



HM Government

FRAUD STRATEGY: STOPPING SCAMS AND PROTECTING THE PUBLIC

May 2023

CP 839



Fraud Strategy: Stopping Scams and Protecting the Public

Presented to Parliament
by the Secretary of State for the Home Department
by Command of His Majesty

May 2023



© Crown copyright 2023

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/official-documents

Any enquiries regarding this publication should be sent to us at public.enquiries@homeoffice.gov.uk

ISBN 978-1-5286-4086-2

E02904361 05/23

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by HH Global on behalf of the Controller of His Majesty's Stationery Office

Contents

Foreword	1
Executive summary	3
The harm fraud causes	7
Pillar 1: Pursue fraudsters	14
Pillar 2: Block fraud	26
Pillar 3: Empower people	37
Enhance key international and domestic capabilities	43
Delivery: how we will make this happen	48
Annexes	51
Annex 1: Links with other government strategies	51
Annex 2: Geographic scope	54
Annex 3: Cost of fraud methodology	56
Glossary	64

Foreword



The publication of this strategy marks a fundamental shift in our approach to tackling fraud. Fraud causes severe harm to the economy, places enormous stress on families and businesses, and ruins people's lives. Fraud also funds other serious crimes. This Government will not tolerate the barrage of scam texts, phone calls, adverts, and emails that causes misery to millions and makes up over 40% of all crime. This strategy sets out a plan to stop fraud at source and pursue those responsible wherever they are in the world.

Most importantly, victims must know that the police will do something about their crime. Fraud now accounts for over 40% of crime but receives less than 1% of police resource. I am changing this by setting up a new National Fraud Squad (NFS) dedicated to pursuing the most sophisticated and harmful fraudsters, with over 400 new specialist investigators, and making tackling fraud a priority for police forces in England and Wales.

I also want victims to get the help they need. With money such a concern for so many, ensuring that victims get their money back quickly is vital. We will soon have the powers to make sure that payment service providers are treating customers fairly. We are replacing Action Fraud, the fraud and cyber reporting service, to ensure that victims can report

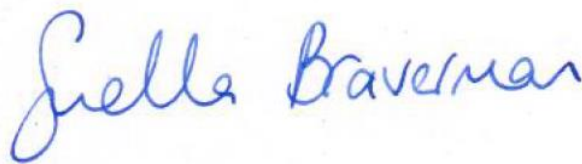
frauds to the police more easily, get more support and information about their case, and to provide police forces with better information to catch more fraudsters.

Industry can do more to protect its customers, our citizens and businesses. The financial sector has worked with us for a long time on fraud. Whilst I welcome their continued efforts, I challenge them to go further. But it is other industries, especially online technology giants, who should do more to stop criminals exploiting their services and should never profit from online crime. We will publish information about which platforms are the safest and ensure that companies are properly incentivised to combat fraud, exploring all avenues to do this. The Online Safety Bill will also ensure that internet users are better protected from fraud online - and I encourage companies to start acting now to prepare for the new regime.

Fraud is not only a problem in the UK. Working with allies abroad, we will pursue fraudsters across the globe. I will hold a summit next year to set up a new international partnership to stop frauds wherever we can. To further drive our response, Anthony Browne MP has been appointed into the new role of the Prime Minister's Anti-Fraud Champion.

I would like to thank the Public Accounts Committee; Treasury Select Committee; Justice Select Committee; Lords Fraud Act and Digital Fraud Committee; and the National Audit Office for their considered reports, which provided insightful and constructive recommendations that have helped shape this strategy.

Government, law enforcement, and industry must now come together and do all we can to show fraudsters that their time is up and that together we can beat fraud.



Rt Hon Suella Braverman KC MP

Home Secretary

Executive summary

Fraud poses a significant threat to the people, prosperity, and security of the UK. It is by far the most common crime and now accounts for over 40% of all offences in England and Wales.¹ This strategy will tackle fraudsters head on and cut fraud by 10%, protecting the British people's hard-earned cash from criminals and putting more fraudsters behind bars.

1. Predatory criminals take money out of the pockets of hard-working people, businesses, and organisations – callously targeting the most vulnerable, online and in their own homes. And fraudsters are becoming more devious – we see many more victims who have been emotionally manipulated to lower their defences. The high volume and severity of the fraud risk threatens our national and economic security, enabling terrorism and organised crime, as recognised by the Government's 2021 Integrated Review of Security, Defence, Development and Foreign Policy. The Integrated Review Refresh 2023 recognises the importance of the Fraud Strategy in stopping the exploitation of the UK's financial systems and economic openness for criminality and corruption.
2. It is imperative we take urgent action to crack down on the ruthless criminals behind these cold-hearted crimes. Bank accounts can be emptied in minutes and life savings lost – victims reported losing £2.35 billion in 2021.² Fraud also causes enormous emotional harm and, in some heart-rending cases, results in people taking their own lives.
3. This strategy sets out how government, law enforcement, regulators, industry, and charities will work together to cut fraud incidents by 10% from 2019 pre-Covid levels by the end of this Parliament. We will put protecting people at the heart of our response.

¹ As of the year ending December 2022. [Crime in England and Wales: Appendix tables - Office for National Statistics \(ons.gov.uk\)](#): Table A1.

² [National Fraud Intelligence Bureau \(NFIB\) Annual Assessment: Fraud crime trends FY 2020-2021.](#)

4. We have already started by committing £100 million of new money to bolster law enforcement in the fight against fraud as part of a wider £400 million investment in tackling economic crime.
5. We will stop fraudsters from trying to make victims of us all. We will:
 - Ban cold calls on all financial products so fraudsters cannot dupe people into buying fake investments.
 - Ban SIM farms which are used by criminals to send thousands of scam texts at once.
 - Review the use of mass text aggregators and explore next steps to stop fraudsters from being able to send scam texts in bulk messages.
 - Stop more scam calls by making it harder for fraudsters to 'spoof' UK numbers to make it look like they are calling from a legitimate UK business.
 - Stop people from hiding behind fake companies and create new powers to take down fraudulent websites.
6. We will make it much easier to report scams. We will:
 - Replace Action Fraud with a state-of-the-art system for victims to report fraud and cyber crimes to the police.
 - Work with industry to make sure that intelligence is shared quickly with each other and law enforcement and that action is taken early to stop frauds.
7. We will ensure victims of fraud are reimbursed and supported. We will:
 - Change the law so that more victims of fraud will get their money back.
 - Overhaul and streamline fraud communications so that people know how to protect themselves from fraud and how to report it.
8. We will improve the law enforcement response to fraud. We will:
 - Launch a new National Fraud Squad with over 400 new specialist investigators, and make fraud a priority for the police.
 - Deploy the UK Intelligence Community and lead a new global partnership to relentlessly pursue fraudsters wherever they are in the world.
 - Put more fraudsters behind bars through better investigation and prosecution processes for fraud and digital offences.
9. We will make sure every part of the system is incentivised to take fraud seriously. We will:
 - Make the tech sector put in place extra protections for their customers and introduce tough penalties for those who do not through the Online Safety Bill.
 - Ensure large tech companies make it as simple as possible for users to report fraud on their platforms, within a few simple clicks.

- Shine a light on which platforms are the safest, making sure that companies are properly incentivised to combat fraud.
10. There are also key cross-cutting themes we will tackle, including working internationally, improving data sharing across and beyond government, and tackling the problem of money mules (a type of money laundering used by fraudsters).
11. Key actions in the Strategy are below:

 Pursue Fraudsters	Establish a National Fraud Squad with over 400 new specialist investigators New UKIC cell and move to intelligence led disruption Replace Action Fraud with a state-of-the-art reporting system Imprison more fraudsters Lead a global partnership to pursue fraudsters worldwide
 Block Fraudsters	Appoint Anthony Browne MP as Anti-Fraud Champion Stop criminals from abusing the telephone network: • Ban cold calls on all financial products • Ban SIM farms • Review use of mass text aggregators • Stop more spoof calls Revolutionise tech company action to block fraud at an industrial scale: • Make the tech sector commit to protect their customers through legislation and voluntary commitments • Make it easier to report fraud on social media and the internet • Create new powers to take down fraudulent websites • Publish information about fraud levels on different platforms Help banks slow down suspicious payments
 Empower the Public	Support more victims Reimburse more fraud victims Better communications about how to protect yourself from fraud, how to report fraud, and what to do if you become a victim of fraud

The harm fraud causes

In the year ending December 2022, 1 in 15 adults were victims of fraud.³ 18% of those victimised became victims more than once.⁴ The sums of money involved are staggering. The total cost to society of fraud against individuals in England and Wales was estimated to be at least £6.8 billion in 2019-20.⁵ This includes the money lost by victims, the cost of caring for victims, and the costs of recovery, investigation and prosecution of fraudsters. Further detail on the cost of fraud can be found at Annex 3.

12. In the year ending March 2021, Action Fraud received victim reports totalling a loss of £2.35 billion.⁶ Industry reporting suggests average personal losses for authorised frauds (these are frauds where the victim has approved a payment) could be almost £3,000.⁷ In some instances, victims can lose hundreds of thousands of pounds. When people become victims of fraud multiple times their losses escalate rapidly. The Crime Survey for England and Wales (CSEW) also provides a view of the value individuals lost to fraud seen in figure 1 below.
13. There is also considerable cost to business and enterprise. UK Finance, the trade body for the banking and finance industry, reported that in 2021 its members lost over £1.3 billion to fraud, increasing costs for everyone who uses banking services. We also know from the Economic Crime Survey⁸ that in 2020 around one in five businesses had been a victim of fraud in the previous three years (18%).

³ Crime in England and Wales: Appendix tables - Office for National Statistics (ons.gov.uk): Table A3.

⁴ Crime in England and Wales: Annual trend and demographic tables: D7

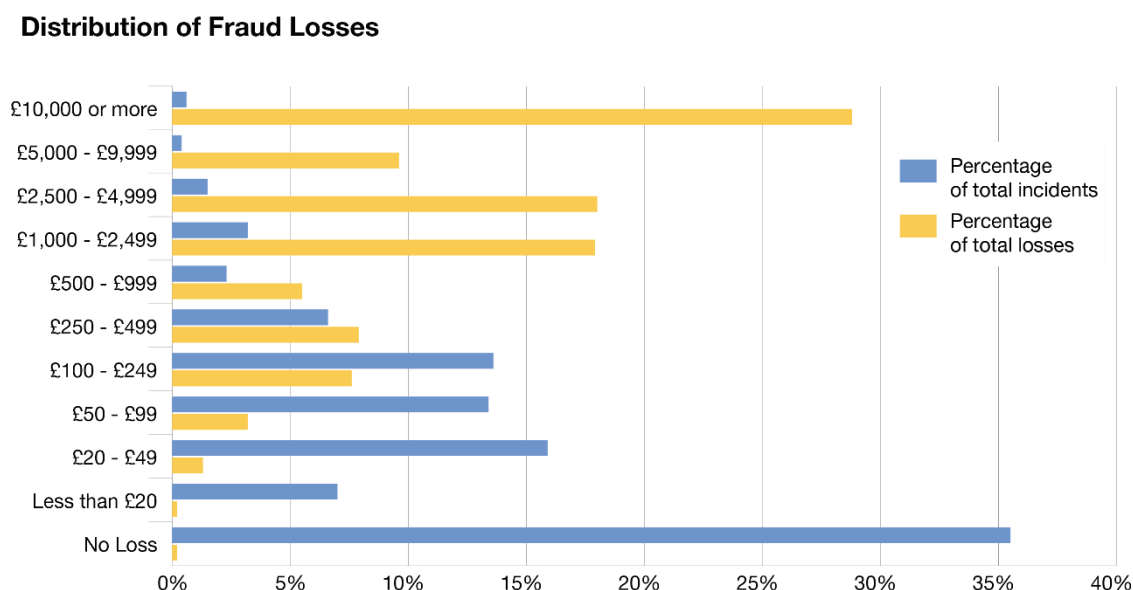
⁵ The Economic and Social Costs of Crime 2022. This figure estimates wider costs to society including preventative spending, emotional harms and the law enforcement response to fraud committed against individuals. Please refer to Annex 3.

⁶ Action Fraud. Fraud Crime Trends 2020-21. Fraud and cyber crime national statistics | Action Fraud

⁷ UK Finance Annual Fraud Report 2022 (p47 taking Value/Volume)

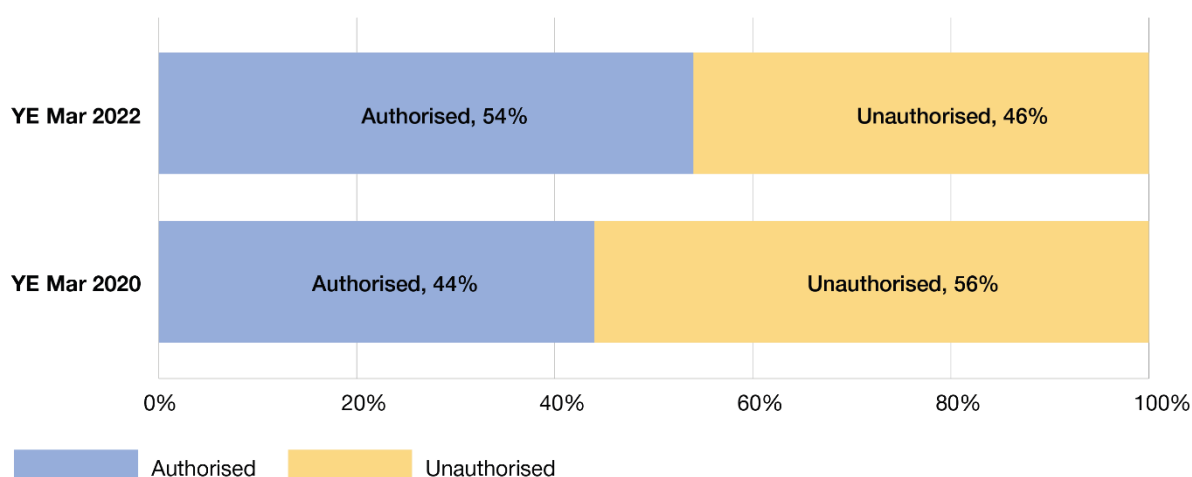
⁸ Economic Crime Survey, Home Office, 2020.

Figure 1 – Distribution of fraud losses, England & Wales



Source: CSEW year end Mar 22

Figure 2 – Estimated change in proportion of authorised/unauthorised frauds



Source: CSEW & NFIB data

14. Figure 1 shows 36% of fraud incidents lead to no financial loss (as the fraud has been attempted, but has not been successful), however many result in high value losses. Over 250,000 incidents (6%) lead to losses above £1,000.⁹ Total fraud losses are largely driven by high value incidents. Despite losses above £10,000 only making up 0.5% of incidents, they are estimated to make up 29% of total financial losses from fraud.

⁹ CSEW Nature of Fraud & Computer Misuse, YE Mar 22

15. Figure 2 shows the nature of fraud is changing.¹⁰ Historically the main form of fraud was unauthorised fraud, which is predominantly bank and credit card related, where money is taken from victims' bank accounts without their authorisation or knowledge. Now, as banks have improved their technology to prevent this type of fraud, the criminals are adapting. As shown above in Figure 2, in the last two years there has been a significant swing towards authorised fraud, where victims are persuaded by the fraudster to authorise a payment themselves – common examples include retail scams, romance, and investment fraud, but there are many other forms.
16. The harms experienced by victims go beyond just financial loss. According to the CSEW, in the year ending March 2020 almost three quarters of victims experienced some sort of emotional impact.¹¹ Action Fraud deal with over 300 calls a year where someone is judged to be at risk of suicide.
17. The volume of fraud, its capacity to undermine public confidence in the rule of law, and its potential negative effect on the UK's financial reputation, means it should be considered a national security threat. Correspondingly, the importance of tackling fraud to stop the exploitation of the UK's financial systems was recognised in the 2023 refresh of the Integrated Review of Defence, Security and Diplomacy. The Royal United Services Institute has also identified evidence that fraud has funded terrorist activity. For example, militants have committed frauds on UK victims to fund their participation in the Islamic State in Syria.¹²
18. There is also evidence showing direct links between fraud and other serious and organised crime, such as modern slavery, human trafficking and drugs. One study found two-thirds of organised crime groups focussed on frauds are also involved in other criminal activities.¹³

What is fraud?

19. A fraud involves an act of dishonesty, normally through deception or breach of trust, with the intent to either make a gain or cause a loss of money or other property. The term 'fraud' is an umbrella term for crimes that vary in nature. In England, Wales, and Northern Ireland most offences come under the Fraud Act 2006. In Scotland most frauds are common law offences.

¹⁰ CSEW data was used to approximate the proportion of authorised and unauthorised frauds. The following fraud types were classified as being indicative of unauthorised frauds: Consumer phone fraud, Cheque, plastic card and online bank accounts (not PSP), Dishonestly retaining a wrongful credit, Other fraud (not covered elsewhere)

¹¹ Nature of crime: fraud and computer misuse. YE March 2020 (most recent year this data was collected)

¹² RUSI: The Silent Threat

¹³ Michael Levi, 'Organized Fraud', in Letizia Paoli (ed.), *The Oxford Handbook of Organized Crime* (Oxford: Oxford University Press, 2014), p. 462

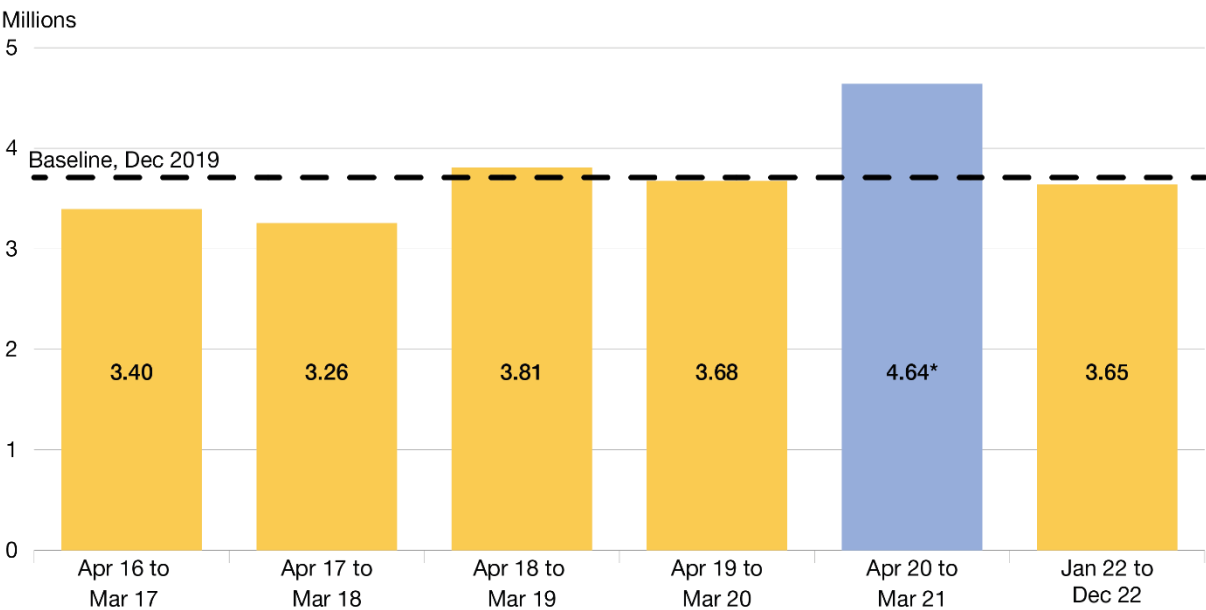
20. Fraud is the largest crime type and levels have grown in recent years. In the year ending December 2022, there were an estimated 3.7 million incidents of fraud in England and Wales – over 40% of all crime. Fraud levels spiked during the Covid pandemic, growing to over 5 million incidents in the year ending December 2021.¹⁴

Figure 3 – Fraud as a proportion of all crime in 2021/22



Source: Appendix tables, year ending December 2022, CSEW

Figure 4 – Incidents of Fraud 2016/17 to 2021/22 from Crime Survey England and Wales



Source: Appendix tables, year ending December 2022, CSEW

*TCSEW

¹⁴ [Crime in England and Wales - Office for National Statistics \(ons.gov.uk\)](#) Appendix Table 2

Technology-driven increase

21. The UK is already an attractive target for fraudsters. City of London Police (CoLP) estimates that over 70% of fraud either originates abroad or has an international element.¹⁵ The financial sector has advised that UK individuals and businesses are a more attractive target for fraud because of our relative wealth, the universality of the English language, our rapid adoption of online technology such as internet banking and online shopping, and the fast and frictionless nature of our payment systems.
22. It is this adoption of new technologies by consumers, businesses and fraudsters that is almost certainly the main driver of recent increases.
23. Advances in technology provide fraudsters more access to victims and data:
 - As more and more data is held online, large scale data breaches enable fraudsters to access and use stolen personal information to commit their frauds.
 - Availability of bulk communications, such as text messaging services, allow fraudsters to target thousands of people at once. Number ‘spoofing’ allows fraudsters to impersonate a legitimate UK number or business and trick people into answering calls they might otherwise ignore.
 - The emergence of new artificial intelligence large language models such as ChatGPT and clever machine learning tools allows fraudsters to target and tailor their scams to be more effective.
24. Consumers and citizens are spending more time online and online business models are proliferating. Whilst there have been revolutionary opportunities for our economy afforded by this shift, these have also been seized upon by fraudsters. Most frauds are now perpetrated – or facilitated in part – online, with online platforms (such as social media) and messages being the most common form of contact by fraudsters.¹⁶
25. Fraudsters are likely to become ever more adept at harnessing technology and identifying vulnerabilities, making frauds much harder for victims to spot. Technological advances, such as deep-fakes¹⁷ and increasingly immersive online environments,¹⁸ can leave users more vulnerable and give rise to new types of fraud-related threats by presenting fake people or information in a way that is impossible to distinguish from the real thing.

¹⁵ International Fraud Offending Recorded on Action Fraud: Professional estimation of international fraud offending by NFIB February 2022

¹⁶ Fraud Crime Trends. According to Action Fraud over 83% of reported fraud is cyber enabled. Social media and encrypted messaging services as an enabler is increasing throughout all aspects of fraud.

¹⁷ See Glossary

¹⁸ See Glossary

26. There are new dimensions to the threat. The US Federal Bureau of Investigation have seen North Korea's state-backed hackers attempt to acquire cryptocurrency through fraud and cyber crime.¹⁹ With the proliferation of complex cyber crime technologies, this overlap between national security and criminal threats will only increase.

Scope of this strategy

27. This is a cross-government strategy that covers fraud where the victims are members of the public or businesses. The response to fraud against the public sector is led by the Public Sector Fraud Authority (PSFA) who work with fraud professionals across government departments and public bodies to prevent fraud, reduce harms and ensure public services go to those most in need. Their Mandate can be found on GOV.UK. The PSFA will publish a Four-Year Functional Strategy that will set out central government's response to fraud against the public sector. We are coordinating these strategies and work closely together, sharing data and techniques to reduce the threat to the public, businesses and the public purse.
28. In 2019, the Government and the private sector agreed an Economic Crime Plan (ECP), setting out actions across both the public and private sectors to tackle the growing threat to national security from economic crime. The second ECP was published this year, setting out the whole-system response to tackle all economic crime including money laundering and illicit finance. It set out the overarching approach, under which this strategy sits, as well as the commitments made through the recent review of the UK's Anti Money Laundering and Counter-Terrorism Financing regulatory and supervisory regime. The Government is also developing a successor to the national Anti-Corruption Strategy 2017-2022, which will address broader economic crime related corruption.
29. Fraud intersects with other policy areas including cyber crime and security, digital policy, identity policy and many more. The relationships between this strategy and other related strategies are set out in Annex 1.

Geographic scope

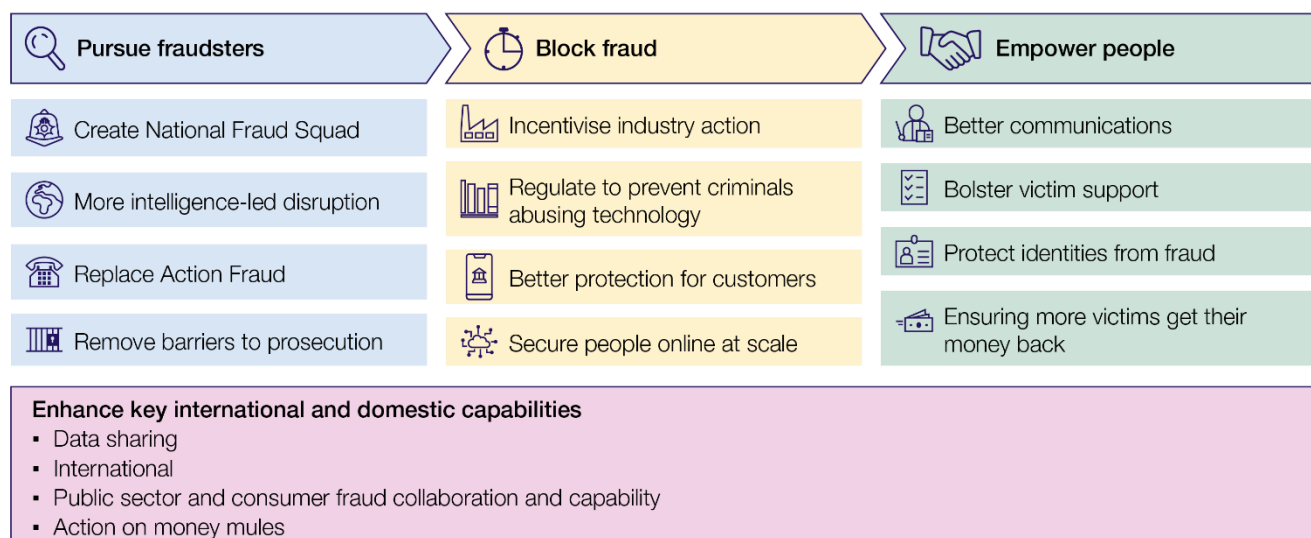
30. This strategy will have material positive outcomes for all four nations of the UK. Both the UK government and the devolved administrations are committed to combatting fraud. We will continue to ensure that collective issues are addressed collaboratively to maintain the resilience of the UK against fraud. A breakdown of geographic scope can be found in Annex 2.

¹⁹ Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe | OPA | Department of Justice

31. Fraud does not respect national borders and this strategy sets out how we will build international consensus for greater action to tackle fraud, as well as to drive forward operational activities with key partner countries to clamp down on fraudsters.

Our new approach to stopping fraud and scams

32. A new approach is needed to keep the public safe and reduce the national security threat. We will take an end-to-end approach to cut fraud by 10% by the end of this Parliament, with three key elements:
- We will **pursue fraudsters**, disrupting their activities and bringing them to justice more often and quicker.
 - We will **block frauds** at source by dramatically reducing the number of fraud and scam communications that get through to the public.
 - We will **empower the British people** to recognise, avoid and report frauds and equip them to deal easily and appropriately with frauds that do get through.



Pillar 1: Pursue fraudsters

The criminal justice system must ramp up the focus it gives to fraud. Modern technology has made it increasingly easy to commit fraud from overseas, frustrating traditional policing methods and impeding our ability to bring fraudsters to justice. We must counteract this, taking on fraudsters more swiftly and putting more of them behind bars. We are investing £100 million to improve the law enforcement, intelligence community and criminal justice system response, preventing over 300,000 more frauds by the end of this Parliament through Pursue interventions alone.

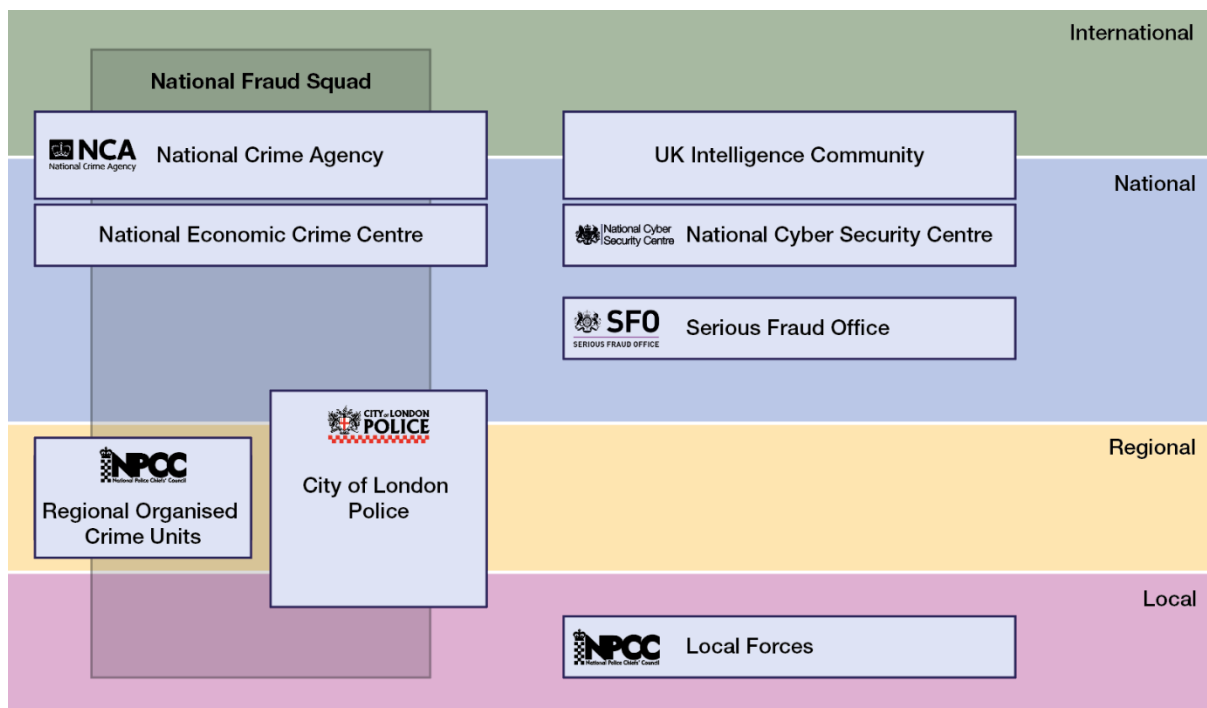
33. As the sophistication and complexity of fraud has increased, prosecuting fraud has become correspondingly much more challenging. Multiple external reviews of the police response to fraud have emphasised the difficulties that the police face. Recent crime statistics show that we continue to see a marked decrease in the number of defendants taken to court for fraud.²⁰ The UK is not alone in this as similar trends are reported by international partners.²¹ We are reprioritising and increasing our investment in how we tackle fraud to deliver better outcomes for victims.
34. We must focus our efforts on disrupting the frauds, fraudsters and enablers that have the greatest impact. To do that we must use all the resources at our disposal, including deploying our highly capable intelligence community and international relationships, investing £100 million in our law enforcement response over the spending review period (Y/E 24/25). We must also make sure that the law keeps up with fraudsters, who exploit any loophole they can to get away with their crimes. We will base this on the clear division of responsibilities that are already in place:
 - Home Office are the overall policy and strategic system lead on fraud against individuals and businesses.

²⁰ MOJ Outcomes by Offence Tool, [Criminal Justice System statistics quarterly: June 2022](https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-june-2022) - GOV.UK (www.gov.uk)

²¹ International criminal justice statistics: [Australia](#), [United States of America](#), [Canada](#), [New Zealand](#)

- The National Crime Agency (NCA), through the National Economic Crime Centre (NECC), are the operational system lead working across UK law enforcement, the intelligence community and industry.
- The City of London Police (CoLP) lead and coordinate the efforts of Regional Organised Crime Units (ROCUs) and 43 police forces in England and Wales (in their role as the National Lead Force for fraud).
- Local police forces across the UK and ROCUs in England and Wales will continue to be responsible for the vast majority of fraud investigations in the UK, as well as leading on support for victims and businesses in their local areas.
- The Serious Fraud Office (SFO) will continue to use their specialist investigatory structures and powers to tackle highly complex frauds.

Figure 5 – the law enforcement response to fraud



Create a National Fraud Squad

- **Launch a new National Fraud Squad that will investigate and disrupt more fraudsters targeting individuals and businesses, with over 400 new specialist investigators across NCA, CoLP and ROCUs.**
- **Make fraud a priority for police forces through the Strategic Policing Requirement.**
- **The NECC and CoLP will launch a new People Strategy to improve recruitment and retention in fraud law enforcement.**
- **Home Office and the College of Policing (CoP) will review overall police training in digital skills.**
- **Bring expertise together, across sectors, to define practices, standards and develop capability of those working to counter fraud, through the development of and alignment to the Counter Fraud Profession.**
- **Undertake a review of fraud law enforcement, assessing the impact the additional posts have made and whether more substantial structural reform is needed.**
- **Deliver additional powers to seize and recover criminal crypto assets through the Economic Crime and Corporate Transparency Bill.**

Boost resources

35. We are boosting the wider law enforcement response by establishing a new National Fraud Squad (NFS). The Squad will take a proactive intelligence-led approach and focus on high-end frauds and organised crime. The Squad will work alongside the Serious Fraud Office (SFO) and collaboratively with the wider fraud ecosystem, to ensure that complex fraud cases are investigated by the most appropriate agency.
36. The NFS will be made up of over 400 new posts across policing and the NCA by 2025 alongside existing resources. Jointly led by the NCA and CoLP, the NFS already has 300 new and existing investigators in post. A further 100 will be in post by January 2024, followed by another 100 by 2025. The NFS will use covert and overt intelligence gathering capabilities to identify and target the worst offenders domestically and overseas. This is an improvement on current reactive approaches based on victim reporting, which makes it difficult to identify and deal with the key perpetrators. New teams in the NECC, CoLP and UK Intelligence Community (UKIC) will work together to share intelligence in real-time to drive enforcement action across government and the private sector.
37. This is the first significant investment to address fraud since 2008. The NFS will transform how we identify, disrupt and prosecute fraudsters. Alongside a new fraud targeting cell in the NCA, every ROCU will have a dedicated fraud

investigations team. CoLP, as the national lead police force for fraud, will increase its view across wider policing's activity on fraud, disseminating intelligence, promoting best practice and holding forces to account for delivery. Given the rapidly growing and complex threat that fraud poses, it is critically important there is a whole-system response.

38. There are other key steps that the Home Office will take. We will increase ministerial oversight of policing on fraud and raise the priority of fraud in key strategic policing documents. The new Strategic Policing Requirement (SPR), which sets the capabilities the Home Secretary wants forces to have, gives greater prominence to fraud, which is captured within the serious and organised crime threat. For the first time, it specifies the capabilities that each force should have in place to tackle fraud. The document outlines how forces can better use NCA capabilities and capabilities offered by CoLP as the National Lead Force, Action Fraud and the Economic Crime Academy. The SPR will focus resourcing and efforts to tackle fraud and maximise the output of existing resourcing, especially at local force level.
39. Local Police and Crime Commissioners are putting greater focus on fraud. For the first time, every Police and Crime Plan that sets local priorities in England and Wales mentions fraud. We are also reviewing how police forces report outcomes against crimes to the Home Office. We want to recognise the disruptive and preventative activity forces carry out with enablers (such as social media sites) and victims (to prevent them falling victim again) that reduce the ability of fraudsters to operate.
40. We will continue to ensure that all government levers that can tackle fraud are available to law enforcement. There are many different organisations in the public and private sectors that play a crucial role in tackling fraud, with differing responsibilities in how they respond to the fraud threat. The SFO, the Financial Conduct Authority (FCA), National Trading Standards (NTS) and other enforcement bodies can provide crucial interventions to stop fraudsters themselves and work with police and the NCA on their investigations.

Building digital skills and capabilities for the future

41. Police and investigators need the digital skills and capabilities that will deliver as criminals get better at exploiting technology to commit fraud on a large scale. This starts with the fundamentals provided by the CoP to all police officers and investigators. CoLP and the NECC are developing a People Strategy. As well as immediate recruitment and retention challenges, it will address longer term issues by offering new and innovative routes into economic and cyber crime roles. This will include education and enhanced use of Special Constables and Police Support Volunteers.

42. We are also exploring avenues to draw on the counter-fraud skills contained within the broader public sector, as well as the private sector. We will look for opportunities to exchange people and skills through the CoLP/NECC People Strategy. We will also build on the success of the Government Counter Fraud Profession, launched in 2018, with c.7,000 members across 59 organisations including the SFO, HMRC and CoLP. The Public Sector Fraud Authority, which the Profession operates from, will introduce a licence to operate model for members to assure the skills and knowledge of those working to counter fraud.

More intelligence-led disruption

- **Deploy the UK Intelligence Community, through a new fraud focused unit, to better understand the international threat and utilise global partnerships to stop fraudsters wherever they are in the world.**
- **Establish a new multi-agency fraud targeting cell in the NCA.**

43. CoLP estimate that over 70% of fraud experienced by UK victims could have an international component - either offenders in the UK and overseas working together, or fraud being driven solely by a fraudster based outside the UK. In 2016, almost half of reported fraud and cyber crimes were estimated to be committed by organised crime groups.²²
44. New investigative capabilities will be driven by better intelligence to identify serious organised crime groups carrying out fraud. Using their world-leading capabilities and international relationships, UKIC will build an understanding of the threat, identify novel interventions for public and private partners, and work with law enforcement to disrupt fraudsters anywhere in the world who target UK citizens, stopping frauds from reaching them.
45. The NECC will establish a multi-agency fraud targeting cell that draws on all source data to improve system-wide understanding of the threat and produce high quality intelligence packages. As a result, collective resources will be directed to where they will have greatest impact.
46. As well as diplomatic and multilateral efforts, we are looking at where we can make a practical difference by joining up with partners worldwide. This includes building relationships with operational partners in countries that, because of their lack of opportunity, infrastructure or global connections, enable the most fraud in the UK.

²² [Police Foundation Organised Fraud in Local Communities Briefing \(police-foundation.org.uk\)](https://www.police-foundation.org.uk/)

Case study

In November 2022, a multi-agency and international law enforcement operation took down a facility that fraudsters had used to target 200,000 victims in the UK alone. This was the UK's biggest fraud operation to date and an example of the sort of operations of which our strategy will deliver more.

Led by the Metropolitan Police Cyber Crime Unit - working with international law enforcement, including the National Crime Agency and authorities in the US and Ukraine - the iSpooof website was taken down. This website was used by fraudsters to impersonate genuine banks to acquire personal information to carry out fraud. At one stage, almost 20 people every minute of the day were being contacted by scammers posing as representatives of the largest high street banks and building societies including Barclays, Santander, HSBC, Lloyds, Halifax, First Direct, NatWest, Nationwide and TSB.

In the 12 months until August 2022, around 10 million fraudulent calls were made globally via iSpooof, with around 3.5 million of those made in the UK. The average loss from those who reported being targeted is estimated to be £10,000. Police have arrested more than 100 people in the UK, including the suspected organiser of the iSpooof website.

Replace Action Fraud

- **Make it easier for victims to report fraud, and for law enforcement to take action on victims' reports, through a new, state-of-the-art national fraud and cyber crime reporting service.**

47. Victims must have confidence that the police take the crimes that they have endured seriously. Action Fraud, run by CoLP, is the place most victims go first, as the UK's centralised fraud and cyber crime reporting service. A centralised service that covers both these crime types offers significant advantages to victims and the police, providing access to specialist services for victims and comprehensive intelligence for law enforcement action.
48. However, reviews of Action Fraud have repeatedly identified shortcomings and the Home Office, the City of London Corporation and CoLP are committed to improving this vital service. For this reason, the Home Office has committed to spend over £30 million across three years, alongside contributions from the City of London Corporation, to replace and improve the service.
49. This new service will provide a wide range of benefits to victims and other users. As part of the upgrade a new reporting website will be launched to make it easier for victims to report their crimes online and access advice on

how to protect themselves. Anyone reporting to the new service will also be able to track the progress of their report and receive far more timely updates.

50. Improvements to the existing service are already underway to enhance the victim reporting experience and the quality and timeliness with which cases are sent to police forces for action. Recent improvements include:
 - Using automation to increase effectiveness through improved technology.
 - Increasing the number of staff in the call centre and introducing a new chat bot for the website to handle greater volumes of reports.
 - Sending cases to forces faster so they can consider whether an investigation can take place.
 - Web reports are now analysed to identify vulnerable victims so their cases can be prioritised for immediate assessment and one-to-one support.
 - The National Economic Crime Victim Care Unit (NECVCU) service that some victims are referred to by Action Fraud has already been rolled out to 41 forces.
51. The full replacement service will launch within a year. For victims this will mean a totally new reporting service, including an upgraded call centre that will reduce waiting times, as well as the new portal for victims to get updates on the progress of their report.
52. Crucially, swifter action will be taken on victims' reports, resulting in more fraudsters being disrupted. The National Fraud Intelligence Bureau (NFIB), the body responsible for assessing victims' reports and passing those that are actionable to investigators across law enforcement, will have access to new and advanced analytic capabilities as well as much more data. This will allow them to act more quickly, reducing the time it will take to pass intelligence packages onto police forces to investigate crimes, or to identify criminal gangs for the NFS to target. They will also be able to take more rapid action with industry, identifying opportunities for banks to stop money from reaching fraudsters, or to take down suspicious websites that are attracting large numbers of victims. More information on these steps will be provided to victims, increasing their confidence that something is being done.

Improve the criminal justice response and put more fraudsters behind bars

- **Conduct a new independent review into the challenges of investigating and prosecuting fraud, considering:**
 - **Modernising the disclosure regime for cases with large volumes of digital evidence.**
 - **Whether fraud offences and the Fraud Act 2006 meet the challenges of modern fraud, including whether penalties still fit the crime.**
 - **Creating civil orders and penalties to prevent fraudsters reoffending.**
 - **Making it easier for individuals to inform on associates in criminal fraud networks.**
- **Embed use of the UK-US Data Access Agreement.**
- **Carry out a full evaluation of the entire life cycle of a fraud case from reporting an offence through to case disposal at court. We will use this evidence base to consult on solutions to increase the volume and speed of such cases.**
- **Make Serious Crime Prevention Orders more effective tools for tackling fraudsters by increasing their use and improving the ongoing monitoring and enforcement.**
- **Explore opportunities for increasing recovery of victims' money through civil powers.**
- **Introduce a new Failure to Prevent Fraud offence in the Economic Crime and Corporate Transparency Bill.**
- **Legislate to make it easier to prosecute corporates for crimes committed by their senior managers, by improving the way decision-makers of the corporate are identified by law.**

Swift and successful prosecutions

53. Due to the nature of fraud cases and the often large volumes of complex evidence they generate, it can require significant time and resource to undertake a thorough investigation and bring a prosecution to court. As the Government launches the NFS, and other measures to increase the law enforcement response capacity, we also plan to remove barriers to justice to ensure that more fraudsters pay for their crimes.
54. There has not been an independent review of fraud since 1986.²³ As such, we will be launching an independent review into the challenges faced when investigating and prosecuting fraud and announcing a lead for the review shortly. The first phase of the review will consider how the disclosure regime can be streamlined for cases with large volumes of digital material, reducing the significant burden on law enforcement and prosecutors. This will include

²³ The Roskill Report on Fraud Trials, 1986

looking at international comparators on disclosure for any lessons we can learn.

55. Effective disclosure is critical to a fair trial and supports public confidence in the administration of justice. However, the volume of digital material can vastly increase the length of time that investigations can take. A modern disclosure regime that reflects the realities of our digital age will make it easier for law enforcement and prosecutors to bring fraudsters to court more quickly.
56. To better target serious organised crime groups committing fraud, the independent review will also consider how provisions under the Serious and Organised Crime Act 2005 can be better used to persuade criminals to bring down associates and fraud networks by giving evidence for the Crown.
57. It has been difficult and time-consuming for investigators of all crimes to acquire data from US-based tech companies. This is particularly true of fraud investigations which rely on large volumes of digital data. We are making it easier for prosecutors to access the digital evidence needed to detect and investigate fraud and secure prosecutions. The UK-US Data Access Agreement, which entered into force last October, permits UK public authorities to obtain data directly from US-based companies, for the purpose of preventing, detecting, investigating, and prosecuting serious crime, including fraud.
58. The Agreement will fundamentally change the way we are able to fight serious crime in the UK by allowing access to more data, more quickly than ever before. The Agreement is already in use and UK and US agencies have made over 3,000 requests which have already resulted in arrests and intelligence breakthroughs including for critical Counter Terrorism operations. We are rolling-out access to all covered agencies over the next 12 months.

Bringing more fraudsters to court

59. Currently, for every 1000 estimated frauds committed there is one successful prosecution.²⁴ We know that not all fraud is reported to law enforcement. There has also been a huge surge in digital evidence²⁵ as well as many offenders being based internationally. This sadly means most victims do not see justice done, and most fraudsters are not punished for their crimes.

²⁴ Calculated taking the ratio between number of sentences (MoJ, YE June 2022 = 3,411) and estimated incidents (CSEW, YE June 2022 = 3,819,000). Does not account for offenders committing multiple frauds or multiple offenders being prosecuted for the same fraud.

²⁵ An inspection into how well the police and other agencies use digital forensics in their investigations - His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) – Home (justiceinspectorates.gov.uk)

Increasing successful prosecution of fraudsters relies on joined-up action across the criminal justice system.

60. The legacy of the pandemic has increased the backlog of cases going through the courts in a timely manner. The Government recognises the impact delays have on victims, witnesses and defendants, and is taking steps to reduce the overall Crown Court backlog which will have the effect of speeding up all types of cases, including fraud. As well as removing limits on the total number of sitting days in the Crown Court for a second year in a row, we are recruiting around 1,000 judges across jurisdictions and taking specific action with the judiciary to increase judicial capacity in the criminal courts with the largest caseloads. We will recruit around 2000 new magistrates by 2025.
61. We will carry out a full evaluation of the entire life cycle of a fraud case from reporting an offence through to case disposal at court. We will use this evidence base to consult on solutions to increase the volume and speed of cases reported to Action Fraud, and the volume and speed that they go through the criminal justice system.
62. We are continuing with the planned construction of the City of London Law Courts, which are scheduled to open in 2026. This will add additional Crown Court capacity in London. This increase will allow up to 550 additional complex fraud, cyber crime and economic crime cases to be heard each year.
63. Judges and magistrates hearing fraud cases receive specific training under the Judicial College on how best to deal with long and complex cases. This training is regularly reviewed to reflect both changes in the law and the nature of the cases coming before the courts. Working with the judiciary and the Judicial Office, we will ensure the court system is equipped for the unique challenges posed by fraud and the evolving nature of the crime.
64. To ensure that less serious fraud cases are dealt with at the right level and do not unnecessarily add to Crown Court caseloads, the independent review will also consider if the Fraud Act 2006 can be updated to increase the number of fraud cases that are heard by Magistrates' Courts.
65. We will also review the support that is available to jurors hearing complex fraud cases. Guidance and support for jurors during a trial is provided by the judge, but there are also practical considerations, such as provision of technology, which prosecutors already make use of, to enable jurors to engage with evidential material more easily.
66. Improving the disclosure regime will also reduce the risk of cases collapsing during trial and increase the chance of successful prosecution. Police and

prosecutors are working more closely together and at an earlier stage of investigations, to build robust cases and prevent fraudsters evading justice.

Proportionate punishment and reoffending

67. A post-legislative review of the Fraud Act 2006²⁶ found that it remains a sound piece of legislation. Some useful suggestions were made on how the wider fraud framework could be improved. Recent reports produced by the House of Lords²⁷ and House of Commons²⁸ noted that there are aspects of the Fraud Act 2006 that merit rethinking. Therefore, the second phase of the independent review of fraud will assess the effectiveness of fraud offences to understand whether they meet the challenges of modern fraud, ensuring the penalties for fraud match the severity of the crime, and its financial and emotional impact on victims.
68. We are looking at alternative ways of tackling fraud through civil powers and preventative orders. The Home Office is consulting on expanding the use of existing Serious Crime Prevention Orders (SCPOs). SCPOs are a powerful tool for preventing and disrupting the activities of the highest-harm criminals involved in serious crime such as fraud, including those who have not been convicted of an offence.
69. We are proposing to make SCPOs more accessible and easier to impose, giving law enforcement more tools to restrict the activities of serious and organised criminals including fraudsters. The Government's response to this consultation will be published in June. The independent review will also consider the scope of further civil powers to tackle fraud, including exploring a fraud-specific order.
70. CoLP are also working with the private sector on a limited pilot to explore whether civil debt recovery and other powers can recover more of victims' money. As this pilot develops, we will review whether there are further civil enforcement powers that could be applied to fraud.
71. Corporate criminal liability must be reformed to ensure companies can be better held to account. We will use the Economic Crime and Corporate Transparency Bill to introduce a new corporate offence of Failure to Prevent Fraud, where a large organisation can be prosecuted when an employee commits a fraud which benefits the company, and which the company did not have reasonable procedures in place to prevent. This will drive a major cultural shift encouraging companies to do more to prevent fraud, creating

²⁶ [Post-Legislative Assessment of the Fraud Act 2006 – June 2022](#)

²⁷ [Lords Fraud Act & Digital Fraud Select Committee Report – November 2022](#)

²⁸ [Justice Select Committee Report – Fraud and the Justice System - October 2023](#)

liability for organisations that do not do enough to prevent fraud committed by employees. This will provide additional protection for the public as companies put measures in place to stop them being targeted.

Case study

Frederick Diji, a prolific romance fraudster, used online dating sites to con 80 victims out of over £400,000 between 2005-2021. Using fake online profiles, he targeted vulnerable people based on their sexuality, age or poor health. After initially gaining a victim's trust, he would lie and emotionally manipulate them to loan him money. One victim had been defrauded over a period of 14 years, during which they gave Fred more than £100,000. Police investigators worked hard to uncover the scale of Fred's crimes and together with the Crown Prosecution Service, successfully built a strong case against Fred, who pleaded guilty and was sentenced to eight years' imprisonment.

Pillar 2: Block fraud

We must stop the barrage of scams plaguing our country and stop fraudsters trying to make victims of us all. According to Citizens Advice, 2 in every 3 adults are targeted by online fraud, and Ofcom research indicates that over 40 million adults in the UK were targeted by at least one suspicious scam text or call in just three months in 2022.²⁹ We can stop this by tackling fraud at source and ensuring every part of the system is incentivised to take fraud seriously, including industry.

72. It is unreasonable to expect the public to be on a constant state of high alert against fraud. Our best defence is to stop fraud attempts from reaching people and businesses before the criminals behind them can cause harm to a victim.
73. Fraudsters use technology and communication methods that are ubiquitous in everyday life. As well as scam texts, phone calls and emails, tactics include emotionally manipulating people through social media, false advertisements and creation of fake websites that impersonate known and trusted brand names or utility services. Not only do we lose money to fraudsters, their actions cause us to lose trust so that we start to question genuine communications, making it harder for legitimate services and businesses to contact us.

²⁹ [New Ofcom rules to fight fake number fraud - Ofcom](#)

Case study

Sarah*, a teaching assistant going through a divorce, met a man on a social networking site in January 2022. This man said he was American and a highly paid employee of a multi-million-pound multinational corporation. He claimed to be around the same age as Sarah, to be the same star sign and to have been adopted, like Sarah was.

Communication then moved onto email, and a number of accounts on instant messaging services, and Sarah tried to transfer £9,000 to those targeting her. Sarah's bank froze the transaction whilst they investigated, but the fraudsters persuaded Sarah to make the transaction through other means.

*Name has been changed

74. The range of methods that a fraudster will use to defraud the public means a coordinated response from government and industry is required, and every part of the system must be incentivised to act. Telecommunication companies and technology firms often provide the infrastructure or service where first contact is made between fraudster and victim, and where they are persuaded to make payments. The financial sector operates the accounts and payment systems that facilitate money loss. We have therefore focused our activity on these three sectors.

Industry action

- **Appoint Anthony Browne MP as newly created Anti-Fraud Champion to drive delivery and increase industry collaboration.**
- **Publish new regular data on patterns of fraud to help inform consumers.**
- **Measure the impact of industry in preventing fraud through the Joint Fraud Taskforce (JFT) and set new voluntary targets for companies to reduce fraud.**
- **Agree a new charter with tech companies by the end of Summer 2023.**
- **Work with tech firms to introduce a simple, seamless and consistent fraud reporting mechanism.**
- **Implement existing Fraud Sector Charters by the end of 2023.**
- **Agree new charters with the insurance and other sectors by early 2024.**

75. Industry, government, law enforcement and regulators must continue to work together to make it as difficult as possible for fraudsters to operate. Companies are in a unique position to protect their customers from fraud.

76. Industry have taken action to prevent fraud and there are examples where this has had a positive effect. The Banking Protocol has prevented many of those who are in the grip of an authorised bank fraud from transferring funds to criminals. The introduction of SMS filtering solutions, agreed through the

Telecommunications Charter, a voluntary agreement signed by the sector (see more information about charters below), has prevented many fraudulent texts from reaching the public. Some large tech companies have brought in checks to ensure that firms advertising financial investments must be registered with the Financial Conduct Authority (FCA).

77. But these successes do not go far enough. While industry can prevent harm on a voluntary basis at the same time as strengthening consumer confidence in their respective markets, changes are not happening in lockstep and some industries have done more than others.

An Anti-Fraud Champion

78. Working with all partners including industry is a key foundation in our efforts to fight fraud. It is incredibly important that this collaboration is effective and seamless.
79. We have therefore appointed Anthony Browne MP to drive collaboration, with UK based and global businesses, to ensure that all key partners are playing their part. As the Anti-Fraud Champion, Anthony will have the authority to position the UK as a leader on the international stage in tackling fraud and ensure the delivery of key strategic aims. As the previous Chief Executive Officer for the British Banking Association, and current member of the Treasury Select Committee, Anthony has the experience and knowledge of fraud and industry to drive this work forward.

Incentivising Action

80. By shining a light on where consumers encounter fraud, we will incentivise those platforms and services which are being abused by fraudsters to do more to protect consumers. We will ask banks to report specified data on authorised fraud rates to the Payment Systems Regulator. Working with regulators and across government, we will publish regular data on patterns of fraud to help inform consumers and ensure that all firms as well as banks are held accountable for preventing fraud from happening in the first place. The Government will ask the new Anti-Fraud Champion to work with industry, including social media and telecommunications firms, to ensure that companies are properly incentivised to combat fraud and explore all avenues to do so.

Joint Fraud Taskforce

81. The Government partners with industry to prevent fraud through the Joint Fraud Taskforce (JFT). This is chaired by the Security Minister and brings together leaders from government, law enforcement, regulators, industry and civil society who are committed to work together to prevent fraud. This was

relaunched in October 2021 and governs the Fraud Sector Charter programme. The JFT works at board and official level across several workstreams including comms, online fraud and victims. Minutes of meetings are available at: www.gov.uk/government/collections/joint-fraud-taskforce.

82. In November 2022, the JFT agreed to work together to measure the impact of the work of industry in preventing fraud. Once a baseline is established, we will set voluntary targets for companies to reduce fraud.

Fraud Sector Charters

83. Fraud Sector Charters are voluntary agreements between industry and government to improve counter-fraud efforts. Through the charters they undertake specific projects, pilots, policy reviews and research to better understand and prevent fraud in signatory sectors. There are already charters with the retail banking, accountancy and telecommunications sectors.
84. Our priority is to agree a new Online Fraud Charter with technology companies. This is vital because of the growing threat from online fraud, and from criminals abusing cutting-edge technology to commit fraud. Just one recent example is the developments in Artificial Intelligence large language models like ChatGPT, Bing and Bard, which can allow fraudsters to create ever more persuasive fraudulent communications, email and voice calls. As part of our continued engagement with the tech sector we intend to work closely with providers to ensure that fraud prevention remains a priority.
85. The Government is already working with the tech sector on the new Online Fraud Charter that will be delivered by the end of summer 2023. We have asked industry as part of this charter to:
 - Improve data sharing with government and other private sector partners to identify and block frauds.
 - Ensure all advertisers of financial promotions are cross-referenced against the FCA authorised list before being published. Following engagement with government, LinkedIn have agreed to use the FCA authorised list alongside other companies like Google, who have seen close to a 100% reduction in paid-for scam advertising for financial services products since using the FCA list.
 - Set out what more they can do to support law enforcement's efforts to tackle online fraud such as investing in a specialist online fraud unit in law enforcement.
 - Streamline and boost counter-fraud education to the public to help them better spot and avoid frauds and seek support when needed.
86. We want to make it as simple as possible for users to report fraud they see online. This includes scam adverts, false celebrity endorsements and fake

user profiles. In discussion with government, many of the largest tech companies have committed to making this process as seamless and consistent as possible. This means, regardless of what social media platform or internet site you are on, you should be able to find the 'report' button within a single click, and then able to select 'report fraud or scams'. This information is sent directly to tech companies to investigate and swiftly remove any scam content which has evaded detection, preventing more users falling victim to scammers in the first place. For example, TikTok and SnapChat already offer quick and seamless reporting for ads, but have committed to extending this to other types of content.

87. The Government is working with TechUK to encourage other tech companies, as well as advertising intermediary services, to follow suit. We will closely monitor progress and consider mandating that all tech companies must offer a simple, seamless, and swift reporting mechanism if voluntary progress towards this is insufficient.
88. There are three current sector charters:
 - The retail banking industry, represented by UK Finance, agreed a charter focused on preventing authorised fraud. Actions included building a shared evidence base on where fraud attempts originate, developing a shared approach to counter the threat of money mules and measures to improve victim support.
 - The accountancy charter focused on building the intelligence picture of fraud affecting the sector. Actions focused on providing a law enforcement assessment of risk in the sector, increasing awareness and changing customer behaviour.
 - The telecommunications charter sets out how, working with government and regulators, the sector will carry out an ambitious programme of work to prevent telecommunications-enabled fraud. This includes blocking scam texts. The sector has already introduced firewalls that detect and stop scam texts from reaching customers. The firewalls also monitor and stop "FluBot malware" used by criminals to infect and take over a victim's phone to steal credit or debit card details. The firewalls have stopped 600 million scam text messages since January 2022. As fraudsters find new ways to attempt to reach customers, telecoms operators continue to work to improve these filters further. The telecommunications charter also includes measures to stop suspicious calls, tackle identity theft, and prevent SIM-swap scams.
89. The Government will secure agreement on charters with other key sectors in the fraud ecosystem, including the insurance sector by early 2024.

Regulate to prevent criminals abusing technology

- **Hold tech companies to account to reduce online fraud and issue significant fines for those who do not, by passing and implementing the Online Safety Bill.**
- **Extend the ban on cold calls to cover all financial and investment products.**
- **Ban SIM farms to make it as difficult as possible for criminals to send scam texts and make scam calls.**
- **Review the use of mass text aggregators and explore user registration of these services.**
- **Together with Ofcom, disrupt more telephone-enabled scams by stopping more spoofed calls.**
- **Deliver the Online Advertising Programme to ensure that UK-facing online advertising is safe from fraud and other harms.**

90. We will root out fraud on social media platforms. User-to-user platforms will be required, by law, to put in place systems to prevent fraudulent content appearing on their platforms. This includes scam adverts and fake celebrity endorsements. We will do this through the Online Safety Bill and work towards making the UK the safest place in the world to be online.
91. Through the Online Safety Bill, internet users will be better protected from fraudulent adverts and scams online. The Online Safety Bill will require 'user-to-user' platforms, such as social media, as well as search services, to put in place systems and processes to tackle fraud where it is facilitated through user-generated content or via search results. The largest in-scope platforms will also need to prevent fraudulent adverts appearing on their services, including where criminals impersonate celebrities or companies to peddle fake financial investments. Robust Codes of Practice, prepared by Ofcom, will set out how in-scope services can comply with these duties. Taken together, these are significant new duties on internet platforms, compelling them to take fraud seriously to make it harder for fraudsters to use these services to scam the UK public, or face substantial fines if they do not take sufficient action.
92. Under the new regime, super-complaints will allow for concerns about systemic issues with particular services to be raised with the regulator, who will be required to respond publicly to them.
93. We will extend the ban on cold calling to cover all financial products. Under the Financial Guidance and Claims Act 2018, this Government has already banned cold calls from personal injury firms and pension providers (unless the consumer has explicitly agreed to be contacted). But we want to do more to stop people being exploited by the practice of cold calling and we will consult on a wider ban on cold calls by the summer, with implementation to follow as

soon as possible, so that fraudsters cannot dupe people into buying fake investments or financial products. This means that the public will know that cold calls about financial products are a scam and should have the confidence to hang up should they receive one of these calls.

Case study

In February 2023, a married couple were sentenced to nine years in prison for a cold calling investment scam where victims lost over £2.7 million. Clint Canning and Eleise Wallace ran Base 2 Trade, which claimed to offer fixed odds betting on the trading performance of a business. The company approached elderly or inexperienced investors via cold calls using an internet portal to show apparent profits so many victims invested more.

When investors tried to withdraw their money, they were fobbed off by the company, ignored, or told they could not. The portal would then show massive losses on the investments and that their accounts had zero money left. The money had been secreted to accounts abroad.

94. We will ban SIM farms. Used by criminals to send out thousands of scam texts in seconds, these are electronic boxes which can hold hundreds of SIM cards. While most frequently used for fraudulent texts we know that they are also used to send drug marketing texts and fuel organised crime. They are currently easy and legal to buy online but we have identified no legitimate use for SIM farms in the UK. We will ban SIM farms and we have launched a consultation on the best way to do this with the intention to legislate when parliamentary time allows. This will be strongly welcomed by the telecommunication industry in particular, whose networks are abused through SIM farms and who lose money as a result.
95. We will review the use of mass text aggregators and explore user registration of these services. While there are many legitimate uses for mass texting services, like restaurant bookings, appointment reminders and delivery updates, there is some evidence to suggest that these services are being abused by criminals. We are working with law enforcement to build a threat assessment and to understand the role these services play in the fraud ecosystem. We will conclude a rapid review of the market by the summer and take swift action on the back of this.
96. We will disrupt fraudsters' ability to spoof UK telephone numbers. Criminals frequently falsify or 'spoof' their numbers to hide their identity when calling and texting potential victims in order to pose as a legitimate organisation, such as our banks or a government agency. In May, new strengthened rules

come into force that will require all telephone networks involved in transmitting calls – either to mobiles or landlines – to identify and block spoofed calls, insofar as current technology permits. Ofcom have also set out clear expectations on the steps that phone companies should take, in accordance with their obligations, to prevent valid numbers being misused, and expect the companies to have a process for responding to reports of potential misuse.

97. We recognise that these measures will not stop all spoofed calls, and that scammers will continue to adapt their tactics. Ofcom will monitor the impact of these measures and will keep all options under review to clamp down on spoofed calls. To that end, Ofcom launched a consultation in April to consider the introduction of Calling Line Identification (CLI) authentication technology (and other measures) so that phone companies can certify that the number used for a call is legitimate. Measures like this will offer a more comprehensive solution to spoofed calls.
98. The Online Advertising Programme will build on the fraudulent advertising requirements in the Online Safety Bill. It will seek to strengthen the existing regulatory framework for paid-for online advertising to reduce harms, such as fraudulent and malicious advertising. The Department for Culture, Media and Sport (DCMS) is committed to tackling the most concerning harms facilitated by online advertising, including fraud, through a package of ambitious legislative and non-legislative reforms.

Financial firms will better protect their customers

- **Enable payment service providers (PSPs) to adopt a new risk-based approach to provide additional time for potentially fraudulent payments to be investigated.**
- **The FCA will undertake assessments of financial firms' fraud systems and controls.**

99. Customers and businesses have enjoyed many benefits from banking online and from being able to make payments quickly. At the same time, fraudsters have sought to exploit the ease of making payments to defraud individuals and businesses and rapidly move money to avoid successful repatriation of lost funds.
100. In response to this, under the supervision of regulators, the financial sector has invested in resourcing and new technologies to better identify and block suspicious payments. Key initiatives that have been taken forward to help prevent fraud are:

- **Strong Customer Authentication** – when customers buy something or make a payment online, the Payment Services Regulations 2017 mandate that all PSPs should verify their customers' identity. This helps to prevent fraudsters making unauthorised payments with someone else's details.
- **Confirmation of Payee** – a verification service that means a payer can see if the name of a payee matches the account details of the person they think they are sending money to. The Payment Systems Regulator (PSR) has issued several directions to extend the reach of Confirmation of Payee across industry to over 400 firms.
- **The Banking Protocol** – an industry initiative led by UK Finance, where bank staff are trained to spot when a customer is about to fall victim to an authorised fraud and work with the police to convince them not to make the payment.

101. Government, regulators and industry are working together to identify opportunities for greater information sharing to better tackle fraud 'up stream'. The PSR has called for shared standards on flagging risky payments to make data comparable. They have also set up an industry working group, including Pay.UK and UK Finance, to agree what data could be shared. As well as this, there are ongoing industry initiatives to share data. The Government and financial regulators welcome the action that is being taken to share relevant information and to use this data to stop fraud from happening in the first place.
102. While in the vast majority of cases data-sharing should enable suspicious payments to be identified in real-time, the Government and financial regulators recognise that in a small number of cases it may be beneficial for payments to be held beyond the usual timescales established in legislation in order to better protect customers. The Government is looking at how legislation might need to change in order to achieve this and has recently consulted on the best way to allow PSPs to adopt a risk-based approach to inbound and outbound payment processing. Such an approach would provide additional time for potentially fraudulent payments to be investigated, and for customers and even law enforcement to be engaged before a payment is executed. This will be done while minimising impacts on legitimate payment flows.
103. Tackling financial crime and, more specifically, Authorised Push Payment (APP) fraud continues to be a priority for the FCA and they continue to proactively consider a range of potential policy initiatives to tackle the scale and impacts associated with this type of crime, both for victims and the firms that they regulate.

104. In addition to their policy work, since January 2020, the FCA has been the anti-money laundering supervisor for crypto asset firms and the rules that apply to these firms have recently been updated, including to align with strengthened international standards.
105. The PSR is delivering a broad package of measures to help tackle the threat of authorised fraud, including measures to increase transparency by requiring the twelve largest PSP groups in Great Britain and the two largest in Northern Ireland to provide data on their performance in relation to APP fraud.

Secure people online at scale

- **NCSC will continue to prevent fraudulent material and attacks from reaching people while investigating further opportunities with industry to reduce the number of scams reaching the public.**
- **NCSC's new national "Share and Defend" hub will stop millions of fraud attempts from ever reaching consumers.**
- **Consult on creating new powers for law enforcement agencies to seize control and take down criminal, fraudulent websites.**

106. We will take down more fraudulent websites by expanding the National Cyber Security Centre's (NCSC) remit to work with financial institutions and tech companies. Currently, the NCSC works with internet service providers and mobile network operators to scour the internet for malicious websites and shares these with industry in real time so they can be removed. The NCSC will now share their findings with financial and tech companies to eliminate more fraud.
107. The internet has provided new opportunities for criminals and national security threat actors, but it also offers opportunities to keep the public safe. The NCSC, a part of the Government Communications Headquarters (GCHQ), is leading government's work to secure citizens and organisations online – at scale and in real time. This is a key commitment within the National Cyber Strategy and will significantly reduce the security burden on the public to act, making them more resilient while living and working online.
108. NCSC scours the internet for malicious websites and attacks, then works with industry to either remove them or, if they cannot be removed, enables them to be blocked from public reach. In the year 1 September 2021 to 31 August 2022, the NCSC identified and removed a total of 2.1 million malicious cyber campaigns.
109. Another way fraudsters reach people is through fraudulent emails. Spam filters have played an important role in reducing the volume of fraudulent emails reaching the public, but not all are caught. As of March 2023, NCSC

had received more than 19 million reports of suspicious emails and websites from the public, leading to the removal of more than 120,000 scams across 220,500 URLs since the service launched in April 2020. We recognise the harm associated with fraud from mass emails and will work with NCSC and industry to further investigate opportunities to reduce the number and impact of fraudulent emails reaching people's inboxes.

110. The NCSC continues to develop ways to protect the public online through the development of its Share and Defend capability. Launched last year, Share and Defend enables NCSC to share malicious websites with industry in near real time to protect the public at scale. Already half of all internet service provider (ISP) customers are able to benefit from this service, and by the end of this year, 80% will be covered.
111. At present, members of the sharing platform are the biggest UK ISPs and mobile network operators (MNOs) in the market. Our ambition is to expand this service to financial institutions and technology companies in the coming year. Alongside this, NCSC will continue to deliver their work to:
- Identify and remove malicious websites and attacks at scale.
 - Enhance repatriation of stolen customer credentials (e.g. credit cards) to providers.
 - Undertake initiatives to improve the security of the internet by working with industry to improve security practices.
 - Secure consumer accounts and devices by default through various initiatives with industry.
112. While the work of NCSC is invaluable in stopping frauds from reaching UK citizens, more needs to be done to enable the swift removal of domain names and IP addresses in cases where voluntary agreements do not work. We are consulting on the creation of new powers to enable law enforcement agencies to seize control and require the takedown of domain names and IP addresses where there is a suspicion of criminality, including fraud.

Pillar 3: Empower people

Fraud is not a victimless crime. Millions of people and businesses are targeted by fraudsters across the UK each year. Too many victims lose money and confidence. Some suffer health problems as a result. To stop people becoming victims and help them recover, we must empower them with the tools and knowledge to keep themselves safe and most importantly ensure they get their money back as quickly as possible.

Case study

Harry*, a barrister in his forties, got a call from a person claiming to be his bank's fraud prevention department about an attempt to hack his account earlier in the week. This rang true because he had received a suspicious message from a delivery firm requiring bank details for unpaid delivery costs that week. Harry was rushing as he was late to get home and was distracted. His immediate reaction was relief that the bank had picked up the issue and contacted him.

The caller said that there were suspicious transactions appearing on the account and described them. Harry had not made these payments and the caller said that to cancel the transactions he would need to read out the one-time passcode code he was being sent. Harry followed these instructions, and this continued a number of times until he became suspicious and hung up the call. The callers were fraudsters attempting to get around Harry's bank security measures. As Harry had given them the one-time passcode, they were able to access his account and transfer out £10,000.

*Name has been changed

113. Despite the prevalence of fraud, there is a widely held misconception that the victims of fraud are elderly or vulnerable. The reality is very different. Those most likely to be victims are between the ages of 45-54, although it is common across all age ranges.³⁰ Those in higher income brackets and those in managerial or professional occupations are a higher relative proportion of

³⁰ CSEW Nature of fraud and computer misuse in England and Wales Appendix Tables: Table 7

fraud victims.³¹ Similarly, those with no qualifications represent a lower proportion of victims than those who have them.

114. Despite our increasing efforts to stop fraud, it is unfortunately inevitable that some fraud attempts will still reach the UK public. Fraudsters will adapt and continue to look for weaknesses and vulnerabilities to exploit. The nature of these frauds will change as rapidly as technology does.

Better communications

- **Overhaul public anti-fraud communications by streamlining and amplifying them across law enforcement, government, non-profits and industry, and launching a simple cross-government campaign.**
- **Improve awareness and increase support by creating a new dedicated police PROTECT network, aligned with the Cyber PROTECT network.**
- **Ensure young people have key anti-fraud and cyber security skills by equipping teachers to deliver new anti-fraud lessons.**

115. The mistaken belief that only the vulnerable are at risk of fraud can lead to misplaced confidence, making some people less likely to take steps to protect themselves. Even when the danger is understood, ruthless fraudsters can emotionally manipulate victims into a state of panic to lower their defences.

116. There are numerous sources of anti-fraud communications across the private, public and voluntary sectors, such as campaigns from Action Fraud, Cyber Aware, ScamSmart, Friends Against Scams, and the UK Finance run Take Five to Stop Fraud. Although these have helped raise awareness of the threat, the proliferation of voices may have led to confusion about what to do. People do not always take action to protect themselves and others, and reporting rates remain low. Government, law enforcement, industry and civil society must unite behind clear, technically accurate and timely messaging so that the public know how to protect themselves from fraud and how to report it. Delivering clear, consistent and effective messaging at key touch points will enable millions more to act on protect advice, stopping fraudsters in their tracks.

117. We will launch a simple cross-government anti-fraud public awareness campaign to further unite messaging. This will make it easier for people to avoid fraud, and to know how to respond and recover if they have been scammed. This will help them protect others and reduce harm to themselves. We will also work in schools and communities to deliver the right messages to those at risk. The NCSC will continue to provide actionable,

³¹ CSEW: Property Crime Tables: Table 11 March 2020

technically accurate and timely advice and guidance on online security for the public.

Bolster victim support

- **Enhance and streamline how victims report fraud, starting with replacing Action Fraud with a state-of-the-art new system.**
- **Implement consistent support for victims across England and Wales by expanding the National Economic Crime Victim Care Unit and National Trading Standards' Multi-Agency Approach to Fraud.**

118. This Government is determined that all victims will get the support they need when they need it most. Simplifying the ways victims report fraud to the police, via Action Fraud, is integral to this. For too many, reporting fraud is a difficult process to navigate, with victims often unsure about how or why to report their experiences or having to repeatedly relive traumatic events. The same is true of recovering or protecting their identity when it has been stolen.

119. Action Fraud's National Economic Crime Victim Care Unit (NECVCU) reaches out to provide a tailored advice service to all victims referred to them. The NECVCU aims to assist victims to feel confident to cope and recover. Research has found that victims were satisfied with the service provided and felt safer, more aware of fraud and cyber crime, and more confident in the police's ability to respond to these crimes. The more vulnerable the victim, the higher the level of service they receive.

120. We are also keen to see vulnerable victims receiving more tailored support at a local level. Driven by the National Trading Standards (NTS) Scams Team, the national rollout of Multi-Agency Approach to Fraud (MAAF) within England and Wales is creating local hubs to bring key partners together to identify victims and ensure they get the support they need, from those best placed to provide it, including NTS, police, social workers or local charities.

121. With the SFO as law enforcement lead, we have established a Victims of Fraud Working Group (VFWG) that brings together leading organisations including NTS, Victim Support, Age UK and Cifas to encourage better system join up.

122. Improving victim support will help prevent re-victimisation, significantly reducing the volume and harm of fraud. The 18% of fraud victims who are repeat victims each year account for 35% of all fraud.³² By exploring what works best to help those most at risk, and reducing the number victimised again, we will improve outcomes for victims and reduce the harm of fraud.

³² CSEW calculation based on [Appendix tables](#) and [Demographics tables](#)

Improved victim support via the expanded NECVCU and MAAF will ensure more people get the help they need to avoid revictimisation, whilst the new Action Fraud service will encourage more victims to report the crime to access support and break the cycle.

Case study

Following a report to Action Fraud, an NECVCU victim advocate reached out to Alastair*, a retired engineer in his seventies with mental health issues. He had been caught in a sophisticated cryptocurrency scam. Initially investing a small amount in a seemingly legitimate company, he eventually lost £45,000 of savings. The fraudsters also took advantage of a bout of ill-health to persuade Alastair to give them control of his computer and rapidly applied for a loan of £25,000 in his name from a high-street bank, before transferring this to themselves via another high-street bank.

The NECVCU advocate, Sarah*, gradually built Alastair's trust. The victim was ashamed to discuss what had happened with his family. He reported feeling 'destroyed, even suicidal' from having lost his life savings and part of his pension. With continued encouragement from Sarah, he took advice from the police and organisations such as Mind and Victim Support. The victim agreed for Sarah to work with his daughter to put in place further preventative measures such as changing passwords, registering with Cifas and obtaining a credit report. They applied to the banks for reimbursement under the Contingent Reimbursement Model. In addition to this, Sarah arranged for his local police force to provide some advice and reassurance.

The banks have since refunded most of the money he'd lost and cancelled the loan. As a result of this, and NECVCU support, Alastair is feeling much better, more confident in spotting scams and feels he can now move on. Alastair told Sarah, *"Just as you said would happen - the scammers keep getting back in touch... I admit to being rather rude to some of them who hold on long enough to feel the full force of my contempt!"*

*Names have been changed

123. We are also supporting NTS to identify those most in need and provide effective interventions to prevent further re-victimisation. This includes supplying doorstep cameras to reduce the chance of victims being defrauded in their homes.
124. Learnings will be drawn from domestic abuse and coercive control to understand how to best support victims of fraud and eradicate the sense of shame they too often feel. This will include creating a toolkit to support practitioners in better assisting victims of fraud.

Protect identities from fraud

- **Establish a trusted and secure digital identity market in the UK through continued work by the Department for Science, Innovation and Technology (DSIT).**
- **Ensure victims of identity theft get the support they need to repair their identities and introduce an identity checklist outlining the steps needed to recover and secure a stolen identity.**
- **Explore new legislation to restrict creating and selling identities and the handling of data copied or obtained through unauthorised access.**
- **Stop people hiding behind fake companies by improving the validity of the information in the companies register and making greater use of it.**

125. Frauds can be extremely sophisticated and difficult for victims to spot. Phishing attempts have become a daily fact of life, with people being bombarded with fraudulent emails and messages. With rapid technological change continuing and fraudsters evolving their techniques, it is harder for the public to spot the genuine from the fraudulent. Many of these scam texts, emails and messages are just a way of harvesting data on individuals.
126. According to Cifas, the UK's largest cross-sector fraud information sharing database, around two thirds of fraud reported to them involves identity fraud. Criminals stealing personal information, more commonly known as identity theft, drives an industry where identities are stolen and sold for fraud. People who have had their identities stolen are often left unsupported to take action to repair their identities and reduce the impact of any frauds committed in their name.
127. New technology and legislation aimed at disrupting those stealing and selling data will make the internet a more hostile place for identity fraudsters. The Government is also working to enable the widespread use of trusted and secure digital identities, to help tackle identity enabled frauds.
128. Fraudsters also abuse the UK's framework for company registration and filing to commit crime. This includes through the creation of companies specifically to perpetrate fraud and the use of an individual or business's personal details or address without their consent, including to obscure ownership and control of a company.
129. The Economic Crime and Corporate Transparency Bill, which is currently before Parliament, will tackle these issues through greater powers for Companies House. New powers to check, challenge and decline dubious information, supported by stronger analytical and intelligence sharing capabilities, will make frauds easier to spot. Individuals whose addresses or

identities have been hijacked will no longer have to suffer further through lengthy administrative or court processes to rectify matters.

Change the law so more victims get their money back

- **Make sure more victims of authorised fraud get their money back by legislating to enable the Payment Systems Regulator (PSR) to require reimbursement by all PSR regulated payment service providers (PSPs).**
- **Evaluate and determine the next steps on ensuring a consistent framework for repatriation of fraud funds to victims.**

130. We are going to take measures to ensure more victims get their money back, while providing greater incentives to PSPs and other industries to prevent these frauds in the first place.

131. As criminals become ever more adept at persuading and grooming their victims to part with their money, it is becoming harder and harder for the public to spot real from fake. Under current regulations, victims of unauthorised fraud are entitled to be reimbursed by their bank within 48 hours. However, no such legal provision is in place for victims of authorised fraud, a fraud type that has grown significantly in recent years.

132. In 2019, nine firms voluntarily signed up to the “Contingent Reimbursement Model Code”, developed under the direction of the PSR. This code introduced a requirement on signatory firms to reimburse their customers when they had been tricked into handing over their money, where the customer could not reasonably have been expected to identify the fraud.

133. However, under this voluntary code, reimbursement rates are inconsistent (averaging around 50% of victims getting their money back), and the process can be protracted and at times difficult. To resolve this, the Government is legislating to enable the PSR to use its regulatory powers to require reimbursement by all PSR-regulated PSPs in relation to the Faster Payments System, where 97% of Authorised Push Payment (APP) frauds currently occur. The Government believes it is right that action is taken to place reimbursement on a mandatory footing without delay. This will be achieved via the Financial Services and Markets Bill.

134. There is currently no obligation for PSPs to attempt to repatriate money to fraud victims. Where firms seek to return funds to victims and originating banks, it can be difficult to identify a victim and there is competing precedents as to the approach to be adopted. Some firms however have higher risk appetites than others, which leads to inconsistent outcomes for victims. We will evaluate and determine the next steps on ensuring a consistent framework for repatriation of fraud funds to victims both in the UK and abroad.

Enhance key international and domestic capabilities

There are a number of cross-cutting issues and capabilities that must be explored and developed to enable delivery of the strategy. These include work with international partners, data sharing, and addressing money mule networks.

International capabilities and cooperation

- **Drive global action on fraud by making tackling it an internationally recognised priority for governments around the world, including by hosting a global fraud summit in the UK, chaired by the Home Secretary.**
- **Work bilaterally with key countries to strengthen their efforts to tackle fraud, agreeing new actions across government, including law enforcement and Foreign, Commonwealth and Development Office (FCDO) and its networks.**
- **Bolster our law enforcement presence in key source countries to build greater capability in those countries and work closely with upstream partners to disrupt more fraudsters.**

135. Fraudsters operate across borders, causing billions of pounds in losses annually for the UK and posing a significant threat to global economic prosperity. Yet so far, we have found that fraud is under-prioritised globally, with the UK having one of the most advanced and comprehensive responses. This new strategy cements our position as a world leader on fraud.
136. Our goal is to create a comprehensive and sustainable international approach to combatting fraud, that will help protect the global community from its devastating effects and promote greater prosperity and security for all.
137. We know this will be difficult. Many countries do not understand the impact fraud has on their economy or international standing. Some may even be financially benefitting from it. Over this coming year, we will work in collaboration with key partners to develop a systematic and evidence-based approach.

A fraud summit to build the international consensus for action

138. It is vital that we make every country see they have a part to play in tackling fraud. Currently, there is no multilateral, co-ordinated, policy level response to fraud against individuals and businesses. The UK is recognised as a leading partner placing us in the strongest position to lead a multilateral response.
139. We will raise the priority of fraud on the international political stage, starting with a global fraud summit in 2024. We will create a new international consensus to tackle fraud, as we have done on other threats, such as child sexual abuse and exploitation, learning from the collaborative approach taken on illicit finance between international industries and governments, especially with the Five Eyes countries.

Case study

Singapore, a key partner of the UK, established their domestic Anti-Scam Command (ASCom) in March 2022. The ASCom partners - and on occasions co-locates with - local and foreign banks, card security groups, non-bank financial institutions, Fintech companies and cryptocurrency houses, as well as remittance service providers in Singapore. Through these partnerships, the ASCom and its partners have been able to swiftly freeze accounts, recover funds and reduce losses suffered by victims. For example, on 2 May 2022, the ASCom worked with DBS Bank to seize US\$10 million.

140. Our first step towards this has been to establish an international working group, the first of its kind. We will also raise fraud at multinational fora including the Roma-Lyon Group (G7) at Hiroshima in May and at the United Nations.
141. Our global summit will bring together leaders from governments, law enforcement, and the private sector, to announce the ambition to deliver a comprehensive and coordinated approach to tackling fraud over the next 5 years. The outcomes of the summit will include a shared understanding of the nature and scope of the fraud threat, the identification of best practices for preventing and responding to fraud, and the proposal to develop a coordinated action plan to dismantle fraud networks.
142. We are committed to taking a leadership role in this effort, and we will work closely with our international partners to achieve this.

Drive action in key countries of risk

143. The fraud threat to the UK is varied, with some international jurisdictions more commonly reported as connected to certain types of fraud than others. Romance fraud is still commonly seen from countries in West Africa, whilst

call centre enabled fraud is commonly linked to South Asia. Investment frauds can emanate from the UK, but are also reported from across different parts of Europe and as far as South East Asia.

Case study

A joint operation between the UK and Ghana into romance fraud resulted in the conviction of a number of criminals in Ghana and the repayment of stolen money to UK based victims. Following investigation in the UK by local and national investigators, and working with the NCA International Liaison Officer and Ghanaian police, 28 victims were identified. Local UK forces provided victim care and advice, while the Ghanaian courts allowed £195,000 to be repatriated to victims. This has led to a strengthened partnership in combatting romance fraud between Ghanaian and UK law enforcement.

144. We will assess with the NCA and FCDO both where frauds may be coming from, and those countries that can help us have the greatest impact on tackling it. Based on these assessments, we will agree across government the actions required to support top jurisdictions of risk to do more to tackle fraud and work with our overseas networks to deliver this. These actions will cover multi-year, long term aims aligned to the Fraud Strategy. These include:

Pursue fraudsters

- Strengthening our understanding of source countries where fraudsters, or infrastructures used for fraud, are located.
- Developing intel-led country action plans to cover the highest priority countries, focusing on proposals such as building law enforcement capacity, victim support capabilities, cyber security responses and asset recovery processes.
- Building on successful law enforcement operational activity in source countries by partnering with relevant agencies to effectively combat fraud and replicate success in other countries.

Block fraud

- Driving forward an international public-private partnership to make coordinated asks of global companies to do more to tackle fraud online, e.g. the tech sector.
- Harmonising legal frameworks and regulations across countries to ensure that fraudsters cannot take advantage of loopholes or inconsistencies.
- Promoting the use of secure payment methods in other countries to reduce the risk of fraud and protect personal and financial information.

Empower people

- Sharing best practice and expertise in developing awareness campaigns to educate individuals and businesses about the dangers of fraud and how to recognise and avoid scams.
- Providing training and capacity building programs for law enforcement agencies and civil society organisations in other countries to enhance their ability to prevent and respond to fraud.
- Supporting the development of fraud reporting and victim support systems in other countries to ensure that people who have been targeted by fraudsters have the access to the help and support they need.

Data sharing and cross-government capabilities

- **Government will continue to work with all sectors and partners to maximise data sharing mechanisms, including through legislation.**
- **Support the Public Sector Fraud Authority by sharing data and threat assessment insight.**

145. Government is addressing some of the legal challenges to information sharing raised by industry partners. The Economic Crime and Corporate Transparency (ECCT) Bill will introduce provisions to disapply civil liability – in particular, for breach of confidentiality – for anti-money laundering (AML) regulated firms who share customer information with each other for the purposes of preventing, detecting and investigating economic crime. The provisions will allow direct sharing of information between two businesses in the AML regulated sector, as well as indirect sharing through a third-party intermediary for businesses in the financial sector. Government will continue to work with all sectors and partners to maximise data sharing mechanisms.

146. In the second Economic Crime Plan (2023-2026), government has committed to develop and implement a Public Private Economic Crime Data Strategy by mid-2024 ³³ that enhances the exploitation of available data across the ecosystem to better prevent, detect and pursue economic crime. The strategy will encompass the governance, prioritisation, and technical changes necessary to manage data better across the system.

147. We will also forge closer engagement between those responsible for preventing fraud directed at the public sector, and those responsible for preventing the defrauding of private individuals and businesses. Broader

³³ [Economic Crime Plan 2 2023-26 \(publishing.service.gov.uk\)](https://publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1154442/Economic-Crime-Plan-2023-26.pdf)

collaboration across the public sector fraud response is led by the Public Sector Fraud Authority.

Addressing money mule networks

- **Publish a new cross-sector money mules action plan to disrupt money mule activity and protect the public.**

148. Fraudsters rely on networks of ‘mule’ accounts to extract and move the money taken from victims. Transactions can pass through financial institutions, or be turned into cash or cryptocurrencies, to disguise the trail before delivering the proceeds to the criminal group. Money mule networks play a significant and growing role in enabling fraud. In 2022, banks identified over 39,000 accounts indicative of mule activity.³⁴ There is also a risk to the public, who are recruited to supply the mule accounts, and may be lured into crime through promises of low risk, easy cash fake ‘jobs’. People are taken advantage of by criminals, and sometimes children are exploited in this way.

149. We will disrupt this crucial money laundering technique and protect the public by delivering a co-ordinated response from government, regulators, law enforcement, industry and organisations working with young people. This will bring together campaigns and education to raise public awareness of the risks of getting involved, innovation by the financial sector to identify mule networks and freeze funds, law enforcement work to target the mule recruiters and controllers, and action by social media companies to close down recruitment routes, balancing deterrents and safeguarding for identified money mules.

³⁴ CIFAS: Fraudscape 2023

Delivery: how we will make this happen

Delivery of the strategy will require close working, coordination and cooperation with partners across the system; utilising the unique capabilities of every partner, each of whom will play a specific and vital role.

Delivery of the strategy is phased over a 3-year programme of work to the end of 2025, led and governed by the Home Office. The Home Office and Home Secretary will have overall accountability for delivery of programme outcomes, with delivery partners responsible for implementing specific elements of the programme. Each relevant Secretary of State has accountability for delivery of the elements within their department's remit, with the Security Minister responsible for leading cross-partnership engagement and delivery, including leadership of cross-sectoral industry engagement through the Joint Fraud Taskforce (JFT). Programme delivery activity for all actions in the strategy is either currently being mobilised or already in progress.

Our delivery partners

150. This strategy will be delivered in close partnership with three stakeholder groups:

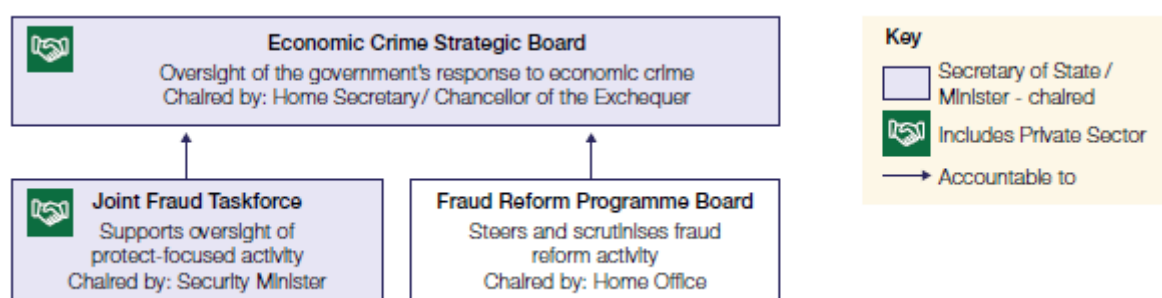
1. Cross-government partners, agencies and regulatory authorities including:
 - Home Office
 - The UK Intelligence Community (UKIC)
 - HM Treasury (HMT)
 - Department for Science, Innovation and Technology (DSIT)
 - Department for Culture, Media and Sport (DCMS)
 - Department for Business and Trade (DBT)
 - Ministry of Justice (MoJ)
 - The Foreign, Commonwealth and Development Office (FCDO)
 - Crown Prosecution Service (CPS)
 - HM Courts and Tribunals Service (HMCTS)
 - The Financial Conduct Authority (FCA)
 - The Payment Systems Regulator (PSR)
 - Ofcom

- The Public Sector Fraud Authority
2. Law enforcement partners:
 - The National Economic Crime Centre (NECC)
 - The National Crime Agency (NCA)
 - The Serious Fraud Office (SFO)
 - The City of London Police force (in its role as lead police force for fraud)
 - Regional Organised Crime Units (ROCUs)
 - Local police forces
 3. Partners across industry and the private sector.
151. The Security Minister is responsible, including through leadership of the Joint Fraud taskforce (JFT), for cross–government and industry partnerships necessary to deliver the departmental commitments of this strategy, with Secretaries of State accountable for the elements of the Strategy within their Department’s remit.

Governance and oversight

152. A programme board has been established to steer and govern delivery of the strategy, monitor progress, oversee the outcomes and manage key risks relating to reform. The board is chaired by the Home Office Director General for Homeland Security with representation from all delivery partners across government and law enforcement. The programme board is overseen by the JFT.
153. This will be supported by local governance infrastructures set up by delivery partners and will work alongside operational governance bodies. Sitting on the JFT and working multilaterally, the Anti-Fraud Champion, Anthony Browne MP will operate between these structures to drive collaboration.

Figure 6 – Governance to deliver the Fraud Strategy



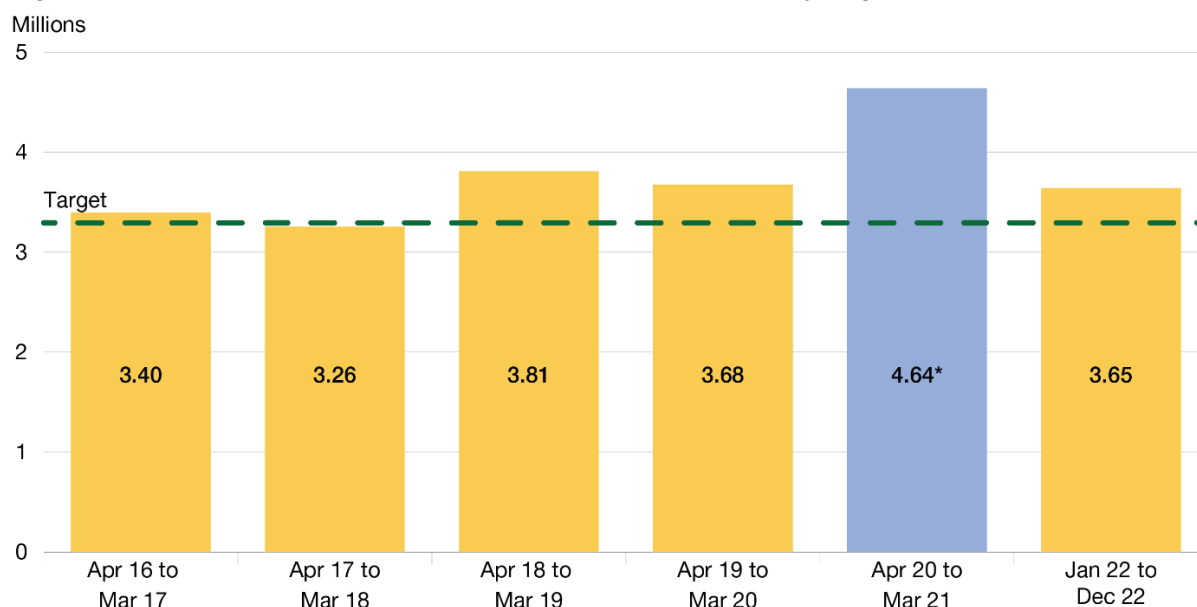
How we will measure success

154. Fraud has returned to pre-pandemic levels as shown in the figure below. Based on the latest figures available from the Office of National Statistics (ONS), in the year to December 2022 there were 3.7 million frauds estimated. **Our ambition is to cut fraud by 10% from 2019 levels**, down to 3.33 million frauds by the end of this Parliament. We will prevent over 300,000 frauds through Pursue interventions alone.

155. The Home Office will continue to engage with industry, academic experts and stakeholders to strengthen the data and measures to track progress. An outcomes framework will be developed in line with action 43 of the Economic Crime Plan 2 to ('develop an outcomes framework for the Economic Crime Plan 2')³⁵ and will track progress against our aims.

156. The Home Office will begin work on an Evaluation Strategy as a key analytical product to help build the evidence base around fraud and the interventions that work to combat it. This will include a clear articulation of the theory of change underlying the fraud strategy which sets out how and why a desired change is expected to happen, exploration of the current landscape of evaluation, an assessment of what evaluation methodologies could be used at this time and a road map setting out what is needed to build evaluation capability.

Figure 7 – Incidents of Fraud 2016/17 to 2021/22 from Crime Survey England and Wales



Source: Appendix tables, year ending December 2022, CSEW

*TCSEW

³⁵ [Economic Crime Plan 2 2023-26 \(publishing.service.gov.uk\)](https://publishing.service.gov.uk)

Annexes

Annex 1: Links with other government strategies

This strategy sits alongside a range of other government strategies and plans that address fraud and other key threats. This section outlines our dependencies across these different strategies.

Economic Crime Plan

The Economic Crime Plan (ECP) 2019-22, published in 2019, agreed a set of public-private sector actions to strengthen our response to economic crime. As part of the March 2021 Statement of Progress we set out short-term goals to kick-start our push on fraud. A new plan was published in 2023. It is the overarching economic crime policy document and summarises the approach of the Fraud Strategy, as well as setting out our approach to tackling wider economic crime including money laundering, kleptocracy and sanctions evasion, and to increase asset recovery from criminals. Within the refreshed Economic Crime Plan are cross-cutting, complementary approaches to driving down fraud, such as tackling money mule network recruitment and use, cryptocurrency and general overlapping illicit finance, and economic crime capabilities and programmes.

National Cyber Strategy

The National Cyber Strategy (NCS) 2022-25, published in December 2021, signals a shift to a more comprehensive national cyber approach, drawing together our capabilities inside and outside government. The strategy is guided by the 5 pillars on strengthening our cyber ecosystem, building resilience, investing in technology, advancing global leadership, and disrupting our adversaries in cyberspace. By improving our resilience to cyber threats, and our ability to respond to them, delivery of the NCS will have a significant impact on cyber facilitated fraud.

Beating Crime Plan

The Beating Crime Plan (BCP), published in 2021, sets out the Government's overall approach to tackling crime and keeping the public safe. It outlines the key means by which it will do this, including by building capability and capacity to deal with fraud and online crime. It previews the Fraud Strategy, indicating our intent to restrict opportunities for fraudsters, protect victims and prosecute the criminals that have committed these harmful crimes. The Fraud Strategy provides the details by which this will be achieved.

Integrated Review

The Integrated Review (IR), published in 2021, focussed on positioning Global Britain to tackle the most serious threats that affect the country's sovereignty, security, and prosperity. The Integrated Review Refresh 2023 updates the Government's security, defence, development and foreign policy priorities to reflect changes in the global context since then. The refreshed IR recognises the importance of fraud as an issue of national security and the importance of the Fraud Strategy in stopping the exploitation of the UK's financial systems and economic openness for domestic and international criminality and corruption. It also highlights the importance of securing the cyber space and protecting the country from transnational harms. The Fraud Strategy details how the country will develop global leadership in tackling this threat, as well as bolstering cyber resilience to fraud threats.

Serious and Organised Crime Strategy

The UK's Serious and Organised Crime Strategy, published in 2018, sets out the UK Government's approach to tackling serious and organised crime, alongside law enforcement, the public sector and the private sector. As a significant driver of serious and organised crime levels and cost to the UK, tackling fraud was identified as a priority, with a particular emphasis placed on designing out fraud from systems and processes that the public rely on, as well as enhanced support for victims and vulnerable people. This emphasis has been expanded as part of the Fraud Strategy but remains at the heart of our approach.

Digital Strategy 2022

The Digital Strategy, published in 2022, is a cross government strategy which sets out the Government's ambitious agenda for digital policy. The Digital Foundation section, which is aimed at strengthening the foundations of the digital economy, includes policies focussed on enabling trusted and secure digital identities, making it easier to verify identities online and share verified identities with trusted partners. Impersonation and identity theft is a key means for fraudsters to commit their crimes and forms an important part of the Fraud Strategy.

Tackling Public Sector Fraud

As set out, we will support those tackling fraud against the Exchequer. There are a number of different government strategies and plans to improve our response to those taking money from the public purse. DWP published its command paper, Fighting Fraud in the Welfare System, in May 2022. It sets out government's plans to address the challenge of fraud, to stay ahead of evolving threats and to reduce the levels of fraud and error in the welfare system through an enhanced front-line operation, taking new powers, when parliamentary time allows, to strengthen government's ability to detect, investigate and punish fraudsters, and bringing together full force of government and the private sector to work collectively to tackle fraud. HMRC is uniquely funded by HMT to deliver the UK's

response to attacks on the tax system and tackle those that deliberately and dishonestly set out to defraud HMRC by evading tax, stealing public funds or cheating the system in other ways. The PSFA will publish a Four-Year Functional Strategy that will set out central government's response to fraud against the public sector.

Anti-Corruption

Development of a new UK Anti-Corruption Strategy is underway with publication expected in 2023. The new Strategy will build on the progress made by the UK Anti-Corruption Strategy 2017-2022 and outline the UK response to strengthen resilience against corruption and illicit finance in the UK and internationally. Corruption and illicit finance undermines national security and global stability, it impedes global prosperity and it erodes trust in institutions while harming its victims. The new Strategy is being developed to combat this threat.

Annex 2: Geographic scope

There are differences in how fraud is dealt with in law across the four nations of the UK. England, Wales and Northern Ireland are covered by the Fraud Act 2006, whereas fraud in Scotland is predominately dealt with as an offence in common law. Policing and criminal justice matters are devolved in Scotland and Northern Ireland.

England & Wales

City of London Police are the national lead force for fraud in England and Wales. They coordinate the reporting, victim support and investigative response to fraud.

There is limited Welsh devolution in the fraud landscape, however, the Welsh government continues to work in partnership with UK government on fraud, including through attendance at the Joint Fraud Taskforce.

Northern Ireland

In Northern Ireland, the Department of Justice is responsible for devolved policing and justice functions, including criminal justice policy, which falls within the competence of the Northern Ireland Assembly. The Police Service of Northern Ireland (PSNI) is the single police service in Northern Ireland and is the lead operational agency for serious and organised crime, working closely with the NCA, HMRC and other relevant agencies. The Public Prosecution Service for Northern Ireland is the prosecuting authority.

The Organised Crime Task Force (OCTF) is an important forum in the fight against organised crime in Northern Ireland. The OCTF brings together law enforcement agencies and relevant government departments and provides strategic leadership for a collective and collaborative response to the threat posed by organised crime in Northern Ireland. Private sector engagement is carried out under the OCTF structures. The work of the OCTF also focuses on collective Pursue and Protect activities to tackle fraud linked to organised crime, key priorities under the Northern Ireland Organised Crime Strategy.³⁶

Fraud and related cyber crime incidents in Northern Ireland are generally reported to Action Fraud or to the PSNI in specific circumstances. Northern Ireland has an established 'Scamwise NI Partnership', chaired by the PSNI, which brings together over 45 organisations with the shared ambition of combatting the threat of fraud. The organisations involved include representatives from faith groups, youth organisations, and the charity sector, in addition to government departments, law enforcement and private sector stakeholders. The work of the partnership includes awareness campaigns to inform the community about the risk and range of scams, and information sharing between organisations.

The Northern Ireland Department of Justice attends the Joint Fraud Taskforce.

³⁶ [Organised Crime Strategy | Northern Ireland 2021-2024 \(octf.gov.uk\)](#)

Scotland

In Scotland, the Crown Office and Procurator Fiscal Service, which operates under the authority of the Lord Advocate, is the prosecuting authority responsible for the investigation and prosecution of crime. Police Scotland is the single police service in Scotland, which works closely with the NCA, HMRC, the FCA and other relevant agencies in investigating economic crime. Scotland is outside the jurisdiction of Action Fraud and the Serious Fraud Office, unlike the rest of the UK. Fraud in Scotland is typically reported directly to Police Scotland, who hold responsibility for fraud investigations. The Scottish Government published a Scams Prevention, Awareness and Enforcement Strategy in March 2021. The strategic framework, as set out in the strategy, supports both protect and pursue activities that seek to reduce the ability of scammers to target and carry out scams and to reduce the severity of consequences when a scam is successful. Alongside the strategy, the Scottish Government also established the 'Scottish Scams Strategic Partnership' which brings together a number of public and private partners to adopt a shared voice and take forward collective advocacy on key issues in relation to scams prevention, awareness and enforcement.

Scottish Government officials attend the Joint Fraud Taskforce.

Annex 3: Cost of fraud methodology

The economic and social cost of fraud estimate helps to identify and indicate the scale of the wider impacts of fraud offences. To calculate this, the costing framework from 'The Economic and Social Costs of Crime' (Home Office, 2018) has been applied.³⁷ This updated estimate captures the impact of fraud against individuals in England and Wales in 2019/20.

This annex sets out the approach taken to estimate the economic and social cost of fraud. Although the cost of fraud can be separated from the total cost of crime, the calculation framework means that it has been calculated simultaneously with the cost of other crime types, for example homicide. To allocate costs to the different crime types, the methodology at times relies on the relative severity of fraud in comparison to the other crimes included within 'The Economic and Social Costs of Crime' (Home Office, 2018). Therefore, the estimate quoted below cannot be calculated using the information provided in this annex alone.

Scope

Various estimates exist of the cost of fraud to the UK, which differ in scope and methodological approach. The economic and social cost of fraud estimates the impact of fraud against individuals in England & Wales. Due to data constraints, the cost of fraud offences committed against businesses and the public sector are out of scope of this estimate.

The estimate is based in the financial year 2019/20. This avoids the use of cost and volume estimates that are affected by the COVID-19 pandemic.

The estimate captures three main cost areas:

1. Costs in anticipation of fraud e.g., the fraud prevention implemented by banks.
2. Costs as a consequence of fraud e.g., the value of financial losses and emotional harm.
3. Costs in response to fraud e.g., costs to the police of investigating a crime.

The costs are calculated from a victim-based perspective, and do not include wider impacts on indirect victims (for example, the emotional harms experienced by friends and family of the victim). The totality of preventative activity taken by industry against fraud has

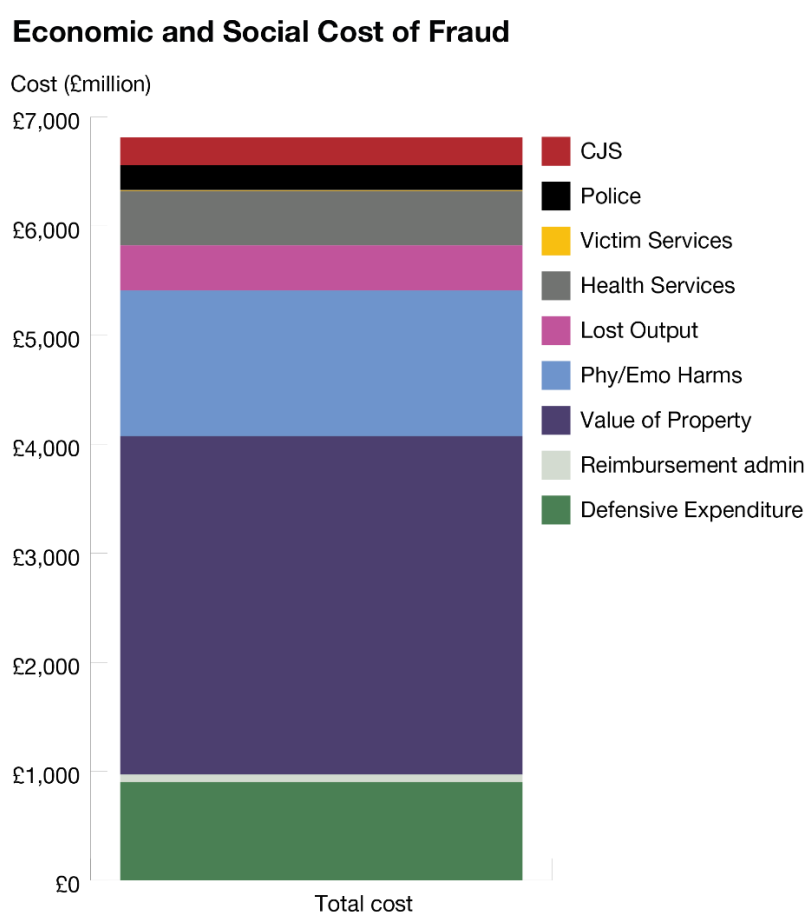
³⁷ Home Office (2018) 'The Economic and Social Costs of Crime, Second Edition'
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/732110/the-economic-and-social-costs-of-crime-horr99.pdf

also not been considered. The cost captured in this analysis is therefore partial and will be an underestimate of the true impact of fraud on society.

Total Cost

The total economic and social cost of fraud to individuals is estimated to be £6.8 billion (2019/20). There were an estimated 3,675,000 fraud offences in 2019/20.³⁸ The largest cost area contributing to the total cost is the financial loss (~£3.1bn), followed by the emotional harms experienced by victims (~£1.3bn). These are both categorised as ‘costs as a consequence’ of crime.

Figure 8 – Breakdown of economic and social cost of fraud 19/20.



Methodology

Volume of Fraud Offences

The Crime Survey England and Wales provides estimates for the number of fraud offences against individuals. In 2019/20, this was estimated at 3,675,000.³⁹

³⁸ [Crime in England and Wales - Office for National Statistics \(ons.gov.uk\)](https://ons.gov.uk/crimeandjustice/crimeandjusticeinenglandandwales)

³⁹ [Crime in England and Wales - Office for National Statistics \(ons.gov.uk\)](https://ons.gov.uk/crimeandjustice/crimeandjusticeinenglandandwales)

Costs in anticipation

Anticipation costs are incurred prior to the incident. There are two costs estimated: defensive expenditure and reimbursement administration.

1. **Defensive expenditure** is defined as money individuals and businesses spend on crime detection and prevention. For fraud, this encompasses expenditure by banks on anti-fraud operations to protect their customers from fraud.⁴⁰ The total cost of defensive expenditure protecting individuals against fraud is estimated to be £0.9 billion in 2019/20.
2. **The administration cost** of setting up and subsequently processing crime-related insurance and reimbursement claims is an opportunity cost of the employees (e.g., premises, salary, and equipment costs) when they could be engaged in other productive activities in society.⁴¹ It is assumed that the value of fraud claims reimbursed is directly related to the amount of administration required. The opportunity cost of processing reimbursements for fraud incidents against individuals is estimated to be £0.07 billion in 2019/20.

Costs as a consequence

These capture costs borne directly after the crime has occurred. All costs are from a victim-perspective and include the financial loss, emotional harms, lost output, health services, and victim services.

1. **Value of property loss** - The CSEW publishes information on the nature of harm of fraud offences against individuals, which includes information on financial loss suffered by victims of fraud.⁴² This data is adjusted to estimate the total financial loss experienced by victims of fraud in 2019/20. The total financial loss due to fraud incidents against individuals is estimated to be £3.1 billion in 2019/20. This data set has been used in recognition that losses from recorded offences alone are likely to be an underestimate.
2. **Emotional harm** - Some victims of fraud experience emotional harms, as per The Economic and Social Costs of Crime (Home Office, 2018) a Quality Adjusted Life Years (QALY) approach is applied to monetise the emotional impacts of anxiety, depression, and fear on victims. The CSEW publishes information on the number of victims experiencing specific emotional harms as a victim of fraud.⁴³ The total

⁴⁰ UK Finance (2020) 'Written evidence submitted by UK Finance'.
<https://committees.parliament.uk/writtenevidence/18646/pdf/>

⁴¹ Fraud reimbursement pay-outs are ignored as they do not represent a cost to society; pay-outs are a transfer of money between an individual and business, and vice versa. The financial loss of fraud is captured in the 'Costs as a consequence' section.

⁴² ONS (March 2020), [Nature of crime: fraud and computer misuse - Office for National Statistics \(ons.gov.uk\)](https://ons.gov.uk)

⁴³ ONS (March 2020), [Nature of crime: fraud and computer misuse - Office for National Statistics \(ons.gov.uk\)](https://ons.gov.uk)

emotional harm caused to direct victims of fraud is estimated to cost £1.3 billion in 2019/20.

1. **Health Services** - Treatment for the emotional harms incurred by victims of fraud may be required, and therefore if fewer people were harmed through crime, the resources used to treat them could be used in alternative activities. This cost estimate aims to reflect the health service cost by considering the probability of experiencing the harm⁴⁴ alongside the cost to the NHS to provide treatment such as counselling. The total cost of treating direct victims of fraud is estimated to be £0.5 billion in 2019/20.
2. **Lost output** - There may be a reduction in economic activity as a result of an individual being a victim of a crime. To estimate this cost, a similar approach to The Economic and Social Costs of Crime (Home Office, 2018) is applied, updating inputs where possible e.g. salary and hours worked. The total lost output from direct victims of fraud is estimated to be £0.4 billion in 2019/20.
3. **Victim services** - To estimate a total cost, the total expenditure on Victim Services is derived from Ministry of Justice (MoJ) funding for the Police and Crime Commissioners to commission victim services and funding for the Citizens Advice to deliver the National Witness Service. This is split into expenditure targeted at different crime types, including fraud, using the relative proportion of total emotional costs attributed to each crime type (as estimated in the physical and emotional harms section above). The total victim services cost to victims of fraud is estimated £3 million in 2019/20.

Costs in response to crime

Fraud offences can result in a cost to law enforcement agencies. This cost depends on the number of offences investigated and charged. The cost is split into two areas of response: Police and other Criminal Justice System (CJS) costs.

1. **Police costs** are incurred when the Police deal with and investigate crimes. The total 2019/20 central Police budget is split out into different activities the Police perform (both crime and non-crime) using 'activity-based costing' (ABC) data provided by Police Forces (2006/07). These activities include a breakdown of the estimated cost of dealing with different crime types, including fraud, and associated overheads. The budget does not include the cost of agencies outside of the Police that will investigate fraud incidents (e.g. National Crime Agency, Serious Fraud Office, Financial Conduct Authority). The police budget allocated to dealing with fraud incidents is estimated to be £0.2 billion in 2019/20.

⁴⁴ONS (March 2020), Nature of crime: fraud and computer misuse - Office for National Statistics (ons.gov.uk)

2. **The CJS (excluding police)** cost captures areas relating to charging and prosecuting, which are described below. The total cost to the CJS is estimated at £0.3 billion in 2019/20.

2.1 **Crown Prosecution Service (CPS)**

The CPS is responsible for prosecuting criminal cases that have been investigated by the police and other investigative organisations in England and Wales. The resource required to deal with the CPS caseload is costed using the CPS Gross Operating Expenditure.

2.2 **Court and Jury**

All court cases start in the Magistrates' court with the most serious cases being subsequently escalated to the Crown court where a jury will hear the case. The Crown and Magistrates cost is estimated using the cost per sitting day of a case and volumes of court cases, and – for Crown court cases – the opportunity cost of jurors.

2.3 **Legal Defence**

Legal assistance can provide legal advice, mediation and representation in court. This support is provided by either Legal Aid or through private defence. The number of cases that are supported via Legal Aid relative to private defence and the respective cost per case is used to estimate the total cost of defence for fraud cases.

2.4 **Probation Service**

Probation is a sentence that is not being served in prison. This can be community sentences or prison release on license or parole. The cost includes probation officers who supervise and support individuals on probation.

2.5 **Prison Service**

Offenders may be sentenced to prison for serious fraud offences. The cost of incarceration is estimated using the MoJ's annual cost per prison place and prison statistics.⁴⁵

2.6 **Youth Offending Teams**

The costs of youth offenders are incorporated in the above CJS costs, except for Youth Offending Teams. Youth Offending Teams support and supervise young people who are arrested, charged, convicted with an offence. This is estimated using the total Youth Offending Team budget in 2019/20.

⁴⁵ MOJ (March 2020) Prison Performance Ratings: 2019 to 2020 GOV.UK (www.gov.uk) and Criminal justice system statistics quarterly: March 2020 - GOV.UK (www.gov.uk)

Cost Area	Cost (£bn)	Calculation	Key inputs
Total	£6.80		
Defensive Expenditure	£0.90	Cost of Tackling Fraud	UK Finance (2020), <u>'Written evidence submitted by UK Finance'</u> . https://committees.parliament.uk/writtenevidence/18646/pdf/
Reimbursement Administration	£0.07	Total fraud reimbursements * Proxy for relative administration cost to total reimbursement ratio	UK Finance (2022), <u>Annual Fraud Report 2022 Policy and Guidance UK Finance</u> Unpublished data provided directly by the Association of British Insurers (ABI) for 2019 (administration costs) and 2019/20 (value of claims).
Financial Loss	£3.10	Sum (volume of CSEW Value of Loss band * Mid-point of band)	ONS (March 2020), <u>Nature of crime: fraud and computer misuse - Office for National Statistics (ons.gov.uk)</u>
Emotional Harms	£1.30	CSEW fraud volume * (CSEW likelihood of sustaining harm * Value of a Life Year * Reduced Quality of Life * Duration of harm)	ONS (March 2020), <u>Nature of crime: fraud and computer misuse - Office for National Statistics (ons.gov.uk)</u> HMT (2021), <u>Green Book</u> Home Office (2018), <u>'The Economic and Social Costs of Crime, Third Edition'</u>
Health Services	£0.50	CSEW fraud volume * (CSEW likelihood of sustaining harm * average number of hours of counselling required * cost of a counselling hour)	ONS (March 2020), <u>Nature of crime: fraud and computer misuse - Office for National Statistics (ons.gov.uk)</u> Curtis and Burns (2020), <u>Unit Costs of Health and Social Care 2020 PSSRU</u>

			Home Office (2018), <u>'The Economic and Social Costs of Crime, Third Edition'</u>
Lost Output	£0.40	Employment rate * [(Hours taken off work * Median hourly salary) + [(Duration of harm – Hours taken off work) * Proxy for reduced productivity * Median hourly salary]] * CSEW volumes	ONS (March 2020), <u>Crime in England and Wales: Annual Trend and Demographic Tables - Office for National Statistics (ons.gov.uk)</u> Home Office (2018), <u>'The Economic and Social Costs of Crime, Third Edition'</u> ONS (March 2020), <u>Earnings and hours worked, all employees: ASHE Table 1 - Office for National Statistics (ons.gov.uk)</u> ONS (March 2020), <u>Nature of crime: fraud and computer misuse - Office for National Statistics (ons.gov.uk)</u> Home Office (2018), <u>'The Economic and Social Costs of Crime, Third Edition'</u>
Victim Services	<£0.1	Victim Service total cost * Relative emotional harm and volume factor	MoJ (2019), <u>Victim and witness funding awards - GOV.UK (www.gov.uk)</u> Citizens Advice (2021), <u>The impact of the Witness Service - Citizens Advice</u> ONS (March 2020), <u>Nature of crime: fraud and computer misuse - Office for National Statistics (ons.gov.uk)</u>
Police Costs	£0.20	2019/20 Police budget * Relative Police Activity Based Costing for fraud in 2006/07 compared to all Police Recorded Crime	Home Office internal Activity Based Costing (ABC) data (2006/07) Home Office (2018), <u>'The Economic and Social Costs of Crime, Third Edition'</u> Police Recorded Crime, <u>Police recorded crime and outcomes open data tables - GOV.UK (www.gov.uk)</u> Home Office Police Funding (July, 2021), <u>Police funding for England and Wales 2015 to 2022 - GOV.UK (www.gov.uk)</u>

CJS Costs	£0.30		
CPS		CPS expenditure * Complexity weighting for fraud (Fraud relative proportion of court hearing time * proportion of CPS volumes)	CPS (2019/20) Bespoke data on CPS caseload provided by CPS ONS (July 2022), <u>Crime Severity Score (Experimental Statistics)</u> - Office for National Statistics (ons.gov.uk). ONS (March 2020), <u>Crime in England and Wales: Appendix tables</u> - Office for National Statistics (ons.gov.uk)
Jury Service		No. of sitting days * No. of hearings * No. individuals on a jury * % Employed/Unemployed * Wage Employed/Unemployed	ONS (March 2020), <u>Earnings and working hours</u> - Office for National Statistics (ons.gov.uk) ONS (December 2020), <u>Index of Labour Costs per Hour, seasonally adjusted</u> - Office for National Statistics (ons.gov.uk) Department for Transport TAG Data Book (January 2023), TAG data book - GOV.UK (www.gov.uk)
Courts		No. of sitting days per hearing * Cost per sitting day * No. of hearings	MOJ (June 2022) <u>Criminal court statistics quarterly: January to March 2022</u> - GOV.UK (www.gov.uk) MOJ Internal Data, (March 2020)
Probation		Fraud Probation Total Cost (2015/16) inflated to 2019/20 prices	Home Office (2018), <u>'The Economic and Social Costs of Crime, Third Edition'</u> GDP Deflator, <u>GDP deflators at market prices, and money GDP November 2022 (Autumn Statement)</u> - GOV.UK (www.gov.uk)
Prison		Vol. sentenced * Av. sentence length * Av. proportion of sentence served * Cost per prisoner per year	MOJ (March 2020), <u>Criminal justice system statistics quarterly: March 2020</u> - GOV.UK (www.gov.uk) MOJ (March 2020), <u>Prison Performance Ratings: 2019 to 2020</u> - GOV.UK (www.gov.uk)
Youth Offending Teams		Relative no. of fraud offences * Relative severity of fraud offences * Youth Justice service budget	MOJ (March 2020), <u>Youth Justice statistics: 2019 to 2020</u> - GOV.UK (www.gov.uk) MOJ (March 2020), <u>Prevention and Diversion Scoping Survey Summary – Youth Justice Board (June 2021)</u> - Youth Justice Resource Hub (yjresourcehub.uk)

Glossary

- **Action Fraud:** The national reporting centre for fraud and cyber crime in England, Wales and Northern Ireland. Housed within the City of London Police.
- **Artificial Intelligence large language models:** Complex technical platforms, like ChatGPT and Google Bard, that employ deep learning and neural networks trained on large volumes of text that to generate text or perform other tasks.
- **Authorised fraud or Authorised Push Payment (APP) fraud:** A form of fraud in which victims are manipulated or tricked into authorising payments to fraudsters, often through social engineering.
- **Cifas:** A not-for-profit fraud prevention service in the United Kingdom.
- **City of London Police (CoLP):** Territorial police force within the City of London. The National Lead Force for fraud and National Police Chiefs Council (NPCC) lead for economic and cyber crime.
- **Cold-calling:** Making an unsolicited call to sell a product – in some cases these are legal, in others they are not (such as when making a call to someone registered with the Telephone Preference Service or when selling certain products like pensions or injury claims services).
- **Cryptocurrency:** A digital currency in which transactions are verified and records maintained by a decentralised system using cryptography, rather than by a centralised authority.
- **Data breach:** The release of secure or private/confidential information to an untrusted environment.
- **DBT:** Department for Business and Trade, a ministerial department which was formed in 2023 to bring business and trade into a single department.
- **DCMS:** Department for Culture, Media and Sport, a ministerial department focussed on supporting culture, arts, media, sport, tourism and civil society.
- **Deep-fake:** A video of a person in which their face or body is digitally altered so that they appear to be someone else, typically used maliciously or to spread false information.
- **Disclosure Regime:** The requirement for prosecutors to disclose to the defence all material that weakens the prosecution's case or strengthens the defendant's case.
- **DSIT:** Department for Science, Innovation and Technology, a ministerial department which was established in 2023 to bring together relevant parts from the former Department for Business, Energy and Industrial Strategy and the former Department for Digital, Culture, Media and Sport.
- **Fake delivery text:** Texts sent by fraudsters claiming to be from a delivery firm. They trick victims into clicking links or filling in personal details to steal personal information or infect devices with malicious software.
- **Financial Conduct Authority (FCA):** Conduct regulator for around 51,000 financial services firms and financial markets in the UK.
- **Five Eyes:** The Five Eyes is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States.

- **His Majesty's Treasury (HMT):** The ministerial department responsible for financial services and for the Money Laundering and Payment Services Regulations.
- **Home Office (UK):** The UK Home Office is a ministerial department responsible for immigration, security and law and order. As part of its responsibility for law and order it is responsible for tackling fraud against individuals and businesses, primarily for England and Wales (noting that this matter is devolved in Scotland and Northern Ireland).
- **Identity fraud:** The use of personal information, stolen through criminal activity, to obtain goods or services by deception.
- **Identity theft:** The taking of personal information.
- **Investment fraud:** Usually involves criminals contacting people out of the blue and convincing them to invest in schemes or products that are worthless or do not exist. Once the criminals have received payment, they cease contact with the victim.
- **Mass texting services:** Services facilitating business-to-customer SMS messaging that usually is routed onto telecommunications networks differently to person-to-person messaging.
- **Money laundering:** The concealment of the origins of illegally obtained money.
- **Money mules:** Mules allow criminals to use their bank accounts to store illicit funds before transferring it to other accounts, helping to hide the dirty money.
- **National Crime Agency (NCA):** The NCA leads the UK's fight to cut serious and organised crime working at the forefront of law enforcement, building an intelligence picture of serious organised crime threats and pursuing the most serious offenders.
- **National Cyber Security Centre (NCSC):** The UK's technical authority for cyber threats, providing a unified national response to cyber incidents to minimise harm, helping with recovery and learning lessons for the future.
- **National Economic Crime Centre (NECC):** The NECC brings together law enforcement and justice agencies, government departments, regulatory bodies and the private sector, with a shared objective of driving down serious economic crime, protecting the public and safeguarding the prosperity of the UK as a financial centre.
- **National Economic Crime Victim Care Unit (NEVCU):** A team of specialist advocates working within the City of London Police that support vulnerable people who have fallen victim to fraud and cyber crime, with the aim of safeguarding them and reducing the possibility of them becoming a repeat victim.
- **National Fraud Intelligence Bureau (NFIB):** Police unit responsible for gathering and analysing intelligence relating to fraud and financially motivated cyber crime. Part of City of London Police.
- **National Trading Standards (NTS):** NTS is responsible for gathering intelligence from around the country to combat rogue traders and a number of priorities including internet scams.
- **Ofcom:** The UK's independent communications regulator, regulating the telecommunications, postal and broadcast industries, and - following the proposed Online Safety Bill - online companies facilitating user-to-user and search services.

- **Organised Crime Groups (OCGs):** A group which consists of three or more people, who act together with the purpose of carrying out criminal activities.
- **Payment Service Provider:** An organisation that facilitates payments between individuals and businesses, such as Mastercard or a bank.
- **Payment Systems Regulator (PSR):** Statutory regulator for the 8 designated payments systems and their participants.
- **Public Sector Fraud Authority:** The Public Sector Fraud Authority (PSFA) works with departments and public bodies to understand and reduce the impact of fraud against the public sector.
- **Purchase scams:** Scams which offer products for sale which don't exist.
- **Regional Organised Crime Units (ROCU):** There are 10 ROCUs across England and Wales, which form part of the policing network. They have specialist policing capabilities focused on tackling organised crime.
- **Romance fraud:** Involves victims being duped into sending money to criminals purporting to be in a genuine relationship with them.
- **Serious Fraud Office (SFO):** Responsible for investigating and prosecuting cases of serious or complex fraud and corruption in England, Wales and Northern Ireland.
- **Serous Crime Prevention Orders:** Court imposed civil orders to prevent individuals involved in serious crime from engaging in certain activities or accessing resources.
- **SIM farms:** SIM farms are devices that can house hundreds of SIM cards, which can send out thousands of scam texts to defraud the UK public of millions of pounds.
- **Social engineering:** The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.
- **Software:** The programs and other operating information used by a computer.
- **Spoofing:** The act of disguising a communication from an unknown source so that it looks like it is from a trusted, known source. Spoofing can apply to emails, phone calls and text messages, or can be more technical such as IP addresses.
- **Strategic Policing Requirement:** The Home Secretary's view of what the current national threats are, and the national policing capabilities needed to respond.
- **Tech sector:** Large, consumer-facing companies, such as Meta, Alphabet and Microsoft, that use online platforms to facilitate significant interaction between users.
- **Unauthorised fraud:** A form of fraud, where the victim does not authorise the transfer of money from their account, such as when they are impersonated to their bank.
- **User-generated content:** Content on online platforms, such as social media, that is created or shared by a user (as opposed to the platform or a business), that another user can interact with, such as a tweet or Instagram post.
- **Vulnerable:** A person who, due to their characteristics or circumstances, is at greater risk of harm, and where they suffer harm, may experience more severe harm.

E02904361

978-1-5286-4086-2