It’s a fraudster’s world

Exploring the scale, impact, and globally interconnected nature of fraud against consumers

Richard Hyde
John Asthana Gibson

SMF Social Market Foundation

It’s a fraudster’s world

Exploring the scale, impact, and globally interconnected nature of fraud against consumers

Richard Hyde
John Asthana Gibson

Kindly supported by

Santander

FIRST PUBLISHED BY

The Social Market Foundation, September 2024
Third Floor, 5-6 St Matthew Street, London, SW1P 2JT
Copyright © The Social Market Foundation, 2024

The moral right of the authors has been asserted. All rights reserved. Without limiting the rights under copyright reserved above, no part of this publication may be reproduced, stored or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of both the copyright owner and the publisher of this book.

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.

CHAIR

Professor Wendy Thomson CBE

DIRECTOR

Theo Bertram

TRUSTEES

Professor Tim Bale
Tom Ebbutt
Caroline Escott
Baroness Olly Grender MBE
Rt Hon Dame Margaret Hodge MP
Sir Trevor Phillips OBE
Melville Rodrigues

CONTENTS

ACKNOWLEDGEMENTS

This report would not have been possible without the partnership of Santander and Teneo, and we extend our gratitude to both. In addition, SMF would like to thank:

- The experts who participated in the interviews we undertook in late 2023 and early 2024. These were:
  - Javahir Askari, Policy Manager, Digital Regulation, TechUK.
  - Professor Mark Button Professor of Criminology and Director of the Centre for Cybercrime and Economic Crime, School of Criminology and Criminal Justice, University of Portsmouth.
  - Brian Dilley, former Group Director of Economic Crime Prevention at Lloyds Banking Group, now Managing Director of BD Consulting.
  - Dr Emily Finch, Senior Lecturer in Law, University of Surrey.
  - Professor Thomas Holt, School of Criminal Justice, Michigan State University.
  - Dr Rasha Kassem, Senior Lecturer in Accounting, Aston Business School, Aston University.
  - Professor Michael Levi, Professor of Criminology, School of Social Sciences, Cardiff University.
  - Anna Martin, Senior Financial Services Officer, BEUC.
  - Professor Nicholas Ryder, Professor of Law, School of Law and Politics, Cardiff University.
  - Nicholas Smart, Director of Blockchain Intelligence and Data, Crystal Blockchain Analytics.
  - Professor Russell Smith, College of Business, Government and Law, Flinders University and Fellow and former President of the Australian and New Zealand Society of Criminology, an Honorary Fellow of the Australian Institute of Criminology.
  - Kathryn Westmore, Senior Research Fellow at the Centre for Financial Crime and Security Studies, Royal United Services Institute (RUSI).
- The more than 28,000 members of the public that responded to the surveys that were conducted across 15 countries.
- George Pinder and Anna Bayley at Focal Data for their help in designing the survey, managing it in the field and subsequently providing the SMF with the data and various data tables.
- Zeki Dolen and Richa Kapoor, SMF's Events and Communications Intern and Impact Officer respectively, for their proofreading of the drafts of the report and for designing and formatting the final report.

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

John Asthana Gibson

John joined the Social Market Foundation in March 2023. Prior to joining the SMF, John worked at the Centre for Cities, where he conducted research on topics including transport policy, devolution and the geography of the innovation economy. He holds a BA Hons in Economics from the University of Manchester.

FOREWORD FROM THE SPONSOR

It comes as no surprise to see that fraud is a big issue in the UK. UK Finance reported over 230,000 cases of authorised fraud in 2023, and nearly 3 million fraud cases in total. The real figure, as this report suggests, may be even higher. That's why banks such as Santander continue to dedicate significant resource into protecting our customers. For example, Santander is proud of its 'Break the Spell' team, a specialist team whose role it is to identify the most complex of scams and help customers come to terms with the fact that they have been scammed, and its dynamic scam warnings, which interrupt the digital payment journey to ask a series of tailored questions to try and prevent money being inadvertently transferred to criminals.

Despite these efforts, the SMF found that 10 million Britons fell victim to fraud between 2021 and 2023. The average victim lost £907, but there is a wider cost to individuals and society. 41% of Britons who were victims of fraud described themselves as less trusting of others as a result, and 35% reported negative emotional impacts. Meanwhile, the SMF estimate that fraud has a wider economic impact on Britain totalling £16 billion over the three years, an amount that would cover the public sector pay rises announced by the Chancellor in July 2024.

Despite these challenges, other countries surveyed by the SMF found fraud to be even more of a threat. Across the fifteen countries surveyed a fifth of respondents reported being subject to fraud, resulting in £168 billion falling into the hands of fraudsters over the three years. The wider economic impact totalled £420 billion.

This research illustrates the truly global nature of fraud, with criminals operating across traditional geographic boundaries to target victims. This global approach makes it even harder to tackle fraud, requiring international co-operation to prevent fraud and punish criminals. But just because it's difficult, that doesn't reduce the importance of tackling fraud. The UK is well placed to lead these efforts, both domestically and abroad. That's why we're pleased to see the SMF call on Government to do more to prioritise fraud at the highest level of Whitehall in order to bring a renewed focus on tackling the fraudemic across Government, banks and the global technology and communications firms that enable criminals to reach their victims.

It's hard to argue with the increasing evidence of the severity of fraud. It a serious domestic and global issue with urgent need of a solution. We simply must act. We owe it to the hundreds of thousands of people across the word, whose hard-earned money is ending up the hands of criminals.

Stephen White

Chief Operating Officer at Santander UK

ABOUT THIS REPORT

The evidence which informs this report was gathered through a number of methods:

- We conducted a wide-ranging desk review of the existing literature on economic crime in general and fraud in particular.
- We undertook a dozen in-depth, semi-structured key informant interviews with academics and practitioners with expertise in UK and international fraud policy and practice, cybercrime, information technology, consumer policy and finance.
- We commissioned a survey of over 28,000 people across 15 countries to generate insights into the scale and nature of fraud across those countries, and creating a better understanding of international public opinion towards the fraud problem and the potential solutions which exist to tackle it (see Annex 1 for more detail on the size of the survey samples for each country).

EXECUTIVE SUMMARY

The aims of this report

- Illustrate the internationalisation of volume fraud and, for the first time, provide a sense of the scale of the fraud being committed and the detriment being suffered by individual victims across the 15 countries we surveyed, in a way that is comparable.
- Better understand the UK's consumer fraud experience in an international context, by providing a clearer picture of the UK's situation, relative to that of other countries.
- Highlight the interdependency between countries over volume fraud against individuals and why this necessitates both a robust domestic response and international collaboration, if there is to be a meaningful impact on the fraud levels experienced by consumers in the UK and many other countries.
- Identify some of the key obstacles which hinder an improved counter-fraud effort from being put in place in the UK and internationally.
- Make policy suggestions for how the UK can significantly improve its own efforts against volume fraud, as well as what the UK government could do at the international level to spur other countries into putting in place the measures which, together, could have strategic effect against high fraud levels in all the countries we surveyed, but especially the UK.

The evidence base for this report

To deliver on the five aims, the evidence presented in this report is derived from:

- Representative polling of over 28,000 adults in 15 countries (Argentina, Australia, Brazil, Canada, France, Germany, Italy, Japan, Mexico, New Zealand, Portugal, Singapore, Spain, United Kingdom, United States (US)).
- 12 in-depth, semi-structured interviews with experts in fraud policy and practice, cybercrime, information technology, consumer policy and finance.

Fraud is committed on a vast scale around the globe

Our survey results revealed that, on average, across the 15 sample countries, 21.5% of adults fell victim to fraud at least once between 2021 and 2023. As a proportion of its population:

- The US experienced the highest level, with nearly a third (31%) of adults falling prey to fraudsters.
- Japan saw the lowest level of fraud, with 8% of Japanese adults experiencing a fraud.
- The UK had the fifth lowest victimisation rate (18%) of the countries we surveyed.

In totality, we estimate that across the countries we polled, there were around 228 million fraud victims over the three-year period. This equates to around 76 million victims a year on average or 7,096 victims annually for every 100,000 adults in the nations that were surveyed.

The cost of volume fraud perpetrated against individuals

The aggregated annual direct financial cost resulting from the only or most recent fraud experienced in the 15 countries averaged £56 billion each year. The typical loss per victim across the whole international sample was £1,060, with significant variation between countries. For example:

- The average loss was highest in Singapore (£2,113) and lowest in Brazil (£282).
- The mean loss by individual victims in the UK was £907.

Relative to the GDP per capita in each of the jurisdictions we examined:

- The highest average relative financial loss for a fraud was experienced by victims in Mexico, which we calculated to be 11% of GDP per capita.
- The lowest was suffered by victims in the US and UK (2%).

Variation in fraud types across the surveyed countries

We found that payment fraud (e.g. the use of stolen credit card details to buy goods) was the most frequently experienced type of fraud by individual victims in the UK. However, across the 15 countries as a whole, Authorised Push Payment (APP) fraud, a type of scam which sees people tricked into sending a payment or making a transfer to fraudsters, was marginally more common.

Overall, the UK compares well with many other countries over the prevalence of the fraud threat

Drawing on our survey results, we developed a "Fraud Threat Prevalence Index" (FTPI), to build up a more holistic picture of the fraud threat against each country. The FTPI also helps us to compare more easily and comprehensively the fraud situation across those same nations. To compile it, we utilised the data from our survey on overall victimisation, repeat victimisation, average direct financial cost to victims (relative to the country with the highest direct loss) as well as the frequency of fraud attempts. Using the FTPI, we believe that:

- The UK suffered from the second lowest fraud threat of the 15 countries we surveyed between 2021 and 2023.
- Singapore had the worst rating in the FTPI and consequently we believe had the worst fraud problem amongst those states we surveyed, during the period 2021 to 2023.

Plausible explanations for the UK's position in our FTPI include the impact of efforts made by payment services providers such as banks in recent years to reduce their liability for fraud reimbursements to consumers, along with the financial regulator including fraud more explicitly in its evaluation of banks' risk management activities. This implies that changing the incentives facing organisations can make a difference to behaviour and perhaps therefore offers a glimpse of one way forward for policymakers.

Whilst other countries are faring worse, fraud remains high in the UK

Fraud remains a significant problem for the UK

Despite the UK's relative position in our FTPI, fraud remains a significant problem for Britain. The data we collected indicates that almost 10 million Britons fell victim to fraud between 2021 and 2023, incurring (short to medium-term) socio-economic costs of around £16 billion over that time. In addition, there are longer-term negative effects that are more difficult to measure, which include the erosion of the rule of law, the cross-subsidy of other crimes like people trafficking and terrorism, which further lowers a society's prosperity.

The "fraudemic" is slowly garnering more attention from politicians

The manifesto of the new government outlined the aim of building upon the previous government's 2023 fraud strategy. The latter was a long overdue recognition of the salience of fraud as the most common type of crime committed against individuals in the UK. Time will tell, however, what a revised fraud strategy might include and whether it will be ambitious enough to make a significant difference to the problem.

The UK's lacklustre response to fraud is a key reason why it remains prevalent

Currently, the UK response remains inadequate. This was a consistent message from the qualitative research that informs this report. Specifically, the lack of a concerted effort to tackle the minimal barriers to entry and the low-risk and high-reward nature of fraud that makes it such an attractive crime for criminals, was highlighted in our expert interviews. Specific criticisms included:

- Fraud is insufficiently prioritised by government which, in turn, is a key determinant of the scale and efficacy of the response to fraud.
- Law enforcement is poorly organised to deal with the nature of the fraud threat and has insufficient capacity and a capability deficit, which prevent it from mounting a serious and sustained crime control effort against fraudsters.
- The organisations that constitute the "fraud chain", such as online platforms, social media companies, payment services providers (e.g. banks) and telecoms companies, have failed to take the necessary measures to prevent and disrupt the fraud propagated through their services.
- There is a significant international dimension to the fraud problem which has not been adequately reckoned with.

Collective action problems bedevil a more effective domestic counter-fraud effort by the UK

There are collective action problems behind the failures of the public and private sectors to take a more effective approach to fraud in the UK. These stem from misaligned interests amongst the parties relevant to the fraud problem and insufficiently strong incentives to create the impetus for improvement. To alter this situation, there is a clear role for policy to ensure that the interests of those entities that make up the "fraud chain" for example are more congruent with the societal good of significantly reducing fraud victimisation with the incentives significant enough to engender the required changes.

Fraud is a global problem requiring effective domestic counter-fraud regimes in order to underpin a successful international global response

Fraud victims and fraudsters are widely distributed across the world

Ultimately, as our survey data shows, the fraud threat is global. It creates hundreds of millions of victims across the world and generates more than £140 billion in (short to medium-term) socio-economic costs each year.

The victims and perpetrators of fraud are widely distributed across the globe, typified by the widely noted observation that more than seven in ten of the frauds committed against individuals in the UK have some overseas involvement. As was observed in our expert interviews, there is an unavoidable interdependency challenge behind the "fraudemic" for countries, which makes it much more difficult to deal with.

States have failed to rise to the fraud challenge

The experts we spoke with pointed out that the spread of digital technology, financial services innovations that utilised those communications technologies and changing consumer behaviour on the back of technological changes, have been central to the "globalisation of fraud". However, they also highlighted that the response from states had lagged severely behind criminals who have quickly taken advantage of these developments in order to reach more victims and find new ways of defrauding people. Indeed, using the law enforcement response to victims as a proxy for the efficacy of the state response in the 15 countries we surveyed, our research shows that the counter-fraud effort is uniformly poor, although as seen in our FTPI, the UK is far from the worst.

The interdependency issue dictates the need for an ambitious international response

There was a widespread consensus amongst the experts we interviewed that the approach to fraud by all governments needs to reflect the interdependency between countries. Therefore, it was argued that there is a clear need for international cooperation, to ensure that all states:

- Are aligned on the goal of tackling fraud.
- Agree on the domestic measures which are needed and will be implemented.
- Galvanise those organisations that constitute the "fraud chain" in every country to instigate the necessary measures to prevent and disrupt fraud.
- Prioritise appropriate cross-border collaboration between law enforcement and regulatory agencies.

A recurring theme in a number of the interviews we undertook was that the international dimension of fraud can only be effectively dealt with when individual countries have sufficient domestic counter-fraud capacity and capabilities. This will create the right foundation for countries to collaborate across borders to better deal with the interdependency problem.

A collective action problem holds back international cooperation on fraud

However, like many of the domestic responses in countries like the UK, the international effort is also plagued by a collective action problem. This would be the

case regardless of the quality of the domestic anti-fraud regimes that are in place. Indeed, global collective action problems are more difficult to tackle because of the number and variety of actors and interests and the different types and levels of cooperation that need to take place. Our expert interviewees were clear that only concerted political action by governments around the world can overcome the obstacles and that, not only would an international convention be the best mechanism for doing so, but such an approach could help unlock some of the problems which governments have putting in place effective counter-fraud regimes.

There are effective and popular solutions governments can implement

Our research revealed areas of policy which could help tackle the domestic collective action problem that constrains the implementation of the most effective measures against fraud in countries like the UK. Further, we believe that our survey data also shows that there are a number of policies that have sufficient public support across the 15 countries we polled, which could subsequently form the basis of an international policy consensus on tackling fraud.

Financial levers to incentivise firms in the "fraud chain" to overcome the collective action problem are popular

We polled adults in 15 countries about the kinds of financial measures which could reduce the collective action problems facing the organisations that constitute the "fraud chain" in places like the UK. By changing the incentives facing "fraud chain" firms, they can be induced into prioritising the fraud that takes place across their services.

We found a considerable degree of support across all countries for both making "fraud chain" organisations share liability for the financial impact of individual frauds committed against consumers, and imposing financial penalties when "fraud chain" actors fail to take effective steps to prevent and disrupt fraud:

- On average, 91% of people across the 15 countries we surveyed agreed that banks and other payment services providers should bear "some" of the cost of fraud, while 71% agreed that banks and other payment service providers ought to be subject to financial sanctions for not taking adequate counter-fraud steps.
- Around 88% of those surveyed supported digital platforms sharing the costs of fraud losses, and 65% agreed that platforms should suffer penalties for not implementing effective counter-fraud measures.
- There were similarly high levels of support for telecoms and internet providers to cover some of the fraud loss costs (84%) and to face fines if they were not taking action to squeeze out fraud from their services (63%).

Data and intelligence sharing commands a plurality of support across most of the countries surveyed

The experts we spoke with for this report were united in their view that data and intelligence sharing between private sector entities in the "fraud chain" and between the private and public sectors was vital if there is to be a significant reduction in fraud levels. Our survey found that:

- Private-to-private data and intelligence sharing between financial services firms was the most consistently supported type of arrangement, with 47% supporting it on average across all 15 surveyed countries.
- More expansive sharing arrangements, which include the digital platforms, telecoms/internet providers and law enforcement as well as financial services firms, garnered 42% support on average.

Explicit opposition to such arrangements was consistently lower than the levels of support and indifference in all the countries we polled, indicating that, in many instances, extensive data and intelligence sharing systems could be implemented without too much controversy.. It also indicates that there are grounds for a potential international agreement among a number of governments on the development and implementation of advanced data and intelligence exchange mechanisms.

Overall more people support rather than oppose frictions in payments systems

In all the countries we surveyed, we found that there were more supporters than opponents of greater frictions in payments and transfers to aid in the fight against fraud. There were consistent majorities (73% on average) supporting enhanced security checks around payments and transfers. There was, however, less enthusiasm for slower payments and transfers. Support was highest in Argentina and Singapore (both 53%), with the UK just behind at 47%. However, in no countries did opposition outweigh support. For example, in Japan, where support was lowest, it was nevertheless at 28% compared to outright opposition at 19%.

Overall, our data suggests that introducing heightened security around payments systems would be accepted by the public in the UK and the other 14 countries we polled. However, slowing payments and transfers down may need to be a more targeted and risk-based response in order to reflect the more equivocal support for such a measure. Both types of actions, however, will require an extensive data sharing arrangement to underpin them in order to be maximally effective.

RECOMMENDATIONS

Domestic measures to tackle the failures in the UK's fraud response

There are a number of policies which could be implemented by the UK government which are likely to substantially improve the domestic response to fraud and provide a solid foundation for a more significant contribution by the UK, to an enhanced international effort against fraud.

Recommendation one: The UK government should prioritise the fight against fraud and, to reflect this, **a cross-departmental Economic Crime Leadership Group (ECLG) should be set-up** and be compromised of the most relevant senior Ministers. The group should set economic crime policy, oversee implementation and hold those leading the operational side accountable. By embedding the prioritisation of fraud at the top of government and with stronger central direction, the public sector collective action problem could be substantially ameliorated.

Recommendation two: The UK government should boost the law enforcement response to economic crime and in particular fraud, by:

- **Funding the recruitment and training of 30,000 specialist police officers and other staff** (e.g. forensic accountants, digital forensic experts) along with a concomitant uplift in the Crown Prosecution Service's economic crime prosecution capacity. We estimate this would cost approximately £2.8 billion each year for 10 years, but these costs will likely be dwarfed by the savings that ultimately accrue to society from reduced fraud levels.
- **Reviewing the law** to identify where the criminal law could be bolstered and how the civil law and administrative powers might be enhanced so that the authorities have the armoury they need to disrupt and pursue fraudsters.
- Increasing the maximum sentences that can be handed out to fraudsters and introducing **minimum sentences for those defrauding multiple victims.**

Recommendation three: To solve the collective action problems inhibiting a more effective response to fraud within the UK by the organisations in the "fraud chain", the government needs to ensure that there is an alignment in interests amongst the businesses that constitute the "fraud chain", in order to push them into implementing robust fraud prevention and disruption measures. To achieve this, government should:

- **Place legal duties on the organisations in the "fraud chain"** to ensure that they prioritise the prevention and disruption of fraud and **bear some of the costs of the fraud that is perpetrated through their services**.
- **Require "fraud chain" firms and relevant parts of the public sector to take part in enhanced data and intelligence sharing arrangements,** overseen by the proposed ECLG, which should facilitate the development of this, with seed funding backed up by a "safe harbour" protection from legal liability risks for participating organisations**.**
- **Overhaul the payments system rules** so that payments and transfers are subject to stronger security measures and those at greater fraud risk are slowed down.

Recommendation four: The government should ensure that the new "Stop! Think Fraud" public awareness campaign has long-term funding to enable it to continue for the next five years and consequently has the best chance of raising levels of awareness amongst the public about fraud risks and delivering improvements in "fraud hygiene" behaviours by consumers.

International measures to boost the global counter-fraud effort

Effective international cooperation against fraud will require the global collective action problem that currently holds it back, to be dealt with. This will need commitment and leadership from governments all around the world and agreement by states to put in place robust domestic counter-fraud frameworks alongside helping to build a conducive environment for much more extensive and intensive cross-border collaboration.

Recommendation five: The UK government should push for a **comprehensive international agreement** in which countries will:

- **Commit to prioritising and investing more resources into tackling fraud,** with a significant emphasis on cross-border law enforcement and regulator cooperation.
- Take actions to **reduce the current disincentives to greater cross-border law enforcement cooperation** e.g. modernising the Mutual Legal Assistance Treaties (MLATs) network.
- **Agree to implement measures which incentivise the organisations in the "fraud chains" of each signatory country** to take the necessary steps to better prevent and disrupt the fraud being perpetrated over their services (e.g. through the introduction of financial penalties).

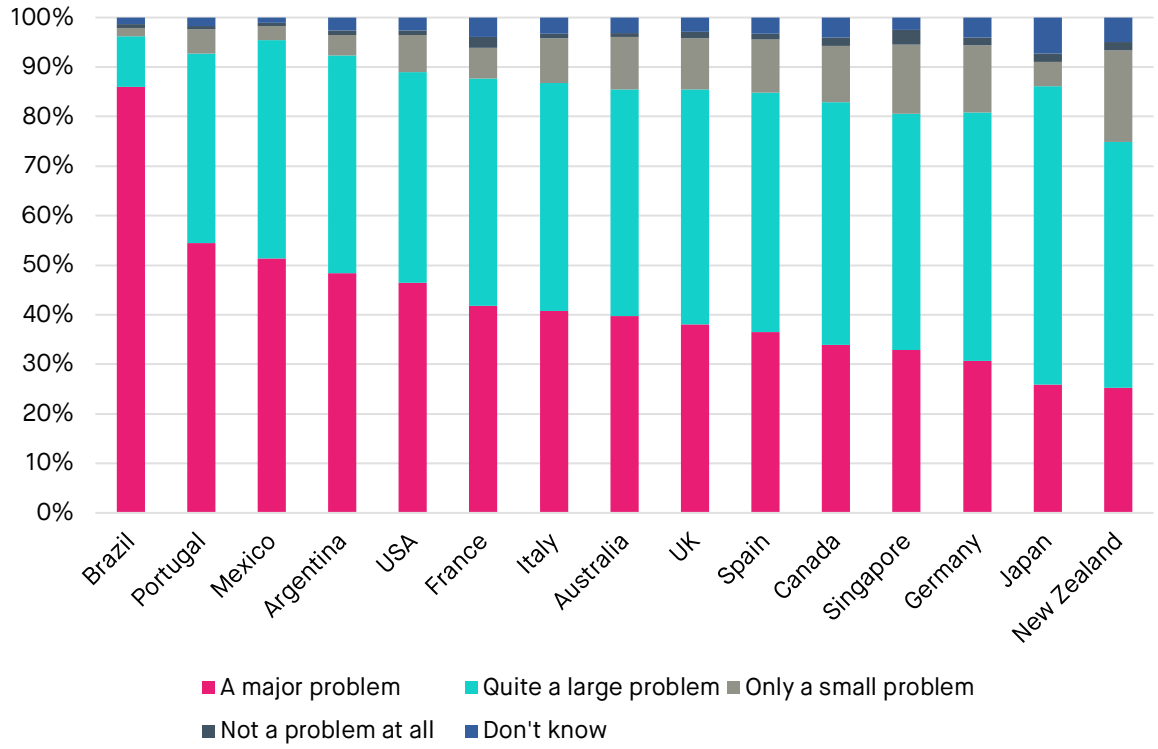
Recommendation six: The UK government should **increase its support for building up the anti-fraud law enforcement and regulatory capacity and capabilities in low and middle-income countries** to enable them to make an increasingly extensive and effective contribution to the global fight against fraud.

CHAPTER ONE – INTRODUCTION

The world is in the midst of a 'fraudemic'

Fraud is proving to be a major challenge to many countries around the world, including the UK. In 2019, for example, it was estimated that all fraud cost the world the equivalent of 6% of global GDP.[1] Within the context of that broader fraud problem, volume fraud against individuals (i.e. consumers) in particular has been growing significantly. The UK is merely one amongst many nations struggling to respond to it and, as a result, it is an issue that populations across the globe are becoming increasingly aware of and see as a problem in need of a solution (Figure 1).

Figure 1: The extent to which fraud is a problem in 15 countries



Source: Focal Data survey

Key drivers behind the explosion of fraud

The low-risk, high-reward nature of fraud drives its popularity amongst criminals

Criminals are, in many instances, rational actors.[2] While situational, egotistical, pathological, and other factors can play a motivating role, for many, particular illegal activities are pursued because they are low-risk but can deliver high rewards, as was highlighted by one of the experts we interviewed: [3] [4] [5]

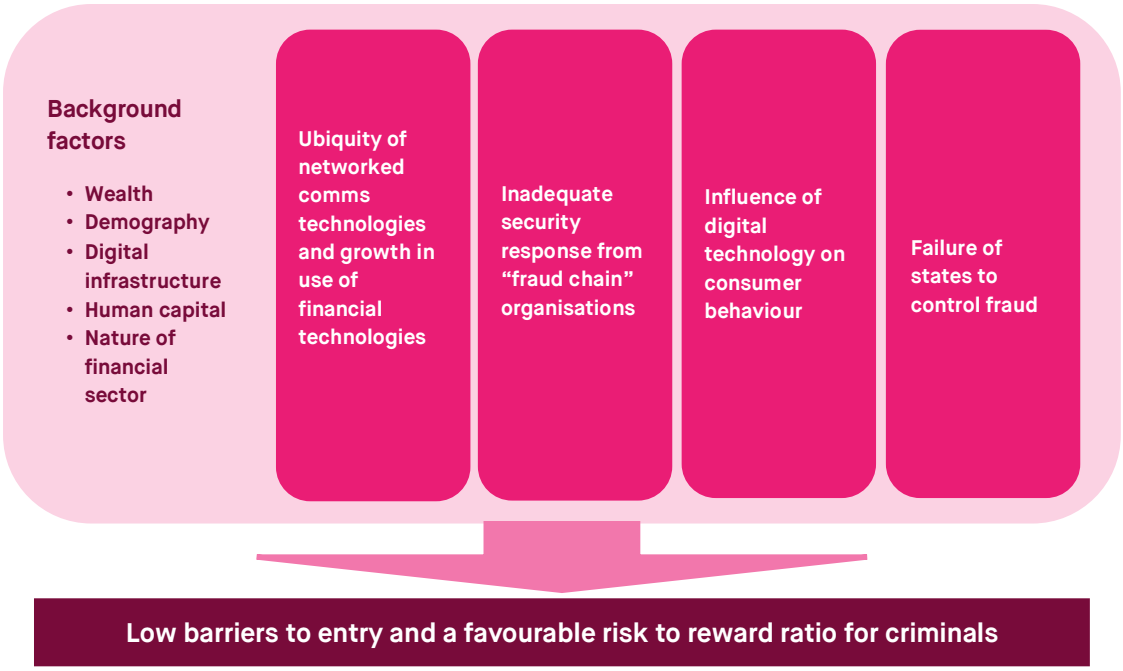
> *"Criminals are rational decision-makers who, just as we make any other decisions, try to maximise benefits and minimise risk…fraud is easy to do…and the risk of getting caught is very low. The question is not why do people commit online fraud, it's why doesn't everybody commit online fraud?"*

The pursuit of financial gain at scale is especially prominent amongst organised criminals, where illicit profits are a central motivation.[6] However, these motives also frequently apply to the more casual and opportunistic fraudster.

A confluence of factors has driven the growth in fraud

The growth in volume fraud perpetrated against individuals has occurred in the context of a range of technological, social, economic and policy factors that have coalesced to create a favourable environment for committing fraud (see Diagram 1).

Diagram 1: Factors that have driven the levels of fraud against individuals up



Source: Expert interviews and SMF analysis

Networked communication and financial technologies have lowered the barriers to entry and increased the range of attack vectors for criminals

The rise of networked communication and financial technologies have made it easier for criminals to target larger numbers of victims, gain access to and deceptively use personal information, induce and receive fraudulent payments and transfers from consumers, and more conveniently, speedily, and anonymously sequester criminal proceeds.[7] [8] [9] As one expert interviewee stated:

> *"Being an adopter of new technologies is a double-edged sword … fraud is often driven by technology across a wide range of areas … [such as] … social media, emails, text messages".*

Information and communication technologies have reduced barriers such as geography, language and culture to fraudsters.[10] The result has been that a large proportion of the fraud perpetrated against consumers in the UK has an overseas element, as a number of the experts we spoke to for this research pointed out:[11]

> *"If you look at fraud committed in the UK, over 70% is [at least partially] overseas … But that applies to the Asia-Pacific Rim, Australia, China, Taiwan … All those committing fraud, a large percentage will be … nationals overseas".*

Digital payment systems have been developed on the back of the ubiquity of networked communication technologies. The combination has seen the costs of payments and transfers cut substantially and the speed at which they are undertaken has increased considerably. This is true for both domestic and cross-border movements in money. In our interviews with fraud specialists, they were clear that the exemplar of this shift to ever swifter movements of money – the UK's faster payments service – was a systemic vulnerability that fraudsters have exploited:

> *"… the main thing is that we [the UK] put everything on the faster payments rails without the necessary checks, balances and controls, to slow things down in certain circumstances".*

In addition, the emergence of new financial instruments such as cryptocurrencies have also facilitated the growth of fraud. Crypto has provided a new vehicle for specific acts of fraud against individuals (e.g. crypto-investment scams) as well as being a conduit through which the proceeds from fraud can be sequestered away.[12]

The mediating role of technology on criminal opportunities and victim behaviour

One academic we engaged with described how the very nature of the networked communication technologies and their influence on human behaviour has played a role in the rise of fraud. More specifically, technology has:

- Enabled fraudsters to enter, almost ubiquitously, into the routines of people's everyday lives, and create a semi-permanent threat.[13] The sheer volume of fraud attempts means those most at risk are more likely to be reached compared to circumstances where technology is less prevalent.
- Helped criminals to commoditise deceptive techniques which exploit human vulnerabilities e.g. pressuring victims through time-limiting decision-making periods, preying on emotions, manipulating reasonable self-interests, or relying on approaches that can exploit the fact that the deception is often on the periphery of a potential victim's attention.[14]
- Induced a false sense of security amongst many consumers and, combined with particular kinds of personality traits, has resulted in heightened risk.[15] For example, poor self-control, risk appetite and emotional understanding have all been linked to fraud victimhood.[16] [17] [18] [19] [20]

Box 1: The evolving nature of the fraud threat and the role of technology

Fraud evolves over time and responds to "push" and "pull" factors driven by technological developments and vulnerabilities, consumer behaviour patterns, policy responses, law enforcement efficacy and innovations in crime "business models" amongst other variables. For example, the shift to 'authorised' fraud (whereby victims are tricked into making transactions that they believe to be legitimate) has occurred because of:

- Push factors such as belated increases in online banking security.[i] [21]
- PI factors including technological changes opening up new avenues for fraudsters to deceive people into making authorised payments, such as dating sites and other forms of social media.

Where the response from states and the organisations in the "fraud chain" are slow and inadequate to the scale of the problem, the fraudsters are highly adaptive and innovate around such counter-efforts.

Criminals are already adopting Artificial Intelligence (AI) tools to help them commit fraud and this trend is likely to continue until sufficiently robust counter-efforts are developed and implemented to deny such avenues of opportunity.[22] Several experts we interviewed raised concerns about the potential for AI to make scams more sophisticated and harder to take precautions against. The FBI in particular, has warned that organised crime is using the technology to generate "synthetic content" such as deepfakes for "spear phishing" (where fraudulent emails or texts are sent from ostensibly trusted sources), or "social engineering" to exploit people's trust.[23]

AI is likely to put the criminals further ahead, if the lacklustre responses from governments and the private sector to the growth of fraud in the recent past is repeated. Not taking action now to get ahead of the problem will only make it more difficult to deal with it later on.

The failure of the state to control the rise in fraud

There was little doubt amongst the experts we interviewed that the failure of the state – in the UK and elsewhere around the world – to live up to its crime control responsibilities has been a key driver of fraud levels. This is an observation consistent with the academic evidence which highlights the crime-related consequences of an incapable state.[ii]

[i] The European Central Bank noted how recent reductions in unauthorised card-not-present fraud across the EU were driven by regulations requiring strong customer authentication measures by payment system providers. Source: Seventh report on card fraud, European Central Bank: Seventh report on card fraud (europa.eu)

[ii] This is consistent with cross-country criminological evidence which shows that poor-quality governmental institutions that cannot ensure the pre-eminence of the rule of law and

The political, policy, law enforcement and regulatory response in England and Wales, for example, has been subject to considerable criticism.[24] [25] [26] However, as the survey data presented in this report shows, the UK is not an outlier. Our research shows that the law enforcement response is typically poor across the all the 15 countries we polled. Indeed, amongst a plethora of poor performances, the UK has one of the better records.

Political leadership on fraud is lagging behind the scale of the problem

Intimately connected to the extent and rigour of the state's response to fraud, is political leadership on the issue. Fraud has slowly crept up the crime agenda in the UK to the point where a new fraud strategy was produced in 2023.[27] While falling short of the kind of ambitious approach needed to tackle this most common of crimes, it was, nevertheless, recognition that fraud is a significant problem. Further, if implemented, the overall impact of the strategy could be expected to be positive, resulting in some degree of strategic effect on fraud levels.

The new government, in its manifesto, suggested it would build on the existing strategy.[28] Time will tell if this leads to a more extensive, intensive and better resourced effort against fraud. If there is to be a step-change in approach, it will need to begin with clear and sustained leadership from the very top, alongside a thorough plan with accountability for performance against realistic objectives.

The purpose of the report

The five aims of this report are to:

- Illustrate the internationalisation of volume fraud and, for the first time, provide a sense of the scale of the fraud being committed and the detriment being suffered by individual victims across the 15 countries we surveyed in a way that is comparable.
- Better understand the UK's consumer fraud experience in an international context by providing a clearer picture of the UK's situation relative to that of other countries.
- Highlight the interdependency between countries over volume fraud against individuals and why this necessitates both a robust domestic response and international collaboration if there is to be a meaningful impact on the fraud levels experienced by consumers in the UK and many other countries.
- Identify some of the key obstacles which hinder an improved counter-fraud effort from being put in place in the UK and internationally.
- Make policy suggestions for how the UK can significantly improve its own efforts against volume fraud, as well as what the UK government could do at the international level to spur other countries into putting in place the measures which could, together, have strategic effect against high fraud levels in all the countries we surveyed but especially the UK.

therefore govern geographies effectively tend to result in higher crime. Source: Kenneth Murray, "When Opportunity Knocks: Mobilizing Capabilities on Serious Organized Economic Crime," in *Frauds and Financial Crimes* (Routledge, 2021).

The structure of this report

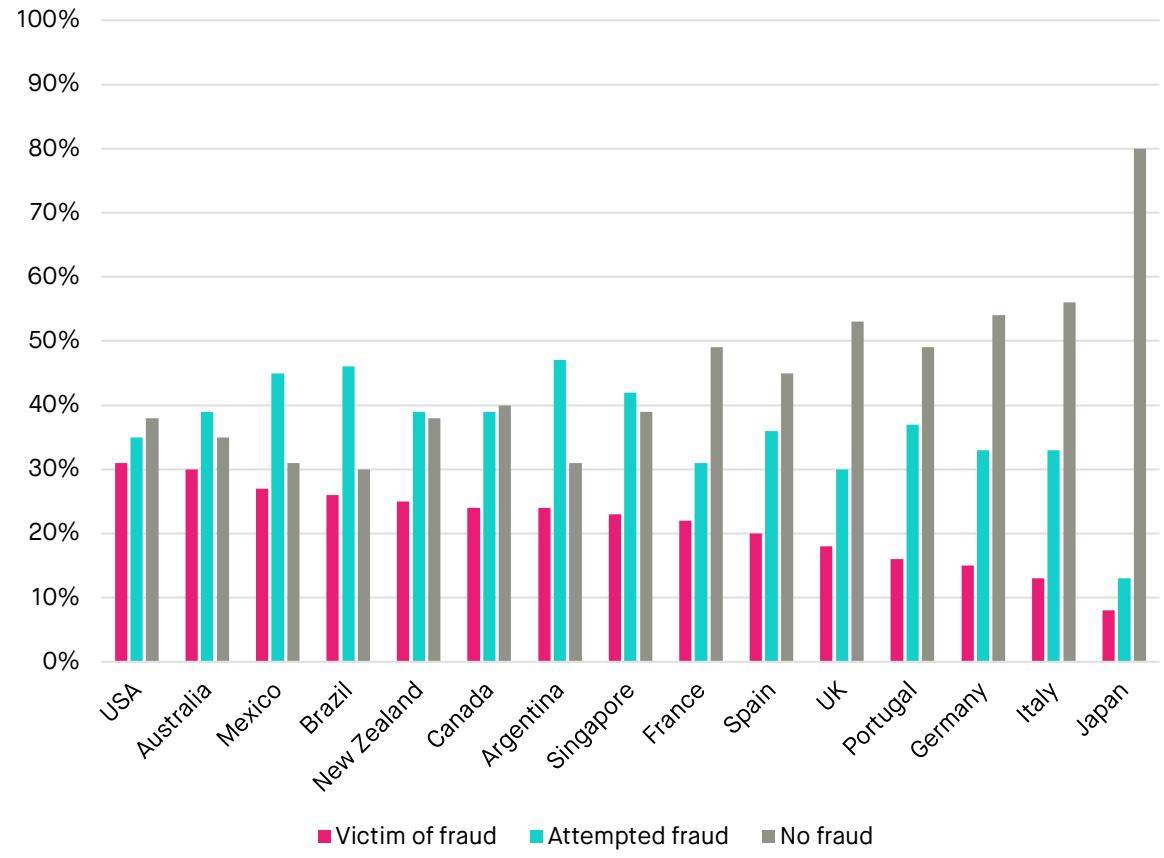
- **Chapter Two** examines the scale and nature of fraud across the 15 countries surveyed for this research, detailing the extent of victimisation and the types of fraud most commonly experienced by victims, and introduces our Fraud Threat Prevalence Index (FTPI).
- **Chapter Three** uses our survey data to show the kinds of impacts which the fraud levels experienced by the people of the 15 countries we polled, are having on both individuals and their societies.
- **Chapter Four** explores the efficacy of the state's response in each of the 15 countries, using the results from questions we asked about the reaction of law enforcement, after victims reported their only or most recent episode of fraud victimisation to the authorities.
- **Chapter Five** identifies the counter-fraud measures which experts believe can make a significant difference to fraud levels, and examines public support across the countries we surveyed, for these different policies.
- **Chapter Six** looks at the UK situation specifically and proposes ways to ameliorate some of the key obstacles standing in the way of a more effective domestic response to fraud.
- **Chapter Seven** highlights the interconnectedness of the fraud problems for all of the countries which were polled. It points out how the global nature of the criminality requires both an effective domestic response and a robust international one, too, with the former providing the best foundations for the latter.
- **Chapter Eight** draws on qualitative research with experts and the polling evidence of public views on different counter-fraud policy measures, to describe what a UK government might do to help strengthen counter-fraud action at the international level.

CHAPTER TWO – THE FRAUD PICTURE ACROSS 15 COUNTRIES

How fraud victimisation in the UK compares to other countries

The data collected in our 15 country survey on the incidence of fraud committed against individuals (Figure 2) showed that between 2021 and 2023, the US had the highest rate of victimisation (31%). By contrast, the lowest was found in Japan (8%). Notably the UK ranks 11th of the 15 countries, with 18% of adults falling prey to fraudsters. This equates to nearly 10 million victims of fraud over the three-year period (see Annex 2, Table 4).

Figure 2: Rate of fraud victimisation against individuals between 2021 - 2023



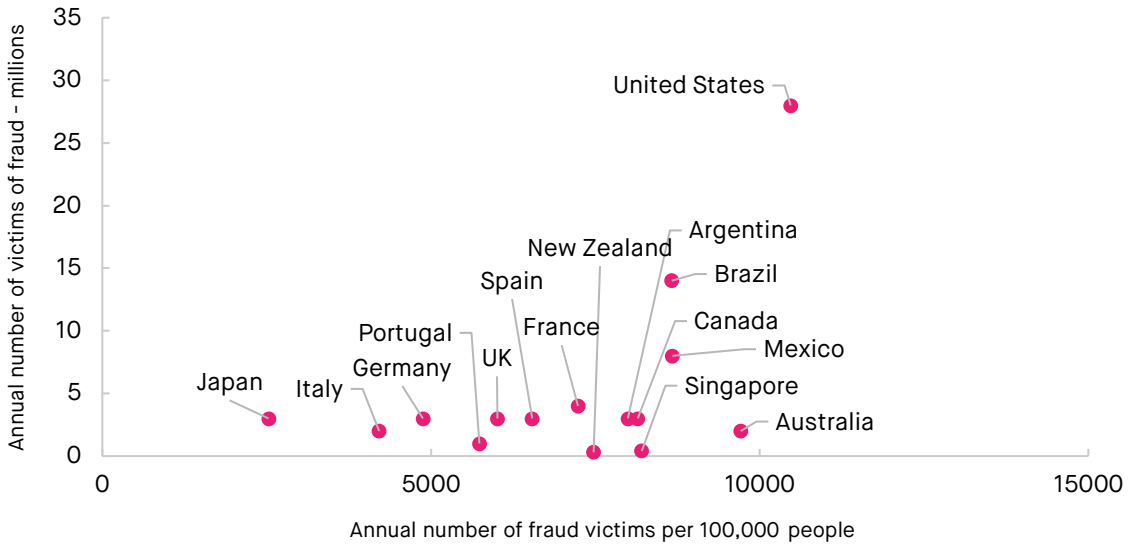
Source: Focal Data survey

Between 2021 – 2023 there were more than 200 million victims of fraud

Our survey results suggest that in total, across the 15 countries, more than 228 million people suffered from fraud (at least once) between 2021 and 2023. On average this equates to 76 million victims a year.[iii] [iv]

It is common to compare victimisation on the basis of the annual number of victims per 100,000 of the adult population. Our data suggests across the surveyed countries, there were, on average, 7,098 victims per 100,000 adults every year.

Figure 3: Average number of annual fraud victims and the average number of fraud victims per 100,000 each year of the adult populations of 15 countries, 2021 - 2023



Source: Focal Data survey, World Bank and SMF calculations

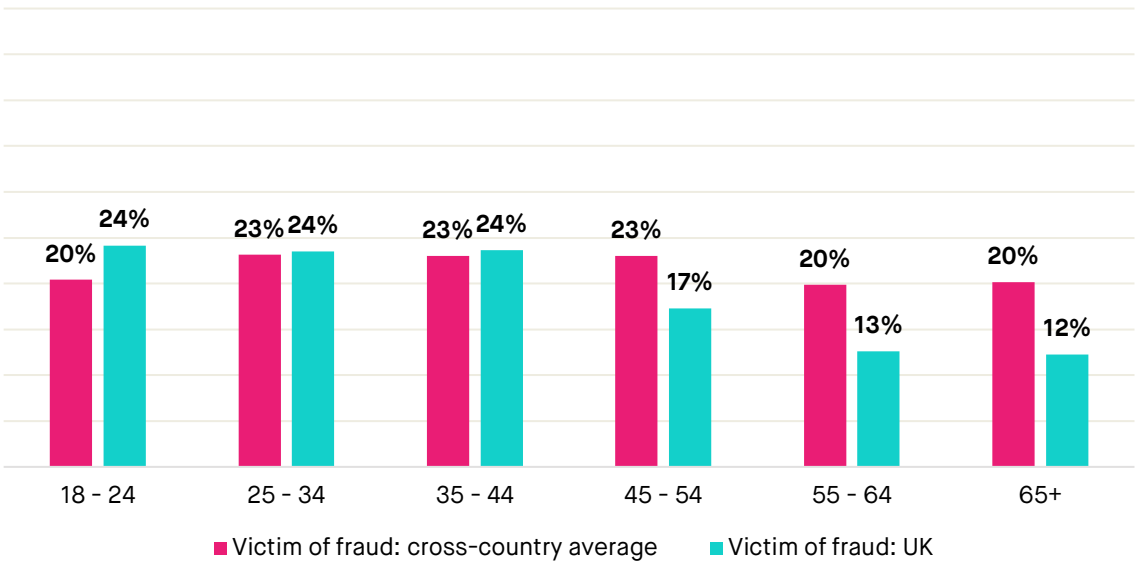
Our analysis indicates that the United States had, on average, the worst annual levels of fraud per 100,000 of the adult population (10,471). In contrast, Japan suffered the fewest victims on average (2,528). The UK had the fifth lowest average annual level of fraud per 100,000 of the population (6,011) of the 15 countries we researched.

Further, in the UK, the victimisation rate was substantially lower amongst older age cohorts than it was on average across the other 14 countries in the survey sample, and marginally higher amongst the youngest (Figure 4).

[iii] Due to sample limitations, data on the rates of victimisation among over 65s in Argentina, Mexico, New Zealand and Singapore was not obtainable. Consequently, for the purposes of estimating the total number of victims across all 15 countries, we assumed that, in those four countries, the victimisation rate for over 65s was the same as that which pertained for the rest of the population (18-65 year olds).

[iv] See Annex Two for a list of the total number of fraud victims in each country we surveyed.

Figure 4: Fraud victimisation across age cohorts – UK and the average across all surveyed countries (exc. the UK), 2021-2023

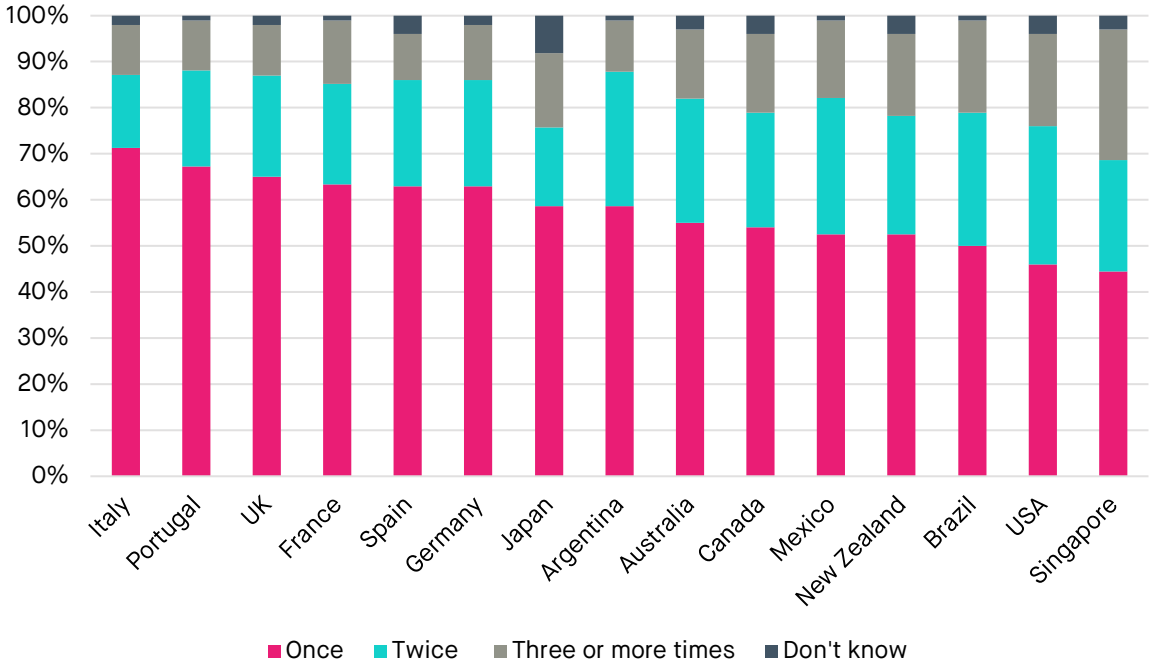


Source: Focal Data survey

Levels of repeat victimisation vary across countries but even in the best performing country a third fall prey more than once

Repeat victimisation is the source of a significant amount of fraud. Across the 15 countries, our survey results suggest that 111 million victims fell prey to fraudsters more than once between 2021 and 2023 (Figure 5).

Figure 5: Repeat fraud victimisation between 2021 and 2023



Source: Focal Data survey

Falling prey to fraudsters more than once, was most common in Singapore with over half (52%) of victims experiencing it in the period 2021 to 2023. By contrast, it was lowest in Italy, with around a quarter (27%) of victims suffering more than once from fraud. The UK had the third lowest (33%) repeat victimisation problem. This equates to around a million repeat victims in Britain, over the three year period.

The Fraud Threat Prevalence Index

Using the results from a number of the fraud victimisation questions we asked survey respondents, we compiled a Fraud Threat Prevalence Index (FTPI) which provides a consolidated picture of the relative severity of the fraud threat against each of the surveyed countries. This has enabled us to rank the countries according to what we believe is a reasonable estimation of the level of threat facing the populations in each nation (Diagram 2).[v]

Diagram 2: Fraud Threat Prevalence Index – country rankings

Source: Focal Data survey and SMF analysis

[v] See Annex Three for more on the way that the Index is constructed.

The country ranked first place in the FTPI experienced the greatest fraud threat over the period 2021 to 2023, whilst the country ranked 15th had the least. The FTPI suggests that Singapore had the worst fraud problem and the people of Singapore face the most threat. In contrast, Italy and Italian were in the best position according to our index. The UK experienced the second lowest threat. Notably, the overall difference in the threat scores of Italy and UK was marginal.

The UK's comparatively positive position in the FTPI

The recent fall in fraud incidents against individuals in England and Wales (down around 17% from a peak in 2019) would be consistent with the picture presented in the FTPI.[29] However, the underlying reasons why the UK does relatively well in the FTPI and why there have been recent falls in volume consumer fraud are, at this stage, unclear.

Plausible explanations as to why the UK has performed comparatively well in the FTPI could include the impact of recent efforts made by payment services providers to reduce their liability for fraud reimbursements to consumers, by introducing stronger anti-fraud measures (e.g. two-factor authentication and the deployment of checks and prompts to ensure consumers are not sending money to fraudsters) along with the financial regulator more explicitly including fraud in its evaluations of the risk management activities of banks.[30] [31] If this is the case, it implies that the combination of a significant financial incentive and sufficient regulatory impetus (backed up by the potential for the levying of sanctions by the regulator) together can galvanise effective action by organisations in at least one part of the "fraud chain". This suggests that the principle of changing the incentives facing organisations can make a difference to priorities and behaviour and perhaps, therefore, offers a glimpse of one way forward for policymakers.

Other contributing factors to the recent fall could include:

- Greater awareness amongst the public of fraud due to its prevalence. Consequently, more people are getting better at avoiding fraud attempts.
- A shift away from targeting individuals in the UK and towards other groups such as the business community. However, the data on business victimisation is poor, so it is difficult to ascertain the exact levels of business victimisation trend over time.
- A move amongst fraudsters towards focusing on potential victims other countries.

Nevertheless, the comparatively positive position of the UK should not blind policymakers to the ongoing challenge of consumer fraud in this country. The problem remains significant. For example:

- Fraud is by the far the most common crime suffered by individuals with victimhood in the millions in the UK each year.
- It continues to cost the UK billions of pounds per annum as well as generate considerable amounts of less measurable individual and societal harm.
- There has been a recent jump (42%) in the fraud precursor crime of personal data theft against people in England and Wales.[32]

- AI may be about to drive a new wave of more sophisticated fraud.

The nature of the fraud being perpetrated varies across countries

Box 2: The main types of fraud committed against individuals[vi]

- **Payment fraud:** Criminals use illegally obtained personal details, e.g. credit or debit card information, to buy products.
- **Authorised Push Payment (APP) fraud**: Fraudsters deceive a victim into sending money to them, typically to a receiving account the fraudster controls, e g, paying for fake goods or services.
- **Identity/impersonation fraud**: Fraudsters pretend to be another person to third parties, in order to access services or obtain property, e.g. dishonestly entering into credit agreements.
- **Deceptive access to personal information fraud**: Individuals are manipulated into giving away personal information e.g. a victim is tricked into revealing financial details which can then be used by fraudsters for illicit gains.

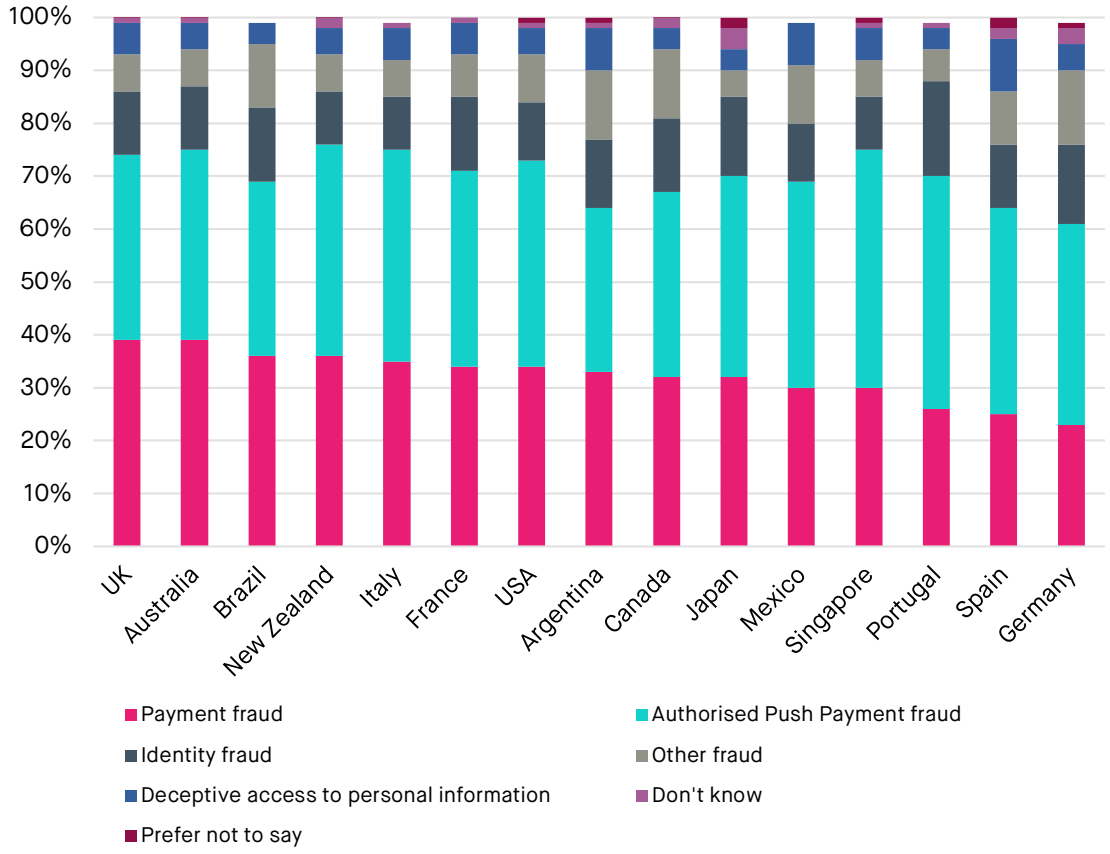
Authorised Push Payment (APP) fraud is somewhat more common across the 15 country sample but there is variation between places

Figure 6 illustrates the mix of fraud types perpetrated against individual victims in each of the surveyed states. Across the sample as a whole, APP frauds were the most prevalent. However, in some countries other types of payment fraud dominated. For example, in Germany, 38% of victims experienced APP fraud whilst 23% suffered from other types of payment fraud. In the UK, Australia and Brazil the latter were marginally more common than APP frauds.[vii]

[vi] These were the main categories of fraud against individuals that we asked the 28,000 adults that were polled in our survey, about.

[vii] This split between fraud types in the UK is broadly in line with industry reporting. Source: "Annual Fraud Report 2023," UK Finance, https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2023.

Figure 6: The nature of the only or most recent fraud suffered by victims across 15 countries, 2021-2023



Source: Focal Data survey

The diversification of fraud victimisation and fraudsters

Fraudsters are based all around the world and frequently target victims in other countries

Organised fraud is a particularly important driver of the "fraudemic".[33] [34] For instance, scholars have identified West Africa, South Asia and Eastern Europe, amongst other places, as important sources of organised crime groups that are committing volume fraud.[35] Further, fraud is increasingly characterised not only by the internationalisation of the perpetrators but the specialisation by different gangs in different categories of frauds, which are underpinned by the growth of cross-border criminal supply chains populated by criminals providing "criminal services", This growing "division of fraud labour" was highlighted by one of the interviewees we spoke with, who observed that:[viii] [36] [37]

[viii] The international "division of fraud labour" includes the provision of criminal "support services" ("crime as a service") that play a growing enabling role, facilitating the committing of fraud at scale and across borders. Sources: "Online Fraud Schemes: A Web of Deceit (IOCTA 2023)," Europol, https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023. and "Cyber-Attacks: The Apex of Crime-as-

> *"We have evidence, especially in Southeast Asia, of active components of hacking and fraud together. The same is true with Nigeria, in certain parts of Africa … there's clusters of activity … they are everywhere".*

To illustrate this point, work by Interpol indicates that Asian fraudsters are a significant source of the investment fraud targeted at Europe, whilst European criminals have been found to be the perpetrators of some of the APP fraud directed at Africa (see Table 6 in Annex 4 for more on the varieties of fraud that emanate from different regions of the world).[38]

Fraudsters are targeting different types of frauds at different countries to increase their chances of successfully defrauding victims

The exact "mix" of fraud perpetrated against populations in particular countries is, a reflection of the relative sophistication that fraudsters have reached. More specifically they have adapted swiftly to new technologies and changes in consumer behaviour in order maximise criminal opportunities.

To some degree, domestic fraudsters for example, may be expected to be able to tailor their criminal methods to local circumstances comparatively easily to optimise their chances of successfully victimising individuals in the same country. This is because the barriers to accessing a pool of potential victims are generally lower than they are for criminals based overseas. However, the proliferation of factors such as digital technologies and cross-border banking has enabled fraudsters to much more easily "export fraud". Such developments have made it much easier for criminals to tailor their fraud attempts to the patterns of online activity and technology use preferences that predominate amongst consumers in particular places and regions, as one of the experts we interviewed for this report noted:[39]

> *"We know that … even a difference in communication platforms matters … Same with technology for payment and financing … So, you'll see these pockets of differential resources, differential payment systems, all of which shape the potential for the fraud experience to look a certain way or be different, depending on where you are".*

a-Service (IOCTA 2023)," Europol, https://www.europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023.

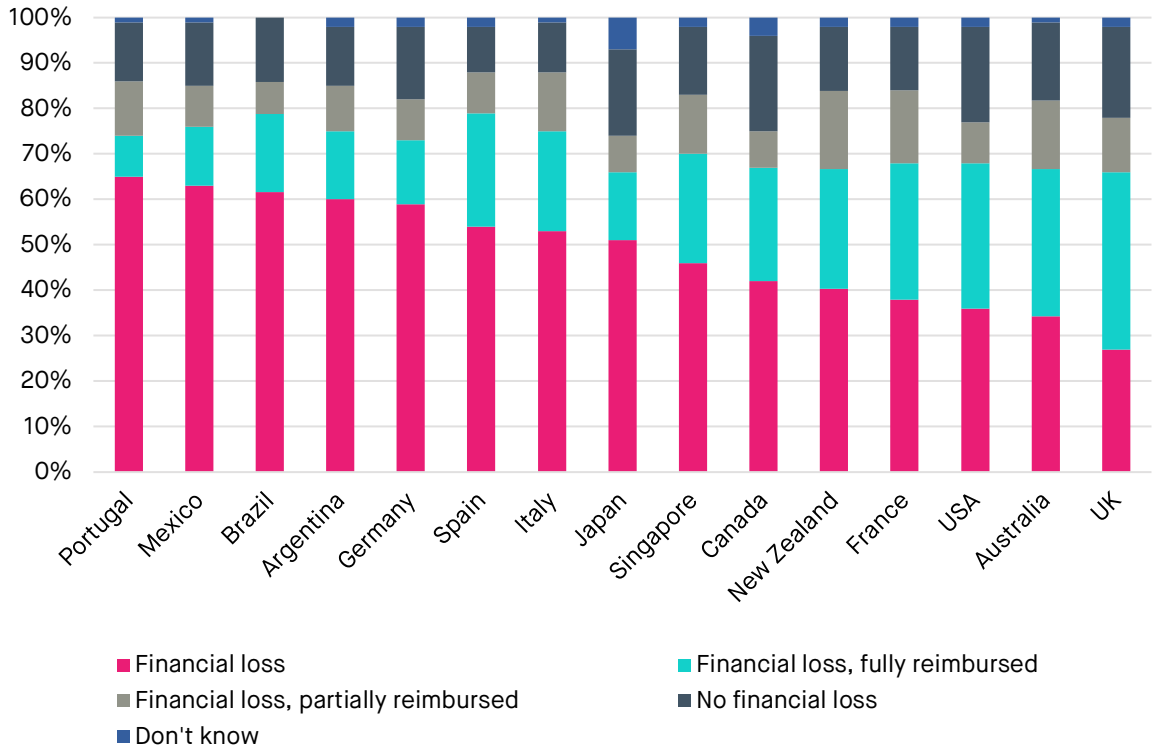
CHAPTER THREE – THE IMPACT OF VOLUME FRAUD ON VICTIMS AND COUNTRIES

Direct financial losses incurred by individual fraud victims

Victims suffering a direct financial loss was common across the 15 country sample

The most prominent impact of fraud against individuals, is the financial loss incurred by the victim. In more than eight out of ten cases of fraud across the 15 country sample, the victim typically incurred a direct financial loss.

Figure 7: Proportion of victims who suffered a direct financial loss as a result of their only or most recent experience of fraud, 2021 – 2023



Source: Focal Data survey

The UK stood out as the country that reimbursed victims most often

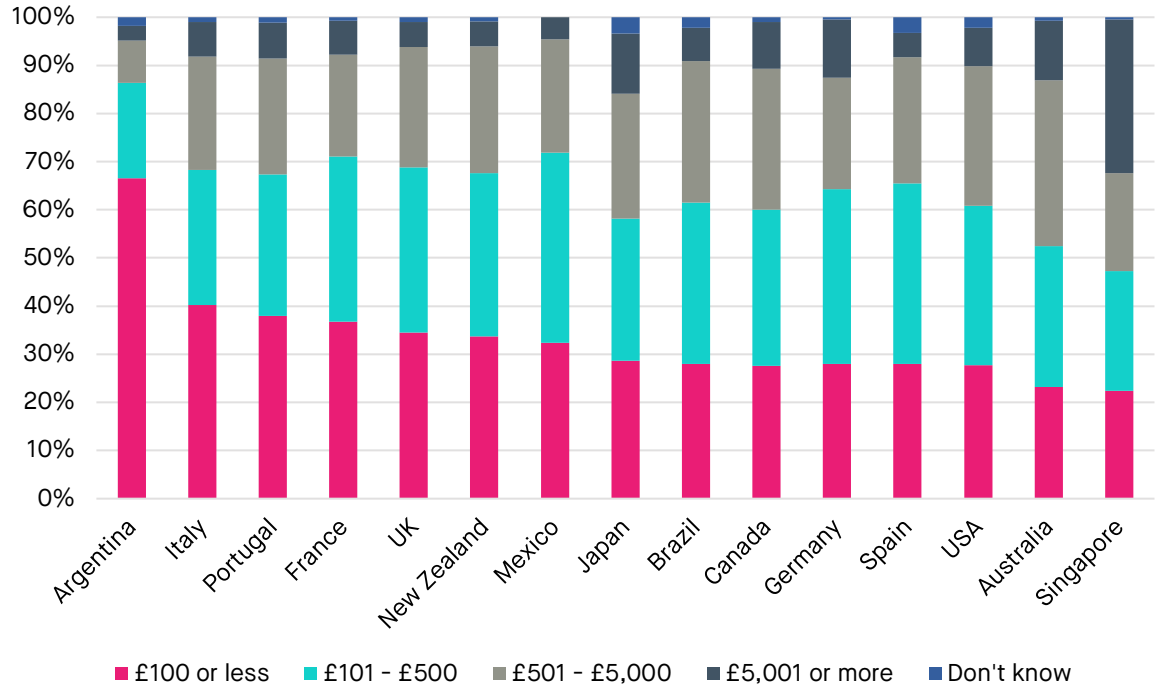
Across the entire sample, more than half (58%) of victim respondents who suffered a direct financial loss received no reimbursement. However, there was considerable variation in the likelihood of victims receiving reimbursement for their fraud losses between countries. For example, victims in the UK were the most likely to receive at least some reimbursement (51%) and the most likely to receive full reimbursement (39%), while, in Portugal, less than one-in-ten (9%) received a full or partial (12%) reimbursement.

The distribution of the quantum of financial losses varied significantly across surveyed countries

Amongst the sample of countries, Singapore stood out as having the greatest proportion of victims who suffered the highest individual losses (Figure 8). For

example, Singaporeans were the most likely to suffer losses of more than the equivalent of £5,000 (32%). In the UK there was a broadly equal preponderance of losses of £100 or less (35%) and between £101 and £500 (34%). Around 1 in 20 UK victims lost £5,000 or more.

Figure 8: Amount of direct financial loss suffered by victims as a result of their only or most recent fraud, 2021-2023

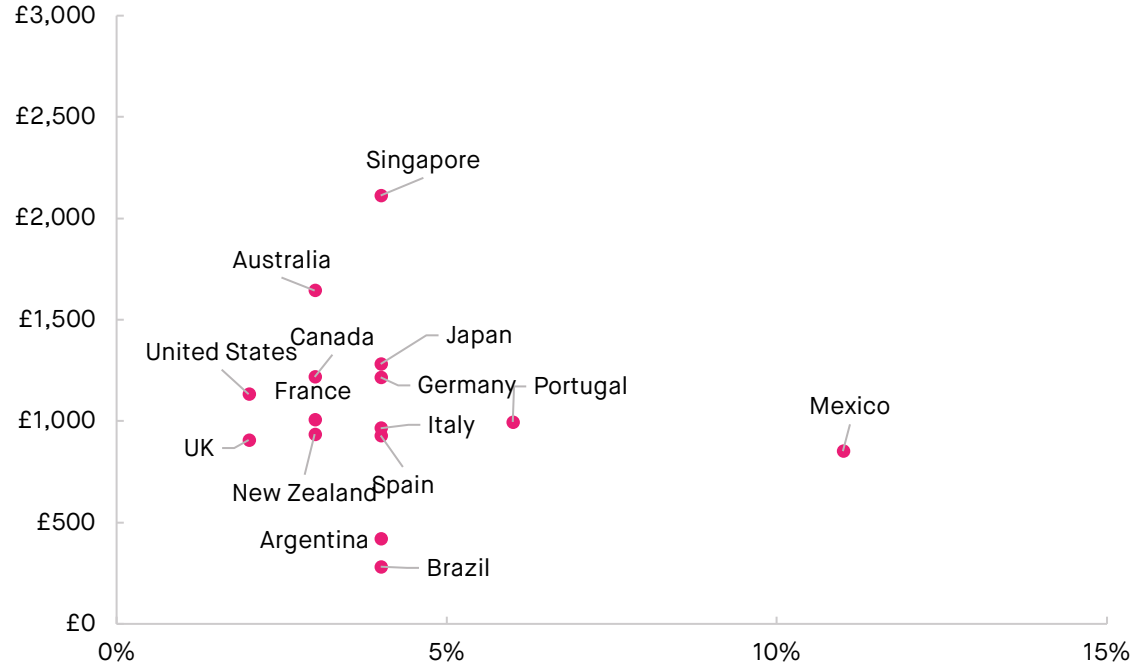


Source: Focal Data survey

The average amount of financial loss was highest amongst Singaporeans

The total direct cost of the only or most recent fraud experienced by all the victims in the 15 country sample was around £168 billion. The average amount of direct financial loss incurred by an individual victim in the survey was just over £1,060.

Figure 9: Average direct financial loss per victim from the only or most recently experienced fraud across 15 countries and the average direct financial loss as a proportion of GDP per capita, 2021 – 2023



Source: Focal Data survey, World Bank, Exchange rates.org.uk and SMF calculations

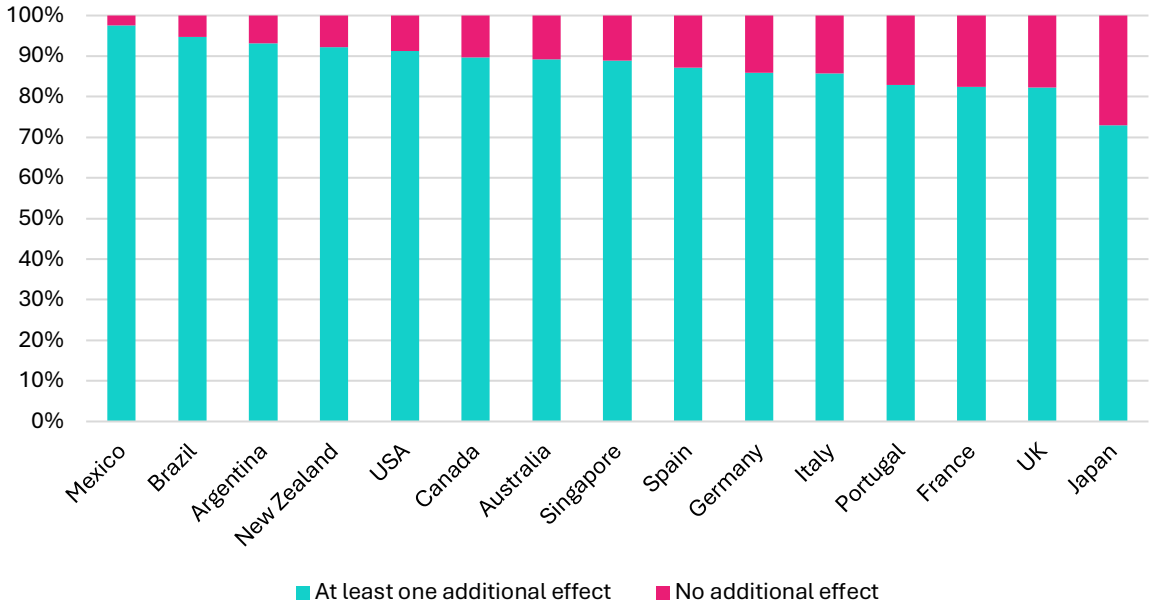
Figure 9 shows that individuals in Singapore incurred the largest average direct financial losses (£2,113). Those in Brazil suffered the smallest (£282). As a percentage of the per capita income of each of the polled countries, victims in Mexico suffered the largest relative loss (11%) and the UK (2%) and United States (2%) the lowest.

The wider negative impacts of being a fraud victim

Wider negative impacts are common amongst fraud victims in all countries

In almost all cases of fraud victimisation (88% across the sample as a whole), irrespective of whether a victim suffered a direct financial loss, victims also reported experiencing at least one wider negative impact (Figure 10).[40] In total, more than 206 million fraud victims across the 15 countries endured one or more additional consequences. These wider effects were the least likely to occur in Japan, where 27% experienced them. They were most common amongst Mexican victims (98%).

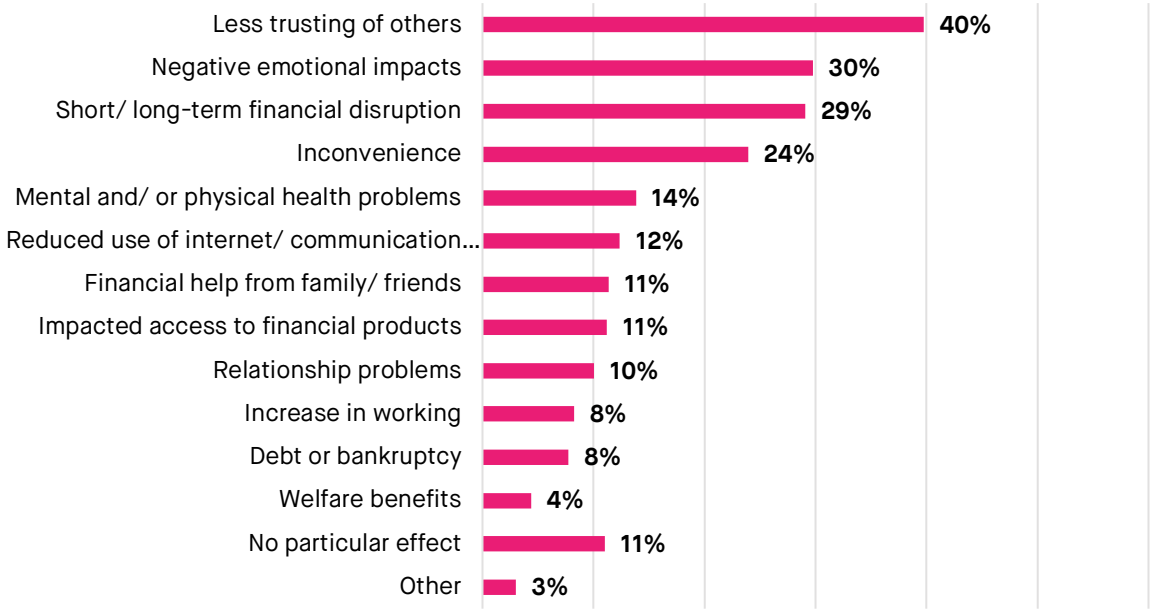
Figure 10: Additional non-financial impacts of the only or most recent fraud experienced by victims, 2021 – 2023



Source: Focal Data survey

Figure 11 highlights the aggregate distribution of the wider negative impacts of fraud victimisation across the whole survey sample.

Figure 11: Types of wider negative impacts experienced by fraud victims aggregated across 15 countries, 2021- 2023

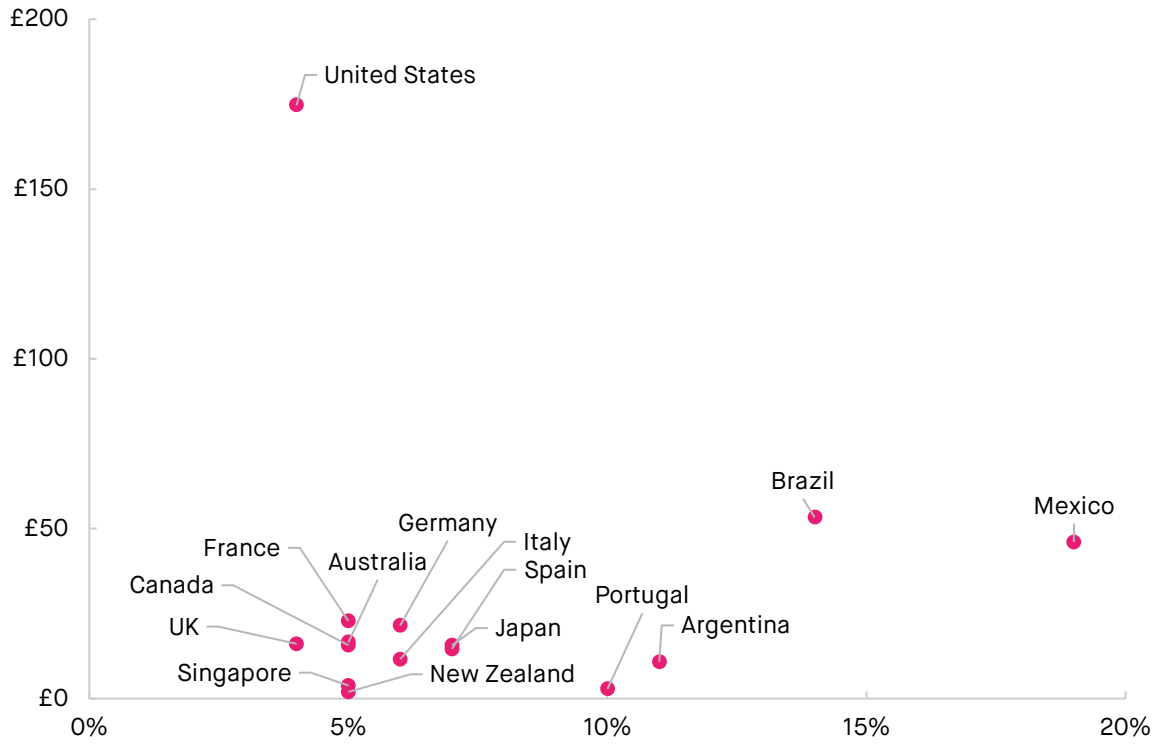


Source: Focal Data survey

The total aggregated (short-to-medium-term) socio-economic cost of fraud across the 15 surveyed countries was more than £420 billion

The wider costs which fraud generates are much harder to quantify than the direct financial losses to victims. However, the UK Home Office has attempted to estimate a number of the (short to medium-term) socio-economic costs associated with fraud victimisation, e.g. health and productivity impacts.[41] Applying some of these to the results from the surveyed countries presented in this report, we estimate that the total (short-to medium-term) socio-economic cost of fraud against individuals between 2021 and 2023 was in the region of £428 billion.

Figure 12: Estimates of the total (short-to-medium-term) socio-economic cost of frauds against individuals and the average socio-economic cost of fraud as a proportion of GDP per capita, between 2021 and 2023



Sources: Focal Data survey, Home Office (2018) estimates of the socio-economic cost of fraud, Exchange rates.org.uk and SMF calculations

In the UK, we estimate the cumulative cost to be £16.1 billion across the three years (£5.4 billion annually). The UK ranked seventh out of the 15 countries for the total (short-to-medium-term) socio-economic cost of frauds committed between 2021 and 2023. As a proportion of a country's GDP per capita, UK victims suffered the least, along with US victims, with a (short-to medium-term) socio-economic cost of a fraud to victims of 4% of GDP per capita.

The longer-term costs of persistent volume fraud

However, the persistently high level of fraud perpetrated against individuals does not just generate short-to medium-term socio-economic costs. It also has longer-term consequences(which are slower to emerge and more subtle) but which ultimately undermine important tenets of a functioning society. However, these are inevitably

even harder to measure than the already difficult to quantify wider negative sets of impacts on victims (Box 3).

Box 3: The long-term costs to societies of high levels of fraud

The true long-term impacts of high and persistent fraud levels on society go much deeper than the short-to medium-term social, psychological and economic costs touched upon in Figures 11 and 12. For example, the accumulated evidence about the long-run impact of crime on societies suggests we can expect fraud, over the long-run, to:[42]

- Contribute to an erosion of the rule of law driven through frauds remaining prevalent, being infrequently investigated by law enforcement and regulators, with most perpetrators remaining largely un-sanctioned.[ix]
- Support the ongoing promulgation of other types of serious crime with high individual and social costs. For example, there are well known links between fraud and terrorism, human trafficking and modern slavery.[43] [44]
- Act as a drag on long-term growth and impact on employment levels.[45] [46] [47] One way in which fraud distorts economies, is through its impact on the price of financial services, because fraud costs become embedded in expectations and prices. There are also demand-side impacts, as evidence suggests that consumer confidence in the financial system is likely to decline, this is likely to manifest itself by the disengagement from the use of some financial products by sections of the population.[48][49][50]

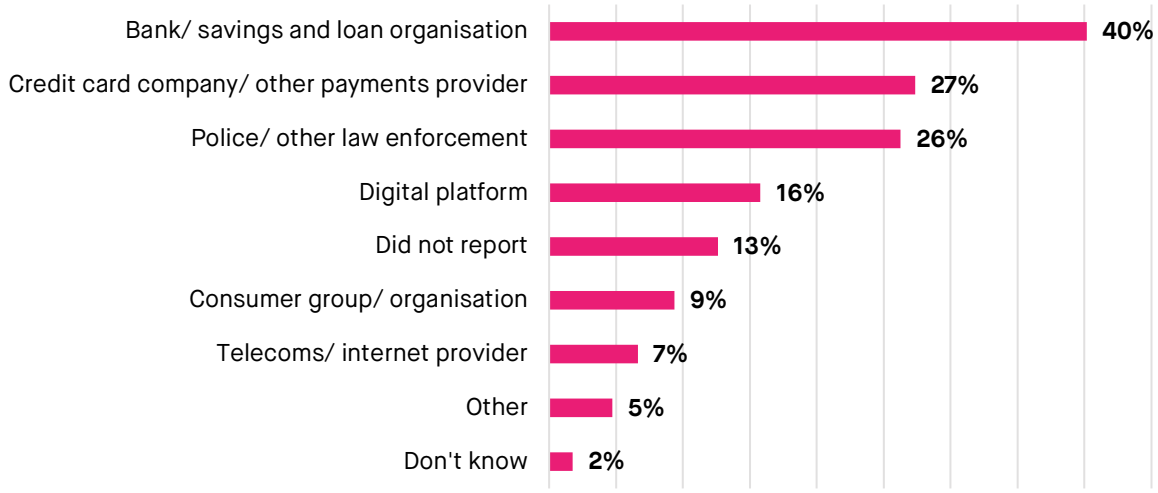
The reporting of fraud by victims across 15 countries

Victims most often report fraud to their bank or other relevant financial institution

The evidence presented in Figure 13 suggests that, across the whole sample, financial institutions are where the plurality of victims primarily reported their only or most recent fraud - 40% to their bank and 27% to the credit card company or other payment services provider. It also shows that just over one in ten (13%) victims did not report their only or most recent fraud experience at all.

[ix] Analysis of 126 countries by Lexis Nexis, suggests that a 1% change in the rule of law (as measured by the World Justice Project's Rule of Law Index) is linked, on average, to a $676 change in GDP per capita. A 10% change is associated with a $7,420 change in average GDP per capita. This indicates that over time, declines in the rule of law in a country like the UK will lead to the UK missing out on considerable future social and economic gains. In the wors case the UK could see an absolute decline in income per head levels driven by falls in the strength of the rule of law. Source: "Measuring the Rule of Law Impact Worldwide - LexisNexis," https://www.lexisnexis.com/en-us/rule-of-law/measuring-the-rule-of-law.page.

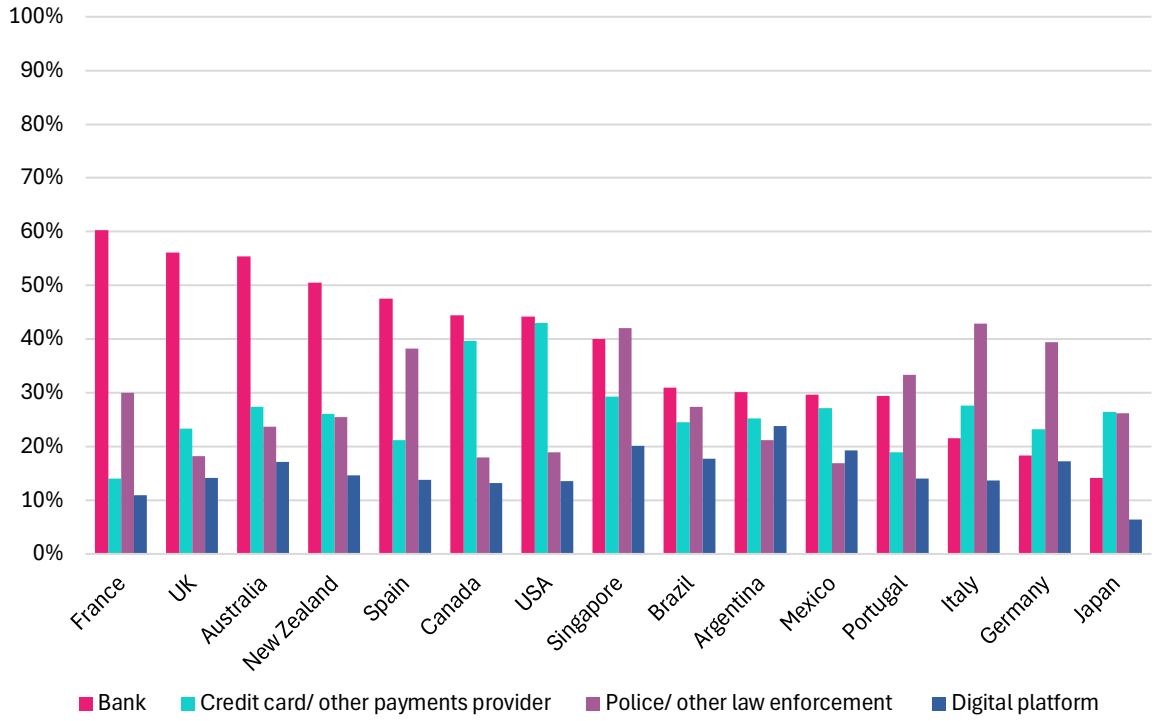
Figure 13: Where victims reported their only or most recent experience of fraud, all international respondents, 2021-2023



Source: Focal Data survey

There was considerable variation between countries in the tendency to not report fraud. For example, the countries with the highest "non-reporting" rates were Portugal (22%), Japan (22%) and Mexico (20%). Overall reporting levels were highest in France and the US.

Figure 14: Where victims reported their only or most recent experience of fraud (top four most frequently given responses), 2021 - 2023



Source: Focal Data survey

The average rate of reporting frauds to law enforcement across the whole sample was 26%. However, reporting varied across countries. Victims in Italy (43%) and Singapore (42%) were the most likely to report their victimisation to law enforcement. By contrast, 17% of Mexican victims and 18% of UK and Canadian victims did so.

The variation in the levels of reporting to law enforcement, shows that the authorities in every country which we surveyed are only directly receiving a partial picture of the fraud threat. Yet a clear and detailed picture of the fraud landscape for law enforcement purposes is an essential starting point for tackling fraud. One implication of this, is that across all 15 countries, a concerted effort to bring together data on fraud held by the wide variety of organisations to which victims report, is likely to be an essential prerequisite for constructing an accurate fraud threat picture at the country level. From such a position, it would then be much easier for each country to mount a well-informed response to volume fraud perpetrated against individuals.

CHAPTER FOUR – THE NATURE OF THE STATE RESPONSE TO VOLUME FRAUD AGAINST INDIVIDUALS ACROSS 15 COUNTRIES

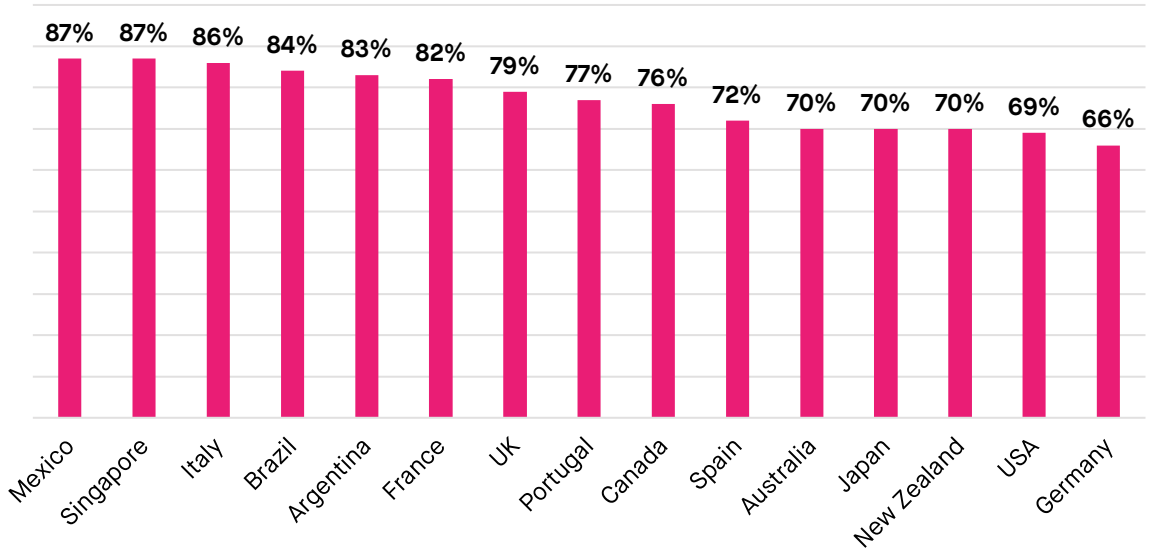
An insufficiently strong response to volume fraud from the state

The inadequate response to fraud against individuals from the state in the UK and many other countries around the world, was identified in our expert interviews as one of the main reasons why this particular crime is so prevalent.[51] Law enforcement is perhaps the most visible manifestation of a state's capabilities and capacity.[x] Therefore, the response of law enforcement to volume fraud is a useful comparative proxy for the wider efficacy of the effort against fraud by the governments of the countries we polled.

The poor law enforcement response to fraud across 15 countries is reflected in high numbers of reported frauds going un-investigated

In every country we surveyed, there was a significant reporting "attrition rate" of fraud incidents. Across the sample as a whole, typically, more than three-quarters (77%) of frauds perpetrated against individuals that are directly reported to law enforcement, fail to reach the stage of being investigated (Figure 15).

Figure 15: Law enforcement attrition for frauds against individuals reported between 2021 and 2023

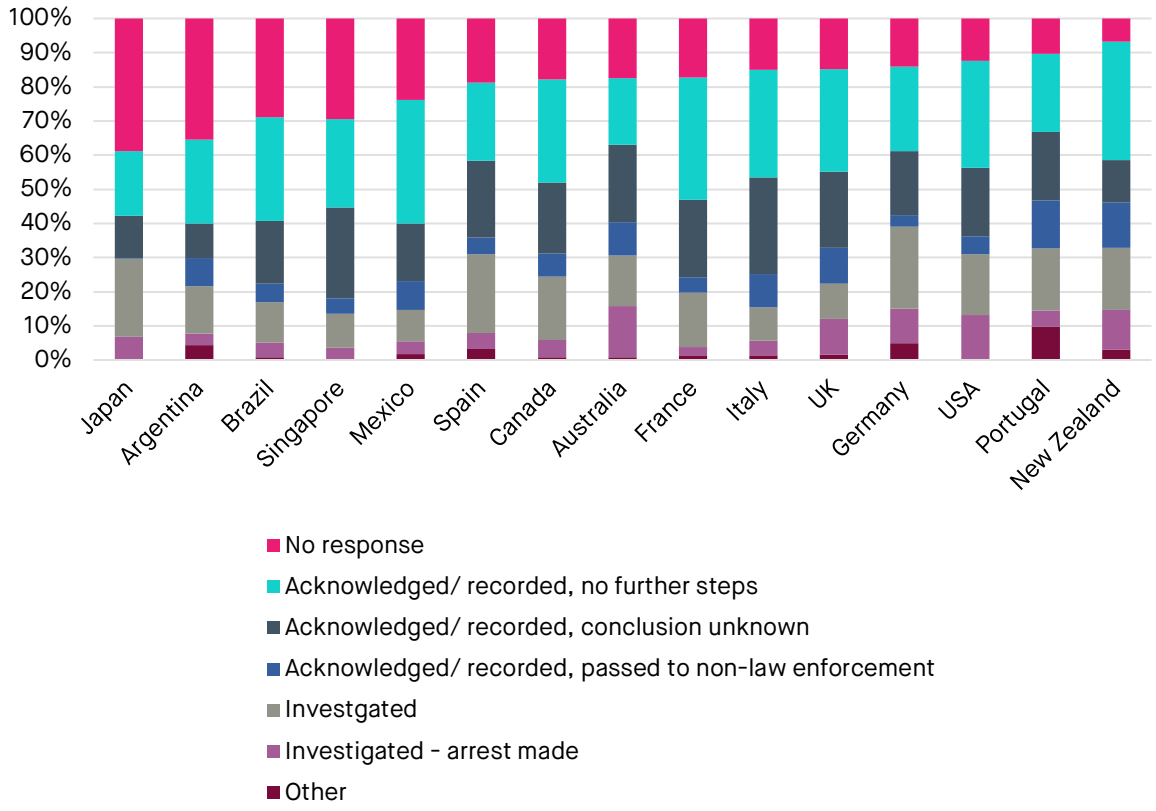


Source: Focal Data fraud survey and SMF calculations

[x] The ability of a state to develop and implement effective policy, control its territory and protect those that reside within it are the hallmarks of its capacity and capabilities. The most visible of the societal consequences of the presence of a high degree of state capacity and capabilities is the strength of the rule of law, central to which is the degree of crime control. Sources: Luciana Cingolani, "The State of State Capacity: A Review of Concepts, Evidence and Measures," 2013 and Global Initiative Against Transnational Organised Crime, "Global Organised Crime Index 2023," 2023, https://globalinitiative.net/wp-content/uploads/2023/09/Global-organized-crime-index-2023-web-compressed-compressed.pdf.

The UK, for example, had the seventh highest "attrition rate" amongst the sample countries, with around one-in-five frauds reported to law enforcement being investigated. Germany was the country where victims were most likely to have their fraud case investigated, with a third of the reports to law enforcement looked into by the authorities.

Figure 16: Response to victims directly reporting their only or most recent fraud to law enforcement, 2021 – 2023



Source: Focal Data survey

The three most common responses from law enforcement to the reporting of a fraud in each country we surveyed, were (Figure 16):

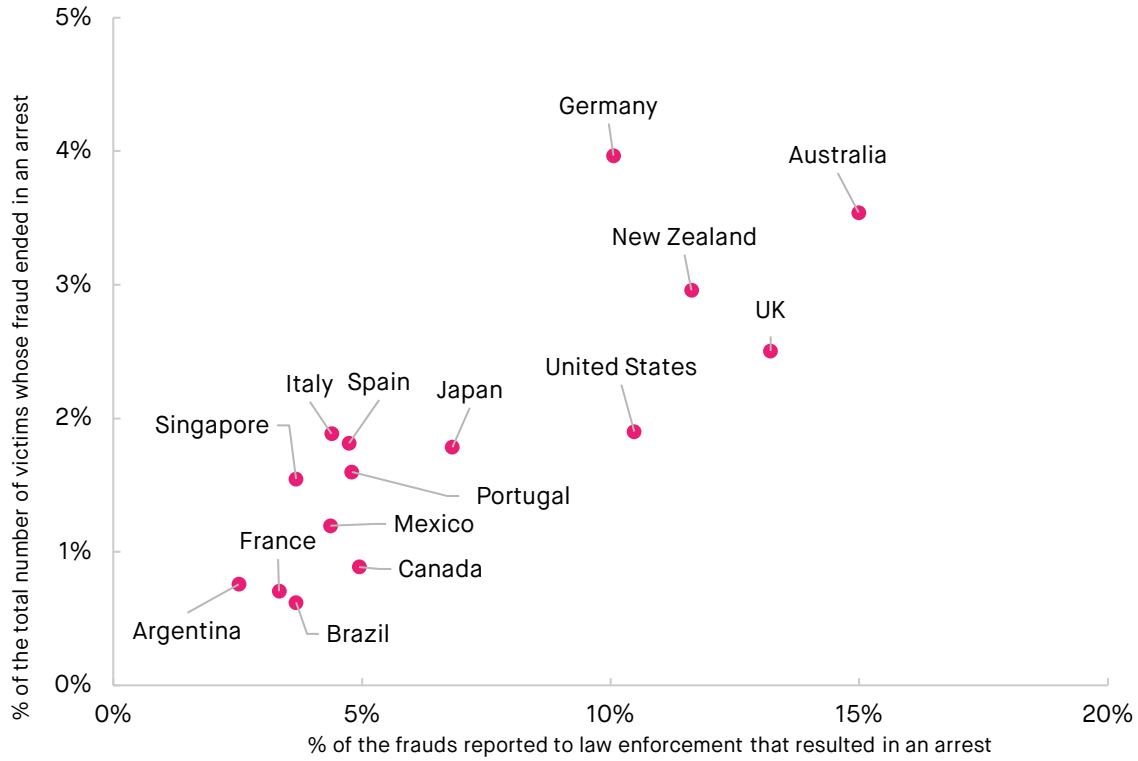
- No response, which was most prevalent in Japan – 39% of reported fraud.
- The recording of the incident but no further action, which was most often experienced by French and Mexican victims (36%).
- The recording of the incident but no further contact, which happened to 28% of Italian victims.

In every country only a small proportion of frauds end up in the arrest of a suspect

Our survey found that on average, across the whole sample of countries, to the best of survey participant's knowledge, 2% of the only or most recent frauds suffered by victims resulted in an arrest. In the context which we found – i.e. a broadly poor law enforcement response to volume fraud against individuals across all 15 countries – Australia and Germany stood out as doing better than the others. Survey responses

from Australian and German victims indicate that as many as 4% of the only or most recent frauds experienced by victims resulted in an arrest of a suspect (Figure 17).

Figure 17: Proportion of the only or most recent fraud suffered by victims that resulted in an arrest of a suspect, 2021-2023



Source: Focal Data survey and SMF calculations

N.B. Please note that as a victimisation survey, the answers are ones given to the best of the respondent's knowledge about what happened in their only or the most recent experience of fraud. In addition, the data presented is from small sub-samples of the total number of respondents. Together, these constraints on the data suggest these results should be seen as indicative only.

Across the 15 country sample as a whole, on average, 7% of the only or most recent frauds suffered by victims directly reported to law enforcement ended up in an arrest – at least, that is, to the best of individual respondent's knowledge. Notably, a cluster of five countries had an arrest rate higher than the average. These were mainly Anglosphere countries plus Germany.

Despite the UK's relatively good performance, the overall law enforcement effort against volume fraud in the UK remains poor. It is beset by under-resourcing, insufficient numbers of skilled officers and other accounting, digital and counter-fraud experts, as well as a poorly organised law enforcement landscape. As a result, it came in for strong criticism from the experts which we spoke to for this research, with one summarising what many had pointed out when they stated:[52]

> *"... the UK's approach to tackling fraud is a huge failure ... the chances of getting caught are very low, and then even if you do get caught, the penalties are very low".*

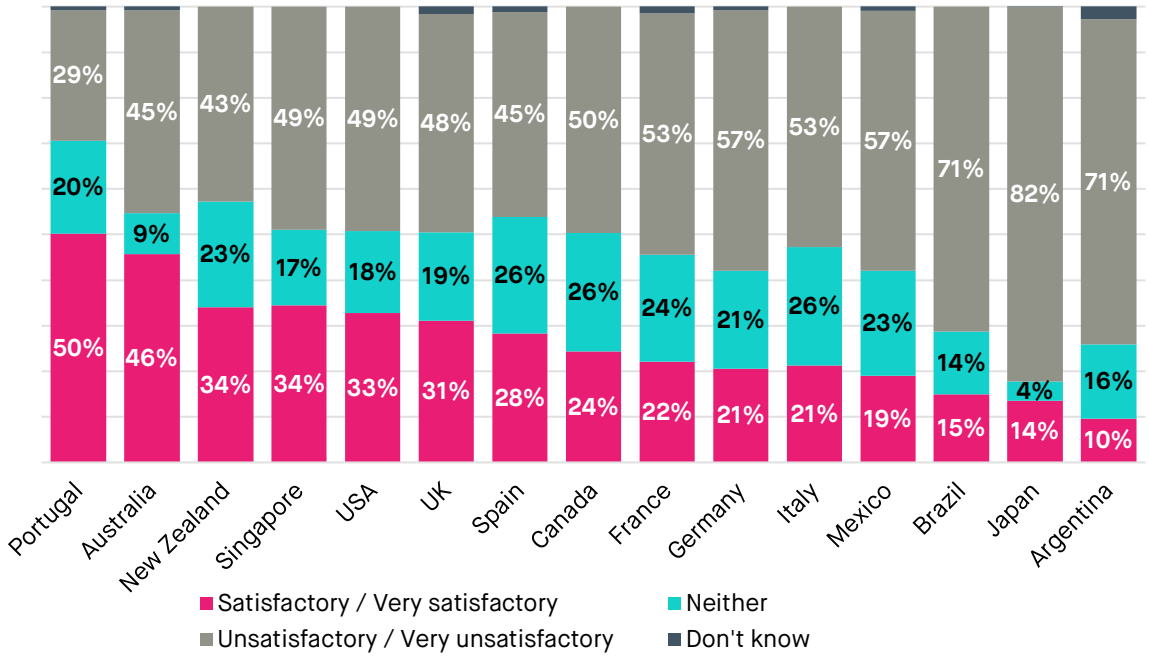
Victim satisfaction is another way to measure the efficacy of the law enforcement response in each country

One of the experts interviewed to help inform this report, highlighted the importance of the link between a poor law enforcement response to victims and people's trust in the efficacy of the authorities:

> *"The way that police respond to fraud victims can enhance the experience of victimisation, or it may reduce future reporting … therefore, dealing with victims well … even if law enforcement can't necessarily investigate the case fully, making the person feel heard at least, is important".*

We asked victims who reported their only or most recent fraud to law enforcement, how satisfied they were with the response they received (Figure 18). Across the 15 countries surveyed, there was an approximate 2:1 ratio of average dissatisfaction (53%) to average satisfaction (27%). Portugal was the country with the highest levels of victim satisfaction (50%) and the second lowest levels of "no response", while the UK ranked sixth amongst the countries on victim satisfaction with the law enforcement response (31%) and had the fifth lowest "no response" rate (Figure 16).

Figure 18: Satisfaction with the law enforcement response to the victim's only or most recent fraud reported to law enforcement, 2021 – 2023



Source: Focal Data survey

CHAPTER FIVE – PUBLIC VIEWS ON COUNTER-FRAUD POLICY MEASURES

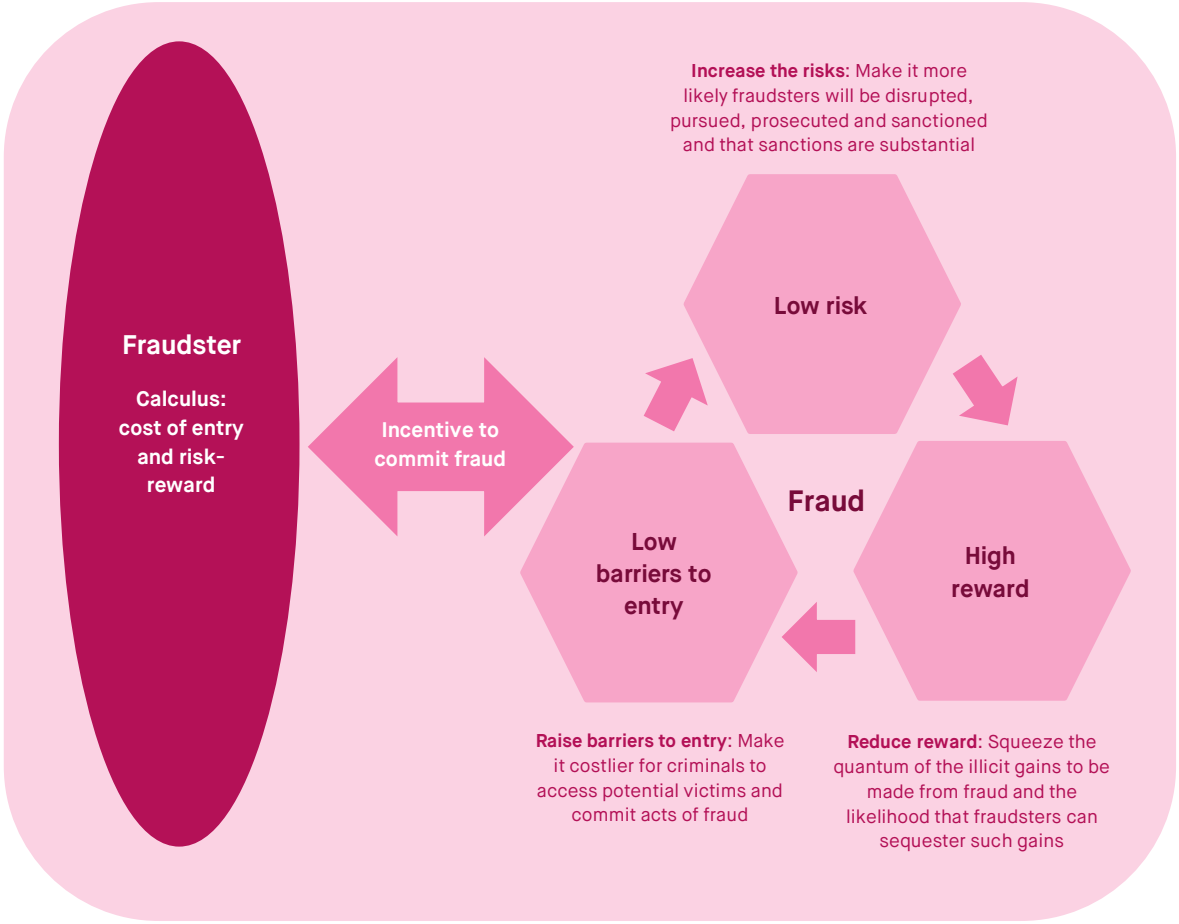
An effective response to fraud requires an enhanced state response

Beating fraudsters requires making fraud costlier for fraudsters and much risker to perpetrate

Our interviews with experts identified the key ingredients of an effective governmental response to the current "fraudemic" (see Diagram 3) which would apply to any country seriously looking to tackle volume consumer fraud. They pointed out that the current favourable environment for fraudsters needs to be much more challenging by focusing the policy response on:

- Increasing the costs of entry for fraudsters, to deter potential fraudsters and consequently prevent frauds from being perpetrated.
- Making it much costlier and riskier to commit fraud by making it more likely that fraudsters will be disrupted, pursued, arrested and robustly sanctioned.
- Reducing the rewards of being a fraudster, by denying them opportunities to commit frauds and making it much more difficult to sequester their illicit gains.

Diagram 3: What counter-fraud measures need to do to succeed against fraudsters



Source: Expert interviews

Collective action problems hold back a more effective effort against fraud

The efficacy of the UK's response to fraud is hindered by collective action problems in both the public and private sectors.[53] These stem from misaligned interests amongst the parties relevant to the fraud problem (i.e. they are not congruent with the societal good of significantly reducing fraud victimisation) and the lack of insufficiently strong incentives on people and organisations such as those in the "fraud chain" to create the impetus for improvement. The consequences of the presence of these coordination failures re:

- Fraud is insufficiently prioritised by those whom can make the most difference to the problem.
- The kinds of steps that can deliver positive and significant impacts across the three domains described in Diagram 3 are either not implemented at all, or only done so in limited ways.

These challenges pervade the counter-fraud landscape in many countries, where the response to fraud is similarly inadequate, as our data on the law enforcement response across the 15 countries we surveyed indicates (Chapter Four) and a number of expert interviews revealed. For example, one described the disjointed state of the US response to fraud:

> *"it's so 'stove piped'... there's all these splintered responsibilities, that make action against fraud difficult... make it hard to deal with... in a meaningful way".*

A key question for policymakers, is how can the public and private collective action problems be minimised? This leads to a further question: whether the public in the UK and across the other 14 countries we surveyed, would support the kinds of counter-fraud measures which an effective response generated through re-aligning incentives would involve? This is particularly pertinent where new inconveniences and burdens for consumers might be involved, including the utilisation of large amounts of personal data. Our findings show that, in many areas, the public of the 15 polled countries do not oppose such measures and are often actively sympathetic towards them.

Tackling the collective action problems holding back the response to fraud

Aligning incentives to deal with the "fraud chain" collective action problem

For the private sector organisations which make up the "fraud chain", for example, financial incentives could be utilised to ensure greater prioritisation is given to volume fraud and effective counter-fraud measures are developed and implemented. This option was raised by several of the experts we interviewed, with one noting that, in the UK:

> *"By making the banks 100% liable for reimbursement it incentivises banks to invest in the preventative tools and techniques. Well, the same would apply for everyone else in the "fraud chain"."*

At the moment, in the UK, as a number of those we spoke with pointed out, apart from payment services providers, many of the organisations that make up the "fraud

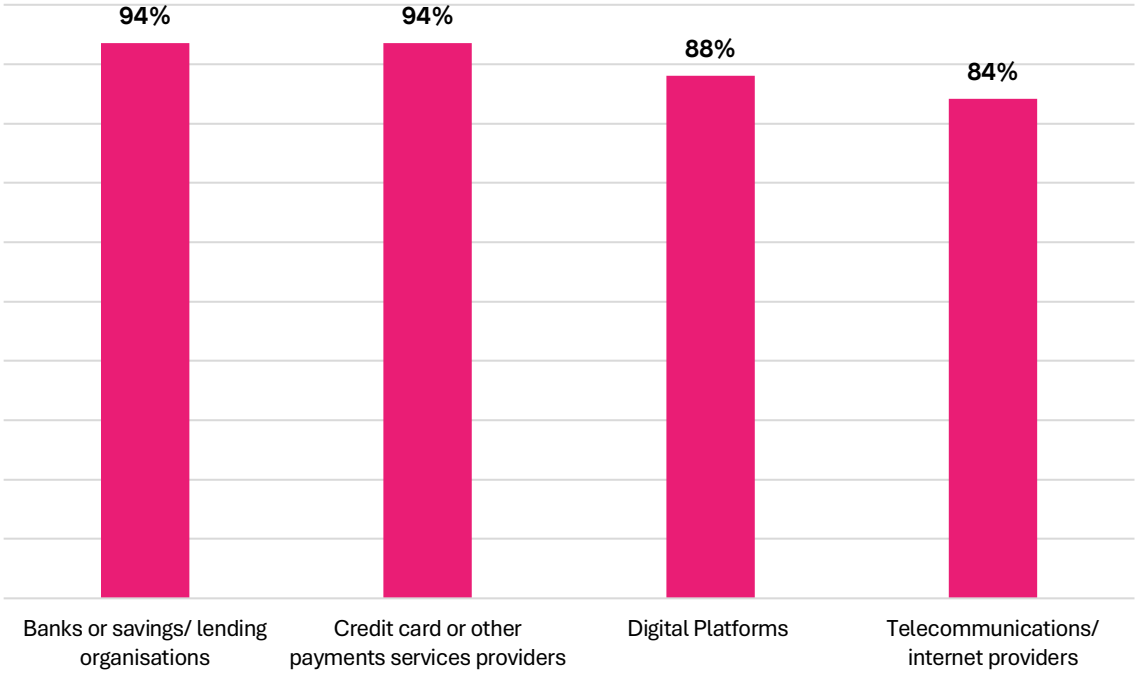
chain" bear none of the cost despite large amounts of fraud being propagated through their services:[54]

> *"Social media firms, tech firms and telcos have almost no financial or regulatory incentive to prevent fraud. While this remains the case these firms will have no reason to cooperate or to take the issue seriously."*

Strong public support for financial incentives that would make "fraud chain" organisations take fraud seriously

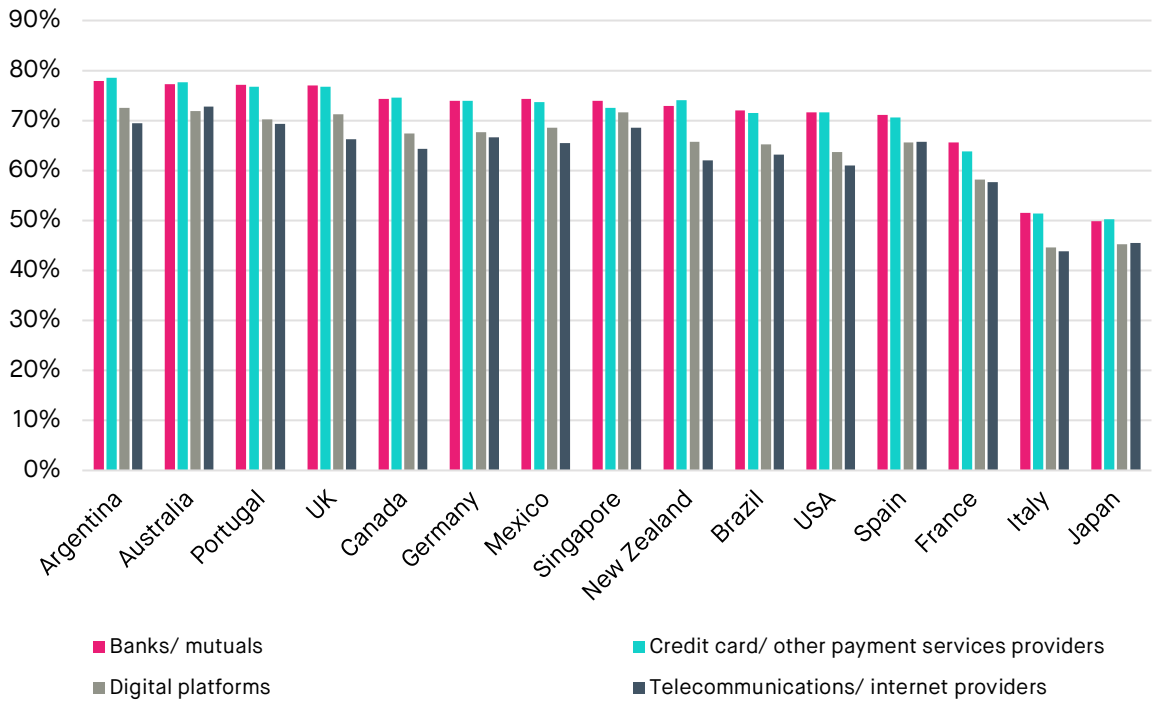
Our polling (Figures 19 and 20) found substantial public support across all of the countries we surveyed, for the kinds of policies which could help align the interests and actions of the organisations in the "fraud chain" with those of the wider public and to push these organisations into taking the prevention and disruption measures, which could make a significant difference to the amount of fraud perpetrated through their services.

Figure 19: Support for different types of organisations in the "fraud chain" bearing some of the cost of fraud reimbursement



Source: Focal Data survey

Figure 20: Support for a sanctions regime against organisations in the "fraud chain" that fail to prevent and disrupt fraud



Source: Focal Data survey

Across the 15 countries, on average:

- 71% of respondents supported banks facing financial penalties.
- 71% agreed that credit card and other payment services providers should be subject to such obligations.
- 65% supported digital platforms being financially sanctioned.
- 63% were agreed that telecoms firms and internet providers ought to face financial consequences.

One conclusion that might be drawn from the aforementioned results, is that there could be scope for multilateral agreements amongst states to put policy frameworks containing such elements in place, in the countries we surveyed.

Data and intelligence sharing underpins an effective response to fraud

Amongst our interviewees, it was widely observed that more extensive data and intelligence sharing between "fraud chain" organisations and the private and public sectors (i.e. law enforcement and regulators) are essential to:

- Helping boost levels of fraud prevention.
- Enabling more proactive and effective disruption of fraud.
- Facilitating more success in the pursuit of fraudsters.[55]

The collective action problems hindering data and intelligence sharing

In many of the countries we surveyed, ameliorating the collective action problem holding back data and intelligence sharing, would enable relevant organisations to

orientate themselves towards such actions and build the necessary human, organisational and physical infrastructure.[56] However, as some expert interviewees noted, the incentives are too weak at the moment to bring this about. For example:

- One interviewee observed the absence of any financial inducements or legal obligations to push organisations into taking the necessary steps:

  "I see a barrier in terms of information sharing … you have enforcement authorities, national competent authorities, PSPs, online platforms, electronic communication providers, and you need to bring them all together … and if we just say, you can voluntary share data, my question would be, where will that actually happen?"

- The second problem is a cluster of practical hurdles which, even in the context of substantial financial incentives and robust legal duties, would still limit actions because of their implications for resources, disruption to existing operations, organisational changes and the concomitant opportunity costs (see Table 1).

Table 1: Practical hurdles to effective data and intelligence sharing arrangements in the UK and elsewhere

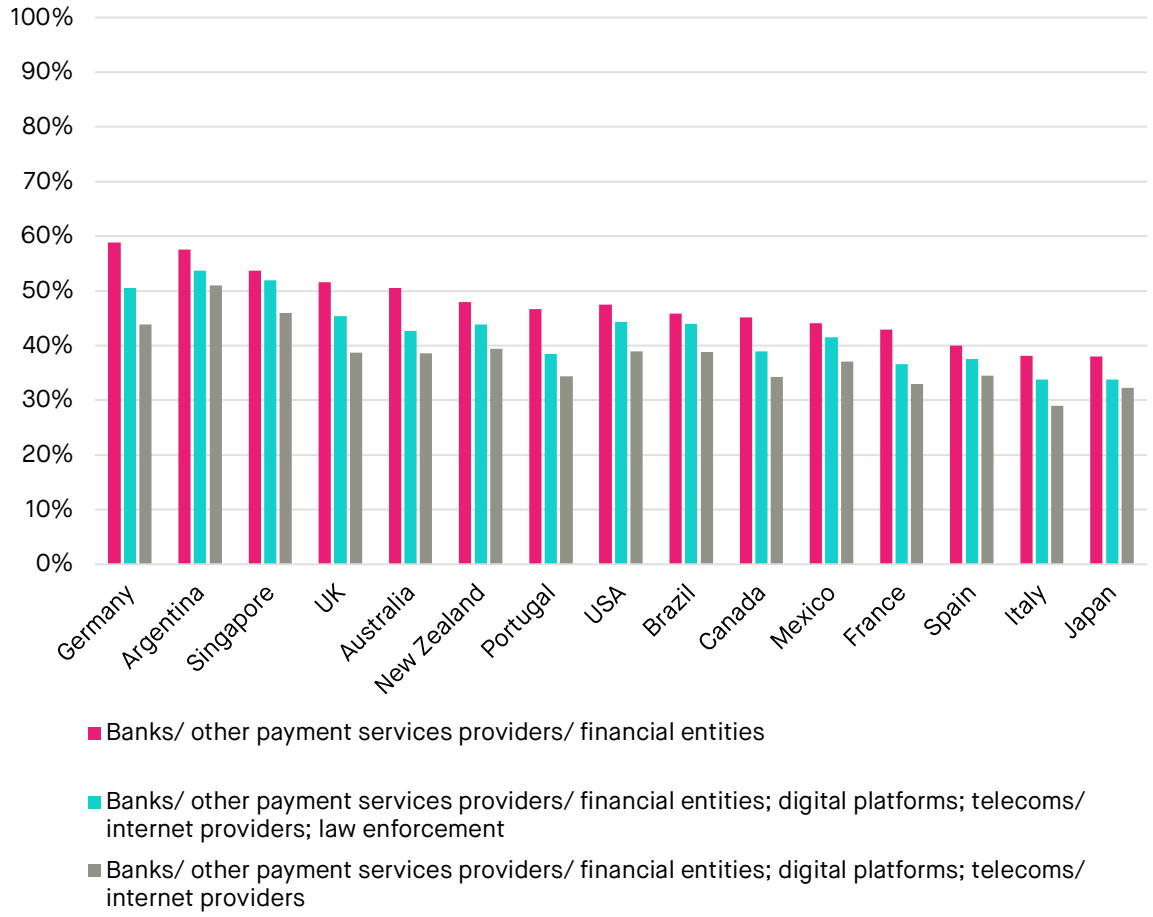
Challenge	Description
Agreeing the scope of the data sharing	Key questions that need to be answered to ensure the design of an effective data and intelligence sharing system include: • What is the aim or aims of the arrangement? • Who are the key stakeholders? • How will information be processed? • Should the data and intelligence sharing operation sit with a private or public body and should it be a separate entity that sits over all the relevant parties? • How will data and intelligence be disseminated?
Legal barriers	Uncertainty and legal risks around data protection laws were raised by several of the experts we interviewed as placing limits on the scope for data and intelligence sharing amongst key parties.[57] The General Data Protection Regulation (GDPR) was singled out as being particularly problematic in the EU in limiting what financial services firms could do.[58] Rules limiting the multiple uses of data were highlighted in other interviews, e.g. it was suggested that it was difficult for data shared for tackling money laundering to then be used to help tackle fraud.
Technical obstacles	There are many technical obstacles to data and intelligence sharing beyond the design, legal and relationship ones. For example, the organisations which would need to share data and intelligence and then act upon it, operate different systems with their own rules and procedures. Therefore, an effective arrangement would need to see technology and processes become more compatible.[59]

Source: Expert interviews and Which? (2023)

Public support for alternative data and intelligence sharing arrangements

Another influence on the nature of any data and intelligence sharing arrangements are the views of the publics in the countries which we surveyed, towards different kinds of possible data and intelligence sharing regimes (Figure 21). As our results show, all of the different options respondents were asked about, received at least a plurality of support in the vast majority of the countries we polled.

Figure 21: Support levels across 15 countries for different data and intelligence sharing arrangements



Source: Focal Data survey

In each country in the survey, there was notable consistency in which the data and intelligence sharing approach garnered the most support - and the least. In aggregate, across the sample:

- Data and intelligence sharing between banks/payment services providers and other relevant financial entities was the most popular approach (47% support).
- Data and intelligence sharing between digital platforms; telecoms/internet providers; banks/payment services providers and other relevant financial entities and the police/other law enforcement agencies was marginally behind in popularity (42% support).
- Data and intelligence sharing between digital platforms; telecoms/internet providers; banks/payment services providers/relevant financial entities was the least popular (38% support).

Explicit opposition to such arrangements was consistently lower than the combined levels of support and indifference in all the countries we polled, indicating that, in many instances, extensive data and intelligence sharing systems could be implemented without too much controversy, although our results may imply that

governments might first wish to make a more determined effort to make the case to their publics for the importance of such approaches. It also indicates that there are grounds for a potential international agreement among a number of governments, on the development and implementation of advanced data and intelligence exchange mechanisms.

Examples of public-private fraud data and intelligence partnerships helping underpin coordinated action

In our expert interviews, emerging examples of effective public-private data sharing collaborations in other countries were highlighted. For example, real time information sharing schemes in Singapore and South Korea were singled out.[60] Two separate experts spoke highly of them, with one noting that:

> *"In South Korea, the authorities are directly linked to the banks. There is much greater coordination, and this means that the response to fraud is considerably quicker".*

> *"...they've got this reporting centre ... as soon as someone's reporting fraud, they're on to the banks to stop the transaction ... immediately they're closing down the bank accounts, and the telephone numbers of the fraudsters ... it's much quicker action..."*

There is considerable support for more frictions in payment systems in many countries

Digital payments inadvertently encourage fraud

There was unanimous agreement amongst those we interviewed for this research that the swiftness with which money moves both through domestic financial systems and across borders is a significant contributor to fraud risk:[xi]

> *"In terms of risk the only thing worse than Faster Payments is probably Faster Payments cross border".*

Part of the problem, is the speed with which a fraud can take place. Another, is the ease with which illicit gains can be sequestered. As explained in Chapter One, the "low friction" financial system makes it attractive to criminals. Particularly helpful to fraudsters is the fact that, as one of the economic crime experts we spoke with noted:

> *"If you can launder the proceeds of your fraud more quickly, this does lead to an increase in fraud".*

Frictions in payment systems are necessary to reduce fraud risk

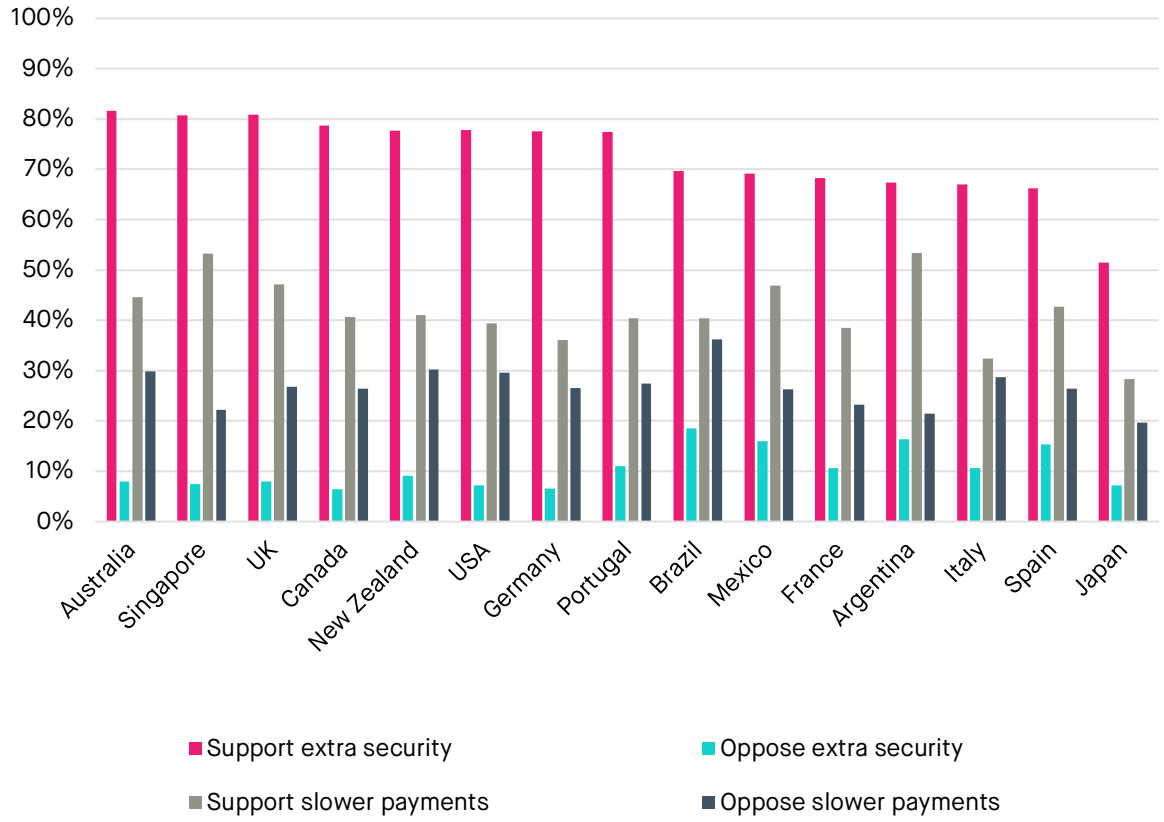
Whilst reforms to payment systems are in no way a panacea to the problem of fraud, several interviewees advocated for reform to the current "low friction" payments system. One fraud specialist we spoke with argued:

[xi] Faster payments are the method of payment used to facilitate 96% cases of the APP fraud in the UK, in 2020. Source: "Fraud - The Facts 2021," UK Finance, https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2021.

"Where there is a concern or a risk flag or a warning, then the banks need longer than they now get to be able to make a decision based on an informed response to questions, rather than a guess..."

Our survey revealed majorities in all of the countries which we polled, for stronger security checks on payments and transfers (Figure 22). Average support for such measures was 73% across the surveyed countries. At the same time, our research also found there was 42% support, on average, for slower payments across the 15 surveyed countries. There were outright majorities in favour of a slower a payments system in Argentina and Singapore and pluralities amongst the publics in the other 13 surveyed countries.

Figure 22: Public support in 15 countries for frictions in payment systems



Source: Focal Data survey

Overall, our data suggests that introducing more security around payments systems (e.g. stronger identity verification of both payers and payees) would be accepted by the public in the UK and the other 14 countries we polled. However, the survey results also imply that slowing payments and transfers down may need to be targeted based upon risk, rather than being implemented as a measure across the board. Ultimately, both kinds of frictions would be most effective against fraud risks, if they are underpinned by effective data and intelligence sharing, of the kind discussed earlier in this report.

Standing in the way of the implementation of a package of frictions in the UK, for example, is the underlying collective action problem which hinders all the actors in

the "fraud chain" from implementing the societally optimal measures.[61] It is likely, therefore, that mandatory reimbursement and perhaps other types of financial incentives would push some payment services providers into taking more action. Nevertheless, in the end, mandates may be required to ensure the adoption across the whole sector, as was the case with two-factor authentication.[xii]

Cryptocurrencies are becoming a more prominent factor in the fraud landscape

In addition to introducing frictions into mainstream payment systems, the issue of cryptocurrencies came up in a number of our expert interviews. Not only are crypto-scams widespread and a growing source of fraud, but cryptocurrency is also used for sequestering illicit funds.[xiii] [62] [63] Experts we spoke with suggested that their importance is only likely to grow and that efforts are needed to clean up this part of the financial system. Not least because doing so could pay significant dividends in the wider fight against fraud, by reducing the attractiveness of crypto for fraudsters:

> *"Governments have to make it more difficult for the criminals to enjoy their money … if you can prevent them from converting it, if you can make it so difficult or so costly that it's not worth it, they'll go and find something else to do".*

Widespread public support for more law enforcement powers to tackle fraud

When the publics' of the 15 countries we surveyed were asked if they would be prepared to support more powers for law enforcement and regulators to disrupt and pursue fraudsters, there was majority support (Figure 23) .[xiv] [xv] In all countries except Japan, a majority was also in favour of more powers for regulators, such as financial services and consumer protection agencies, where appropriate.[xvi]

[xii] In the UK, rules around payment speeds brought in under the auspices of the Payment Services Regulations 2017 are likely going to need to be revised. Before the 2024 election was called, the then government was exploring such reforms to help tackle fraud risk in the UK payments system. Source: "The Payment Services (Amendment) Regulations 2024 – Policy Note," GOV.UK, https://www.gov.uk/government/publications/the-payment-services-amendment-regulations-2024-policy-note.

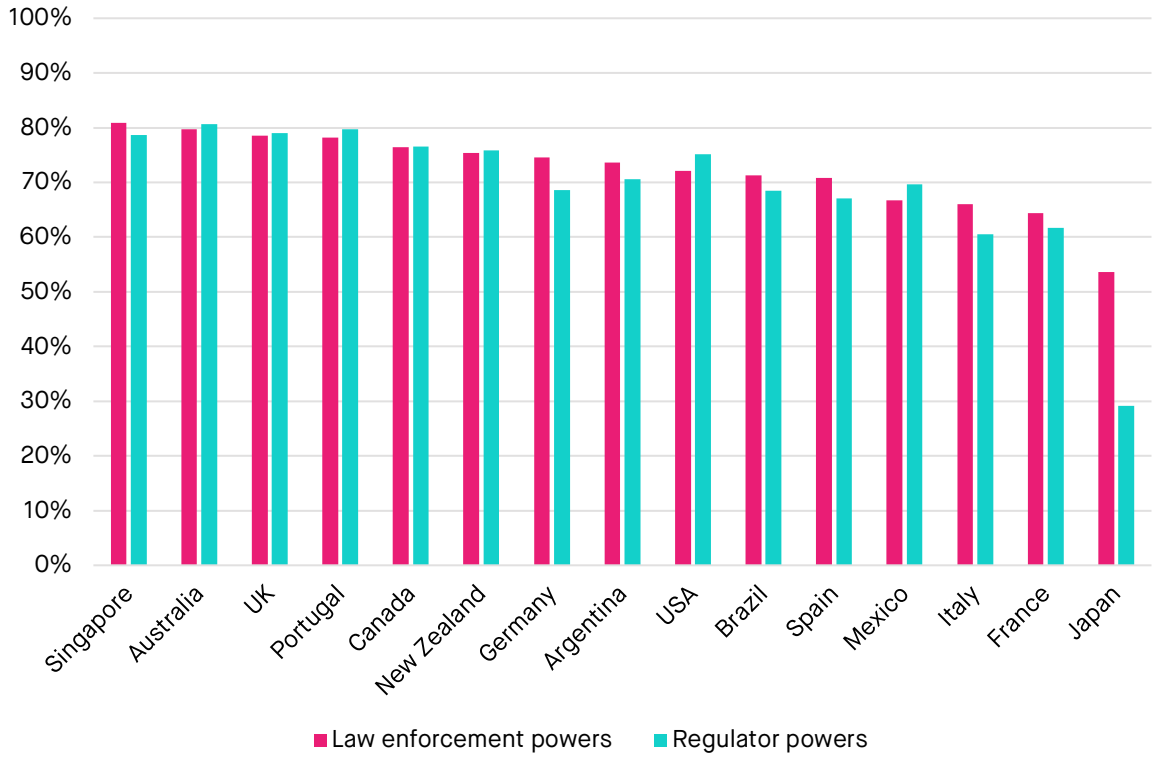
[xiii] One review identified 47 different types of cryptocurrency based fraud. Source: Arianna Trozze et al., "Cryptocurrencies and Future Financial Crime," *Crime Science* 11, no. 1 (January 5, 2022): 1, https://doi.org/10.1186/s40163-021-00163-8.

[xiv] The intuition being expressed by those we polled is consistent with the established criminological evidence which shows that, in general, effective policing at sufficient scale delivers crime reduction. Source: "Crime, Deterrence and Punishment Revisited | Empirical Economics," https://link.springer.com/article/10.1007/s00181-019-01758-6.

[xv] More specifically, as one study of crime in England and Wales showed, increases in arrest rates can deliver substantial reductions in frauds. Source: Lu Han, Siddhartha Bandyopadhyay, and Samrat Bhattacharya, "Determinants of Violent and Property Crimes in England and Wales: A Panel Data Analysis," *Applied Economics* 45, no. 34 (December 1, 2013): 4820–30, https://doi.org/10.1080/00036846.2013.806782.

[xvi] For the first time, in 2022, the UK'S Financial Conduct Authority (FCA) set out plans to prioritise the consumer fraud threat, after acknowledging the seriousness of it. Source: "How We Work," FCA, March 24, 2022, https://www.fca.org.uk/about/how-we-work.

Figure 23: Support for enhanced powers for law enforcement and regulators to tackle fraud



Source: Focal Data survey

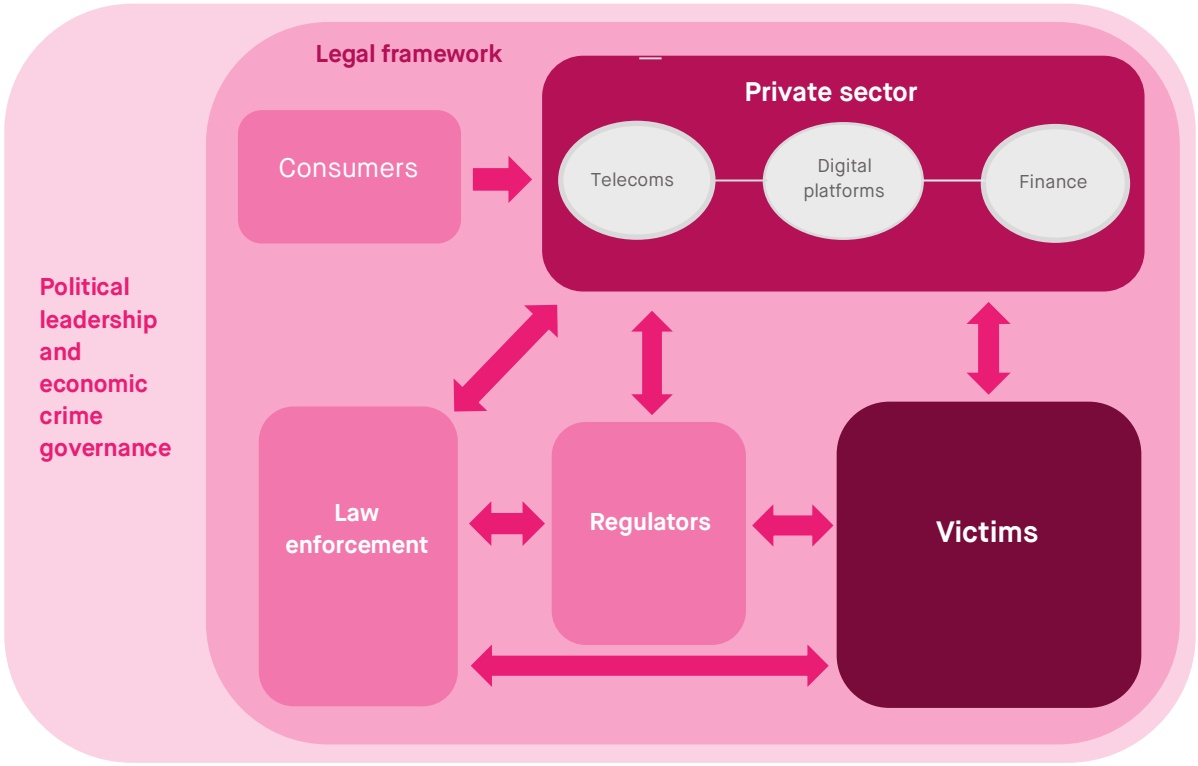
The cross-country support for more authority for law enforcement and regulators, should be helpful for policymakers in the 15 nations we surveyed, considering how the current, largely inadequate, state response to fraud might be improved. It suggests that the public in a significant number of places around the world, would be happy to see a more muscular law enforcement and regulatory effort.

CHAPTER SIX – DEVELOPING AN EFFECTIVE COUNTER-FRAUD STRATEGY FOR THE UK

The UK government should put much greater priority on tackling fraud

Building an effective counter-fraud policy in the UK is a challenging task because of the many interconnected domains relevant to the problem. Any such effort will need to align them in order to deliver a robust and sustainable response that is likely to have a sizeable strategic effect against the fraud problem. Diagram 4 illustrates these interconnected spheres.

Diagram 4: The key domains relevant to the fraud challenge facing the UK



Source: SMF

Reflecting this complexity, a "systems approach" is needed to tackle the fraud problem. Such a method has to begin with clear aims and determined leadership.[64] These starting points then need to be reflected in new structures at the heart of government in order to institutionalise them.[65]

Recommendation One: The UK government should establish a cross-departmental Economic Crime Leadership Group (ECLG) comprised of the most senior relevant Ministers to prioritise the fight against fraud

The Fraud Champion role created by the last government, was a welcome step forward in trying to boost the profile of fraud at the heart of policymaking and help to bring about more coordination in the effort to tackle it.[66] However, the public sector response to fraud in the UK has been inadequate to the task of fully overcoming the collective action problem, holding back a significantly more effective response. The latter requires there to be:

- Long-term buy-in at the top of government and by key departments.
- A clear direction to be set, with accountability for achieving objectives and outcomes.
- Suitable resourcing.

From the right structures, priorities and actions across the interconnected domains (see Diagram 4) can be set and coordinated in a considered and coherent way.

Therefore, the prioritisation of and leadership on economic crime (and within that envelope, primarily fraud) needs to be institutionalised at the top of government. The cross-departmental ECLG should include the relevant senior Ministers such as the Chancellor of the Exchequer, the Home Secretary, the Secretary of State for Justice, the ,Secretary of State for Science, Innovation and Technology and the Attorney General. The group would set the goals for policy on economic crime and drive the implementation of the latter through government. The ECLG would need appropriate resourcing to monitor and evaluate implementation and impacts and hold those leading operational activity to account. The ECLG should report regularly and publicly on performance. Without such a reformulation of the machinery of government at the senior levels, the collective action problem holding back the public sector response to fraud is unlikely to improve and therefore the law enforcement and regulatory efforts needed to beat fraud remain unlikely to happen at the speed and to the extent and on the scale that is needed.

Correcting the domestic law enforcement failure against fraud

Law enforcement needs stronger leadership on economic crime issues

Part of the answer to the public sector collective action problem, that hinders the law enforcement and regulatory effort against fraud across the UK (and in England and Wales in particular) is the marshalling of the disparate elements of the counter-economic crime response into a more coherent system. This requires a greater

degree of coordination and integration under stronger direction from the centre, as one expert we spoke with observed: [xvii] [67]

> *"Ultimately, you need the Home Office to give much stronger central direction to bodies such as police forces".*

For the greater central control to be effective, structural reorganisation will also be required, with the main counter-fraud effort no longer distributed across the 43 constabularies of England and Wales and multiple other agencies.[xviii] Rather, it should primarily be national, with strong regional elements and buttressed by a more prominent international dimension.[68]

Enforcement capacity and capabilities need to more closely match the scale of the problem

In addition, law enforcement needs resources that more closely reflect the scale of the problem, in part because the pursuit of fraudsters is a labour intensive activity.[xix] Currently, around 1% of the total police workforce in England and Wales is devoted to tackling economic crime, despite fraud accounting for approximately four in ten of all crimes committed against individuals.[69] [xx] This capacity limit is a severe constraint on what law enforcement can do.[70] Equally important, is ensuring that those who police fraud have the right skills and technology at their disposal, to disrupt and pursue fraudsters.[xxi] One academic which we spoke with pointed out:

> *"There is a problem with the lack of skills of police officers have in dealing with fraud, which goes hand-in-hand with the lack of training for officers"*

[xvii] Recent changes announced in the fraud strategy move in the direction of a more national-level approach to fraud control, e.g. the creation of a National Fraud Squad (NFS) and making fraud a Strategic Policing Requirement (SPR). Source: "Fraud Strategy," GOV.UK, June 1, 2023, https://www.gov.uk/government/publications/fraud-strategy.

[xviii] One estimate suggested that (inclusive of the 43 constabularies in England and Wales) there could be more than 80 organisations (and sub-organisations) in the UK public sector, with an interest in economic crime. Source: Mark Button, Branislav Hock, and David Shepherd, *Economic Crime: From Conception to Response* (London: Routledge, 2022), https://doi.org/10.4324/9781003081753.

[xix] Analysis of the City of London's counter-fraud successes reported in their Annual Report 2020-21, shows that the force took on 427 new cases, i.e. 1.3 cases for every person working on economic crime. They secured 98 convictions that same year, which on average, equates to one conviction for every three members of the team. In addition, they delivered £204 million worth of disruption in 2020-21, which is the equivalent of £618,000 worth of disruption per officer and support staff member working on economic crime. Source: City of London Police, "Annual Report 2020/2021," Annual report, 2021.

[xx] For context, the Government's recent fraud strategy announced the launch of a new National Fraud Squad with 400 specialist investigators, which is a small welcome uplift. Source: "Fraud Strategy," GOV.UK, June 1, 2023, https://www.gov.uk/government/publications/fraud-strategy.

[xxi] The kinds of specialist skills needed at scale for a more effective fight against fraud include: forensic accountants, fraud analysts and investigators and digital forensics experts. The shift towards creating a fraud investigation profession in the UK should help create a pipeline of people in the long-term. Source: "Government Counter Fraud Function and Profession," GOV.UK, https://www.gov.uk/government/groups/counter-fraud-standards-and-profession.

Remedying this capability deficit will require policymakers to be prepared to overhaul workforce composition, training and development and compete with the private sector over recruitment and retention, which is going to be difficult, as was highlighted in one of our interviews:

> *"Why would I make £40k as a police officer doing this kind of work, when in the private sector, I can make double that".*

Whilst better pay and conditions would no doubt help, it seems likely that more imaginative ways of overcoming the public sector's recruitment and retention disadvantage would need to be considered. This should involve learning lessons from countries such as South Korea and Singapore, where there are attempts underway to better integrate law enforcement and the private sector expertise at scale. One of the academics who contributed to our interview series for this report argued that:

> *"We have these large entities in the banking and insurance sector, doing a great deal to protect their organisations, they should be working much more closely with each other and with the state … ideally, what you should have is people regularly working with one another, seconding into the police from the private sector, and vice versa".*

Specific ideas that might be utilised include joint investigation teams (JITs) and formal deputisation arrangements for fraud specialists, to add disruption and pursuit capacity and capability.[xxii]

Backing-up law enforcement with the powers and punishments for fraudsters

Bolstering the law around fraud

The government should also consider enhancing the legal powers which law enforcement have available, for dealing with those who perpetrate fraud. There is considerable public support for bolstering law enforcement powers (79% of adult Britons support such actions).

While experts interviewed for this research were broadly happy with the Fraud Act 2006, the US model of having a range of federal offences for specific types of fraud was raised by one expert, as proven to be particularly useful for prosecuting fraudsters in the US. It would be remiss if a government did not look into whether the Fraud Act could be bolstered further, not least by learning lessons from other countries where there has been a track record of success. The potential for the civil law and administrative powers to play a stronger role in disrupting economic criminal activity should also be explored.[71]

[xxii] The Dedicated Card and Payment Crime Unit (DCPCU) has been in operation for two decades and comprises City of London and Metropolitan Police officers and other specialist staff and utilises funding from the financial services sector. The work of the unit has led to the conviction over a thousand criminals in its twenty years of operating and has prevented more than £750 million of fraud. Source: "Dedicated Card and Payment Crime Unit," UK Finance, https://www.ukfinance.org.uk/dedicated-card-and-payment-crime-unit.

Increasing the penalties for fraudsters

The sentencing of fraudsters has long been considered one of the weaknesses in the response to fraud in England and Wales.[72] [73] It was subsequently raised by a number of the economic crime specialists which we interviewed for this report.[74] The Fraud Act 2006 enables sentences of up to 10 years for offences proscribed under it. However, few fraudsters are imprisoned for the maximum term.[75]

Further, given the scale of the fraud that is perpetrated against the UK and the magnitude of the financial, social and psychological harms, there is a strong case for reflecting this cumulative harm to individuals and society more explicitly in the sentencing of fraudsters. US and UK evidence shows that longer sentences tend to act as more of a deterrent against recidivism, whilst the incarceration effect is well known, i.e. fraudsters that are locked away cannot commit more frauds.[76] [77] The low numbers of arrests and prosecutions for fraud reinforce the case for longer sentences. While the likelihood of getting caught may be low, to help shift the risk-reward balance for fraudsters towards the former, those who are arrested and convicted of multiple fraud offences should expect a sentence commensurate with the accumulated harm that they have caused.

Recommendation Two: The UK government should boost the law enforcement response to economic crime and fraud, in particular

In order to achieve this, the UK government should:

- Fund the recruitment and training of 30,000 specialist police officers and other staff (e.g. forensic accountants, digital forensic experts) along with a concomitant uplift in the Crown Prosecution Service's (CPS) economic crime prosecution capacity
- Review and identify where criminal law could be bolstered and how the civil law and administrative powers might be enhanced, so they can be utilised more effectively against fraudsters
- Increase the maximum possible sentences for fraudsters and introduce minimum terms for those defrauding multiple victims

A robust domestic fraud control effort by law enforcement is an essential element of any effective "systems" response to the fraud threat. This requires prioritisation and investment in the capacity and capabilities of law enforcement, in order to be able to disrupt and pursue fraudsters sustainably and at scale, whether based in the UK or abroad.

The available evidence suggests that investigating fraud is a labour-intensive activity which requires skilled individuals and teams. Consequently, to have a positive strategic impact against fraud, law enforcement is going to require resourcing for new specialist personnel. This will require pay and other factors that bear on recruitment and retention to be overhauled to attract the kind of workforce that is needed. This applies to the prosecutorial authorities, too. If there is more success in pursuing fraudsters, the Crown Prosecution Service is also going to need

an uplift in specialist prosecutors and support staff to increase prosecutorial capacity and capabilities. These challenges should be reflected in a 10-year workforce strategy for the NCA, policing and the Crown Prosecution Service.

Using the cost of the recent Police Uplift programme as a guide, we estimate that an additional 30,000 specialist police officers and staff and concomitant increases in prosecutorial capacity will cost somewhere in the region of £28 billion over 10 years, or £2.8 billion per year.[78] With the short- to medium-term socio-economic cost of fraud against the UK estimated to be £5.4 billion a year, and the negative long-term societal impacts of high and persistent levels of fraud (see Box 3), this investment will more than pay for itself over time.[79]

To be maximally effective, law enforcement also needs the powers to disrupt and pursue fraudsters. Whilst the Fraud Act 2006 is a good piece of law, experts have suggested there could be a case for complementary fraud offences, with countries like the US offering a model for such additional crimes.[xxiii] However, as has been recognised more and more often in recent decades, the powers available to the authorities should not stop at criminal law. Civil powers have been given more prominence as a vector of attack against criminals.[xxiv] Therefore, to identify how the civil law and administrative rules could also be utilised more extensively against fraud, an expert review should be set up to identify reforms.[80]

Tackling the collective action problem that holds back effective counter-fraud action across the "fraud chain" in the UK

The collective action problem which is holding back organisations in the "fraud chain" from taking the needed steps to prevent and disrupt fraud can be significantly reduced by transforming the incentives such organisations face. The right policy framework can help ensure fraud risks are prioritised by "fraud chain" firms and that the benefits to individual organisations of taking action, outweigh the costs. Table 4 sets out two options.

[xxiii] In the UK for example, the absence of a specific offence of identity theft has long been considered a gap in the legal framework that could be closed.

[xxiv] Perhaps the most notable currently available civil powers are the forfeiture ones in the Proceeds of Crime Act 2002.

Table 2: Cost-sharing and a sanctions regime for ameliorating the collective action problem across the "fraud chain"

Proposed incentivisation measure	Description	Downsides
Fraud victim reimbursement cost-sharing mechanism	• Ensures all companies in the "fraud chain" bear some of the cost of the fraud that takes place across their services. • Firms subject to the sharing of liability, would be able to lower or eliminate their costs by taking steps which reduce the levels of fraud promulgated across their services.	• The complexity of setting up such a liability sharing system has been highlighted by critics.
Sanctions regime for companies that fail to take robust steps to prevent and disrupt fraud	• Makes sure that all organisations in the "fraud chain" pay a financial cost for the fraud being conducted across their services. • This approach has precedents in the Online Safety Act 2023 the failure to prevent fraud offence, and the Economic Crime Levy.[xxv] [xxvi] [xxvii] 81 82	• Critics point out the blunt nature of such an approach, as it is likely to be less directly linked to the specific number and value of incidents of fraud that take place through the services of "fraud chain" firms.

[xxv] The provisions of the Act do allow for the sanctioning of firms that fail to prevent paid-for fraudulent advertising on their platforms. Source: "Online Safety Act 2023" (King's Printer of Acts of Parliament), https://www.legislation.gov.uk/ukpga/2023/50/contents.

[xxvi] The Online safety Act places obligations on large digital platforms to tackle fraudulent advertising. Many fraud experts believe that the Online Safety Act does not go far enough. This is partly because it only covers the largest tech companies operating in the UK, and there is a risk that by only targeting these fraudsters will simply move to platforms not covered by the law. Furthermore, there are other ways platforms enable fraud to take place beyond allowing fraudulent advertising, such as the operation of slack user verification processes.

[xxvii] The failure to prevent fraud offence is the latest in a list of corporate offences such as the failure to prevent tax evasion and obligations to take steps to mitigate modern slavery in corporate supply chains. The former was introduced under the Criminal Finances Act 2017. Source: "Corporate Criminal Offences of Failure to Prevent the Facilitation of Tax Evasion," Pinsent Masons, January 8, 2024, https://www.pinsentmasons.com/out-law/guides/corporate-criminal-offences-of-failing-to-prevent-the-facilitation-of-tax-evasion-.

Recommendation Three: The government should ensure that there is an alignment in interests amongst the businesses that constitute the "fraud chain"

To achieve this, the government should:

- Place legal duties on the organisations in the "fraud chain" to ensure that they prioritise preventing and disrupting fraud and bear costs that reflect the scale of the frauds which are perpetrated across their services
- Require "fraud chain" firms and relevant parts of the public sector to participate in enhanced data and intelligence sharing arrangements and, under the oversight of the ECLG, encourage the development of an enhanced system with seed funding backed up by a "safe harbour" protection from legal liability risk, for those participating in such a scheme
- Overhaul the payments system rules, so that those payments and transfers with a greater fraud risk are subject to more frictions such as additional security checks

Solving the collective action problem which inhibits a more effective domestic response to fraud from the entities in the "fraud chain" would require those organisations to face stronger incentives that change the cost-benefit ratio around taking robust and extensive action . We propose that this could be achieved through a combination of legal duties to deal with fraud, building on precedents such as those in the Online Safety Act, arrangements which ensure "fraud chain" organisations bear some of the cost of volume fraud (Table 2) and steps to reduce technical obstacles to measures such as data and intelligence sharing.

To deliver on this, the proposed ECLG (see Recommendation One) should seize on the direction set by the Economic Crime Plan 2, for a better public-private data sharing dispensation.[83] It should task key stakeholders such as the National Economic Crime Centre (NECC) and the Information Commissioners Office (ICO) with bringing together the technology, finance and telecoms sectors, law enforcement and relevant regulators, to ensure an effective regime is put in place.[xxviii] This should be supported by

[xxviii] There are a number of data sharing arrangements currently operating but they are, for example, limited in their scope and disjointed. These include CIFAS's National Fraud Database, UK Finance's Information and Intelligence Unit, the NECC's Joint Money Laundering Intelligence Taskforce and the UK Financial Intelligence Unit. Notably, the NCA is currently trialling enhanced data sharing schemes with a number of banks. The experiences of and lessons from those existing systems needs to be brought together under the joint auspices of the NECC and ICO and used as a platform on which to pursue the development of the enhanced data and intelligence sharing regime that is needed in the UK. Sources: "Annual Fraud Report 2024," UK Finance, https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2024.; "National Economic Crime Centre," https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-

providing some start-up funding to enable a pilot data sharing project to be developed. Further, to make sure that legal risks do not stand in the way, participants are likely to require an exception from data rules.[84]

The new framework should encourage measures which add some additional frictions into the payments system to help squeeze out more fraud from this area of high vulnerability. For example, high value payments, payments made by personal customers to new payees and payments to recipients in high-risk countries should be subject to delays and extra assurance measures, to give banks and other payment operators the necessary time to determine the fraud risk and take preventative action where appropriate.

The government should expand initiatives that increase public awareness about fraud risks

The ability of fraudsters to target and manipulate particular interests, personality traits, preferences and personal, social and economic vulnerabilities, as we noted in Chapter One, means that consumer behaviour is also a factor in explaining the high prevalence of digital fraud. Consequently, as research evidence suggests, there is likely to be some benefit in ensuring that consumers have a degree of awareness of how high the fraud risk is, the methods which fraudsters are using to target people in the UK, and the kinds of defensive actions that can be taken to minimise their chances of becoming victims.[85]

As the last line of defence against fraud, it is imperative that consumers are well equipped to recognise when they are at risk of being defrauded and what to do when they have been victimised. To that end, in February 2024, the UK government launched the "Stop! Think Fraud" campaign, targeted towards adults and designed to advise individuals on how to spot the signs of fraudulent behaviour.[86] [xxix]

centre. and "Focus: UK Banks to Ramp up Data Sharing in Dirty Money Crackdown | Reuters," https://www.reuters.com/business/finance/uk-banks-ramp-up-data-sharing-dirty-money-crackdown-2023-06-22/.

[xxix] There are also other schemes such as the 159 initiative run by Stop Scams UK (it encourages individuals to call 159, when they believe someone is trying to trick them into transferring money, in order to be connected directly to their bank) and Take Five operated by the banking sector. Sources: "159," Stop Scams UK, https://stopscamsuk.org.uk/159. and "Take Five - To Stop Fraud | Take Five Is a National Campaign Offering Straightforward and Impartial Advice to Help Everyone Protect Themselves against Fraud.," Take Five to Stop Fraud, https://www.takefive-stopfraud.org.uk/.

Recommendation Four: The government should ensure that the new "Stop!! Think Fraud" public awareness campaign has long-term funding to enable it to continue for the next five years

The record of the impact of public information campaigns on behaviour change amongst the public is decidedly mixed. However, analysis suggests that there are four key ingredients to the more successful awareness and behaviour change campaigns. These are:[87]

- Taking a long-term strategic approach to the campaign
- Having a clear understanding of the target audience for the campaign and what the appropriate channels are for reaching them
- Undertaking evaluations of a campaign's impact and learning from the findings
- Fostering strong relationships between all those involved in the design, development and implementation of the campaign

Only with long-term funding can the "Stop! Think Fraud" campaign succeed in embedding its message in the population's consciousness and bringing about sustained changes in the "fraud hygiene" behaviours of people. With the security of such resourcing the Home Office can ensure the campaign is built around all the elements of best campaign practice described above.

CHAPTER SEVEN – AN EFFECTIVE COUNTER-FRAUD EFFORT REQUIRES A HIGH QUALITY DOMESTIC FRAUD RESPONSE TO UNDERPIN INTERNATIONAL COOPERATION

UK fraud policy needs to recognise the interdependency between all countries over fraud

A common problem such as fraud should generate a mutual interest amongst governments

The high proportion of volume fraud with a cross-border element – with many states being both "importers" and "exporters" of fraud – creates an unavoidable interdependency between countries over fraud. This international dimension adds a further level of complexity for those tasked with preventing and disrupting fraud and pursuing fraudsters. For example, it is not uncommon for a single fraud to have connections to many different jurisdictions. The scammers might be based in one country, much of the digital infrastructure used to commit it in a second, an enabler providing "crime as a service" support based in a third, the organised crime gang "kingpin" ultimately running the scams in a fourth country, the victims in a fifth and the illicit gains laundered through a sixth country.

For law enforcement the result of this complicated tapestry of legal jurisdictions, geographical dispersion and political, economic, cultural and linguistic variation is that pursuing fraudsters is a much more difficult task, requiring more resources per case than those which take place within a single country. One economic crime specialist who participated in our interviews for this research, succinctly explained that in order to deal with this problem, a concerted international effort is needed:[88]

> *"For the police to effectively fight online fraud, you're going to need effective international cooperation because you can't use jurisdictional policing to police something that doesn't have a jurisdiction".*

Extensive cooperation has not developed because of a global collective action problem

Building up an international response to fraud involves dealing with a number of obstacles

Despite the imperative for international cooperation, to date, there has been too little, as an expert interviewee observed:[xxx]

[xxx] The lack of impetus at the international level is evident in a number of ways. For example there has been a failure to develop a programme of MLAT modernisation is symptomatic of this inaction. Equally, since at Since at least 2010, it has been widely recognised for example, that the UN Palermo Convention is in need of revision to keep up with developments in organised crime, but, as of yet, no significant effort has been made to instigate one. Sources: Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age | Harvard National Security Journal," https://harvardnsj.org/2015/01/28/problematic-alternatives-mlat-reform-for-the-digital-age/. and "The Global Regime for Transnational Crime | Council on Foreign Relations," https://www.cfr.org/report/global-regime-transnational-crime.

> *"...it's the interdependency between different countries ... it would make sense to address it internationally ... [yet] ... despite the fact that the problem has been there for many years, there is little which has been actually done, to get more coordinated..."*

Another economic crime specialist who participated in our interviews pointed out that the lack of international action on fraud put it somewhat at odds with other crimes that have a significant intentional dimension:

> *"...money laundering, bribery, corruption, terrorism, non-proliferation, but nothing on fraud anywhere. So you've got a gap ... in terms of the normal model of regulating financial crime at an international, regional and domestic level".*

The cost of cross-border cooperation currently outweighs the benefits in too many instances

The collective action problem that hinders international cooperation over fraud is caused by a number of factors. These include the multiplicity of actors and interests, competing priorities, the numerous potential domains of action (see Diagram 6) and the consequent size of the investments in people, equipment, organisations and processes required for sustained and strategically effective collaboration, in the context of resource constraints.[xxxi] For instance, as was observed by one contributor to our interview series, the most effective anti-fraud effort will require the involvement of all countries, i.e. more than 190 states:[xxxii]:

> *"International cooperation only works if everybody cooperates, otherwise your problem stays in countries that are outside the cooperation ... that's an issue".*

The confluence of limited resourcing, competing priorities and the time, financial and administrative burdens of cross-border cooperation for law enforcement agencies, regulators and "fraud chain" organisations mean that the negative impacts that are caused by most individual frauds (or indeed clusters of frauds) rarely reach the threshold for instigating an international law enforcement effort. This was noted by several experts we engaged with for this report, with two in particular making the point that:

> *"There's a question of scale ... for victims something like £5,000 is a significant loss. But for the criminal justice system, it wouldn't trigger an international policing effort, that's the problem".*

[xxxi] It should be noted that cross-border enforcement networks and a range of regional and international entities do exist to try and facilitate cross-border cooperation on law enforcement and regulation. Nevertheless, their development lags far behind that of the criminals they are trying to pursue. Source: Tim Legrand and Christian Leuprecht, "Securing Cross-Border Collaboration: Transgovernmental Enforcement Networks, Organized Crime and Illicit International Political Economy," *Policy and Society* 40, no. 4 (2021): 565–86, https://doi.org/10.1080/14494035.2021.1975216.

[xxxii] The United Nations has 193 member countries. Source: "What Is the United Nations and What Does It Do?," *BBC News*, September 23, 2019, sec. World, https://www.bbc.com/news/world-49796807.

"...it is too costly to undertake cross-border policing and so, it tends to only happen where the stakes are very high..."

The virtuous circle of an improved domestic response to fraud and an effective contribution to the international counter-fraud effort

Effective domestic counter-fraud regimes provide a base for more international cooperation

A recurring theme in a number of the interviews we undertook for this research, was the implication that overcoming the challenges of international cooperation would be helped by countries putting in place effective domestic arrangements first. Building the necessary state capacity and capability at the national level creates a strong foundation for countries to collaborate across borders to better deal with the interdependency problem (Diagram 5).

Diagram 5: The dynamics of the interconnection between the efficacy of the domestic response to fraud and the international counter-fraud effort

Source: Expert interviews

Better national counter-fraud responses are unlikely to be enough

Higher quality domestic regimes would ameliorate some of the obstacles to more effective cross-border responses, because there would be greater prioritisation of and more capacity and capabilities to engage in collaboration. This would ease some of the constraints which currently contribute to the international collective action failure. Nevertheless, politicians and policymakers could not rely solely on improved domestic responses to deliver the kind of global response that is needed to deal with the scale and depth of the interconnectedness problem. Specific measures aimed at forging more coordination and facilitating more intensive and extensive global cooperation would be required.

Further, what also emerged from our qualitative research, was the view that appropriate international arrangements could encourage countries to put in place those domestic measures, which would in turn enable them to make an effective contribution to a mutually beneficial global effort against fraud. In other words, agreements at the global level could help governments tackle some of the collective action failures that hold back domestic responses in different countries and in turn,

help put in place effective counter-fraud regimes where they may not otherwise have been implemented. Consequently, there is a mutual dependence between counter-fraud action at both the domestic and international level, which the right international framework for facilitating cooperation could help nurture.

CHAPTER EIGHT – THE KEY COMPONENTS OF AN EFFECTIVE INTERNATIONAL COUNTER-FRAUD EFFORT

Building an international consensus about the importance of fraud

The starting points for overcoming the international collective action problem have to be, first, countries recognising the importance of tackling fraud and second, seeing the mutual benefit to be gained from enhanced collaboration. One of the experts spoken to for this research succinctly described the process which needs to take place:

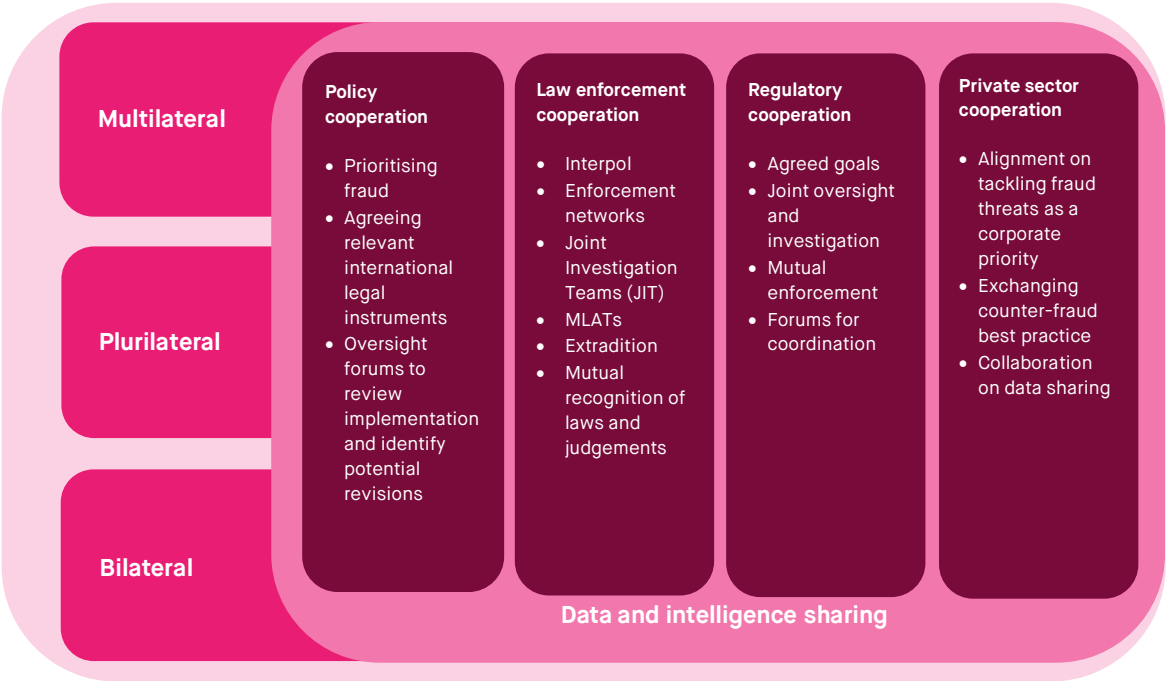
> *"States have to take fraud much more seriously and develop an agreed programme around dealing with it..."*

The UK government's recent international fraud summit, along with the work already being done by Interpol and the UN Office for Drugs and Crime (UNODC), provide foundations upon which a coherent and sustainable multinational coalition against fraud could be built.[89]

International action on fraud needs to take place across a number of domains

Diagram 6 outlines the variety of domains across which countries such as the UK need to cooperate, for there to be an effective cross-border response to transnational fraud.

Diagram 6: The dimensions of international counter-fraud cooperation



Source: Expert interviews and SMF analysis

A global fraud convention is needed to encourage and organise cross-border cooperation

To organise and facilitate collaboration across all the domains outlined in Diagram 6, robust commitments to act, clear timelines and implementation along with oversight mechanisms and reductions in the structural disincentives to cross-border cooperative activity are needed. To deliver these, a new multilateral framework is likely to be required. According to many of our interviewees, that framework should primarily take the form of a new fraud convention:

> *"Give fraud the same international standing as money laundering, terrorism, other types of financial crime, and I think that's what's missing … for money laundering we have the Vienna Convention, Palermo Convention for organized crime and the convention against corruption…"*

A convention would formally commit governments, and by extension relevant agencies operating under the auspices of the signatory states, to prioritise fraud and facilitate concerted action across the full range of areas outlined in Diagram 6. Chapter Five showed that there are counter-fraud policy measures which command considerable public support in the 15 countries surveyed for this research, which could provide a basis on which to move forward with developing the content of a convention.

Recommendation Five: The UK government should push for the creation of a comprehensive international convention on fraud

This international convention would ensure that countries:

- Commit to prioritising and investing more resources into tackling fraud, with a significant emphasis on cross-border law enforcement and regulator cooperation.
- Take actions to reduce the current disincentives to cross-border law enforcement cooperation.
- Agree to implement measures that will incentivise the organisations in the "fraud chain" of the signatory countries to take the necessary steps to better prevent and disrupt the fraud being perpetrated over their services.

The most effective convention would cover all four domains for international action at all three levels (Diagram 6). To do this, the convention would need to commit signatory states to implementing measures which:

- Place obligations on "fraud chain" organisations in each participating country to take steps to prevent and disrupt the fraud taking place through their services.
- Make sure the fraud laws in each jurisdiction are "fit for purpose", including taking steps to modernise key enabling laws such as

MLATs, in order to help reduce the bureaucratic barriers to cross-border cooperation against fraudsters.[xxxiii]

- Require domestic law enforcement and relevant regulatory agencies to prioritise fraud and invest in counter-fraud capacity and capabilities commensurate to the scale of the problem.
- Commit the law enforcement and (appropriate) regulatory agencies of each state that has signed-up, to deepen bilateral collaboration efforts, strengthen plurilateral cross-border cooperation networks and strengthen their involvement with multilateral fora such as Interpol.
- Any convention would be one more element in a growing body of international arrangements (treaties and institutions) that are aimed at helping to tackle a range of transnational crime. As such, the fraud convention should be crafted with the wider landscape in mind and designed to fit alongside existing agreements on areas of criminality with a significant international dimension that are closely associated with fraud (e.g. transnational organised crime, money laundering and cybercrime) and bolster existing relevant international bodies such as Interpol.

The UN is the best forum for building an international framework for overcoming the collective action problem

A UN convention would encompass most countries and is likely to result in a high degree of compliance

As noted in Chapter Seven, given the distribution of victims and perpetrators of fraud around the world (also see Table 6 in Annex 4), in order to be effective, a global anti-fraud effort would need to encompass all nations. Further, it will necessarily have to be a treaty that all signatories implement and continue to adhere to. As result of these imperatives, it has to be developed through a forum which all parties see as legitimate and reasonably capable. Therefore, as one expert we spoke with argued, the UN provides the most obvious forum for such a treaty:

> *"We expect members of the UN to implement and ratify the conventions and then to include key parts within their domestic legal frameworks".*

In addition, another benefit of the UN acting as the sponsoring institution for the development of such an instrument, is that it is the home of other treaties on crimes with a significant international dimension, which have a significant degree of synergy with fraud. Consequently, agreeing the treaty through the UN would make it easier to ensure the fraud convention is fully complementary to these other legal instruments. Further, the ultimate aspiration might be the creation of a coherent body of

[xxxiii] MLATs can be slow, and they have been criticised for not keeping up with the demands of modern law enforcement and the complexity of a lot of modern crime. Source: Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age | Harvard National Security Journal," https://harvardnsj.org/2015/01/28/problematic-alternatives-mlat-reform-for-the-digital-age/.

international anti-crime agreements that are mutually supportive and maximise the scope for cross-border law enforcement and regulatory cooperation.

Interpol and the UNODC have the capabilities to help build a wider ecosystem of support for a fraud convention

Another expert we interviewed argued that to be maximally effective, an UN convention will need to be supported by a constellation of supporting bodies that will help facilitate its successful implementation by countries (and their respective relevant agencies):

> *"There needs to be a mix of organisations ... you need to bolster what Interpol's doing ... and then you probably need a body to deal with some of the other activities, which don't fall under Interpol and UNODC ... such as help in the coordination of developing networks, sharing intelligence, those types of things".*

A second expert highlighted the particular importance of such an ecosystem in encouraging the development and densification of cross-border policy and enforcement networks, which could help deepen collaboration and the sharing of best practice, which are essential for making international cooperation against fraud effective:

> *"The ability to share the sorts of things that different states are doing is valuable, because there are initiatives in other jurisdictions that other countries can learn from".*

It was suggested by the same interviewee that the Financial Action Task Force (FATF) model might be copied, as the latter is a positive aspect of the international cooperation around money laundering:

> *"...of all the international bodies, it's probably the most effective in terms of the reach and the impact that's had on anti-money laundering policy and practice".*

FATF, for example, monitors the implementation of agreed anti-money laundering measures by states and ensures good practice is spread amongst participating countries. In contrast, there have been a number of concerns raised about the weak monitoring of implementation of the UN Convention against Transnational Organised Crime (UNTOC).[90] Any convention on fraud aiming to be effective would likely need to embed a strong system for ensuring implementation.

Support for fraud control capacity and capability building in poorer countries is essential for an effective international counter-fraud regime

Many of the states whose participation in any such convention would be essential lack sufficient domestic crime control capacity and regulatory capabilities to mount the kind of robust and sustained response to fraud that is needed, even where there is the will to do so. As more than one expert we spoke with for this research pointed out, some nations:[91]

> *"...don't have the capacity, internally ... we could all have the blueprint across the world, but it's the supervision and the regulation, which is hard, and the delivery of that".*

> *"We know law enforcement agencies in North Africa and West Africa, and wherever else ... their police officers are good ... the sad thing is though ... they don't have the tools, our tools cost tens of thousands of pounds..."*

Therefore, alongside commitments from developed countries to boost their own counter-fraud capabilities, pledges to increase the levels of assistance for poorer signatory states to do the same would need to be embedded in the new international counter-fraud architecture,. Over time, such investment would enable less developed countries to make increasingly effective contributions to the international effort against cross-border volume fraud.

Recommendation Six: The UK government should increase its support for bolstering the anti-fraud law enforcement and regulatory capacity and capabilities in low and middle-income countries

A country's domestic counter-fraud capacity and capabilities would help determine how usefully they could contribute to any international effort against fraudsters. In order to help developing countries overcome the deficits they have in these areas, more developed countries such as the UK (while acknowledging the paucity of the UK's anti-fraud response) should provide support for building up capabilities and capacity.

To ensure this happens, assistance should be reflected in the convention. The only way this could be done is through setting out a set of minimum anti-economic crime capability principles that developed countries would help developing countries achieve. Specifically, the UK should look to help through:

- The provision of training for investigators, prosecutors and regulators in developing countries.
- Seconding more UK law enforcement officers and regulators to the equivalent agencies in developing countries.
- Expanding the use of JITs.
- Subsidising the acquisition of the tools needed to investigate and prosecute fraud more effectively, either through direct donations of equipment, or matched funding schemes.

ANNEX 1: TOTAL NUMBER OF FRAUD VICTIMS IN 15 SURVEYED COUNTRIES

Table 3: Sample sizes in each of the countries surveyed

Country	Sample size (adults)
Argentina	2,045
Australia	2,102
Brazil	2,017
Canada	2,108
France	2,044
Germany	2,014
Italy	2,101
Japan	2,002
Mexico	2,104
New Zealand	1,007
Portugal	2,117
Singapore	1,053
Spain	2,069
UK	2,011
United States	2,107

Source: Focal Data survey

ANNEX 2: TOTAL NUMBER OF FRUD VICTIMS IN 15 SURVEYED COUNTRIES

Table 4: Total number of fraud victims in each of the 15 countries, 2021 - 2023

Country	Total victims
United States	83 million
Brazil	43 million
Mexico	24 million
France	12 million
Germany	10 million
UK	10 million
Argentina	8 million
Canada	8 million
Japan	8 million
Spain	8 million
Australia	6 million
Italy	6 million
Portugal	2 million
New Zealand	1 million
Singapore	1 million

Source: Focal Data survey, World Bank and SMF calculations

N.B. All numbers are rounded to the nearest million.

ANNEX 3: THE COMPONENT PARTS OF THE "FRAUD THREAT PREVALENCE INDEX"

This index uses results from the 15 country survey. Specifically, it utilises the answers to the questions in the questionnaire about:

- Victimisation.
- Instances of repeat victimisation.
- The average cost to the victims of the only or most recent fraud suffered in each country.
- Attempted frauds.

To reflect the relative importance of actual victimhood over attempted frauds, the overall score for each country weights the attempted fraud scores at 50% of the scores for instances of victimhood. Further, the direct financial loss score reflects the percentage of the average direct financial loss for each country relative to the country with the highest average direct financial loss per fraud (which is Singapore in our survey). Finally, the overall score is a simple sum of the various component scores.

The country breakdowns and overall scores are set out in Table 5 below.

Table 5: The country scores for each component of the "Fraud Threat Prevalence Index"

	Victim once	Victim twice	Victim three or more times	Attempted fraud	Two attempted frauds	Three or more attempted frauds	Direct average loss relative to the highest	Overall score
				Weighted at 50%				
Argentina	0.24	0.29	0.11	0.47	0.31	0.39	0.2	**1.42**
Australia	0.3	0.27	0.15	0.39	0.21	0.42	0.78	**2.01**
Brazil	0.26	0.29	0.2	0.46	0.26	0.47	0.78	**2.12**
Canada	0.24	0.25	0.17	0.39	0.22	0.46	0.58	**1.77**
France	0.22	0.22	0.14	0.31	0.21	0.44	0.58	**1.64**
Germany	0.15	0.23	0.12	0.33	0.24	0.38	0.58	**1.56**
Italy	0.13	0.16	0.11	0.33	0.27	0.37	0.46	**1.35**
Japan	0.08	0.17	0.16	0.13	0.17	0.25	0.61	**1.38**
Mexico	0.27	0.3	0.17	0.45	0.30	0.37	0.4	**1.70**
New Zealand	0.25	0.26	0.18	0.39	0.24	0.45	0.44	**1.67**
Portugal	0.16	0.21	0.11	0.37	0.23	0.46	0.47	**1.48**
Singapore	0.23	0.24	0.28	0.42	0.26	0.46	1.0	**2.32**
Spain	0.2	0.23	0.1	0.36	0.23	0.46	0.44	**1.50**
UK	0.18	0.22	0.11	0.3	0.23	0.32	0.43	**1.36**
United States	0.31	0.3	0.2	0.35	0.29	0.30	0.54	**1.82**

Source: Focal Data Survey; SMF methodology

ANNEX 4: INTERNATIONAL DISTRIBUTION OF FRAUD

Table 6: Predominance of fraud types in different regions of the world

Fraudsters	Victims	Fraud Type	Prevalence
Africa	Africa	• Romance fraud	High
		• Push payment fraud	Moderate
	Europe	• Investment fraud	Minor
The Americas	Africa	• Push payment fraud	Minor
	Americas	• Push payment fraud	Moderate
		• Investment fraud	Moderate
	Asia	• Business email compromise	Moderate
	Europe	• Business email compromise	Minor
Asia	Africa	• Push payment fraud	High
	Americas	• Business email compromise	Minor
	Asia	• Impersonation fraud	High
		• Romance fraud	Moderate
		• Identify fraud	Moderate
	Europe	• Investment fraud	High
		• Business email compromise	Moderate
Europe	Africa	• Push payment fraud	Moderate
		• Business email compromise	Minor
	Asia	• Business email compromise	Minor
	Europe	• Business email compromise	High
		• Investment fraud	High

Source: Interpol (2024)

ANNEX 5: THE WIDER NEGATIVE IMPACTS OF FRAUD ACROSS 15 COUNTRIES

Table 7 outlines the numbers of people in each country surveyed that suffered from at least one wider negative impact due to the only, or most recent fraud they experienced, over the period 2021 to 2023.

Table 7: Fraud victims suffering wider negative impacts as a result of their only or most recent fraud, 2021 - 2023

Country	Number of fraud victims experiencing at least one wider cost	Most frequently highlighted wider negative costs
United States	75 million	• Less trusting of others – 40% • Short/long-term financial disruption – 31% • Negative emotional impacts – 29%
Brazil	41 million	• Less trusting of others – 35% • Negative emotional impacts – 23% • Short/long-term financial disruption – 18%
Mexico	23 million	• Less trusting of others – 39% • Negative emotional impacts – 35% • Short/long-term financial disruption – 34%
France	10 million	• Less trusting of others – 35% • Negative emotional impacts – 26% • Inconvenience – 21%
Germany	9 million	• Less trusting of others – 37% • Negative emotional impacts – 30% • Short/long-term financial disruption – 26%
UK	8 million	• Less trusting of others – 41% • Negative emotional impacts – 33% • Short/long-term financial disruption – 18%
Argentina	8 million	• Less trusting of others – 33% • Negative emotional impacts – 29% • Short/long-term financial disruption – 27%
Canada	7 million	• Less trusting of others – 44% • Short/long-term financial disruption – 36% • Inconvenience – 35%
Spain	7 million	• Less trusting of others – 47% • Short/long-term financial disruption – 41% • Negative emotional impacts – 36%

		• Inconvenience – 36%
Japan	6 million	• Less trusting of others – 44% • Short/long-term financial disruption –40% • Inconvenience – 39%
Australia	6 million	• Less trusting of others – 41% • Short/long-term financial disruption – 40% • Inconvenience – 34%
Italy	5 million	• Negative emotional impacts – 32% • Less trusting of others – 28% • Short/long-term financial disruption – 23%
Portugal	1 million	• Less trusting of others – 35% • Negative emotional impacts – 26% • Short/long-term financial disruption – 21%
Singapore	1 million	• Less trusting of others – 47% • Negative emotional impacts – 30% • Inconvenience – 17%
New Zealand	1 million	• Less trusting of others – 44% • Short/long-term financial disruption – 34% • Negative emotional impacts – 27%

Source: Focal Data survey and SMF calculations

ENDNOTES

[1] Jim Gee and Mark Button, *The Financial Cost of Fraud 2019: The Latest Data from Around the World* (Crowe UK, 2019).

[2] "The Reasoning Criminal : Rational Choice Perspectives on Offending : Free Download, Borrow, and Streaming : Internet Archive," https://archive.org/details/reasoningcrimina0000unse.

[3] Kyle J. Thomas, Thomas A. Loughran, and Benjamin C. Hamilton, "Perceived Arrest Risk, Psychic Rewards, and Offense Specialization: A Partial Test of Rational Choice Theory," *Criminology* 58, no. 3 (2020): 485–509, https://doi.org/10.1111/1745-9125.12243.

[4] "Understanding the Psychology of a Fraudster | Crowe UK," Crowe, , https://www.crowe.com/uk/insights/understanding-the-psychology-of-a-fraudster.

[5] Mark Button, Branislav Hock, and David Shepherd, *Economic Crime: From Conception to Response* (London: Routledge, 2022), https://doi.org/10.4324/9781003081753.

[6] Jay S. Albanese, "Organized Crime as Financial Crime: The Nature of Organized Crime as Reflected in Prosecutions and Research," *Victims & Offenders* 16, no. 3 (April 3, 2021): 431–43, https://doi.org/10.1080/15564886.2020.1823543.

[7] Button, Hock, and Shepherd, *Economic Crime*.

[8] "Internet Organised Crime Threat Assessment (IOCTA) 2017," Europol, https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2017.

[9] "Annual Report 2017," Interpol, "Documents," https://www.interpol.int/en/Resources/Documents.

[10] "Trafficking into Forced Criminality: The Rise of Scam Centres in Southeast Asia," https://rusi.orghttps://rusi.org.

[11] "House of Lords - Fighting Fraud: Breaking the Chain - Fraud Act 2006 and Digital Fraud Committee," https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/8702.htm.

[12] "Crypto Investment Scams," FCA, March 7, 2023, https://www.fca.org.uk/consumers/crypto-investment-scams.

[13] Button, Hock, and Shepherd, *Economic Crime*.

[14] "The Psychology of Internet Fraud Victimisation: A Systematic Review | Journal of Police and Criminal Psychology," https://link.springer.com/article/10.1007/s11896-019-09334-5.

[15] "Risk Factors for Fraud Victimization: The Role of Socio-Demographics, Personality, Mental, General, and Cognitive Health, Activities, and Fraud Knowledge," , https://doi.org/10.1177/02697580231215839.

[16] Joanna Curtis and Gavin Oxburgh, "Understanding Cybercrime in 'Real World' Policing and Law Enforcement," *The Police Journal* 96, no. 4 (December 1, 2023): 573–92, https://doi.org/10.1177/0032258X221107584.

[17] "The Psychology of Internet Fraud Victimisation: A Systematic Review | Journal of Police and Criminal Psychology."

[18] Emily A. Mueller et al., "Older and Wiser: Age Differences in Susceptibility to Investment Fraud: The Protective Role of Emotional Intelligence," *Journal of Elder Abuse & Neglect* 32, no. 2 (March 14, 2020): 152–72, https://doi.org/10.1080/08946566.2020.1736704.

[19] "Mass-Market Consumer Fraud in the United States: A 2017 Update," Federal Trade Commission, October 31, 2019, https://www.ftc.gov/reports/mass-market-consumer-fraud-united-states-2017-update.

[20] Hongliang Chen, Christopher E. Beaudoin, and Traci Hong, "Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors," *Computers in Human Behavior* 70 (May 1, 2017): 291–302, https://doi.org/10.1016/j.chb.2017.01.003.

[21] European Central Bank, "Seventh Report on Card Fraud," no. 2021 (October 29, 2021), https://www.ecb.europa.eu/press/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html.

[22] CapX Contributor, "The AI Fraudsters Are Coming – We Need to Act Now," CapX, October 30, 2023, https://capx.co/the-ai-fraudsters-are-coming-we-need-to-act-now/.

[23] Federal Bureau of Investigation, "Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations," March 10, 2021, https://www.ic3.gov/Media/News/2021/210310-2.pdf.

[24] "House of Lords - Fighting Fraud: Breaking the Chain - Fraud Act 2006 and Digital Fraud Committee," https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/8702.htm.

[25] "Hiding behind the Veil of Action Fraud: The Police Response to Economic Crime in England and Wales and Evaluating the Case for Regionalization or a National Economic Crime Agency | Policing: A Journal of Policy and Practice | Oxford Academic," , https://academic.oup.com/policing/article/15/3/1758/6273115.

[26] "State of Policing: The Annual Assessment of Policing in England and Wales 2021," His Majesty's Inspectorate of Constabulary and Fire & Rescue Services, https://hmicfrs.justiceinspectorates.gov.uk/publication-html/state-of-policing-in-england-and-wales-2021/.

[27] "Fraud Strategy," GOV.UK, June 1, 2023, https://www.gov.uk/government/publications/fraud-strategy.

[28] "Labour Party Manifesto 2024: Our Plan to Change Britain," The Labour Party, June 13, 2024, https://labour.org.uk/updates/stories/labour-manifesto-2024-sign-up/.

[29] "Crime in England and Wales - Office for National Statistics," , https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/latest#fraud.

[30] "Comparison of Banking Providers' Fraud Controls," FCA, March 6, 2020, https://www.fca.org.uk/data/banks-fraud-controls-comparison.

[31] "Reducing and Preventing Financial Crime," FCA, February 2, 2024, https://www.fca.org.uk/publications/corporate-documents/reducing-and-preventing-financial-crime.

[32] "Crime in England and Wales - Office for National Statistics."

[33] "Organised Crime Groups Involved in Fraud | SpringerLink," https://link.springer.com/book/10.1007/978-3-319-69401-6.

[34] "Organized Fraud and Organizing Frauds: Unpacking Research on Networks and Organization - Michael Levi, 2008," https://journals.sagepub.com/doi/10.1177/1748895808096470.

[35] Mark Button, Branislav Hock and David Shepherd. Economic Crime: From Conception to response. 2022.

[36] Mark Button, Branislav Hock, and David Shepherd, *Economic Crime: From Conception to Response* (London: Routledge, 2022), https://doi.org/10.4324/9781003081753.

[37] Chidubem Izuakor, "Cyberfraud: A Review of the Internet and Anonymity in the Nigerian Context," March 1, 2021.

[38] Trong Van Nguyen, "The Modus Operandi of Transnational Computer Fraud: A Crime Script Analysis in Vietnam," *Trends in Organized Crime* 25, no. 2 (June 1, 2022): 226–47, https://doi.org/10.1007/s12117-021-09422-1.

[39] "Social Media: What Countries Use It Most & What Are They Using?," Digital Marketing Institute, https://digitalmarketinginstitute.com/blog/social-media-what-countries-use-it-most-and-what-are-they-using.

[40] "It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud," https://ieeexplore.ieee.org/document/7310826.

[41] "Evaluation Report on Grip and Bespoke-Funded Hot Spot Policing," GOV.UK, , https://www.gov.uk/government/publications/hot-spot-policing-in-england-and-wales-year-ending-march-2022/evaluation-report-on-grip-and-bespoke-funded-hot-spot-policing.

[42] "Fraudulent Times: Identifying a Consensus for an Agenda to Beat Fraud," Social Market Foundation., https://www.smf.co.uk/publications/a-consensus-to-beat-fraud/.

[43] Professor Nic Ryder, "Written Evidence Submitted by Professor Nic Ryder (Cardiff University)," n.d.

[44] "Dark Triad: Organized Crime, Terror and Fraud | Office of Justice Programs," https://www.ojp.gov/ncjrs/virtual-library/abstracts/dark-triad-organized-crime-terror-and-fraud.

[45] "Does Crime Affect Economic Growth? - Detotto - 2010 - Kyklos - Wiley Online Library," https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-6435.2010.00477.x.

[46] Kyriakos C. Neanidis, Maria Paola Rana, and Keith Blackburn, "An Empirical Analysis of Organized Crime, Corruption and Economic Growth," *Annals of Finance* 13, no. 3 (August 1, 2017): 273–98, https://doi.org/10.1007/s10436-017-0299-7.

[47] "Does More Crime Mean Fewer Jobs and Less Economic Growth? | European Journal of Law and Economics," https://link.springer.com/article/10.1007/s10657-012-9334-3.

[48] "Fraudemic: Adding to the Evidence Base on the Scale and Impact of Fraud on the UK," Social Market Foundation., https://www.smf.co.uk/publications/impact-of-fraud-on-the-uk/.

[49] "Financial Fraud in Developing Countries: Common Scam Detection Tips Do Not Help Distinguish Scam from Non-Scam Messages," CEPR, November 8, 2023, https://cepr.org/voxeu/columns/financial-fraud-developing-countries-common-scam-detection-tips-do-not-help.

[50] Gady Jacoby et al., "The Effect of Fraud Experience on Investment Behaviour," *Emerging Markets Review* 55 (June 1, 2023): 101007, https://doi.org/10.1016/j.ememar.2023.101007.

[51] "Fraudscape: The Size of the Fraud Problem around the World," Social Market Foundation., https://www.smf.co.uk/publications/fraudscape-international-fraud/.

[52] "Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up," Social Market Foundation., https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/.

[53] "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," Social Market Foundation., https://www.smf.co.uk/publications/fraud-view-from-the-ground/.

[54] "House of Lords - Fighting Fraud: Breaking the Chain - Fraud Act 2006 and Digital Fraud Committee," https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/8702.htm.

[55] Tim Stacey Asiedu Billy Barham, Bethany Marson, Hilda, "Sharing Data to Tackle Fraud - Which? Policy and Insight," Which?, https://www.which.co.uk/policy-and-insight/article/sharing-data-to-tackle-fraud-asPdg6M5DtVC.

[56] "Data Sharing for Counter Fraud Activities," Institute for Government, January 11, 2023, https://www.instituteforgovernment.org.uk/publication/data-sharing-counter-fraud-activities.

[57] Asiedu, "Sharing Data to Tackle Fraud - Which?"

[58] "What Is GDPR, the EU's New Data Protection Law?," GDPR.eu, November 7, 2018, https://gdpr.eu/what-is-gdpr/.

[59] Asiedu, "Sharing Data to Tackle Fraud - Which?"

[60] "Anti-Scam Centre And UOB Bank Used Technology In Joint Operation To Prevent Potential Losses Of Over $5.19 Million From More Than 900 Victims," Singapore Police Force, http://www.police.gov.sg/Media-Room/News/20230619_anti_scam_centre_and_uob_bank_used_tech_in_joint_op_to_prevent_potential_losses.

[61] "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," Social Market Foundation., https://www.smf.co.uk/publications/fraud-view-from-the-ground/.

[62] "Crypto Investment Scams," FCA, March 7, 2023, https://www.fca.org.uk/consumers/crypto-investment-scams.

[63] Chainalysis Team, "2024 Crypto Money Laundering Report," *Chainalysis* (blog), February 15, 2024, https://www.chainalysis.com/blog/2024-crypto-money-laundering/.

[64] "Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up," Social Market Foundation., https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/.

[65] "Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up."

[66] "Simon Fell Appointed as New Anti-Fraud Champion," GOV.UK, https://www.gov.uk/government/news/simon-fell-appointed-as-new-anti-fraud-champion.

[67] "Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up," Social Market Foundation., https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/.

[68] "Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up," Social Market Foundation., https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/.

[69] "Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up," Social Market Foundation., https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/.

[70] "Fraud Strategy."

[71] "Fraud Is Now Britain's Dominant Crime, but Policing Has Failed to Keep Up," Social Market Foundation., https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/.

[72] Mark Button, Branislav Hock, and David Shepherd, *Economic Crime: From Conception to Response* (London: Routledge, 2022), https://doi.org/10.4324/9781003081753.

[73] Michael Levi, "Hitting the Suite Spot: Sentencing Frauds," *Journal of Financial Crime* 17 (January 5, 2010): 116–32, https://doi.org/10.1108/13590791011009400.

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

[75] "What Is the Average Sentence for Fraud in 2023? Get the Answer Here," Stuart Miller Solicitors, https://www.stuartmillersolicitors.co.uk/sentences/fraud/.

[76] "Length of Incarceration and Recidivism," United States Sentencing Commission, April 28, 2020, https://www.ussc.gov/research/research-reports/length-incarceration-and-recidivism.

[77] "Proven Reoffending Statistics: July to September 2017," GOV.UK, https://www.gov.uk/government/statistics/proven-reoffending-statistics-july-to-september-2017.

[78] "The Police Uplift Programme - Committee of Public Accounts," https://publications.parliament.uk/pa/cm5803/cmselect/cmpubacc/261/report.html.

[79] Jim Gee and Mark Button, *The Financial Cost of Fraud 2019: The Latest Data from Around the World* (Crowe UK, 2019).

[80] "Administrative Approaches to Crime - Enaa," https://administrativeapproach.eu/publications/sed-magna-purus-fermentum-eu.

[81] "Economic Crime and Corporate Transparency Act 2023: Factsheets," GOV.UK, March 1, 2024, https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-act-2023-factsheets.

[82] "Economic Crime and Corporate Transparency Act 2023: Factsheets," GOV.UK, March 1, 2024, https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-act-2023-factsheets.

[83] "Economic Crime Plan 2023 to 2026," GOV.UK, June 29, 2023, https://www.gov.uk/government/publications/economic-crime-plan-2023-to-2026.

[84] "Fraudulent Times: Identifying a Consensus for an Agenda to Beat Fraud," Social Market Foundation., https://www.smf.co.uk/publications/a-consensus-to-beat-fraud/.

[85] "Risk Factors for Fraud Victimization: The Role of Socio-Demographics, Personality, Mental, General, and Cognitive Health, Activities, and Fraud Knowledge," , https://doi.org/10.1177/02697580231215839.

[86] "Major Campaign to Fight Fraud Launched," GOV.UK, https://www.gov.uk/government/news/major-campaign-to-fight-fraud-launched.

[87] James Kite et al., *Mass Media Campaigns and the 'File Drawer Problem': A Delphi Study of How to Avoid Campaign Failure*, 2023, https://doi.org/10.1101/2023.11.01.23297917.

[88] John Billow, "No Country Is an Island: Embracing International Law Enforcement Cooperation to Reduce the Impact of Cybercrime," *Journal of Cyber Policy* 0, no. 0 (n.d.): 1–10, https://doi.org/10.1080/23738871.2023.2245417.

[89] "Global Fraud Summit Communiqué: 11 March 2024," GOV.UK, https://www.gov.uk/government/publications/communique-from-the-global-fraud-summit/global-fraud-summit-communique-11-march-2024.

[90] Cecily Rose, "The Creation of a Review Mechanism for the UN Convention Against Transnational Organized Crime and Its Protocols," *American Journal of International Law* 114, no. 1 (January 2020), https://doi.org/10.1017/ajil.2019.71.

[91] Osmond Okonkwo, Donald Emayomi, and Akamike Joseph, "Impact of Fraud and Financial Crimes on the Growth and Development of the Nigerian Economy," *Direct Research Journal of Social Science and Educational Studies* 11 (September 20, 2023): 80–87, https://doi.org/10.26765/DRJSSES04235816217.