Source: Opinium survey of fraud victims

Further, respondents in the lowest income bracket were, overall, more likely to report that when they were defrauded it had either a "moderate" or "major" impact on their economic circumstances (71%). Only 9% of victims in this income group said that the most recent fraud had "no impact".

The impact of fraud on the economic circumstances of victims across different occupation groupings

Closely related to annual income is occupation. Figure 4 illustrates how the severity of the impact on a victim's economic circumstances varies across occupation groupings. Broadly, the findings reinforce the picture painted in Figure 3 with a greater proportion of those in what tend to be lower income jobs experiencing more severe impacts on their economic circumstances. A larger portion of those in the typically higher paying occupations reported that fraud had the least severe impacts.

Figure 4: Occupational groupings and the impact of fraud on a victim's economic circumstances, 2020-23



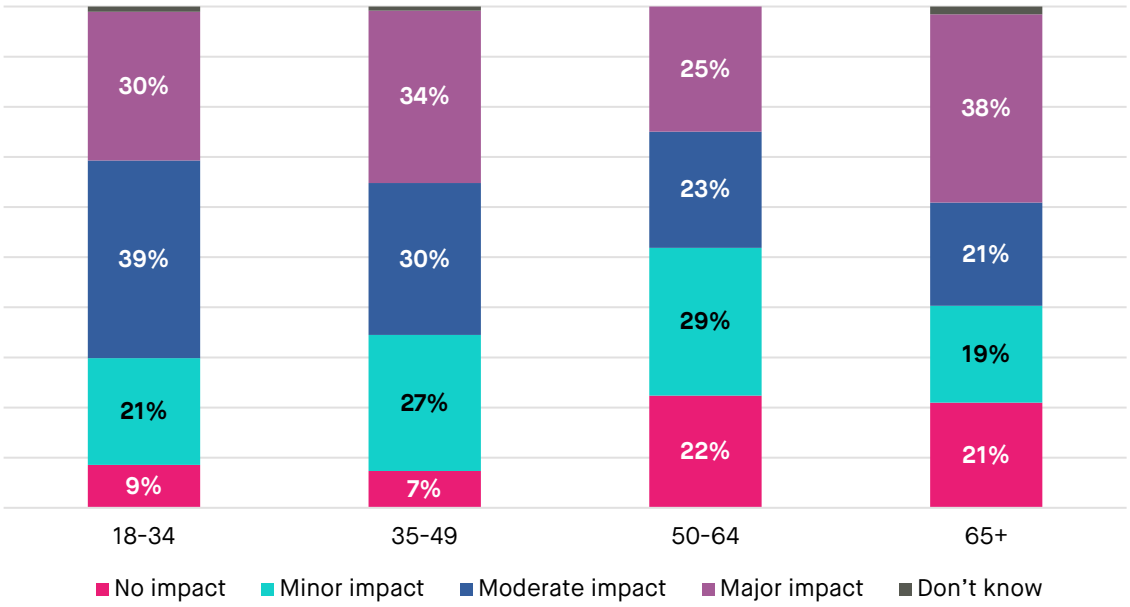
Source: Opinium survey of fraud victims

- Overall, 64% of victims from C2, D and E categories reported that the most recent fraud they suffered from had a "moderate" or "major" impact on their economic circumstances, while 59% of A, B, C1s respondents reported the same. More than half of the 64% of C2, D and E respondents said that the impact was "major".
- 41% of A, B, C1s said the most recent fraud they had been subject to had a "minor" or "no" impact on their economic circumstances, compared to 34% of those in C2, D and E categories.

How the impact of a fraud on a victim's economic situation varies across age groups

Figure 5 indicates that pensioners are most likely to report being victims of a fraud that has a "major" impact on their economic circumstances (38%). Close behind were those victims in the 35–49 years of age cohort (34%). Notably, data presented in "Fraudemic" showed that victims in this age group tended to suffer the lowest direct financial loss on average.[36]

Figure 5: Severity of the economic impact of being a victim of fraud among people of different ages, 2020 – 2023



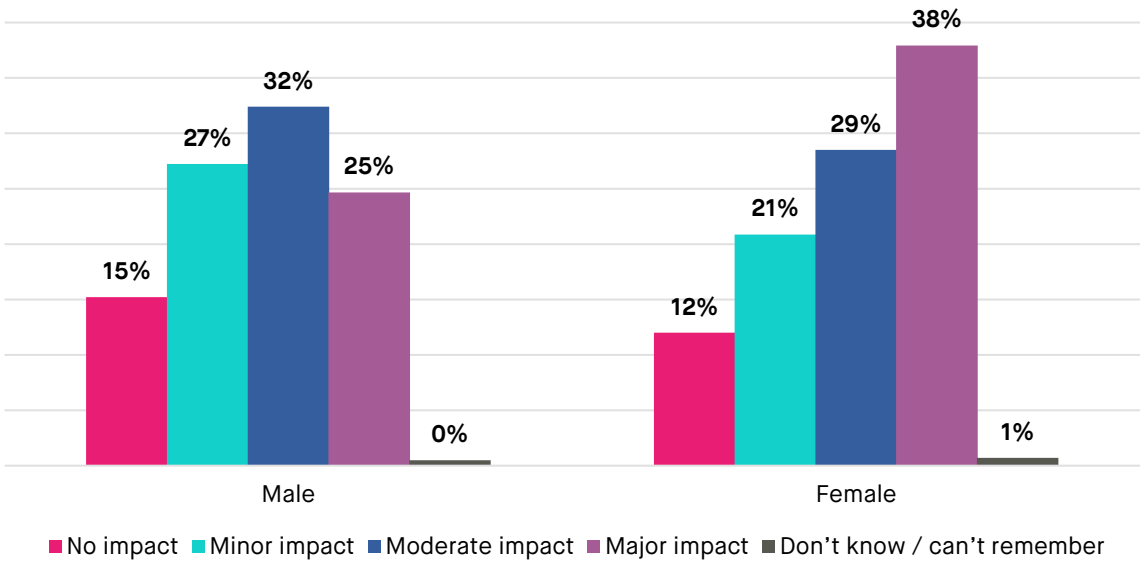
Source: Opinium survey of fraud victims

- Victims in the two youngest age groups (18-34 and 35-49) were the most likely to report that the fraud they were most recently a victim of had "major" or "moderate" impact on their economic situation, with 69% of the youngest victims saying this, and 64% of those aged 35-49. Further, victims in the same two youngest age cohorts, were the least likely to say their victimisation had "no impact".

How the impact of a fraud on the economic situation of men and women differs

Figure 6 shows that, in broad terms, fraud impacted women's economic circumstances negatively more often and more substantially than among men.

Figure 6: Severity of the economic impact on men and women of being a victim of fraud, 2020 – 2023



Source: Opinium survey of fraud victims

- Overall, 67% of women found that the last fraud that they suffered from resulted in either "moderate" or "major" negative impact on their economic circumstances. By contrast, 57% of male respondents said the same.
- More men than women described the impact of fraud on their economic situation as "minor" or having "no" negative impact (42% compared to 33%).

Implications for politicians and policymakers

The evidence set out in this chapter indicates that the financial impact of fraud on victims cannot be understood as just the direct financial losses incurred. There is a more complex context to consider, which varies across different cohorts within the fraud victim population. The implications of this for policy, include:

- Whether and how the differences in relative impacts might influence reimbursement best practice standards, in the context of the FCA's Consumer Duty. The latter requires financial institutions to be more sensitive to the circumstances of their customers.[37]
- More systematically integrating the fraud reporting and reimbursement services in relevant financial institutions with victim care provision, such as that offered by the National Economic Crime Victim Care Unit (NECVCU)[38] and Victim Support.[39]

Recommendation 3: Under the auspices of the Consumer Duty, best reimbursement practices should be developed by the regulator, alongside a requirement for relevant financial institutions to systematically integrate access to official victim support services with the reporting and reimbursement of frauds

The requirements of the FCA's Consumer Duty places additional responsibilities on financial services providers to take account of their customers capacities and circumstances. In the context of fraud, this should extend to the reporting reimbursement process, the handling of which by financial institutions should explicitly take account of the victim's characteristics and situation.[x] This should include a proactive approach towards helping victims access support services, including helping them access NECVCU or other relevant support services.

Married with the proposed for mandatory fraud reporting obligations (Recommendation 2), financial institutions should become the central conduit for fraud reporting and accessing help after victimisation. This would involve numerous financial services providers explicitly taking on a role with a very clear public benefit. In that vein, the Government should not shy away from providing direct support to reflect this.

[x] The Banking Protocol already sees many banks and building societies taking specific steps (e.g. through additional staff training) to take into account the particular circumstances of vulnerable and elderly customers who are at risk from fraud. Therefore, the precedent for developing additional support has been set and the principle could be extended to other times banks and building societies have occasion to interact with customers over a fraud e.g. the reimbursement process. Source: Chiara Cavaglieri, 'Bank Anti-Fraud Protections to Cover Telephone and Online Banking - Which? News', Which?, 11 September 2020, https://www.which.co.uk/news/article/bank-anti-fraud-protections-to-cover-telephone-and-online-banking-aJPKL7B7mwyj.

CHAPTER FOUR – THE WIDER IMPACTS OF FRAUD

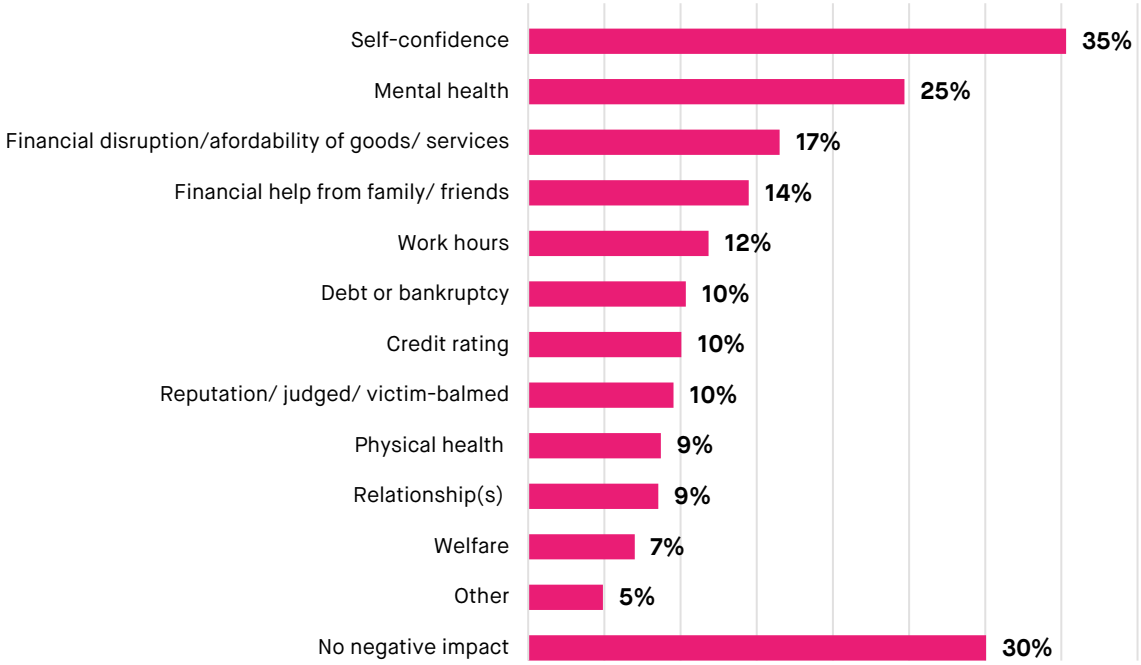
There is a small body of evidence that highlights some of the wider psychological and social consequences of fraud victimisation. [40] [41] [42] [43] These might be thought of as second-round effects. SMF's "Fraudemic" was able to add to this body of evidence by highlighting new survey data which showed how common these second round effects are.[44] This chapter builds on the data published in "Fraudemic" by illustrating how some of those wider costs are distributed across different demographic groups.[xi]

The consequences of fraud are much wider than the direct financial cost and the concomitant economic impact

How wider impacts are distributed across the UK fraud victim population

Figure 7 shows that, among those that were victims of fraud between 2020 and 2023, 70% suffered from at least one second round impact as a result of what they experienced.

Figure 7: The wider impacts of fraud victimisation, 2020-2023



Source: Opinium survey of fraud victims

[xi] Please note SMF did not ascertain from survey respondents whether they had any specific vulnerabilities such as a physical disability. We did not have the resources to capture all aspects of financial vulnerability in our research. However, we are aware that a personal vulnerability can be associated with financial vulnerability. Vulnerable individuals may be reliant on others to access banking services and consequently, they may be more at risk of financial abuse, which can include being defrauded. Source: Lending Standards Board, 'Access for d/Deaf Customers in Banking & Credit', LSB (blog), n.d., https://www.lendingstandardsboard.org.uk/resources/access-for-d-deaf-customers-in-banking-credit/.

In the in-depth interviews with fraud victims that help inform this report, one interviewee re-told their story of how they had been defrauded twice. Both began with ID theft. The first involved the victim's credit card details being stolen and used to buy products. The second saw the victim's personal details used to set-up fake online shopping accounts which the fraudsters used to buy goods with. They reported that the second incident in particular had caused considerable distress for them and their family beyond the direct financial impact:

> *...it was closer to home...it wasn't just money...it was my details, pretending to be me. That's not nice. That's not a nice thing to have...that causes a lot more anxiety and stress and disturbance...".*

Part of the stress was caused by the difficulty of proving they had been scammed and the length of time the problems generated by the fraudsters persisted for:

> *"...They didn't take my word for it... then it actually went to the debt collectors...that was worse...it was £1000...it was hard to get it back and prove it wasn't me...".*

> *"...six months...that was a long time...obviously you're asking the household, the older child, did you order it? I was doing a lot of thinking...I'm looking at him thinking, you did do it. And then...we're going to the oldest daughter, did you go and order stuff?...there..[were]...arguments in the house, to be honest...".*

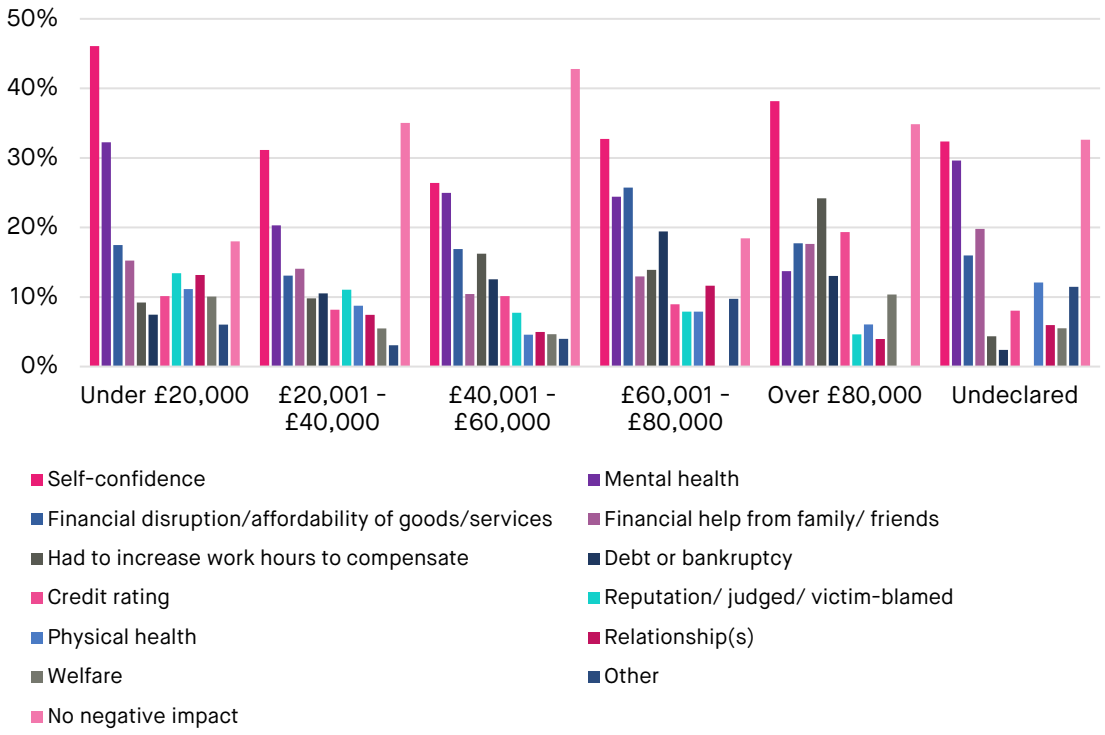
In addition to the interviewee having their privacy violated and the anxiety and stress of the disruption caused by the fraud, including the family tensions the situation generated, there was a further concern that they had, which stemmed from how easily such frauds were committed and therefore how vulnerable they might be again:

> *"...how easy to set it up in the first place...that is really worrying...".*

How wider impacts of fraud are spread across income groups

Figure 8 indicates how the wider impacts of fraud are distributed among victims in different income cohorts.

Figure 8: Distribution of the wider impacts of fraud victimisation across annual income groups, 2020 - 2023



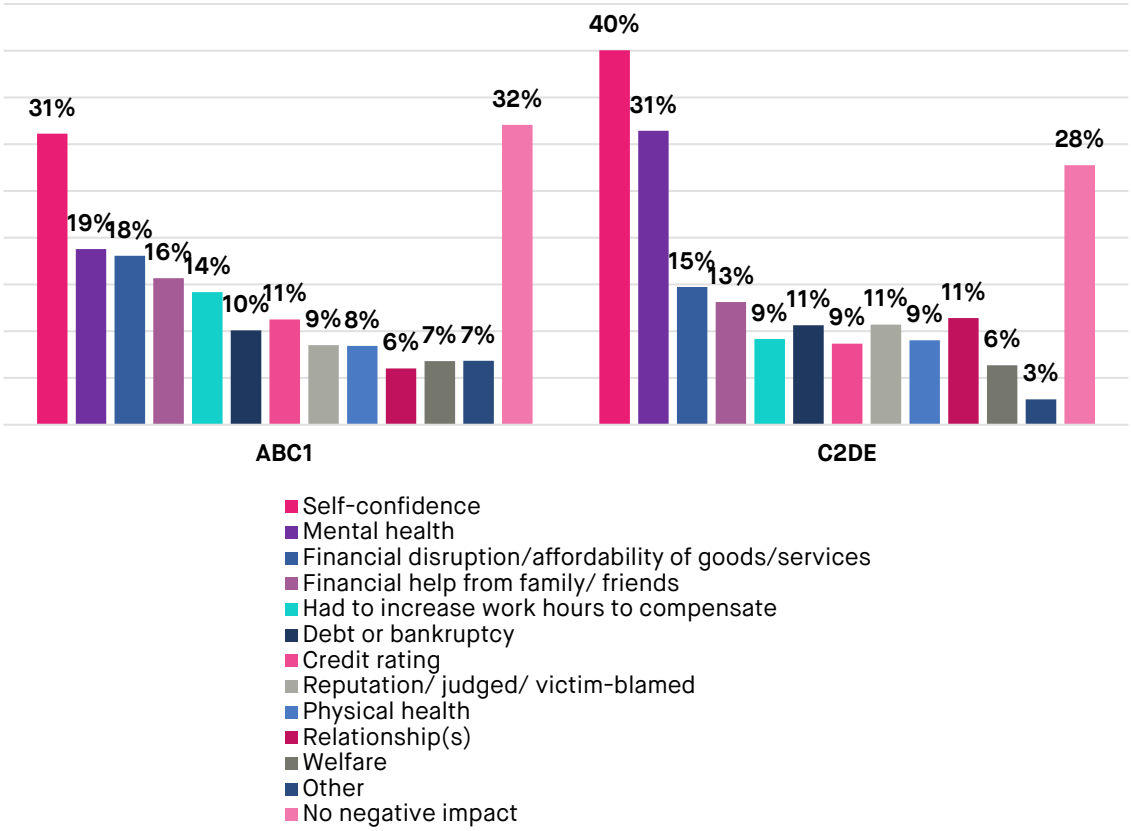
Source: Opinium survey of fraud victims

- Those most likely to report experiencing at least one of the wider impacts were those with annual incomes of £20,000 or below and victims in the £60,001 to £80,000 income group (both 82%), with those victims in the "£40,001 and £60,000" income bracket the least likely (57%).
- Victims in households earning £20,000 or less a year were the group that most commonly experienced a loss of self-confidence (46%) and mental health problems (32%) as a result of fraud.
- Respondents in the £60,001 - £80,000 income cohort were the group that most often reported the most recent fraud led to "financial disruption" (26%). Those in this same group were also the more likely than victims in other income cohorts to go into debt as a result of being subject to fraud (19%).

How the wider impacts of fraud are dispersed across different occupation groupings

Figure 9 shows the distribution of the wider impacts that many victims suffer from, as they vary across occupation groupings.

Figure 9: Occupational groupings and the instances of wider negative impacts as a result of fraud victimisation, 2020-23



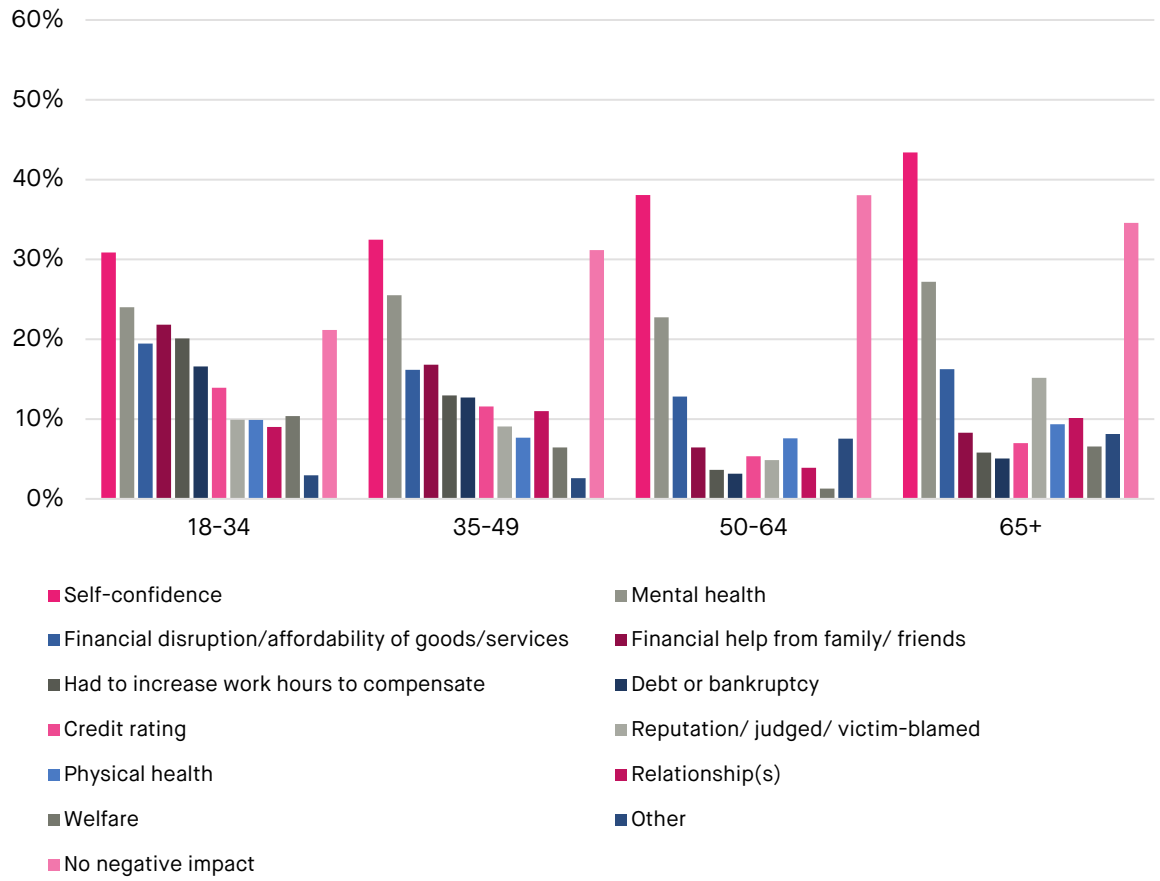
Source: Opinium survey of fraud victims

- Those fraud victim respondents in occupations that fall into the social classification categories C2, D and E were more likely to report suffering at least one wider negative impact (72%) as a result of the most recent experience of fraud than those in categories A, B and C1 (68%).
- Those in C2, D and E categories were also more likely to say they suffered a reduction in self-confidence (40%) and negative mental health effects (31%) than respondents in A, B and C1 categories (31% and 19% respectively). Those in the former circumstances more frequently reported detrimental impacts on relationships (11%) compared to survey participants in the A, B and C1 occupations (6%).

How the wider effects of fraud victimisation are spread across age cohorts

Figure 10 illustrates how the wider consequences experienced by fraud victims are spread across different age groups.

Figure 10: Age and prevalence of wider negative impacts as a result of being a victim of fraud, 2020 – 2023



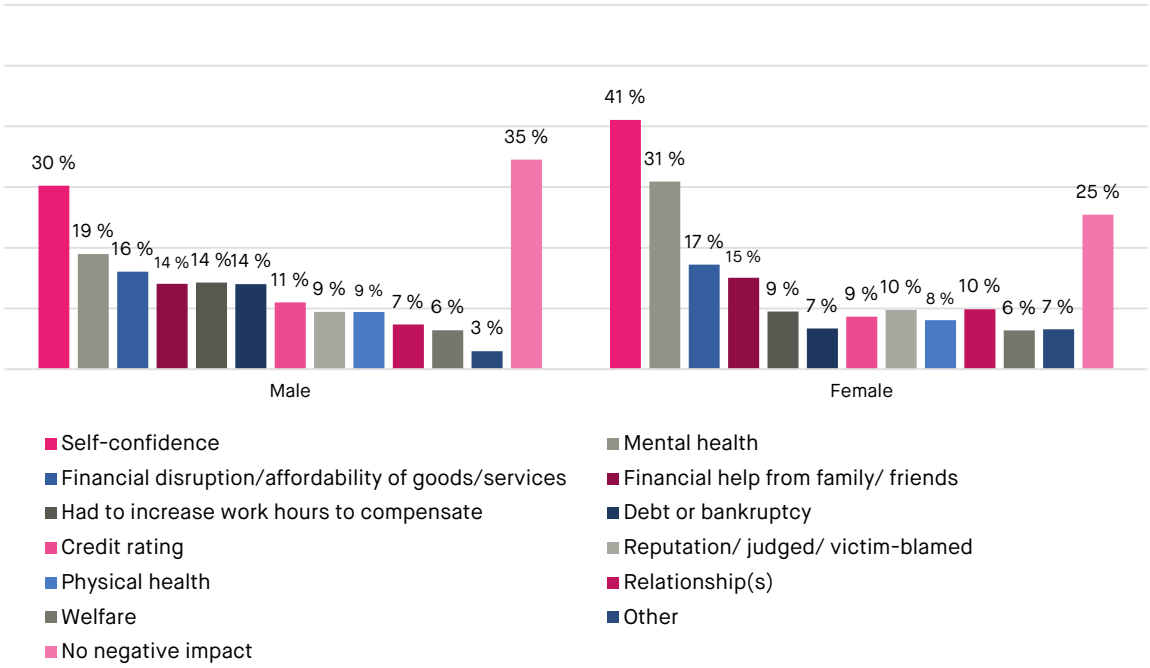
Source: Opinium survey of fraud victims

- Victims aged between 50 and 64 years, were the least likely to report having suffered from at least one of the wider consequences of being subject to fraud, with 62% experiencing one or more. Those aged 18–34 were the most likely to say they experienced at least one wider negative consequence (79%).
- A negative impact on self-confidence (43%) and mental health (27%) was cited most often by those aged 65 and over, as a result of the most recent incident of fraud that they had suffered from.
- The youngest victims (18-34) were the most likely to say that their situation resulted in them having to rely on help from family or friends (22%), increase their hours of work to compensate for the losses (20%) and incur debts (17%).

How the wider impacts of fraud are experienced by men and women

Figure 11 points out how the wider impacts of being a victim of fraud divide up between those of different sexes.

Figure 11: The incidence of wider negative impacts among men and women as a result of being a victim of fraud, 2020 – 2023



Source: Opinium survey of fraud victims

- More female victims said that they experienced one of the wider impacts as a result of the most recent fraud (75%), than male victims (65%).
- Women more frequently reported that fraud negatively impacted their self-confidence (41%) and mental health (31%), compared with 30% and 19% of men, respectively.
- More than twice as many men (14%) than women (7%) reported going into debt as a result of their most recent fraud victimisation experience.

Implications for politicians and policymakers

The data presented in this chapter illustrates that wider negative impacts are prevalent among fraud victims and that, in general terms, are particularly prevalent among those on the lowest incomes, the youngest and women victims. Although there is a wide spread across the whole victim population. Despite how common they are, these second order effects are not well understood and rarely factored into the debate about the impact of fraud on both the UK as-a-whole nor on individual victims.

Understanding that the consequences of fraud include these other aspects, is an important step towards filling the fraud evidence deficit. Further, a deeper and more complete understanding of the detriments generated by fraud, could feed through into justifying more robust policy in a number of areas, for example:

- A tougher sentencing regime for fraudsters.[45] Currently convicted fraudsters are widely seen as not being served with sufficiently strong punishments.[46] Consequently, the typical deterrent and incarceration effects of custodial sentences for fraudsters are small.[47] [xii] Further, inadequate punishments may reduce any sense of justice among victims. Research shows that victims want punishments that are appropriate and proportionate to both the amount and the type of harm they experienced.[48]
- A boost to the support offer to fraud victims in order to ensure as many victims as possible who suffer from the second order effects associated with fraud victimisation can access the support services they need.[49] [50]

Recommendation 4: Develop a robust standard methodology for capturing more definitively the differential impact fraud has on a victim's economic circumstances and the wider psychological and social costs that can accrue

The Home Office should bring together an expert group to develop a better methodology for working out the cost of fraud to individuals and society more accurately. The expert group should include the Office for National Statistics (ONS) and relevant academics. The real cost of fraud to individuals and society does not end at the direct financial cost suffered by victims or the liabilities faced by financial institutions. The severity of the impact on individuals' economic situations and the psychological and social costs need to be better reflected in the estimates of the consequences of fraud. So too are some of the very long-term impacts on facets of society such as the rule of law and economic effects on the market for consumer financial services, which are highlighted in "Fraudemic" as poorly understood.[51]

The work should build on the Home Office's existing efforts to identify a more accurate cost of crime more broadly, in their "Economic and Social Cost of Crime" work.[52] The focus on fraud specifically would provide an opportunity to develop the most detailed estimate of the cost of fraud to individuals and the UK as a whole. The improved evidence base that should, in-time, accrue as a result of implementing Recommendations 1 and 2, could help inform the development of the methodology.

[xii] It should be noted that there is mounting evidence that suggests longer sentences can have a notable deterrent effect alongside their more widely known incarceration effect, the potential gains in fraud prevention and harm reduction, from a shift in sentencing policy therefore could be substantial. Source: United States Sentencing Commission, 'Length of Incarceration and Recidivism', 2022, https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2022/20220621_Recidivsm-SentLength.pdf.

Recommendation 5: Toughen the sentencing of convicted fraudsters with reforms to the rules so that they take into account the wider impacts that victimisation has on individuals and also reflect the scale and cost of the current fraud epidemic to society

The Government's fraud strategy indicates that there is to be more robust sentencing for convicted fraudsters.[53] The harms element in sentencing decisions should take account of the wider impacts that fraud has on victims and society. For example, the vulnerability of many fraud victims needs to be more clearly reflected in sentencing with the characteristics of the victims and their circumstances seen explicitly as influencing factors e.g, there should be exemplary penalties for those fraudsters that victimise particularly vulnerable individuals such as the elderly, sick and other socially and economically vulnerable people.

Crimes that are committed in the context of wider public disorder can attract more severe sentences.[54] There may not be any immediate physical threat from fraudsters, but the scale of fraud and its cumulative costs are vast. Currently, the authorities do not have fraud under control. Therefore, a similar approach to sentencing in situations where there is widespread public disorder should be taken with fraudsters in the current context.

Recommendation 6: Establish an arrangement, similar to the Criminal Injuries Compensation Authority scheme for providing short-term financial support for victims of serious physical crimes, for vulnerable fraud victims

Low-paid victims of violent crime are able to access short term financial support through the Criminal Injuries Compensation Authority.[55] Politicians and policymakers should develop a similar scheme for vulnerable fraud victims and those who suffer from catastrophic losses due to fraud. Support should primarily be paid for out of a fund replenished by the seized proceeds of crime.[xiii] It should be topped up with a "vulnerable victims levy" on the organisations in the "fraud chain" that are not taking reasonable steps to try and squeeze out the fraud that is propagated and perpetrated using their services. The scheme should be delivered through NECVCU and Victim Support.

[xiii] A similar precedent has been set by NECVCU and Lloyds Bank. In 2021 they partnered to pilot a scheme which utilised the seized proceeds of crime to, in-part, fund victim support services. Source: City of London Police, 'Lloyds Banking Group Launches Pioneering £7 Million Fraud Crackdown', 2021, https://www.cityoflondon.police.uk/news/city-of-london/news/2021/december/lloyds-banking-group-launches-pioneering--7-million-fraud-crackdown/.

CHAPTER FIVE – THE REIMBURSEMENT PROCESS CAN MAKE THE IMPACT OF FRAUD VICTIMISATION WORSE

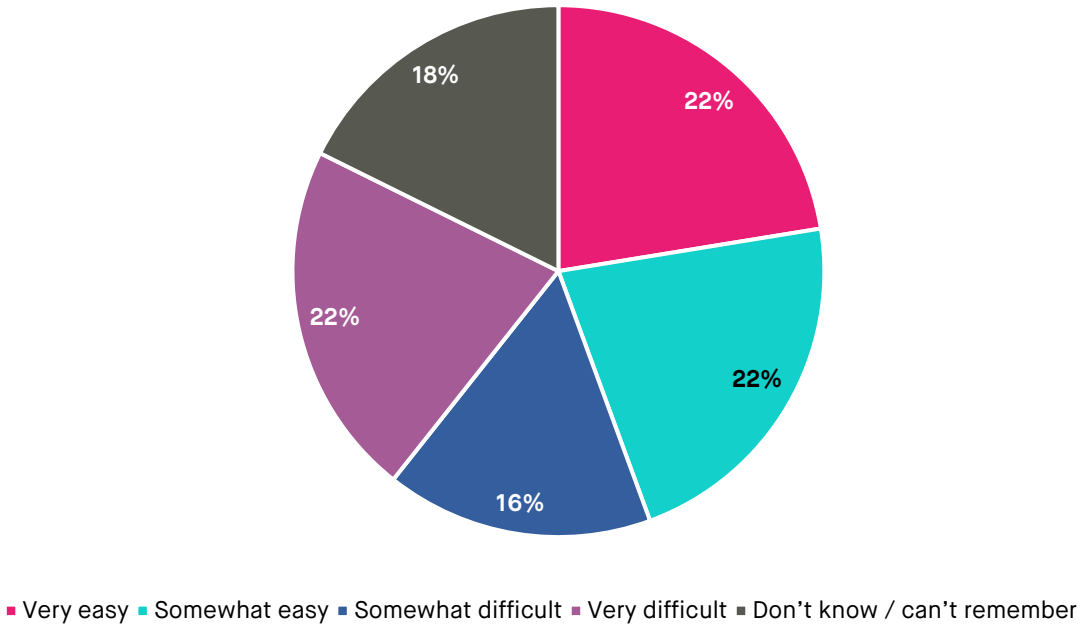
Reimbursement and its contribution to the impact on a victim's economic circumstances

The victim survey data presented in "Fraudemic" showed that most (66%) victims were reimbursed for the fraud that they most recently experienced.[56] However, 34% were not.[57] In addition, among those that were reimbursed, 20% did not get refunded the full amount of direct financial losses. Failing to be reimbursed or not being fully reimbursed can add to the cumulative negative impact of being subject to fraud.

Exacerbating the negative economic and wider impacts of being a fraud victim

Problems for victims may also be made worse if the reimbursement process is a difficult one, even if the full amount lost is reimbursed in the end.

Figure 12: Ease of the reimbursement process after being a victim of fraud, 2020 - 2023



Source: Opinium survey of fraud victims

Figure 12 shows that, of those who fell victim to fraud at least once between 2020 and 2023 and were reimbursed, 44% described the process as "very easy" or "somewhat easy". A substantial minority (38%) described the reimbursement process they went through as "somewhat difficult" or "very difficult". More than 1 in 5 (22%) stated that it was "very difficult".

The length of time it can take some to be reimbursed was raised in the interviews with victims carried out to inform this research, as a compounding factor adding to the challenges of an already difficult situation. One elderly interviewee who had been defrauded twice, once as a result of ID theft and the second through a fake holiday provider initially accessed through an advert, described how the time it took to be reimbursed for the latter saw her having to rely on her family for money which was detrimental to her sense of dignity:

> *"...It was quite a long time...my kids...put in money for me...I didn't want the money from them...I'm afraid it's like being taken over from being the parent".*

Difficult reimbursement processes may be about to impact more victims

The additional detriment created by a difficult fraud reimbursement process may be about to increase as more fraud victims are soon to become routinely eligible for reimbursement. The 34% that are currently not reimbursed are soon going to benefit from it, however, concomitantly, it also means more will be exposed to instances of difficult reimbursement.[58]

Reimbursement customer service as a contributor to competitive advantage

If 1 in 5 customers were receiving poor customer service from a commercial organisation, that would likely be seen as a serious failing in service quality. The high proportion of poor experiences should worry banks, building societies and others who reimburse customers for fraud losses, because a good reimbursement experience can boost a customer's view of their bank, in what are difficult circumstances. Conversely, a bad experience can alienate a customer from their provider as a participant in the in-depth interviews for this report described. They had their debit card details stolen and more than £700 taken from their account:

> *"...you trust to put your money in and then they're not supporting you on it...I presumed I could have rung the fraud department and they would have helped me out..."*

The same interviewee added:

> *"...there was a lack of care...I don't think my issue is the first one that they've ever encountered...so, I would have expected them to have...taken it a bit more seriously...so yeah, just really disappointed to be honest...not too long after I changed banks...I just didn't trust them afterwards...I wasn't banking with them again".*

Consequently, this aspect of a financial services company's service, which may often be thought as of secondary importance, could make a contribution to an organisation's competitiveness[59] and help with customer retention.

The link between a poor reimbursement experience and losing a customer as a result seems like a clear risk firms would want to avoid. Further, it is easy to envisage how an efficient reimbursement service that also helped connect victims with formal victim support provision could sit alongside enhanced efforts by providers to prevent fraud victimisation. Together this might help boost customer loyalty by making victims feel more supported in a challenging time.[60]

Implications for politicians and policymakers

A difficult reimbursement process would be expected to compound what is already a tough time for most victims. This raises the question of whether the reimbursement process could be improved such that extra problems are minimised? This question is particularly pertinent in the context of the requirements of the FCA's Consumer Duty which, on the face of it, would be expected to provide an impetus to relevant financial institutions to ensure that reimbursement services are reflective of customer needs and whether there might be more of a role for the Financial Ombudsman Service (FOS) in feeding into effort to raise and maintain reimbursement standards.[xiv]

Recommendation 7: Banks, building societies, credit card providers and other payment services firms that reimburse fraud victims should evaluate their reimbursement offers to ensure they meet high customer services standards, and that they are especially sensitive to vulnerable customers who have been fraud victims

Reimbursement difficulties experienced by fraud victims would appear to be an avoidable source of additional detriment for many fraud victims, if service standards were made consistently high across the relevant parts of the financial services industry. Payment services firms that provide reimbursements should commit to speedily undertaking an evaluation of their service quality levels (including gathering extensive user feedback evidence) with the aim of identifying ways in which the process could be optimised to make it as easy as possible and particularly sensitive to vulnerable customers and their circumstances.

The results of the evaluations should be shared with the FCA and, working with the FOS and industry, a set of best practice standards should be developed which in-turn should ultimately inform FCA guidance on this matter (see Recommendation 3).

[xiv] Distress and inconvenience are recognised by FOS as relevant factors in a dispute and under the Consumer Duty, these may become even more pertinent to the reimbursement service offering of relevant financial institutions as these are clearly linked to socio-economic and other consumer demographic factors (see Chapters Three and Four). Source: 'Compensation for Distress or Inconvenience', Financial Ombudsman, accessed 11 September 2023, https://www.financial-ombudsman.org.uk/consumers/expect/compensation-for-distress-or-inconvenience.

CHAPTER SIX – FRAUD AS A COLLECTIVE ACTION PROBLEM

The three dimensions of counter-fraud cooperation

Cooperation between the myriad departments, agencies and organisations with an interest in fraud across the public and private sectors is key to a more effective response to the fraud epidemic. Across all its various iterations, fraud policy (since the Fraud Review in 2006) has highlighted the need for greater cooperation, especially in the form of data sharing.[61] The contours of that cooperation have been evident for a long time and are illustrated in Diagram 1.

Diagram 1: The three dimensions of cooperation that are needed to effectively tackle fraud

Source: SMF analysis

Box 3 provides examples of some of the most notable current efforts at cooperation between different actors with an interest in the fraud problem. The persistent scale and cost of fraud is a clear indication of the inadequacy of the present, somewhat ad-hoc, arrangements. Therefore, while all data sharing that can help improve the response is welcome, current efforts are largely limited to discrete areas and fall short of the extensive and deeper cooperation that is required.

The inadequate law enforcement response to fraud

The low levels of fraud reporting to law enforcement are one reason why the response of the latter has been lacklustre for so long. However, more broadly, the current organisation of counter-fraud policing is now widely agreed to have fundamental failings:[62]

- A review by HM Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) noted the lack of regional and national coordination in both fraud prevention and in the investigation of cases.[63]
- The recent House of Lords Committee on the Fraud Act 2006 and Digital Fraud Committee report[64] pointed out that the resourcing of law enforcement which they observed falls substantially short of the scale of the problem.[65] [xv]
- A Home Affairs Select Committee analysis highlighted the counter-fraud capability and capacity of law enforcement is inadequate to the size and complexity of the task of pursuing and disrupting fraudsters.[66]

[xv] Less than 1% of all police personnel in England and Wales are tasked with investigating fraud despite fraud accounting for around 4 in 10 crimes perpetrated against the people of England and Wales. Source: Richard Hyde, Scott Corfe, and Anderson-Samways, 'Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up', Social Market Foundation. (blog), 4 March 2022, https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/.

- There are indications that parts of the police continue to view fraud as a largely "victimless crime"[67] or at best, primarily a "civil matter".

Box 2: Evidence of the poor law enforcement response to fraud

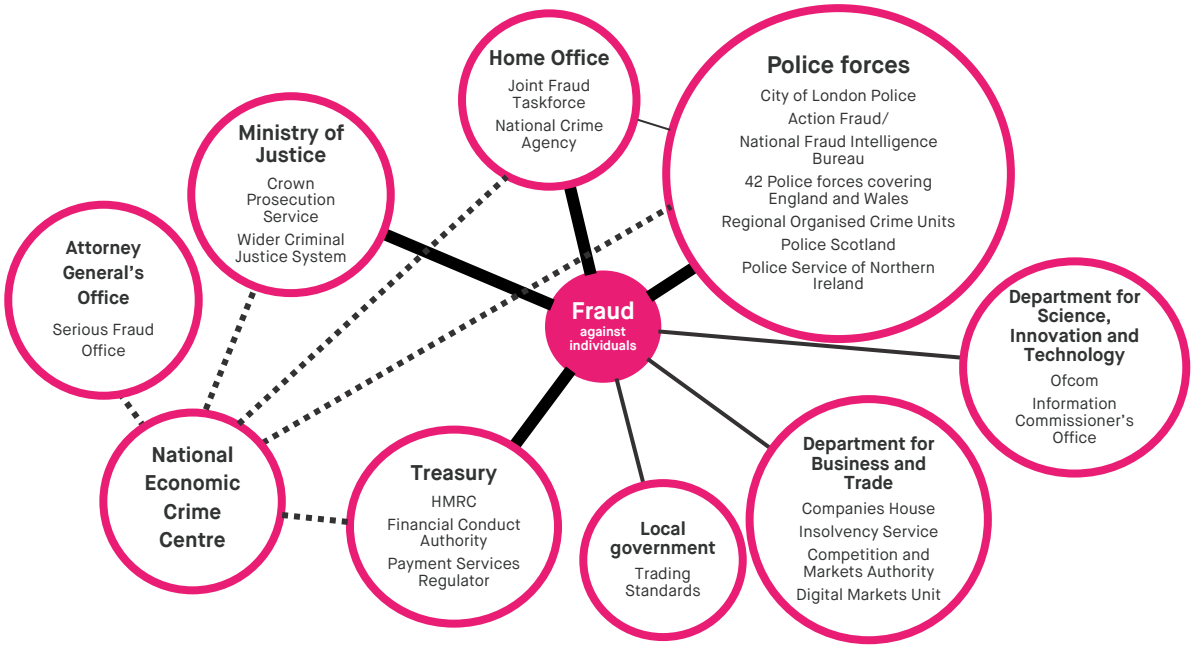
The Police Foundation estimated that across the period July 2020 to June 2021, 0.1% of frauds recorded by the Crime Survey of England and Wales (CSEW) ended up in a charge or summons.[68] They also calculated that 0.6% of frauds recorded resulted in a charge or summons. [69] The latter was down from 0.8% in 2016-17.[70]

The national lead force for fraud, the City of London Police, have an arrest rate of around 9% for the frauds they investigate. However, the City of London Police only opened around 400 cases in 2020-21.[71] A small minority of the number of frauds reported to Action Fraud and an even smaller proportion of those recorded by the CSEW. Each case under investigation attracts, on average, around three-quarters of the time of a full-time officer or specialist member of staff. This is in contrast to the situation across England and Wales as-a-whole, where there are 2.1 police officers and other staff primarily focused on economic crime for every 1,000 recorded fraud offences.[72]

The disjointed public sector fraud landscape of which law enforcement is one part

The public sector's interest in fraud against individuals does not end with law enforcement. As Diagram 2 illustrates, there are a plethora of government departments and agencies with either a direct or at least tangential interest in fraud of various kinds. The diagram provides a glimpse into the range of entities that need to be galvanised into concerted action in order to make significant inroads against the fraud epidemic.

Diagram 2: Government departments and public sector agencies with an interest in fraud against individuals



Source: SMF analysis

The insufficient efforts of the private sector against fraud

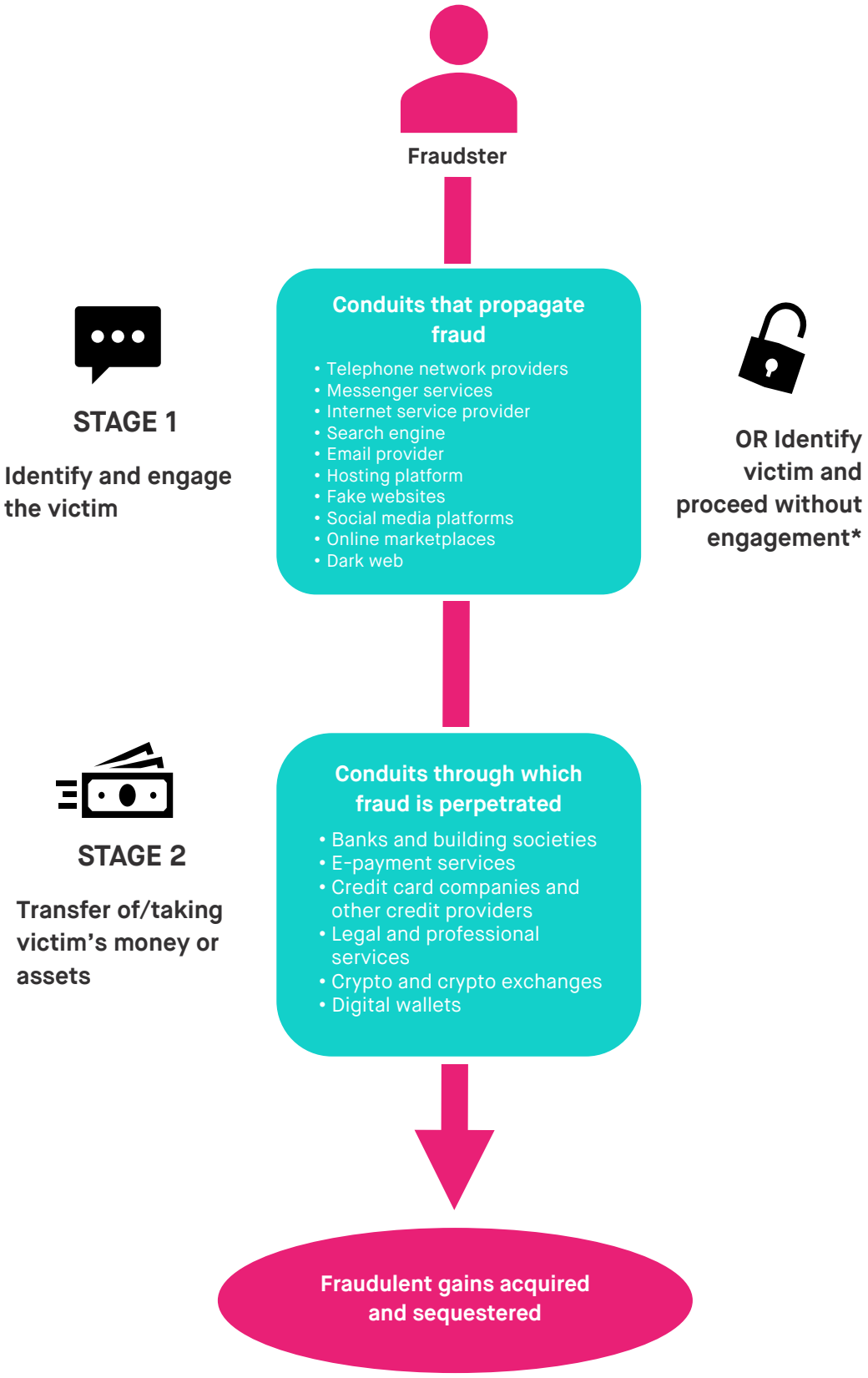
The report by the House of Lords Committee on the Fraud Act 2006 and Digital Fraud pointed to widespread failings in the response to fraud by the private organisations and industries that are part of the "fraud chain".[xvi] [73] Other analyses have made similar observations.[74]

The complexity of the "fraud chain"

The "fraud chain" is complex due to the myriad organisations that are often connected to a single act of fraud. Further difficulty comes from the volume of attempted frauds. There are tens of thousands of attempted frauds against residents of the UK being perpetrated each week and tens of millions each year. Diagram 3 provides a simplified illustration of the fraud chain and the various actors that can be involved in it.

[xvi] The term "fraud chain" describes the process by which a fraud takes place. It is sometimes referred to as the "fraud supply chain". Sources: 'Fighting Fraud: Breaking the Chain' (House of Lords: Fraud Act 2006 and Digital Fraud Committee, 12 November 2022). National Audit Office, "Progress Combating Fraud," 2022, Progress combatting fraud (nao.org.uk) and Experian, 'What Is the Fraud Supply Chain? | Blog | Experian', Experian UK, July 2016, https://www.experian.co.uk/blogs/latest-thinking/fraud-prevention/fraud-supply-chain/.

Diagram 3: A simplified representation of the "fraud chain"



*Source: SMF analysis; *Many fraudsters do not engage with the victim but, for example, buy hacked/ stolen personal and financial data often from other criminals from places such as the dark web.*

Cooperation among the organisations in the "fraud chain"

Bringing together the organisations in the "fraud chain", in order to take coordinated action against the fraud that is propagated and perpetrated through the services they provide will be difficult. Such efforts face a number of entrenched obstacles which mitigate against collective action (see Table 1).

Some of these barriers were raised at the expert roundtable that SMF convened to help inform this research. One contributor pointed out that large-scale unilateral action (which would inevitably involve considerable investment and organisational disruption) would be likely to put those organisations a competitive disadvantage, creating a dilemma for firms:

> *"I can't see many financial institutions taking [such] steps on their own. Because immediately others will take advantage in a competitive way…".*

It was also pointed out that there is a significant information problem because each actor in the fraud chain can only observe the part of the process of perpetrating a fraud that takes place through their service offering. This partial picture makes unilateral action difficult in any case:

> *"…each industry has only a snapshot does that victims journey…".*

Another roundtable attendee gave an illustration of how the information problem can arise, by describing how fraudsters often move potential victims around different platforms, in part because they know there is little cooperation between them:

> *"… what's happening is…users, often internationally based…are…phishing…if you want concert tickets, or car insurance, whatever, hit me up on [a different platform/ messenger service]…speak to somebody and let me get you off this platform… [or]…let me take you to a website where you can print the details off…and then a week later, a text message from the bank…".*

Box 3: Existing private sector coordination efforts against fraud

It should be noted that there are efforts underway to help coordinate public and private sector effort better. The National Economic Crime Centre (NECC) and the Home Office's Joint Fraud Taskforce (JFT) both aim to do this in different ways. Further, law enforcement–financial services data sharing activity has been improving under the auspices of the Fraud Intelligence Sharing System (FISS).[75] However, the most advanced private–public sector data sharing is money laundering focused. The latter may offer lessons for other areas of crime like fraud.

In addition, parts of the private sector have made notable strides in enhancing their response to fraud. Cifas has helped improve information sharing among financial services firms about fraud. UK Finance pointed out that in 2021, bank and card companies prevented £1.4 billion in unauthorised bank and card fraud.[76] Data sharing through Cifas was an important component of that effort. In the telecoms sector, under the sponsorship of the regulator, telecoms companies have made strides in trying to tackle fraud attempts that begin using the phone networks, as one expert roundtable contributor noted:

> *"Telecoms have, over the last 10 years, become far more involved…to the point where, now, some of the firms do some amazing stuff, although some more than others, but the point is that they're…moving the dial up".*

A lack of sufficient cooperation hindering the fight against fraud

An essential step towards putting in place the effective cooperation on the scale that is needed to substantially reduce fraud below the levels it has reached today, is to recognise that there are two collective action problems[xvii] preventing it, which politicians and policymakers, the relevant departments and agencies in the public sector and the organisations which comprise the "fraud chain", need to overcome. Table 1 describes these in more detail.

[xvii] See Box 10 in Annex II for more on collective action problems.

Table 1: The two collective action problems constraining efforts to tackle fraud more effectively

Type of collective action problem	Causes of the collective action problems across the relevant parts of the public sector	Causes of the collective action problems among private sector actors in the "fraud chain"
Coordinated implementation	A cost – benefit balance that skews against counter-fraud action on the scale needed. Other priorities, limited budgets and the cost of investing in counter-fraud activity and the associated organisational disruption, along with little direct benefit for doing so, together disincentivise engaging in the kind of coordinated action across the public sector and in conjunction with the private sector, that is required. Information gaps as a result of inadequate public data collection about the scale and impact of fraud, as well as insufficient flow of information being shared by organisations in the "fraud chain" with relevant public sector agencies for intelligence purposes, which is needed to build up a clear picture of fraud threats and pursue and disrupt fraudsters.	Cost – benefit ratios that disincentivise actions of the type and magnitude required to tackle fraud. Commercial priorities and the cost and disruption involved with investing in counter-fraud capacities and capabilities with little direct return for the individual organisation, and the risk of placing rivals at a competitive advantage if such efforts are not mutual, are, in sum, substantial barriers to putting in place the measures needed on the scale that will make a difference. Incomplete information about the fraud being propagated and perpetrated across the services offered by the organisations in the "fraud chain". Each actor in the "fraud chain" only has a partial picture of what both ordinary and malevolent users are doing. Consequently, no one has an "end-to-end" picture of the fraud process, which constrains the ability of individual actors to take countervailing action.
Negative externality	The lack of action against fraudsters and fraudulent activity by agencies in the public sector, means that fewer fraudsters are disrupted or arrested which results in more future victims than there might otherwise be. Those agencies rarely bear any of the costs that are borne by the victims or paid-out by organisations that may have to reimburse victims, as a result of the inaction	The operations of some organisations in the "fraud chain" (e.g. those whose services propagate fraud) result in negative consequences for others e.g. those who are victims of the fraud and the financial institutions that have to reimburse victims. At the same time, the organisation further up the "fraud chain" that (albeit unintentionally) facilitated those negative impacts often face little, if any, of the costs themselves.

Examples of collective action problems in other crime domains

Collective action problems are not new in relation to dealing with crime. In the area of cyber security and cyber-crime for example, potential solutions to deal with similar collective action problems that persist with fraud have been debated for a long time (see Box 4). Further, while it has taken a long time, the kinds of measures which can help correct, for example, negative externalities are, albeit often partially and slowly, being applied by policymakers, in discrete areas to help tackle cyber security risks.[77]

Box 4: Solutions to the collective action problems associated with cyber-crime

The problem of negative externalities resulting from insecure digital products such as software programmes that are exploited by criminals or malicious actors using digital platforms to commit cyber-crimes have been discussed for many years. The use of liability or fines for the harms caused to others as a way of incentivising the relevant actors (e.g. software developers, vendors or platform providers, etc) to take effective steps to reduce the propagation of cyber threats through their products or over their services have been regularly proposed.[78] In the case of fraud, liability for reimbursing fraud victims creates that incentive for relevant financial institutions to take more aggressive steps to try and reduce incidents of fraud and may provide a similar stimulus to digital services providers and phone networks.

Implications for politicians and policymakers

As noted in Chapter Two, the Government's new fraud strategy contains a number of steps that are likely to prove impactful on fraud levels. However, with measures like the voluntary Online Fraud Charter for technology firms, there are concerns that this will fall short of making the kind of difference that will significantly help ameliorate the collective action problems that hamper the fight against fraud.[79] Therefore, at least two key questions remain for politicians and policymakers:

- How can the cost and information barriers to coordinated action be lowered in order to facilitate greater and more efficacious cooperation between organisations in the "fraud chain" and between the public and private sectors?
- Is there a role, and if so what, for incentivising organisations in the "fraud chain" to take more account of and sufficiently prioritise the externalities they propagate and invest adequately to ameliorate them?

Recommendation 8: Start the process of developing a new set of policy proposals, for introduction in 2025, for improving the coordination of the fraud response by solving the collective action problems. These should include the measures proposed in recommendations 10, 11, 12 and 13

The collective action problems that plague the response to fraud require more extensive measures to ameliorate them than those currently in place and being proposed in the Government's fraud strategy. Therefore, alongside its implementation, politicians and policymakers should start to look beyond activities and plans and begin the process of developing the next phase of policy measures, which attack the collective action problems and the barriers to their being resolved more aggressively.

Recommendation 9: Prioritise the fraud threat with new investment in the capacity and capability of law enforcement

The fraud strategy outlined proposals for structural reform to the police to improve the response to fraud by establishing a new National Fraud Squad (NFS).[80] Four hundred new fraud specialists, while welcome, are unlikely to make a substantial difference to fraud levels given the scale of the threat.[81] Making fraud a Strategic Policing Requirement (SPR) is also a positive change. However, given the current way the law enforcement response to fraud is organised and its lack of adequate capability and capacity, such a change on its own is unlikely to lead to a step change in the efforts against fraudsters.

SMF has previously suggested that an uplift of around 30,000 specialist officers and investigative support staff e.g. forensic accountants and digital forensic experts in England and Wales, is needed to deliver a significant reduction in fraud levels.[xviii] [xix] The positive impact of the increase in counter-fraud capability and capacity would be maximised if it took place alongside other policy, organisational, operational and legal changes[82] that empowered law enforcement with the tools they needed, and facilitated:

- Greater pooling of expertise to create a critical mass of skilled specialists where collaboration, knowledge sharing and other complementarities can be more easily exploited.
- More straight-forward command and control in order to deliver consistent, coherent and coordinated activity.
- The generation of economies of scale and scope in the use of resources.

[xviii] SMF previously outlined a detailed plan for significantly improving the law enforcement response to fraud. Source: Richard Hyde, Scott Corfe, and Anderson-Samways, 'Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up', Social Market Foundation. (blog), 4 March 2022, https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/.

[xix] Assuming (conservatively) each of the 30,000 specialists could investigate four frauds a year, this would add the capacity to investigate approximately 120,000 additional frauds per annum.

CHAPTER SEVEN – THE PUBLIC'S VIEWS ON KEY COUNTER-FRAUD POLICY DEBATES: REIMBURSEMENT AND LIABILITY

Apart from infrequent opinion polling highlighting the public's overall dissatisfaction about current efforts by the government and the police against fraud (see Figure 1), the views of the public have been largely absent from the debate over how fraud can and should be tackled. This chapter, as well as Chapters Eight and Nine, will examine public opinion in light of some of the policy discussions that took place at the expert roundtable that SMF convened in June 2023.

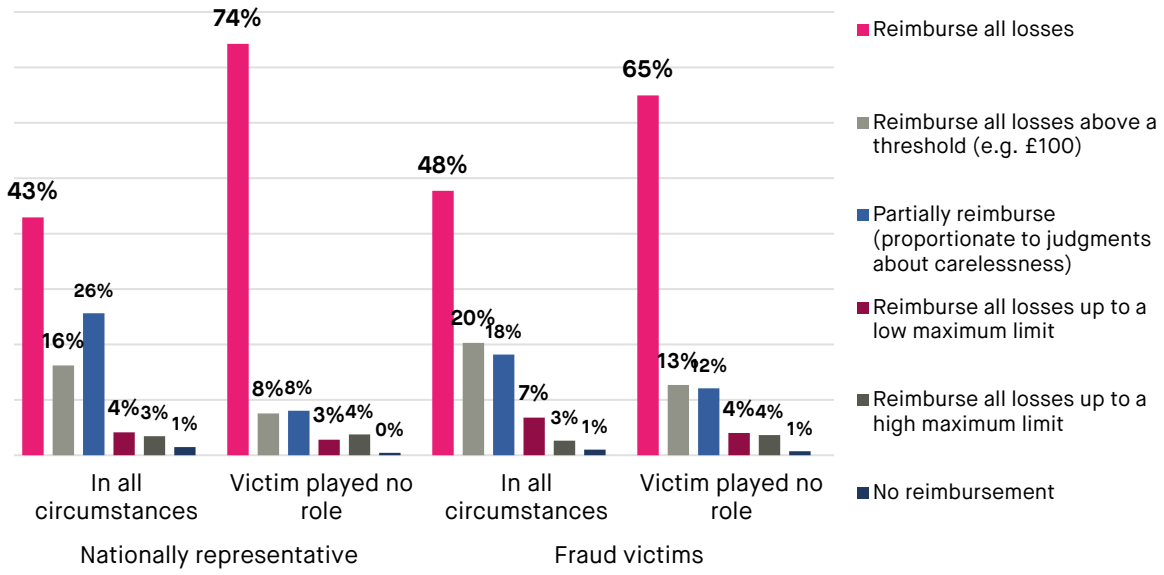
Reimbursement policy

Reimbursement is perhaps the most salient policy issue pertaining to fraud at the moment. The Payments Service Regulator (PSR) is currently taking forward the policy of extending reimbursement to instances of authorised push payment (APP) fraud so that the reimbursement system is broadly aligned between frauds where the victim had no role in it, and those where the victim does unwittingly enable it.[83] As was noted in this project's interim report, this should see the proportion of victims that are reimbursed (at least to some degree) increase significantly.[84]

The public's view on reimbursement

The public's view on reimbursement is nuanced, as Figure 13 shows. It should be noted that there is overwhelming support (more than nine in ten respondents) for at least some losses being reimbursed in almost all circumstances. This is consistent with older evidence collected from victims on this topic, which also identified a high degree of support for reimbursement.[85]

Figure 13: Support for reimbursing fraud victims among the UK population and fraud victims



Source: Opinium surveys of the UK adult public and fraud victims

- Less than half of UK adults (43%) and victims (48%) supported full reimbursement in all circumstances. By contrast, in situations where the victim had no role, support for full reimbursement was 74% among the wider population and 65% among fraud victims.
- Where the victim played a role in the fraud that took place, 26% of the general public, felt that partial reimbursement based upon judgments about the victim's carelessness was valid. Among fraud victims, a substantial minority (18%), thought similarly.
- When fraud victims were presented with the suggestion that, in instances where there would be full reimbursement for anyone no matter the culpability of the victim, 20% supported a *de minimis* threshold of £100 for refunds, while 16% of the UK adult population supported this approach in such circumstances.[xx]

Where liability for reimbursement should reside

Liability for reimbursement is an example of incentives in action

An issue of some debate at the expert roundtable was the topic of where liability for reimbursement might fall. Reimbursement liability creates an incentive for an organisation to take action to deal with the problem they are reimbursing for, as its continuation will mean perpetual payouts (see Box 4). It is a tried and tested way of solving externality-based collection action problems, which, as Table 1 showed, is pertinent to the fraud problem.

There was widespread support for the principle of sharing more liability along the "fraud chain" among contributors to the roundtable. It was seen as an effective way of creating incentives to galvanise the kinds of actions needed. One noted that distributing liability can drive changes in priorities and behavioural shifts:

> *"...by assigning liability and taking cases against people and fining them, guess what, we've eliminated a lot more of the harm because...the intermediaries, the networks are taking a damn sight more care...".*

A second proposed the possible contours of a potential reformulation of reimbursement liability along the "fraud chain":

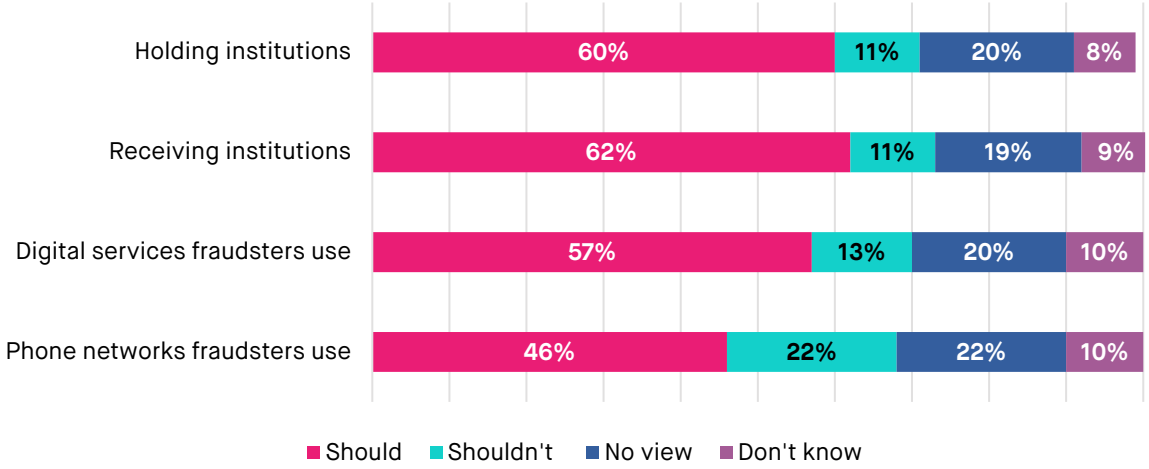
> *"...the primary liability rests with the merchant...however, there should be liability back up the value chain...".*

[xx] Such an approach would make the reimbursement regime similar in this regard, to that which applies to credit cards under the Consumer Credit Act 1974, and is being considered by the PSR.

The view of the British public and fraud victims on where policy should place liability

Public polling evidence shows most of the UK adult population in general and fraud victims in particular, were comfortable with policy placing liability not only on financial institutions[xxi] but the digital services firms, whose services fraudsters utilise, too (Figure 14).

Figure 14: The degree to which the public support liability being placed on different key actors in the "fraud chain"



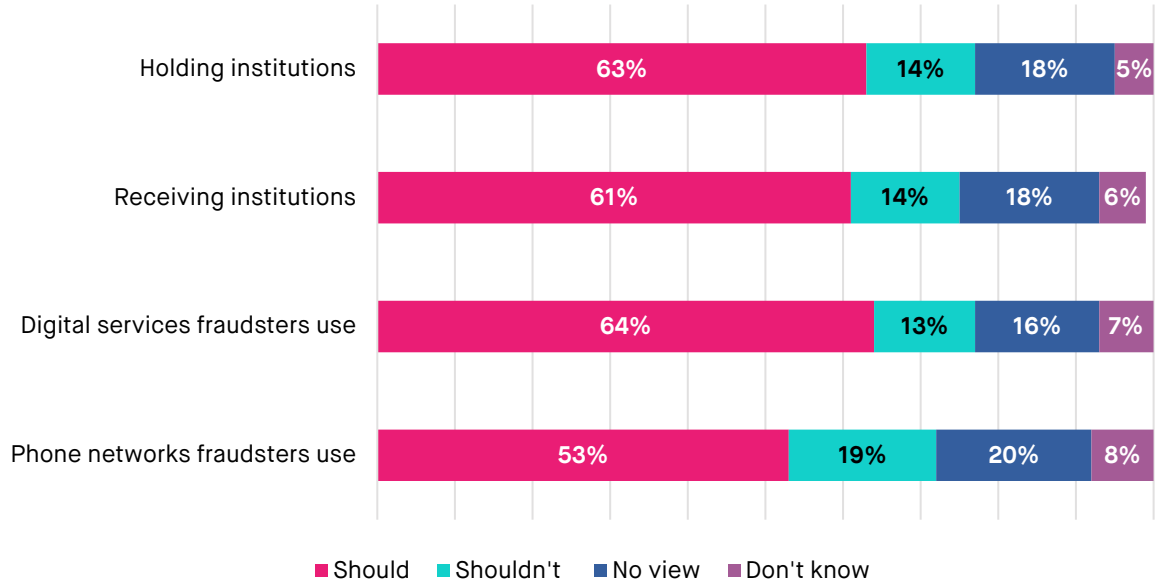
Source: Opinium survey of the UK adult public

Figure 14 also shows that a plurality of the public (46%) were happy for policy to place liability for at least some of the costs of reimbursement on the telecoms networks too.

Amongst fraud victims (Figure 15), the proportions agreeing they would be happy to see liability for reimbursement placed upon the institutions holding (63%) or receiving (61%) payments and transfers were similar to those in the wider population.

[xxi] "Holding institutions" are those financial institutions (typically a bank or building society) where the money or asset normally resides. "Receiving institutions" are those where the money or asset is paid or transferred to.

Figure 15: The degree to which victims of fraud support liability being placed on different key actors in the "fraud chain"



Source: Opinium survey of fraud victims

The largest differences in the views of the UK adult population as a whole and fraud victims was in the levels of support for digital services (64% of fraud victims against 57% of the UK population) and telecoms companies (53% of fraud victims against 46% of the UK population) bearing at least some responsibility for reimbursement.

Digital services are the farthest behind in counter-fraud efforts

A substantial proportion of the fraud afflicting the population of the UK is propagated through digital services such as webmail services, search engines, web hosting services and social media platforms.[86] It was noted at the roundtable that of all the organisations in the "fraud chain", it was the digital platforms that have the farthest to go:

> *"...many of the platforms are behind...there's got to be...equivalence, in that sense of all sectors being accountable for taking the steps they can take..."*

One roundtable participant drew an analogy with financial services and how the latter have had to (and continue to) develop processes that manage risks associated with possible malevolent actors accessing their services and potential criminal activity taking place through them.[xxii] The contributor suggested there were lessons for others in the "fraud chain":

[xxii] Undertaking fraud risk assessments is a low priority for many companies, as research from Deloitte showed: Deloitte, 'The Nature of Fraud Is Changing: Act Now to Beat It', 2021, https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/financial-advisory/deloitte-uk-the-nature-of-fraud-is-changing.pdf.

> *"...there's usually an intermediary who aggregates...and then there's the network operators themselves. And at each level, there's a degree of everything...you have to...know your customer...at onboarding, due diligence, risk assessment, risk control... a new risk assessment associated with the client and...continuous monitoring of what's going on...that doesn't mean every transaction...[and if there are]...complaints about a particular service, find out why..."*.

A different contributor to the roundtable outlined an example of the kind of fraud risk warning service that might be developed for users, by platforms:

> *"...platforms know the first time someone's confronted by a message from a particular user and that user has never contacted them before...[there]...could be convenient 'rating' or colour coding to draw attention to the fact..."*.

Sharing liability will require an infrastructure which does not yet exist

A note of caution was raised by another roundtable attendee. They highlighted the lack of infrastructure for any distributed liability system. A secure and durable infrastructure would be essential if such an approach was implemented:

> *"...changes to liability...it's a really good thing, but there's no infrastructure in the background to manage the settlement, and will be required...but we don't have any...to manage it..."*.

Implications for politicians and policymakers

The implications for politicians and policymakers of the evidence presented in this chapter are numerous:

- A straight full reimbursement system for all fraud victims regardless of circumstances is neither supported by a majority of the wider population nor fraud victims. However with the policy well underway, unpicking some of what has now been set in motion is unlikely to prove realistic.
- The PSR's proposal for splitting the liability across the "holding" and "receiving" institutions where the fraud involves a payment or transfer is aligned with the majority view of both the wider public and fraud victims.
- Consistent with tried and tested solutions to externality-based collective action problems, the public are also content to see liability distributed more widely along the "fraud chain". In principle, such a change should incentivise more action from more organisations in the "fraud chain" as they will bear some of the costs of what is propagated through their services.

However, the cost–benefit obstacles to organisations in the "fraud chain" taking action on sufficient scale to make a substantial difference to the fraud epidemic are still going to be significant.[xxiii] Firms will likely have to make investments that divert resources away from more commercially attractive alternatives. There is likely to be disruption to current modes of organising and operating internally and the retraining of existing staff or taking on additional employees to service the stronger focus on countering fraud. Policymakers will need to cognisant of these realities as they thing about policy measures.

Recommendation 10: Continue with the PSR's reimbursement plans to share liability between "holding" and "receiving" institutions and prepare for a second phase, where other organisations in the "fraud chain" are made eligible for some of the costs of reimbursement

The negative externality collective action problem can be ameliorated by ensuring that those whose services result in the perpetuation of fraud internalise more of those costs. The key is to push firms into shifting their priorities and actions, by changing the balance of the cost–benefits they face when confronting the problems of fraud so that taking steps (individually and in coordination with others) on the scale needed to tackle the fraud epidemic becomes the optimum option.

A mechanism that achieved this would create stronger incentives for action by the individual organisation and for organisations to collaborate on solutions. Politicians and policymakers should commit to this route in principle. The design and implementation of how to deliver it should be consulted upon as there are numerous methods that might be utilised. For example, an alternative option might be levying civil penalties on organisations in the "fraud chain".

Further, given the substantial societal gains from more effective counter-fraud efforts, politicians and policymakers may need to consider the role of subsidy to help put in place the necessary infrastructure required to operate a system where liability is distributed across multiple parties.

[xxiii] One recent analysis of the cost of compliance with obligations placed on financial services firms to counter economic crime including fraud, suggested the annual costs were in the region of £34 billion. Source: Lexis Nexis, 'Report: True Cost of Compliance 2023', LexisNexis Risk Solutions | Transform Your Risk Decision Making, 2023, https://risk.lexisnexis.co.uk/insights-resources/white-paper/true-costs-of-compliance.

CHAPTER EIGHT – THE PUBLIC'S VIEWS ON KEY COUNTER-FRAUD POLICY DEBATES: INCREASING ASSURANCE IN THE PAYMENTS SYSTEM

The role of "frictions" in the payments system

The House of Lords Committee on the Fraud Act 2006 and Digital Fraud recommended more "frictions" be introduced to the payments system, especially around "high risk" payments and transfers.[87] At the expert roundtable hosted by the SMF, there was much concurrence with this proposition. One participant made the point that:

> *"...when it comes to scams more time is helpful. Whether you have a customer who suddenly realises five minutes later what they've done...or just that little bit of extra time to carry out an investigation...".*

Removing "friction" is a key reason why fraud has grown significantly

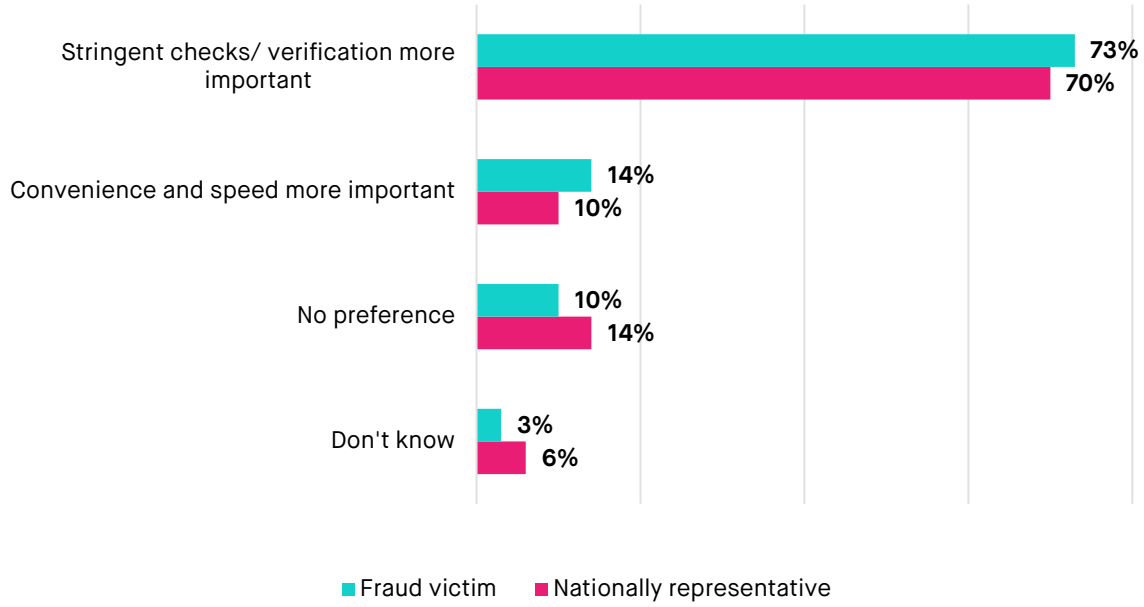
As more economic activity has been sped up by technology, convenience and swiftness have become components of product competitiveness. At the forefront of this shift has been banking and other financial activities.[88]

The introduction of faster payments reduced the ability of financial intermediaries to conduct assurance checks on payments and transfers.[89] This change in the UK has been seen by many as one of the key catalysts behind the growth in fraud over the last decade.[90]

More "frictions" to reduce fraud

There is a widespread perception that consumers would be resistant to more "frictions" in their banking even if they helped to reduce fraud risks. However, the survey evidence presented below and the findings from qualitative research with fraud victims suggests the opposite.

Figure 16: Policy preference – stringent checks and verification on payments and transfers or convenience and speed



Source: Opinium surveys of the UK adult public and fraud victims

As Figure 16 shows, overwhelmingly, both adults in the UK (70%) and fraud victims (73%) more specifically, say they are happy to accept less convenient and slower payment and transfer services if the corollary is reduced fraud risk.

The fraud victims interviewed in-depth for this report were asked for their reactions to the possibility of more "friction" in their payments and transfer activities, and how willing they would be to accept them, if it reduced fraud risk. There was a general acceptance of extra "frictions" in such circumstances. However, for a number the details were important, for example, longer periods between payment and receipt seemed to influence levels of contentment:

> *"...if it was necessary, then that I don't have a problem with it...if it was within an hour, then it probably wouldn't affect me at all. If it was 24 hours plus that, then yeah...but again...if it was necessary..."*.

Another of the victims interviewed, a retired individual who fell victim to fraudsters that were using his card details in the United States to buy goods worth up to £3,000 in total, was marginally more positive, emphasising that extra security would boost their confidence in online banking:

> *"...I log into my bank, they will either text or email me with a code...it's no problem. If there is something else you've got to do and that's going to stop these fraudsters, go for it...it's not a big deal when you think about that...if any extra protection can be had, I'm all for it...that...makes me feel safer"*.

Future developments and the convenience – speed and fraud risk trade-off

In the two surveys that help inform this report, respondents were asked to consider possible future developments in financial services technology that might mean greater assurance over the security of payments and transfers and consequently much lower fraud risk. However, there was a real prospect that these might reduce convenience and payment and transfer speed further. Despite this prospect, as Figure 17 shows, on the face of it such developments were broadly popular among respondents, with 54% of the UK adult population sample saying they would "support" such developments, and 64% of fraud victims positive too.

Figure 17: Policy preference – development and deployment of new technologies that substantially lower fraud risk at the cost of payment system convenience and speed

Source: Opinium surveys of the UK adult public and fraud victims

What additional "friction" might involve

"Frictions" range from outright blocking through to flagging possible risks at customers as they access products and services or undertake tasks. Other specific ideas for the kinds of "frictions" that could be introduced into payments systems in the future, were described at the roundtable, and included:

> *"...individual banks customising their apps to allow customers to self-select cooling off periods, reduce payment limits per day...automatic looks at payments with lower thresholds than they used to have...".*

"Frictions" and collective action problems

The cost – benefit obstacle to introducing more "frictions"

The internalisation of many of the costs of fraud through reimbursement has pushed some in the financial services sector to consider more seriously, the introduction of more "frictions". As one attendee noted at the expert roundtable:

> *"...very large fraud losses...[for people]...and reimbursement bills are all now supportive of the right levels of friction..."*.

It was indicated by others however, that, despite the impetus that reimbursement has helped provide towards taking more action befitting the scale of the fraud problem, there remained cost–benefit obstacles that mean the incentives are still not yet strong enough to bring about a decisive shift in priorities and galvanise sufficiently substantial actions:

> *"...more friction will be a positive thing if they're going to get more protection. However...in terms of policymaking...how can you get the industry to...put in the friction that's needed to be able to be secure?"*.

The process of designing and implementing new "frictions" could take considerable investment. For example, serious efforts that involve the greater integration of authentication, fraud-risk management, and customer experience[91] will likely come with organisational disruption. Further, consumers have preferences for "frictions" that they are familiar with but which are not always the most effective.[92] As a result, consumer education and the use of transition periods as systems changeover and consumer adapt are all likely to be needed. Further, the benefits may be long-term and so any return i.e. the reduction in reimbursement payouts, may only emerge slowly.

In addition, introducing stronger "frictions" in particular, comes with risks. For example, high-risk transactions that were blocked but were "false positives" may cause considerable inconvenience and unhappiness to consumers. Therefore, the possibility of these arising would need to be taken into account.[93] Consequently, processes for overcoming this potential downside of more "stringent frictions" would need to be introduced.

The risk involved in introducing more "frictions" unilaterally, which could put first movers at a commercial disadvantage, mitigate against leaving it to industry alone to develop more solutions to the fraud threat piecemeal in a competitive environment. As a result, only a regulatory push may bring about the coordinated implementation of counter-fraud measures such as more "frictions" that are needed.

Implications for politicians and policymakers

The main implication of the evidence set out above, seems clear. Introducing more "frictions" that can help reduce fraud risk is likely to be accepted by the public, but doing so is difficult because the incentives for relevant financial institutions do not encourage it. To overcome this example of the "coordination implementation problem", intervention may be needed.

Recommendation 11: Introduce more "frictions" into the payments system by placing stronger obligations on financial services firms in the "fraud chain" to lower fraud risks for customers so that there is greater assurance over the legitimacy of payments and transfers, including the provenance of senders and receivers of payments and transfers

In 2019 banks and building societies were mandated to introduce the extra "friction" of two-factor authentication for accessing online banking services.[94] This overcame any coordination implementation problem that may otherwise have emerged had it not been mandated but instead relied upon industry norms, encouragement and individual organisations to implement it at their own initiative. The context of growing fraud reimbursement obligations was also, no doubt, important in pushing its implementation along. Lawmakers now need to be prepared to go further. In order to overcome the collective action problem policy needs to step in to ensure payments providers move together and introduce further "frictions" to help reduce instances of fraud involving the payments system.

CHAPTER NINE – THE PUBLIC'S VIEWS ON KEY COUNTER-FRAUD POLICY DEBATES: DATA SHARING

Data sharing underpins much successful counter-fraud activity

As highlighted in Chapter Six, effective data sharing has been an ambition of fraud policy for a long time and needs to sit at the heart of the cooperation that is needed across the organisations in the "fraud chain", within the public sector and between the public and private sectors (see Diagram 1). A contributor to the expert roundtable highlighted it as the central area where policy might be able to make the most difference:

> *"...there is an awful lot that we could be doing ...in terms of more sharing of data...the obvious policy gap...is that this is something that could be done, that would very much benefit the consumer".*

Data sharing is widely seen as essential by all experts on the fraud challenge because it can help overcome the information problems that hinder effective collective actions (see Table 1) against fraud.[95] A participant in the roundtable described succinctly the point of data sharing:

> *"...the scam starts over here, and the ends there. So what we are trying to do is take information from over here in order to protect you over there".*

The counter-fraud benefits of data sharing

The optimal data sharing arrangement (i.e. sharing the right data, in a timely manner on the appropriate scale) can help reduce the information obstacles that contribute to the coordination implementation problem holding back the fraud response (see Box 5 for an outline of benefits that can accrue from more extensive and deeper data sharing).

Box 5: Important counter-fraud benefits of data sharing

In general, data sharing can help prevent frauds succeeding, limit the number of attempted frauds by facilitating pre-emptive actions and better enable those pursuing and disrupting fraudsters to do so successfully. More specifically, data sharing helps improve the accumulation, collation and analysis of data and its formulation into actionable intelligence and dissemination to those who can utilise it, including for the effective identification and tracking of suspicious individuals and behaviours, early detection of emerging threats, protection of data and crime prevention, investigation, the disruption of criminals and risk management.

It was pointed out at the expert roundtable that more extensive and deeper data sharing arrangements is likely to reduce the reliance on "frictions" (discussed in the preceding chapter) as a tool for reducing fraud risks:

> *"...if you get great data sharing, in real time, across all industries...you will...minimise the 'frictions' because you are providing more...protection information...".*

Sufficiently extensive and deep data sharing would enable payment and transfer assurance measures to be more targeted and flexible in the face of a dynamic risk landscape. Further, in the context of the emerging use of artificial intelligence (AI) for malicious purposes by fraudsters, the benefits of data sharing are likely to become more stark, as the picture it provides is likely to prove a vital tool for countering this emerging sophisticated threat.[96] [97]

Box 6: What effective data sharing across the "fraud chain" should include

Expert roundtable contributors were candid about some of the data sharing that was needed to tackle fraud. For example, one detailed a scenario of the kind that, if routine and done in real-time, would help make significant in-roads on the fraud threat:

> *"...there's a scenario where an online platform...could be any type of platform...can recognize what is an interaction between an individual and a fraudster. And that will be the pattern in their records, on their system. That pattern will contain some information that relates to a physical human being who is a victim and some information that relates to the physical organisation or the fraudster. Every single platform has their own version that if they recognize when that has happened, and an individual user of the platform could be exposed to the harms that result, that is the information...[the banks]...want....to see if customers have been in a high risk interaction on an online platform so that the...[account holding institution]...can wrap its arms around their accounts and attach some kind of heavier monitoring...in the...same way that if any intelligence [is] receive[d], for example there's been a data compromise, flags [are put] on accounts...turn the dial on the...monitoring...".*

In addition, internet history data was raised as likely to be useful to tackling fraud risk, as well as:

> *"...transaction related data sharing is one part of It, but we...need additional data, it's data that people are freely giving to make that contract or payment....and there's not a lot of it that we need to make a big advance. Then there's another type which is...slightly outside of the transaction, which is 'transaction data analytics'. So looking at the 'pool of information', because there's so much potential there...if we bring in...the payment system operator, and you look at the intelligence that commercially driven...card networks...credit platforms, etc, have...".*

Extensive and deep data sharing requires an infrastructure to enable it

It was noted at the expert roundtable, that advanced data sharing capabilities would require investment in new data sharing infrastructure, including improvements to the current payments system. It was suggested that the way it currently operates means that it could not support the extent and depth of data sharing and intelligence dissemination that many envisage in needed:

> *"...we should be...thinking about what kind of payment system could operate creatively with this 'pool effect'...the crudity of the existing payment system doesn't really allow that to happen but if we have an intervention that allows us to talk to a receiving bank and say, we've got an amber or red feeling about a payment, you will have an amber and red flag about receiving".*

Improving data sharing between private and public sectors

Equally important to a more effective effort against the fraud epidemic, as Diagram 1 intimated, is data sharing and subsequent intelligence dissemination between the private sector and the authorities, whether in the shape of law enforcement or relevant regulators. The sharing of data between the private and public sectors enables, for example, law enforcement agencies or regulators to ameliorate many of the information barriers that inhibit their ability to build a high quality intelligence picture about fraud and fraudsters. Ultimately, a rich seam of actionable intelligence built from an extensive pool of good quality data, increases the opportunities for investigating and arresting fraudsters and disrupting their activities.[98]

Box 7: Examples of data sharing and the development of and dissemination of effective intelligence that could have lessons for tackling fraud

The anti-money laundering (AML) experience may offer lessons for fraud. The establishment of the Joint Money Laundering Intelligence Task Force (JMLIT) in 2015 to share information about organised crime, between law enforcement and the financial sector, is an example policymakers should look at for possible lessons.[99] According to one report, this taskforce, after five years in operation had led to 970 operational cases being completed, over 4,000 bank accounts identified and 250 arrests made.[100] Particular lesson might include the role of trust, which was key to the success.[101] Investing in the appropriate infrastructure was also vital. The latter included a "trust framework" of rules to help build and sustain relationships which could help resolve difficulties that arose.[102] [xxiv]

Others have highlighted specific examples of data and intelligence sharing success that could be adapted for use by public and private sectors in the UK. One such model is the "Intelligence Fusion Centre",[103] which has been found to be effective in the military intelligence context. Those who advocate for it argue that it would bring together data and analysis about fraud and linked criminality such as cyber-crime from a wide range of sources and evaluate it, compile it into actionable intelligence and disseminate it for action.[104] [105]

There are signs in the private sector that some organisations are seeing the connections between different kinds of economic crime and how efforts against one can inform and complement actions against others. Consequently, some firms are bringing together more systematically, their AML and fraud efforts in order to benefit from economies of scope, scale and knowledge sharing and other complementarities.[106] [107]

Reforming the law to enable deeper and more extensive data sharing

Setting up and running more extensive and deeper data sharing arrangements raises issues about the suitability of the current laws governing data i.e. what can be collected, how it can be utilised and by whom. Current clarifications of the carve outs from data protection rules for example may not go far enough in creating the "space" that is required for the kind of data sharing that is needed.[108] To mitigate this possible problem, some have suggested re-engineering data rules to focus regulation on phases of analysis and use, rather than data collection, storage and sharing.[109]

[xxiv] In the public sector, the provisions of the Digital Economy Acy 2017 around data sharing, have been identified as key to improving the quantity of quality of data sharing that takes place. Source: Paul Shepley and Gavin Freeguard, 'Data Sharing for Counter Fraud Activities', 2023, https://www.instituteforgovernment.org.uk/sites/default/files/2023-01/data-sharing-for-counter-fraud-activities.pdf.

There is a "moment to be seized" in data sharing

Many believe there is currently a "moment to be seized" which can propel data sharing to the next level of efficacy, and deliver a step-change in the fight against fraud.[110] However, there are some doubts, for example, that much of the public sector are ready to seize it. For example, the record of law enforcement with regard to the use of data is largely one of possibilities unfulfilled. Efforts so far are widely seen to have fallen short of exploiting the full range of opportunities for more effective crime fighting provided by modern data analytics.[111] [112] [113]

Therefore, before any new approach to data sharing is developed and infrastructure created, issues related to the capacity and the capabilities of key actors need to be resolved. Among law enforcement, sorting out capacity and capability constrains will likely require improvements in organisation, management, skill levels and technological procurement and adoption processes, in order to be ready to take full advantage of the potential that data and modern data analytics offers.[114]

The public's view on data sharing

Any new data sharing arrangement that is a significant step beyond what already occurs will no doubt have to be implemented with public acquiescence. However, privacy is highly valued by much of the public. Albeit previous analyses suggest there is considerable nuance in the UK public's view on the collection and use of data.[115] Therefore, before data sharing across relevant organisations within private industry and between the public and private sectors is extended and deepened, politicians and policymakers would do well to understand what the public's view on such measures is, and the likely scale of any concern, perhaps even outright opposition beyond that which regularly comes from particular interest groups.

Private sector data sharing

As Figure 18 shows, there is not overwhelming support among the British public for policy preferencing extensive and deep information sharing e.g. among organisations in the "fraud chain", even where it is pointed out that this will help the fight against fraud. Among the general public the balance of opinion is in favour of policy that leans towards privacy and data security rather than sharing (38% against 31%). Notably this reverses somewhat among fraud victims (40% to 34%).

Figure 18: Policy preference – private sector data sharing to reduce fraud risk or strong privacy and data security

Source: Opinium surveys of the UK adult public and fraud victims

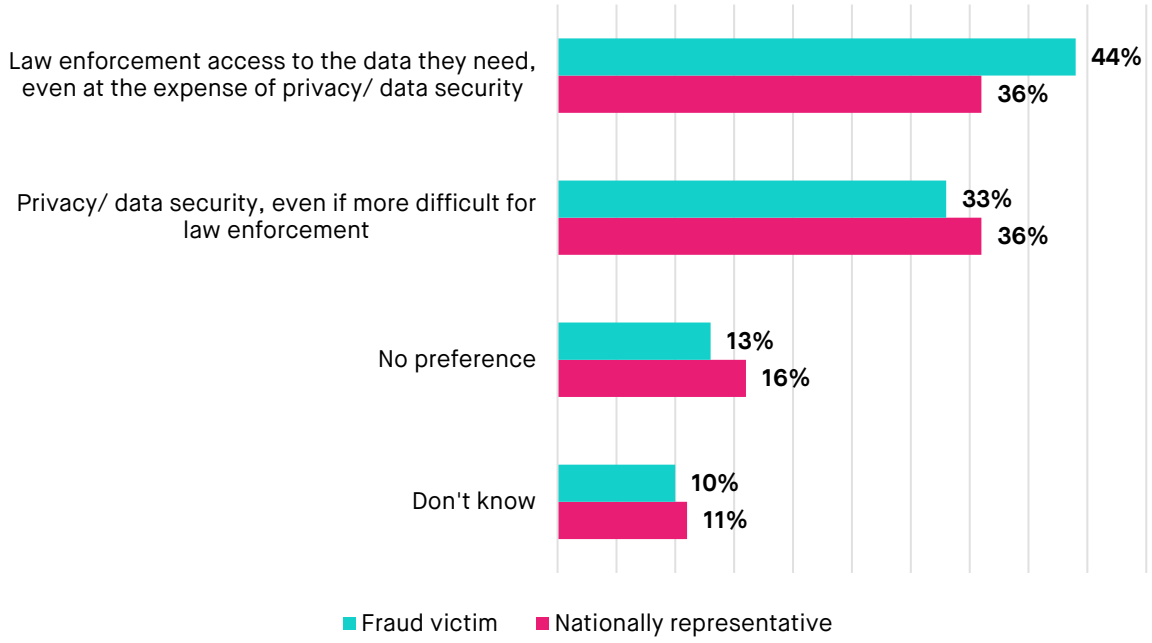
If the respondents that are indifferent were considered to be unopposed to more extensive and deeper data sharing the cumulative proportion of the population either supportive or unconcerned is 51% of UK adults and 59% of victims.

Further, it might be reasonable to expect that the balance between outright opposition and support to change over time among the UK population as more people fall victim to fraud and for that experience to feed through into a higher percentage of people supporting a policy stance that favours greater degrees of data sharing.

Public (law enforcement) – private data sharing

Figure 19 shows an equal split (36%) among the UK public between policy prioritising law enforcement having access to the data they need to pursue and disrupt fraudsters, over one that favours privacy and data security. Figure 19 also demonstrates that, among victims, there is a notable plurality of support for a policy approach that ensures law enforcement's data needs are met so they can pursue and disrupt fraudsters (44%). It also demonstrates that the proportion of victims choosing a policy which privileges privacy and data security (33%) is less than the percentage of the wider public that do so (36%).

Figure 19: Policy preference – law enforcement access to the data they need to pursue and disrupt fraudsters or strong privacy and data security



Source: Opinium surveys of the UK adult public and fraud victims

Taking indifference to mean lack of opposition to a policy that favoured law enforcement access to the data needed to pursue and disrupt fraudsters, the proportion either supportive or accepting of such a policy preference would be 52% of the UK public and 57% of victims. Further, as with private sector data sharing, it seems reasonable to expect that the balance might shift over time as more become fraud victims.

When fraud victims were asked, in the in-depth interviews conducted for this research, about whether it was most important that policy favoured the needs of law enforcement on the one hand or privacy and data security on the other, they provided nuanced views. For example, one victim of a scam advert for foreign exchange services highlighted how it was only the police that are likely to take any action:

> *"...I don't think we should block the police from primary details... if we're blocking the police from trying to find out, I don't think that's a good thing...I don't have a great deal of competence in these sites, because they don't seem to do anything when things go a bit pear shaped, don't seem to change, they don't seem to take any precautions or do something about it".*

There was an attempt by a number of the interviewed victims to try and reconcile their desire for strong privacy protection policies with the ability of law enforcement to ultimately access the information they need to. An interview participant who fell victim to credit card fraud was typical of several of those spoken to:

> *"...if you can prevent it happening in the first place, then there's nothing to investigate. That is the theory. However, what we're told is that you can prevent something this week, and the criminals will find a way around it next week. So that end of the spectrum worries me...how effective would that be? The other end of the spectrum would be a concern if they couldn't investigate things of national security..."*.

However, one interviewee was clear in their preference for privacy and data security in government policy, reflecting that third of fraud victims that want to see privacy and data security prioritised over law enforcement needs. They explained why they took the view they did:

> *"...I think being proactive to the problem is, number one, it should be the focus, because...it then obviously, prevents loads of cases...Police haven't got a lot people...working on these things that you need...and so... the police are not up to date with what's going on...the things happening every single day...the problems are always a step ahead of the police..."*.

Persuading the public that data sharing needs to be more extensive and deeper

A participant in the expert roundtable suggested that the case for the importance of data sharing needed to be made to the public, in order to put in place the kind of extensive and deep data sharing approach necessary to make inroads into the levels of fraud currently being experienced:

> *"...fraud, most consumers do not understand what it is...those who are policy makers...in the industry have...need to get involved in making sure consumers are aware of what the risks are, trade-offs are and help to shift the dial on some of this"*.

Another raised parallels with other efforts in the past that have brought about substantial shifts in public opinion around from scepticism and even outright opposition to a new consensus:

> *"...we need to...help consumers understand what goes on...about 30 years ago consumers gave up on drink and drive. We've moved a long way from that because what's acceptable migrated to the safety piece"*.

Box 8: Messaging to persuade more of the public of the central importance of data sharing and law enforcement's access to personal, financial and other data

A participant at the expert roundtable convened by SMF outlined their view on the kinds of messaging needed to help persuade more of the public to support the extensive and deep data sharing needed to bring about a better response to the problem of fraud:

> *"...collectively, we need to decide what it is we're telling them, what we want to share to help protect them and the system...if we say, look, this has...been done to protect you...it's not going to be used to profile you in every financial institution in the UK".*

There is international research that has looked at what arguments and messages about police access to and use of data the public can find persuasive. While what works is always likely to be culturally contingent to some degree, the evidence suggested that public backing can be increased if the benefits to maximising citizen's freedoms and improving the protection of their personal security is emphasised.[116]

Implications for politicians and policymakers

Data sharing is essential because it helps reduce the information gaps that prevent more coherent and coordinated counter-fraud efforts being taken by the organisations in the "fraud chain" and agencies in the public sector such as law enforcement. Despite some scepticism among parts of the public, the centrality of data and its role in building an actionable intelligence picture is unavoidable. This indicates that politicians and policymakers should be looking to act on two fronts to significantly ameliorate the information barriers currently stifling the response to fraud, through data sharing:

- Working to persuade as much of the public as possible of the importance of data sharing across the "fraud chain" and between the private and the public sectors.
- Establishing an appropriate data sharing environment where organisations in the "fraud chain" can share the data they require and the public and private sectors are able to share the data that is necessary, in order to maximise benefits of intelligence in the fight against fraud.

Recommendation 12: Develop a more extensive and deeper data sharing arrangement across the organisations that are part of the "fraud chain" and between the private sector and appropriate parts of the public sector

The Government's fraud strategy envisages enhancing current data sharing arrangements.[117] However, it is unlikely to deliver to the extent and the depth of data sharing that was envisaged at our expert roundtable, and which is essential in order to make a substantial and sustained impact on fraud levels.

As part of politicians' and policymakers' thinking about what comes after the current fraud strategy is implemented, the government should develop a plan for putting in place a new, extensive and deep, data sharing architecture that all relevant public and private actors are part of. The development process should include a number of elements:

- Identifying the necessity for a new legislative framework to facilitate a more extensive and deeper sharing arrangement between organisations in the "fraud chain", agencies and departments in the public sphere and between the public and private sectors.[xxv] This should include consideration of whether the current laws on data need to move away from the current regime and towards one that regulates phases of analysis and use, in the pursuit of a more effective data sharing approach.
- The desirability of a power to mandate participation if the organisations in the "fraud chain" refuse to get involved voluntarily and appropriate public sector agencies fail to engage sufficiently.
- Utilising existing data sharing expertise in building the more advanced data sharing approach. For example Cifas has established itself as an important service by building up and operating a successful data sharing operation for the financial services sector. This expertise should be leveraged where useful to do so.
- Learning lessons from other areas of economic crime such as AML, where data sharing is more advanced and tools such as Suspicious

[xxv] Some of the lessons as to what a new regime may need to take account of and reflect can be learnt from other experiences at creating a more conducive data sharing environment to tackle crime, such as the changes made to the law to enable more public sector data sharing in the Digital Economy Act 2017, those currently envisaged in the Data Protection and Digital Information Bill and those in the economic Crime and Corporate Transparency Bill. Sources: 'Digital Economy Act 2017' (n.d.), https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted; Adam Clark et al., 'The Data Protection and Digital Information (No. 2) Bill 2022-23', 28 March 2023, https://commonslibrary.parliament.uk/research-briefings/cbp-9746/ and Russell Taylor, 'Economic Crime and Corporate Transparency Bill', 2023, https://researchbriefings.files.parliament.uk/documents/LLN-2023-0008/LLN-2023-0008.pdf

Activity Reports (SAR) are widely used to help build an intelligence picture, rather than relying primarily on the formal reporting of crimes.

- Borrowing intelligence sharing models from outside economic crime where appropriate, for example, examining the case for adopting the Data Fusion Centres approach to sharing, which have proven successful models in the military context.
- Formally aligning laws and policies and integrating approaches and activities where there are clear benefits to doing so. For example, in the private sector fraud and AML efforts are beginning to be brought together. There may be lessons for the public sector from such trends. Similarly, there has been a close interconnection between fraud and cyber-crime for a long time.[xxvi] The somewhat artificial division in the policy and operational treatment of these two types of crime in particular, can be somewhat perplexing.
- Using the NECC as the fulcrum for the new data sharing architecture. As more extensive and deeper data sharing could deliver significant societal benefits, the government should not be afraid to reflect that by helping to support the development of a better data sharing infrastructure financially, outside of any law enforcement contribution.

Recommendation 13: Set-up a national ID protection service to help reduce the risk of ID related fraud

The government and the FCA should encourage the development of a service, or support the extension of the current Cifas Protective Registration service,[118] to offer greater protection against ID fraud to UK consumers who want it. With a more extensive data sharing arrangement in place, it would be a national service that alerted consumers to efforts to use their personal information to access financial services products, which consumers would be able to halt in real time, through an appropriate app or registration service account. Such a service would help reduce instances of ID fraud where credit or other financial products are obtained using someone else's ID. Over time, the expectation would be that this service could be rolled into the improved data sharing regime described in Recommendation 12.

[xxvi] The SMF has argued in the past that the divisions between fraud, cyber-crime and serious and organised crime (SOC) are somewhat nominal because of their close interconnection and these three categories of crime should be treated more holistically by both policy and law enforcement. Source: Richard Hyde, Scott Corfe, and Anderson-Samways, 'Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up', Social Market Foundation. (blog), 4 March 2022, https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/.

ANNEX I – THE GOVERNMENT'S FRAUD STRATEGY

The main components of the Government's fraud strategy

The fraud strategy has set out the ambition to reduce fraud against the population of England and Wales by 10% below the pre-Covid level.[119] To achieve this, it proposes steps to try and address some of the deficiencies in the current counter-fraud landscape. For example, the creation of the new Anti-Fraud Champion role is an attempt to bring some leadership to the issue across government and coordinate actions.

Box 9: Some of the most salient proposals contained in the Government's fraud strategy

The fraud strategy proposed measures to:

- Reduce abuse of telephone network services by banning cold calling about financial products as well as SIM farms, regulating mass texting services and tackling number "spoofing".[120]
- Increase transparency about fraud on digital platforms by publishing data on the amount of fraud going on different platforms, as well as encourage the platforms to do more to tackle fraud through making it easier for consumers to report scams and agree a new voluntary charter which is aimed at boosting the efforts of the technology platforms against fraud that is propagated through them.[121]
- Enhance the law enforcement response the strategy proposed replacing Action Fraud with a new and improved service, making fraud a Strategic Policing requirement (SPR) and creating a new NFS jointly overseen by the NCA and City of London Police, improving intelligence sharing between industry and the police and bringing in the intelligence services to help improve the fraud intelligence picture.[122]
- Improve consumer education about fraud threats by overhauling the current approach to consumer awareness raising and information provision.[123]
- Galvanise the intentional community into greater action against fraud, in the first instance by hosting a global fraud summit in 2024.[124]

While the fraud strategy includes some steps forward, which should be welcomed, it falls short of the kind of step-change in the response to fraud that is needed to deal with the scale of the fraud being perpetrated against the UK. Common criticisms have included:

- The missed the opportunity to make bigger structural reforms to strengthen coordination and control over both fraud policy-making and law enforcement activity.[125]
- The likely impact of the small uplift of only 400 new NFS.[126] [127]

- The lack of clarity over the long-term funding of counter-fraud activity.[128]
- The weakness of a voluntary charter for technology companies to drive prioritisation and behavioural change. It is a measure that has been used in conjunction with other industries previously to try and improve the response to fraud from them.[129] [130] Critics were sceptical that, given the significant role technology services play in propagating fraud and the jurisdictional complexities involved when dealing with transnational technology firms, that such a charter will make much difference.[131]

ANNEX II – COLLECTIVE ACTION PROBLEMS

Box 10: Collective action problems

The degree of collective action between organisations or individuals in any particular circumstances can vary widely. Frequently, there is not one collective action problem but many. Three collective action problems tend to reoccur often:

- Public good provision problems.
- Coordinated implementation problems.
- Problems of correcting externalities

Various obstacles prevent societal problems from being resolved in the optimum way. Many of the relevant actors to a problem have common interests but also conflicting interests and are mainly motivated to optimise their own positions. Consequently issues such as the costs that agents will incur by taking societally beneficial actions compared to the benefits, are determinants of behaviour.[132] Further, information asymmetries between the parties to a common problem lead to knowledge gaps and an inability to make the best decisions. Consequently these inhibit collection action, too.

The heterogeneity of relevant actors to a problem makes cooperation more challenging still, as the differences that need to be abridged to undertake collective endeavours raises the costs further. Homogeneity can make collective action easier. Therefore, collective action between similar agents, say within a single industry, would be expected to be easier to organise than that between agents spread across different industries.

ENDNOTES

[1] Richard Hyde, 'Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud on the UK', Social Market Foundation., accessed 11 September 2023, https://www.smf.co.uk/publications/impact-of-fraud-on-the-uk/.

[2] Hyde.

[3] Aaron Chalfin, 'Economic Costs of Crime', The Encyclopedia of Crime and Punishment, 2015, https://scholar.google.com/citations?view_op=view_citation&hl=en&user=wJJLcZoAAAAJ&citation_for_view=wJJLcZoAAAAJ:aqlVkmm33-oC.

[4] Charles Hymas, 'Suella Braverman: Police Must Investigate Every Theft', *Daily Telegraph*, 28 August 2023, https://www.telegraph.co.uk/politics/2023/08/28/suella-braverman-police-must-investigate-every-theft/.

[5] Hymas.

[6] Crime in England and Wales - Office for National Statistics (ons.gov.uk)

[7] 'Fraud Poll Feb 2022' (Find Out Now, 16 February 2022), https://www.electoralcalculus.co.uk/blogs/ec_fraudpoll_20220216.html.

[8] National Audit Office, "Progress Combating Fraud," 2022, Progress combatting fraud (nao.org.uk).

[9] Progress combatting fraud (parliament.uk)

[10] House of Commons Home Affairs Select Committee, 'Policing for the Future', 2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/515.pdf.

[11] 'Fighting Fraud: Breaking the Chain' (House of Lords: Fraud Act 2006 and Digital Fraud Committee, 12 November 2022). National Audit Office, "Progress Combating Fraud," 2022, Progress combatting fraud (nao.org.uk).

[12] 'Fraud Poll Feb 2022'.

[13] 'Fraud Strategy: The Right Target but Not Enough Fire Power', Social Market Foundation., 2023, https://www.smf.co.uk/commentary_podcasts/fraud-strategy-the-right-target-but-not-enough-fire-power/.

[14] Richard Hyde, 'Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud on the UK', Social Market Foundation., accessed 11 September 2023, https://www.smf.co.uk/publications/impact-of-fraud-on-the-uk/.

[15] Hyde.

[16] Anna Gekoski, Joanna R Adler, and Tim McSweeney, 'Profiling the Fraudster: Findings from a Rapid Evidence Assessment', 2022, https://www.tandfonline.com/doi/epdf/10.1080/17440572.2022.2137670?needAccess=true&role=button.

[17] Yaniv Hanoch and Stacey Wood, 'The Scams Among Us: Who Falls Prey and Why', *Current Directions in Psychological Science* 30, no. 3 (2021), https://doi.org/10.1177/0963721421995489.

[18] HMICFRS, 'Fraud: Time to Choose - An Inspection of the Police Response to Fraud' (HMICFRS, 2019), https://www.justiceinspectorates.gov.uk/hmicfrs/publications/an-inspection-of-the-police-response-to-fraud/.

[19] Sarah Garner, Ruth Crocker, and Michael Skidmore, 'Organised Fraud in Local Communities' (Police Foundation London, 2016).

[20] HM Government, 'Fraud Strategy: Stopping Scams and Protecting the Public', 2023, Tackling fraud and rebuilding trust (publishing.service.gov.uk).

[21] Mark Button, Chris Lewis, and Jacki Tapley, 'A Better Deal for Fraud Victims' (National Fraud Authority, 12 December 2009).

[22] Blakeborough and Correia, 'The Scale and Nature of Fraud', 8.

[23] Button, Lewis, and Tapley, 'A Better Deal for Fraud Victims', 26.

[24] Blakeborough and Correia, 'The Scale and Nature of Fraud'.

[25] Button, Lewis, and Tapley, 'A Better Deal for Fraud Victims', 26.

[26] Button, Lewis, and Tapley, 27.

[27] Mark Button and Martin Tunley, 'Explaining Fraud Deviancy Attenuation in the United Kingdom', *Crime, Law and Social Change* 63, no. 1 (1 March 2015): https://doi.org/10.1007/s10611-015-9551-0.

[28] Mark Button, Chris Lewis, and Jacki Tapley, 'Not a Victimless Crime: The Impact of Fraud on Individual Victims and Their Families', *Security Journal* 27, no. 1 (1 February 2014): 36–54, https://doi.org/10.1057/sj.2012.11.

[29] Ministry of Justice, 'The Code of Practice for Victims of Crime in England and Wales and Supporting Public Information Materials'.

[30] National Audit Office, "Progress Combating Fraud," 2022, Progress combatting fraud (nao.org.uk).

[31] Richard Hyde, Scott Corfe, and Anderson-Samways, 'Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up', *Social Market Foundation.* (blog), 4 March 2022, https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/.

[32] Mark Button, Chris Lewis, and Jacki Tapley, 'A Better Deal for Fraud Victims' (National Fraud Authority, 12 December 2009), 49.

[33] Richard Hyde, 'Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud on the UK', Social Market Foundation., accessed 11 September 2023, https://www.smf.co.uk/publications/impact-of-fraud-on-the-uk/.

[34] Hyde.

[35] Button, Lewis, and Tapley, 'Not a Victimless Crime'.

[36] Hyde, 'Fraudemic'.

[37] 'Consumer Duty', Financial Conduct Authority, 15 September 2022, https://www.fca.org.uk/firms/consumer-duty.

[38] Action Fraud, 'Specialist Victim Care Unit Which Supports Thousands of Vulnerable Fraud Victims Rolled out across the UK', Action Fraud, 2023, https://www.actionfraud.police.uk/news/specialist-victim-care-unit-which-supports-thousands-of-vulnerable-fraud-victims-rolled-out-across-the-uk.

[39] maintenance, 'Fraud', *Victim Support* (blog), accessed 11 September 2023, https://www.victimsupport.org.uk/crime-info/types-crime/fraud/.

[40] Cassandra Cross, 'No Laughing Matter: Blaming the Victim of Online Fraud', *International Review of Victimology* 21, no. 2 (1 May 2015): 187–204, https://doi.org/10.1177/0269758015571471.

[41] Mark Button, Chris Lewis, and Jacki Tapley, 'Not a Victimless Crime: The Impact of Fraud on Individual Victims and Their Families', *Security Journal* 27, no. 1 (1 February 2014): 48, https://doi.org/10.1057/sj.2012.11.

[42] Mark Button, Chris Lewis, and Jacki Tapley, 'A Better Deal for Fraud Victims' (National Fraud Authority, 12 December 2009).

[43] Blakeborough and Correia, 'The Scale and Nature of Fraud'.

[44] Richard Hyde, 'Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud on the UK', Social Market Foundation., accessed 11 September 2023, https://www.smf.co.uk/publications/impact-of-fraud-on-the-uk/.

[45] Monidipa Fouzder3 July 2017, 'More Prosecution Data Needed to Tackle Online Fraud', Law Gazette, 3 July 2017, https://www.lawgazette.co.uk/law/more-prosecution-data-needed-to-tackle-online-fraud/5061833.article.

[46] Mark Button et al., *Fraud and Punishment: Enhancing Deterrence through More Effective Sanctions: Main Report* (Portsmouth: University of Portsmouth, 2012).

[47] Jane Kerr et al., Research *on Sentencing Online Fraud Offences* (London: Crown Copyright, 2013).

[48] Commissioner for Victims and Witneses in England and Wales, 'Victims' Views of Court and Sentencing: Qualitative Research with WAVES Victims', 2011, https://www.justice.gov.uk/downloads/news/press-releases/victims-com/victims-views-court-sentencing1011.pdf.

[49] 'The Action Fraud National Economic Crime Victim Care Unit (AF-NECVCU)', Action Fraud, accessed 11 September 2023, https://www.actionfraud.police.uk/economic-crime-victim-care-unit-ecvcu.

[50] maintenance, 'Fraud', *Victim Support* (blog), accessed 11 September 2023, https://www.victimsupport.org.uk/crime-info/types-crime/fraud/.

[51] Richard Hyde, 'Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud on the UK', Social Market Foundation., accessed 11 September 2023, https://www.smf.co.uk/publications/impact-of-fraud-on-the-uk/.

[52] Matthew Heeks et al., "The Economic and Social Costs of Crime: Second Edition," Research Report, (2018), The economic and social costs of crime (publishing.service.gov.uk).

[53] HM Government, 'Fraud Strategy: Stopping Scams and Protecting the Public', 2023, Tackling fraud and rebuilding trust (publishing.service.gov.uk).

[54] Brian Bell, Laura Jaitman, and Stephen Machin, 'Crime Deterrence: Evidence From the London 2011 Riots', *The Economic Journal* 124, no. 576 (2014): 480–506, https://doi.org/10.1111/ecoj.12137.

[55] 'Get Financial Support as a Victim of Crime', GOV.UK, accessed 11 September 2023, https://www.gov.uk/financial-support-victim-of-crime.

[56] Richard Hyde, 'Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud on the UK', Social Market Foundation., accessed 11 September 2023, https://www.smf.co.uk/publications/impact-of-fraud-on-the-uk/.

[57] Hyde.

[58] Payment Services Regulator (PSR), 'Fighting Authorised Push Payment Fraud: A New Reimbursement Requirement - Response to September 2022 Consultation', Policy Statement, 2023, PS23/2 Fighting authorised push payment fraud: a new reimbursement requirement (psr.org.uk).

[59] Richard Detura et al., 'A New Approach to Fighting Fraud While Enhancing Customer Experience | McKinsey', accessed 11 September 2023, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-approach-to-fighting-fraud-while-enhancing-customer-experience.

[60] Detura et al.

[61] Alan Doig and Michael Levi, 'Editorial: The Dynamics of the Fight against Fraud and Bribery—Reflections on Core Issues in This PMM Theme', *Public Money & Management* 40, no. 5 (2020): 343–48, https://doi.org/10.1080/09540962.2020.1752547.

[62] Helena Wood and Karen Baxter, 'Towards a New Model for Economic Crime Policing: Target 2030', 2022, https://static.rusi.org/towards-a-new-model-for-economic-crime-policing.pdf.

[63] 'Fraud: Time to Choose - An Inspection of the Police Response to Fraud' (HMICFRS, April 2019), https://www.justiceinspectorates.gov.uk/hmicfrs/publications/an-inspection-of-the-police-response-to-fraud/.

[64] 'Fighting Fraud: Breaking the Chain' (House of Lords: Fraud Act 2006 and Digital Fraud Committee, 12 November 2022).

[65] 'Fighting Fraud: Breaking the Chain'.

[66] House of Commons Home Affairs Select Committee, 'Policing for the Future', 2018, https://publications.parliament.uk/pa/cm201719/cmselect/cmhaff/515/515.pdf.

[67] Mark Button, Chris Lewis, and Jacki Tapley, 'Not a Victimless Crime: The Impact of Fraud on Individual Victims and Their Families', *Security Journal* 27, no. 1 (1 February 2014): 36–54, https://doi.org/10.1057/sj.2012.11.

[68] Blakeborough and Correia, 'The Scale and Nature of Fraud'.

[69] Blakeborough and Correia.

[70] Josh Robbins, 'Exclusive: More than 96% of Reported Fraud Cases Go Unsolved - Which? News', Which?, 24 September 2018, https://www.which.co.uk/news/article/exclusive-more-than-96-of-reported-fraud-cases-go-unsolved-apfql3E0JxDz.

[71] City of London Police, 'Annual Report 2020/2021', Annual report, 2021.

[72] Hyde, Corfe, and Anderson-Samways, 'Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up'.

[73] 'Fighting Fraud: Breaking the Chain' (House of Lords: Fraud Act 2006 and Digital Fraud Committee, 12 November 2022).

[74] Sneha Dawda, Ardi Janjeva, and Anton Moiseienko, 'The UK's Response to Cyber Fraud: A Strategic Vision', 2021, https://static.rusi.org/cyber_fraud_final_web_version.pdf.

[75] UK Finance, 'Fraud - The Facts 2021: The Definitive Overview of Payment Industry Fraud', 2021, https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf.

[76] 'Annual Fraud Report: The Definitive Overview Of Payment Industry Fraud In 2021' (UK Finance, 2022), 7, https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022_FINAL_.pdf.

[77] Department for Digital, Culture, Media and Sport, 'New Fines for Essential Service Operators with Poor Cyber Security', GOV.UK, 8 August 2017, https://www.gov.uk/government/news/new-fines-for-essential-service-operators-with-poor-cyber-security.

[78] Tyler Moore, 'The Economics of Cybersecurity: Principles and Policy Options', *International Journal of Critical Infrastructure Protection* 3, no. 3 (2010): 103–17, https://doi.org/10.1016/j.ijcip.2010.10.002.

[79] HM Government, 'Fraud Strategy: Stopping Scams and Protecting the Public', 2023, Tackling fraud and rebuilding trust (publishing.service.gov.uk).

[80] HM Government.

[81] 'Fraud Strategy: The Right Target but Not Enough Fire Power', Social Market Foundation., 2023, https://www.smf.co.uk/commentary_podcasts/fraud-strategy-the-right-target-but-not-enough-fire-power/.

[82] Hyde, Corfe, and Anderson-Samways, 'Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up'.

[83] Payment Services Regulator (PSR), 'Fighting Authorised Push Payment Fraud: A New Reimbursement Requirement - Response to September 2022 Consultation', Policy Statement, 2023, PS23/2 Fighting authorised push payment fraud: a new reimbursement requirement (psr.org.uk).

[84] Richard Hyde, 'Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud on the UK', Social Market Foundation., accessed 11 September 2023, https://www.smf.co.uk/publications/impact-of-fraud-on-the-uk/.

[85] Button, Lewis, and Tapley, 'A Better Deal for Fraud Victims'.

[86] Lloyds Banking Group, 'Two-Thirds of All Online Shopping Scams Now Start on Facebook and Instagram', 30 May 2023, https://www.lloydsbankinggroup.com/media/press-releases/2023/lloyds-banking-group-2023/two-thirds-of-all-online-shopping-scams-now-start-on-facebook-and-instagram.html.

[87] House of Lords, 'The Government Must Take the Fight to the Fraudsters by Slowing down Faster Payments and Prosecuting Corporates for Failure to Prevent Fraud', 12 November 2022, https://www.parliament.uk/business/lords/media-centre/house-of-lords-media-notices/2022/november-2022/the-government-must-take-the-fight-to-the-fraudsters-by-slowing-down-faster-payments-and-prosecuting-corporates-for-failure-to-prevent-fraud/.

[88] UK Finance, 'UK Payment Markets Summary 2021', 2021, https://www.ukfinance.org.uk/sites/default/files/uploads/SUMMARY-UK-Payment-Markets-2021-FINAL.pdf.

[89] Tom Groenfeldt, 'Will Faster Payments Lead To Faster Fraud?', Forbes, accessed 11 September 2023, https://www.forbes.com/sites/tomgroenfeldt/2020/02/04/will-faster-payments-lead-to-faster-fraud/.

[90] Julie Conroy, Trace Fooshée, and David Mattei, 'Faster Payments, Faster Fraud', Impact Report, 2023, https://aite-novarica.com/sites/default/files/storage_0/20230503_Faster%20Payments%2C%20Faster%20Fraud_Summary.pdf.

[91] Lindsay Anan et al., 'Fraud Management: Recovering Value through next-Generation Solutions | McKinsey', 20 August 2018, https://www.mckinsey.com/industries/financial-services/our-insights/fraud-management-recovering-value-through-next-generation-solutions#/.

[92] Gabrielle Inhofe, 'Global Consumers' Authentication Preferences', Impact Report, 2023.

[93] Richard Detura et al., 'A New Approach to Fighting Fraud While Enhancing Customer Experience | McKinsey', accessed 11 September 2023, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-approach-to-fighting-fraud-while-enhancing-customer-experience.

[94] 'The Payment Services Regulations 2017', n.d.

[95] PaymentsJournal, 'Data Sharing as a Means to Combat Fraud', *PaymentsJournal* (blog), 16 December 2022, https://www.paymentsjournal.com/data-sharing-as-a-means-to-combat-fraud/.

[96] Luke Stevens, 'Generative AI and Fraud – What Are the Risks That Firms Face?', Deloitte United Kingdom, accessed 16 June 2023, https://www2.deloitte.com/uk/en/blog/auditandassurance/2023/generative-ai-and-fraud-what-are-the-risks-that-firms-face.html.

[97] Mercedes Page, 'Malicious AI Arrives on the Dark Web', Policing Insight, 25 August 2023, https://policinginsight.com/feature/analysis/malicious-ai-arrives-on-the-dark-web/.

[98] Alan Santos et al., 'Investigative Analytics - Leveraging Data for Law Enforcement Insights', Deloitte Insights, 21 February 2019,

https://www2.deloitte.com/us/en/insights/industry/public-sector/law-enforcement-investigative-analytics.html.

[99] Paul Shepley and Gavin Freeguard, 'Data Sharing for Counter Fraud Activities', 2023, https://www.instituteforgovernment.org.uk/sites/default/files/2023-01/data-sharing-for-counter-fraud-activities.pdf.

[100] Shepley and Freeguard.

[101] Shepley and Freeguard.

[102] Shepley and Freeguard.

[103] Department of Homeland Security, 'Role of Fusion Centers in Countering Violent Extremism Overview', n.d., https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/roleoffusioncentersincounteringviolentextremism_compliant.pdf.

[104] Stephen Lazenby, 'Building Resilience to Financial Crime: The Convergence of Cyber Intelligence, AML and Fraud Prevention', 13 January 2022, https://www.inetco.com/blog/the-convergence-of-cyber-intelligence-aml-and-fraud-prevention/.

[105] Duncan Ash, 'Fraud, Finance, and Fusion Centres: Tackling Cybercrime in 2023', 2023, http://www.futuresparity.com/business/fraud-finance-and-fusion-centres-tackling-cybercrime-in-2023/.

[106] FICO, 'Fraud and Financial Crime Management Are Converging – But How Fast?', FICO Decisions Blog, 12 September 2019, https://www.fico.com/blogs/fraud-and-financial-crime-management-are-converging-how-fast.

[107] T J Horan, 'Fraud and Financial Crime Convergence: It's Really Here!', FICO Decisions Blog, 28 May 2020, https://www.fico.com/blogs/fraud-and-financial-crime-convergence-its-really-here.

[108] Adam Clark et al., 'The Data Protection and Digital Information (No. 2) Bill 2022-23', 28 March 2023, https://commonslibrary.parliament.uk/research-briefings/cbp-9746/.

[109] Dennis Broeders et al., 'Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data', *Computer Law & Security Review* 33 (1 April 2017), https://doi.org/10.1016/j.clsr.2017.03.002.

[110] Taavi Tamkivi, 'How to Facilitate Fincrime Intelligence Sharing without Compromising Privacy or Regulatory Compliance', UK Finance, n.d., https://www.ukfinance.org.uk/news-and-insight/blogs/how-facilitate-fincrime-intelligence-sharing-without-compromising-privacy-or-regulatory-compliance.

[111] Alexander Babuta, 'Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities', 6 September 2017, https://www.rusi.orghttps://www.rusi.org.

[112] Babuta.

[113] Ian Weinfass, 'Getting a Grip on Policing's Data Analysis and Performance Management Problems', Policing Insight, August 2023, https://policinginsight.com/feature/analysis/getting-a-grip-on-policings-data-analysis-and-performance-management-problems/.

[114] Alan Santos et al., 'Investigative Analytics - Leveraging Data for Law Enforcement Insights', Deloitte Insights, 21 February 2019, https://www2.deloitte.com/us/en/insights/industry/public-sector/law-enforcement-investigative-analytics.html.

[115] Vian Bakir et al., 'Public Feeling on Privacy, Security and Surveillance', 2015.

[116] Youngsub Lee and Jongchan Park, 'Using Big Data to Prevent Crime: Legitimacy Matters', *Asian Journal of Criminology* 17, no. 1 (2021): 61–80, https://doi.org/10.1007/s11417-021-09353-4.

[117] HM Government, 'Fraud Strategy: Stopping Scams and Protecting the Public', 2023, Tackling fraud and rebuilding trust (publishing.service.gov.uk).

[118] Jarrett & Lam Limited, 'Protective Registration | Identity Protection Service | Cifas', n.d., https://www.cifas.org.uk/pr.

[119] HM Government, 'Fraud Strategy: Stopping Scams and Protecting the Public', 2023, Tackling fraud and rebuilding trust (publishing.service.gov.uk).

[120] HM Government.

[121] HM Government.

[122] HM Government.

[123] HM Government.

[124] HM Government.

[125] ICAEW Insights, 'UK Fraud Strategy: What It Delivers, What It Lacks | ICAEW', 4 May 2023, https://www.icaew.com/insights/viewpoints-on-the-news/2023/may-2023/UK-Fraud-Strategy-what-it-delivers-what-it-lacks.

[126] 'Fraud Strategy: The Right Target but Not Enough Fire Power', Social Market Foundation., 2023, https://www.smf.co.uk/commentary_podcasts/fraud-strategy-the-right-target-but-not-enough-fire-power/.

[127] Helena Wood and Kathryn Westmore, 'RUSI Experts React to The UK Government's New Fraud Strategy', 3 May 2023, https://www.rusi.orghttps://www.rusi.org.

[128] Wood and Westmore.

[129] Home Office, 'Fraud Sector Charter: Accountancy', GOV.UK, 26 October 2021, https://www.gov.uk/government/publications/joint-fraud-taskforce-accountancy-charter.

[130] Home Office, 'Fraud Sector Charter: Telecommunications', GOV.UK, 21 November 2022, https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter.

[131] ICAEW Insights, 'UK Fraud Strategy: What It Delivers, What It Lacks | ICAEW'.

[132] William D. Ferguson, 'Collective-Action Problems and Institutional Systems', in *The Political Economy of Collective Action, Inequality, and Development*, ed. William D. Ferguson (Stanford University Press, 2020), 0, https://doi.org/10.11126/stanford/9781503604612.003.0002.