HOUSE OF LORDS

Fraud Act 2006 and
Digital Fraud Committee

Report of Session 2022–23

Fighting Fraud: Breaking the Chain

Ordered to be printed 31 October 2022 and published 12 November 2022

Published by the Authority of the House of Lords

HL Paper 87

Fraud Act 2006 and Digital Fraud Committee

The Fraud Act 2006 and Digital Fraud Committee was appointed by the House of Lords on 19 January 2022, and re-appointed on 12 May 2022 "to consider the Fraud Act 2006 and Digital Fraud".

Membership

The Members of the Fraud Act 2006 and Digital Fraud Committee were:

Lord Allan of Hallam
Baroness Bowles of Berkhamsted
Lord Browne of Ladyton
Viscount Colville of Culross
Lord Gilbert of Panteg
Baroness Henig
Baroness Kingsmill
Baroness Morgan of Cotes (Chair)
Lord Sandhurst
Baroness Taylor of Bolton (to 22 June 2022)
Lord Triesman (from 22 June 2022)
Lord Vaux of Harrowden
Lord Young of Cookham

Declaration of interests

See Appendix 1.

A full list of Members' interests can be found in the Register of Lords' Interests: http://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests

Publications

All publications of the Committee are available at: https://committees.parliament.uk/committee/582/fraud-act-2006-and-digital-fraud-committee/publications/

Parliament Live

Live coverage of debates and public sessions of the Committee's meetings are available at: http://www.parliamentlive.tv

Further information

Further information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is available at: http://www.parliament.uk/business/lords

Committee staff

The staff who worked on this Committee were Alastair Taylor (Clerk), Francesca Crossley (Policy Analyst) and Mark Gladwell (Committee Operations Officer).

Contact details

All correspondence should be addressed to the Fraud Act 2006 and Digital Fraud Committee, Committee Office, House of Lords, London SW1A 0PW. Telephone 020 7219 4450. Email hlfraudactcomm@parliament.uk

Twitter

You can follow the Committee on Twitter: @HLFraudActCom

CONTENTS

Evidence is published online at https://committees.parliament.uk/committee/582/fraud-act-2006-and-digital-fraud-committee/ and available for inspection at the Parliamentary Archives (020 7219 3074).

Q in footnotes refers to a question in oral evidence.

EXECUTIVE SUMMARY

"People are being wronged on a massive scale." Joe Lycett[1]

"The state has retreated from the investigation and prosecution of fraud over the last 15 years." Mark Fenhalls KC[2]

Fraud is the most commonly experienced crime today

Fraud is the most commonly experienced crime in England and Wales today. It accounts for approximately 41% of all crime against individuals.[3] A person aged 16 or over is more likely to become a victim of fraud than any other individual type of crime, including violence or burglary.[4] It costs the economy billions every year.[5]

Even though fraud is a massive problem affecting every section of society and all age groups which, in evidence to us, the Bank of England admitted directly affects consumer confidence, successive Governments have failed to tackle fraud with the priority it deserves. The former Chancellor, Kwasi Kwarteng MP, commented earlier this year that fraud was not a crime that people experience in their "day-to-day lives".[6] While the data on fraud and its perpetrators is incomplete, we can identify an increase over recent years. In the year ending March 2022, fraud had increased by 25% since the pre-pandemic year to March 2020.[7] While these figures have begun to stabilise, fraud remains higher than before the pandemic and latest data shows that losses over the past year total a staggering £4 billion.[8] This may explain why the Government has excluded fraud statistics from public statements on crime rates and claimed that crime is falling.

If citizens were being routinely mugged and having millions of pounds stolen from their wallets in broad daylight, every organisation involved in allowing this to happen would have no choice but to deal with it swiftly, and the perpetrators would be brought to justice in court. Because most fraud is now happening online and often involves social engineering of the victim, the exponential

---

1 Q 99 (Joe Lycett)
2 Q 199 (Mark Fenhalls KC)
3 ONS, 'Crime in England and Wales: Appendix tables' (27 October 2022), Table 1: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables [accessed 1 November 2022]
4 ONS, 'Crime in England and Wales: year ending June 2022' (27 October 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2022#fraud [accessed 1 November 2022]
5 Estimates for the cost of fraud to the UK vary. For example, see UK Finance, 'Cross-sector action needed as criminal gangs steal more than £1.3 billion' (August 2022): https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2022 [accessed 1 November 2022] and NCA, 'The threat from fraud': https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime [accessed 1 November 2022]
6 BBC, 'Sunday Morning' (6 February 2022): https://www.bbc.co.uk/iplayer/episode/m00149kt/sunday-morning-06022022 [accessed 1 November 2022]
7 ONS, 'Crime in England and Wales: year ending March 2022' (21 July 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2022 [accessed 1 November 2022]
8 ONS, 'Crime in England and Wales: year ending June 2022 (27 October 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2022#fraud [accessed 1 November 2022] and City of London Police, 'NFIB Fraud and Cyber Crime Dashboard : 13 months of data': https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46 [accessed 1 November 2022]. The total lost to individual victims rather than organisations or those recorded as 'unknown' was £1.9 billion.

growth in fraud and scams has been invisible and fraudsters face little risk of being caught. This has to stop.

The COVID-19 pandemic accelerated the shift towards digitalisation, with more people turning to online technologies to conduct their daily activities. Online banking and shopping have become mainstream, online dating has become widely adopted, and online messaging platforms and social media are used to communicate with friends, family and businesses. It is through these channels that the tendrils of domestic or overseas Organised Crime Groups are being extended to reach victims in the UK. The UK's widespread use of the English language, its position as a digitalised, global financial hub, the enthusiastic adoption of the Faster Payments system, and the emergence of cryptoassets make for a fertile ground for fraudsters.

The result has been an increase in digital fraud. 80% of reported frauds are cyber-enabled; they could have taken place offline, but their scale, reach and impact have been expanded by the use of online services and digital technology.[9] These conditions have contributed to a monumental increase in authorised push payment (APP) fraud, which happens when a person or business is tricked into sending money to a fraudster posing as a genuine payee. For this reason, we have chosen to focus our inquiry on APP fraud and the impact of digital fraud on individual consumers.

Fraud is rightly being taken seriously by both Houses of Parliament. The Justice Committee recently published its fourth report of session on *Fraud and the Justice System*. While the scope of our inquiry differs from that of the Justice Committee, we have considered their findings and are pleased to have drawn many similar conclusions, which are highlighted throughout this report.

Law enforcement is under-resourced for the fight against fraud

Law enforcement agencies are chronically underfunded for the fight; only a paltry 1% of law enforcement is focussed on tackling economic crime.[10] Moreover, digital investigation remains outside the capacity of mainstream policing despite police forces operating in a highly digitalised society facing many digital forms of crime.[11] The organisational structure for policing fraud is complex and confusing. Action Fraud (probably better re-named as 'Report Fraud') remains inactive and misunderstood, and local police forces are so preoccupied with competing priorities that they cannot effectively manage cross-border frauds that so often sit outside their local purview. The effect of such under-prioritisation has been to create a permissive culture across Government and law enforcement agencies towards fraud and the criminals who perpetrate it. This then permeates through to affect the attitudes of private sector players in the fraud chain, which describes the steps involved in a fraud, who have not stepped in to do what they can to prevent consumers being scammed.

---

9 Action Fraud, *Fraud Crime Trends 2020–21*: https://data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/2020–21-Annual-Assessment-Fraud-Crime-Trends.pdf [accessed 1 November 2022] and Cabinet Office, 'National Cyber Strategy 2022' (7 February 2022): https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 [accessed 1 November 2022]

10 Oral evidence taken before the Treasury Committee on 25 January 2021 (Session 2019–21), Q 2 (Graeme Biggar) and Q 222 (Andy Cooke)

11 Q 222 (Andy Cooke)

The criminal justice system has also failed to keep pace with the threat, resulting in a significant decrease in the prosecution of fraudsters over the last decade.[12] This is not a by-product of failing legislation. While there is scope for increasing maximum sentencing, the Fraud Act 2006 is, as we have heard, still a highly effective piece of legislation that has simplified the fraud landscape and it has the flexibility to adapt to future technological developments. It is true that the efficacy of the Act is hindered by backlogs in the courts as well as an outdated disclosure process that has not kept pace with the changing technological landscape, however these issues cannot be blamed for the failure to find and prosecute fraudsters.

Without fear of facing investigation or justice, organised criminals around the world turn to the UK as a lucrative market to commit fraud. They know that they can operate with limited fear of prosecution or redress for their crimes, the proceeds of which they use to fund further criminal activity including human trafficking and the drugs trade, and they do not have any regard for their victims.

The 'alphabet soup' of responsible bodies is ineffective

The decline in investigation and prosecution of fraud must be laid, at least in part, at the feet of Government inaction. Counter-fraud policy is spread across a "complicated map" made up of multiple departments, taskforces and Ministers.[13] This results in a plethora of agencies and bodies, a vacuum of responsibility and a culture of blame-shifting.[14] We recognise the mind-boggling variety of acronyms that make up this alphabet soup and have provided a glossary to accompany this report.

Fraud is far from a victimless crime. The financial impact can be significant, particularly in the context of the current cost-of-living crisis, which ruthless fraudsters are exploiting to manipulate vulnerable consumers. The emotional impact can be even more traumatising. Victims of fraud are socially engineered by malicious fraudsters, many will face a crisis of confidence and lose trust in the authorities and people that surround them, and some may suffer devastating mental health consequences. Unlike almost any other crime, fraud victims are often blamed for the crimes that have been committed against them, which reduces their incentive to report fraud to the authorities. Some will never recover the funds they have lost, and those that do may remain emotionally shattered by their experience. Many will never see the perpetrator face justice. However, given the scale, pace and ease with which fraud is developing, it is also clear that we cannot arrest our way out of this challenge.[15]

Organisations that make up the fraud chain are not uniformly incentivised to tackle fraud

Fraudsters use a variety of channels to reach their victims, and they follow a series of steps before they are able to 'cash out' their stolen funds. Within this fraud chain, there are multiple stakeholders across several sectors that enable fraud to take place and often fail to put adequate systems in place to prevent it. For too long, these businesses have been allowed to enable and facilitate fraud.

---

12 Figures available at Written Answer UIN 120774, Session 2021–22.
13 Q 253 (Tom Tugendhat MP)
14 Written evidence from RUSI (FDF0036)
15 Written evidence from the Association of Police and Crime Commissioners (FDF0064) and Tim Harvey (FDF0097)

The telecoms sector has no real incentive to prevent fraud and has allowed blame to be placed elsewhere for too long. It must do more to tackle phishing emails and smishing texts before they reach victims, and must prevent fraudsters from making spoof phone calls using easily accessible technology to manipulate vulnerable victims into thinking they are a trusted organisation. Similarly, web-hosting providers must prevent fraudsters from registering fraudulent website domains. The tech sector must slam the brakes on fraudsters using online advertising and social media platforms to reel in consumers, and do more to verify the identity of those using online dating platforms before they commit romance fraud. Plans to hold platforms to account via the Online Safety Bill for online fraudulent advertising appearing on their services must not be allowed to slide and should be strengthened.

We recognise that many organisations are rightly signifying their ambitions to tackle such fraud, but they are not yet comprehensively incentivised to put practical measures into action at the pace required. While it could do more, the financial services sector has been bounced into action due to the burden of reimbursing customers who lose out to fraud. Processes including Confirmation of Payee are proving effective in heightening awareness of the risks of making online payments.

Until all fraud-enabling industries fear significant financial, legal and reputational risk for their failure to prevent fraud, they will not act. Companies continue to play their part in public-facing talking shops whilst at the same time relying on individually managed consumer awareness campaigns that shift the blame onto victims. At the same time, these organisations are failing to build in futureproofed counter-fraud mechanisms either at the point of design or retrospectively.

The private sector must be encouraged to combat fraud not only through facing the threat of corporate criminal liability or regulatory action, but also through the creation of a safe harbour for the sharing of data for the purposes of preventing fraud. It is only through a holistic approach involving every part of the fraud chain that fraud will be prevented upstream before money leaves a victim's account. Industry solutions are clearly possible and effective; we only have to look at the success of chip-and-PIN in tackling face-to-face 'analogue' fraud to see that.

And when fraudulent payments do slip through the net, it should not be the sole responsibility of the financial services sector, in particular the victim's bank, to pick up the bill. All stakeholders in the fraud chain, including the payee's bank, must know they have a duty both to prevent fraud and to address their failings and the victims' losses once it has occurred. They must lend their support to a united, centrally-led public awareness campaign that takes its lead from best practice exhibited in public health campaigns.

Six steps to break the fraud chain

Fraud costs the UK and its citizens billions of pounds a year. Security Minister Tom Tugendhat MP told us that "fraud is a scourge on UK people: it is a tax on businesses and people, and it not only damages the integrity of our financial and economic system but undermines trust in our economy and reduces our ability to trade freely."[16] Its financial and emotional cost to the millions of

16 Q 250 (Tom Tugendhat MP)

victims is immeasurable. The Government must take this opportunity to revisit its criminal justice priorities and begin by placing the UK's biggest crime at the forefront of the national agenda. As priority steps to break the fraud chain, we recommend the following:

- The UK's advanced payments infrastructure is one of the key reasons why it has become a global centre for fraud. The speed with which payments can be made must be delayed in certain circumstances to allow more time for banks to review risk signals and contact their customer about the proposed payment. The Payment Systems Regulator should consult on measures to achieve this (see paragraph 229).
- To move fraud to its rightful place as a top priority for law enforcement, fraud should be included within the Strategic Policing Requirement (see paragraph 327).
- To address the mind-boggling variety of acronyms and alphabet soup of departments, taskforces and Ministers with responsibility for fraud, a cabinet sub-committee with a clear mandate to tackle fraud should be established, chaired by and accountable to the Security Minister (see paragraph 286).
- Several sectors involved in the fraud chain have failed to prevent rampant fraud for too long. The Government must introduce a new corporate criminal offence of 'failure to prevent fraud' across all sectors to address this (see paragraphs 521).
- The Online Safety Bill contains several important measures to prevent fraudulent content and scam advertising from appearing on online platforms and to hold tech companies accountable when they fail. It must be brought forward urgently (see paragraph 559–562).
- To create clear advice for consumers to follow to help them to prevent fraud and report it if they become a victim, the Government should oversee the introduction of a single, centrally funded consumer awareness campaign in partnership with industry (see paragraph 418).

Fighting Fraud: Breaking the Chain

CHAPTER 1: BACKGROUND

1. Fraud is the act of gaining a dishonest advantage, often financial, over another person.[17] Colloquially, fraud may be known as a 'scam', 'swindle', 'con', 'hoax', 'trick' or 'extortion'.[18] It is a form of economic crime, which covers activities involving money, finance or assets with the purpose of unlawfully obtaining a profit or advantage or causing loss to others.[19]

2. Digital fraud describes fraud conducted using online services and digital technology. Fraudsters may use emails, websites, malicious software or other digital tools to steal personal details or money.[20] Digital fraud is often cyber-enabled, which happens when technology like computers and networks are used to advance the fraud (see Box 1).

3. In the UK, digital fraud is committed at scale and with relative impunity. Our digitised society has transformed fraud from being the preserve of opportunist individuals to the illegal revenue streams of Organised Crime Groups and global malign actors. These organised criminals use the profits from fraud to fund further organised crime, including human trafficking and the drugs trade. Fraud is the most commonly experienced crime in England and Wales, accounting for approximately 41% of all crime against individuals.[21] Criminals turn to fraud because it can be conducted cheaply, at pace and without fear of likely or successful prosecution.

4. In the first half of 2022, it is estimated that over 40 million UK adults were targeted by scammers and data shows that a total of £609.8 million was lost to all types of fraud.[22] In this time period, losses due to Authorised Push Payment (APP) fraud, which happens when a person or business is tricked into sending money to a fraudster posing as a genuine payee, were £249.1 million. Impersonation scams, such as when a fraudster impersonates bank staff, were the largest category in terms of loss (£90.5 million), followed by investment scams (£61.2 million). While APP losses were down 17% in the first half of 2022 compared to 2021 (13% down for all types of fraud), UK Finance suggests this is due to the first half of 2021 being "an exceptionally

17 CPS, 'Fraud and economic crime': https://www.cps.gov.uk/crime-info/fraud-and-economic-crime [accessed 1 November 2022]

18 House of Commons Library, *Consumer protection: online scams*, Briefing Paper CBP9214, 20 May 2021

19 HM Treasury and Home Office, 'Economic Crime Plan, 2019 to 2022, accessible version' (4 May 2021), para 1.11: https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version [accessed 1 November 2022]

20 Commbank, 'Digital Fraud': https://www.commbank.com.au/support/security/digital-fraud.html [accessed 1 November 2022]

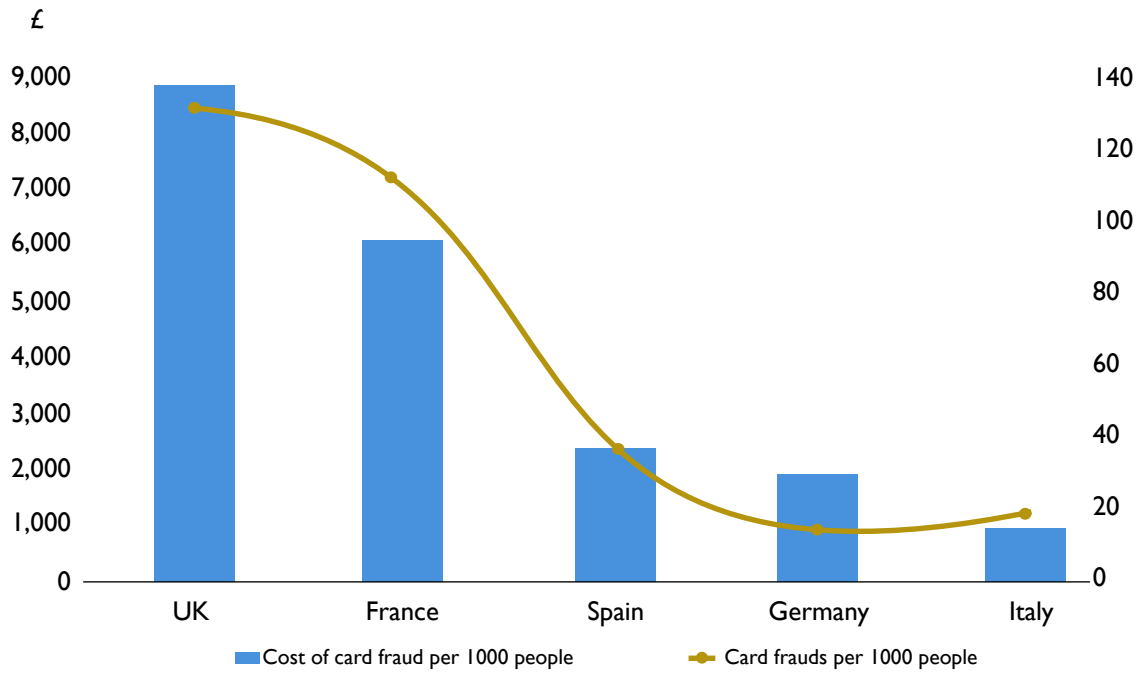
21 ONS, 'Crime in England and Wales: Appendix tables' (27 October 2022), Table 1: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables [accessed 1 November 2022]

22 Citizen's Advice, 'Over 40 million targeted by scammers as the cost-of-living crisis bites' (12 June 2022): https://www.citizensadvice.org.uk/about-us/about-us1/media/press-releases/over-40-million-targeted-by-scammers-as-the-cost-of-living-crisis-bites/ [accessed 1 November 2022]; UK Finance, *2022 half year fraud update* (13 October 2022): https://www.ukfinance.org.uk/system/files/2022–10/Half%20year%20fraud%20update%202022.pdf [accessed 1 November 2022]

high period for fraud, rather than the start of a downward trend".[23] Total losses due to APP fraud were £583.2 million in 2021.[24]

5. The scale and volume of APP fraud is complex to measure and difficult to compare with fraud rates in other countries. Data appears scarce and is compounded by challenges linked to under-reporting. However, estimates of the impact of other types of fraud by country do exist. Using European Central Bank data from the pre-pandemic year 2019, the Social Market Foundation has found that, the UK had the highest number of card fraud victims per 1000 people as well as the highest losses to fraud in comparison with other European countries (see Figure 1).

Figure 1: Cost and number of victims of card fraud per 1000 people in major European countries



Source: Social Market Foundation, 'UK is card fraud capital of Europe: think tank' (3 August 2022): https://www.smf.co.uk/uk-is-card-fraud-capital-of-europe-think-tank/ [accessed 1 November 2022]

6. Despite the scale of fraudulent activity in the UK, Chair of the Bar Mark Fenhalls KC told us that "the state has retreated from the investigation and prosecution of fraud over the last 15 years".[25] Only 1% of police and support staff are working on economic crime issues.[26] Estimates suggest that despite the substantial growth in fraud, the decline in convictions could be as high as by two-thirds in 10 years.[27] The Government appears to suffer from a culture of complacency when it comes to getting a grip on fraud

23 UK Finance, *2022 half year fraud update* (13 October 2022): https://www.ukfinance.org.uk/system/files/2022-10/Half year fraud update 2022.pdf [accessed 1 November 2022] and UK Finance, 'UK Finance calls for urgent action from all sectors as fraud continues to threaten the UK' (13 October 2022): https://www.ukfinance.org.uk/news-and-insight/press-release/uk-finance-calls-urgent-action-all-sectors-fraud-continues-threaten [accessed 1 November 2022]

24 UK Finance, *Annual fraud report* (July 2022), p 47: https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022_FINAL_.pdf [accessed 1 November 2022]

25 Q 199 (Mark Fenhalls KC)

26 Q 222 (Andy Cooke)

27 Written evidence from the Social Market Foundation (FDF0026)

(see Chapter 5). This was echoed by former Treasury and Cabinet Office Minister Lord Agnew of Oulton, who described an attitude of complacency towards tackling fraud in evidence to us.[28]

7. Tackling digital fraud requires a collective effort across the public and private sector. The fraudsters' business model starts with approaching a victim and ends with cashing out stolen goods. Along the way criminals interact with numerous platforms and services. Within this fraud chain it should be the responsibility of the stakeholders along the way to recognise the threat of fraud and act to mitigate the risk of it wherever they are in the chain. Unfortunately, the UK's response is too often driven by siloed working and the shifting of responsibility to other actors within the chain. The UK's response to fraud appears largely to focus on the financial harm caused, with little attention given to the devastating wider impacts that this crime has on victims or bringing the perpetrators to justice.

Our inquiry

8. With these challenges in mind, the House of Lords appointed this Committee in January 2022 "to consider the Fraud Act 2006 and Digital Fraud."[29] On 12 May 2022, we were re-appointed at the start of the new parliamentary session.[30]

9. We are grateful to all who contributed expertise and time to this inquiry. The Committee published a call for evidence in March and received over 90 individual submissions from a range of respondents. We have also heard oral evidence from over 45 witnesses ranging from academics to victims and law enforcement representatives. We are grateful to Tom Tugendhat MP, Minister for Security at the Home Office and Damian Collins MP, former Parliamentary Under Secretary of State at the Department for Digital, Culture, Media and Sport (DCMS), and their respective senior officials, who appeared before the Committee on 17 October 2022.

10. We are especially grateful to victims of digital fraud who shared their experiences with us. Our thanks go also to members of the Midlands Fraud Forum who hosted the Committee on 7 July in Birmingham.

11. Justice is devolved in Scotland and Northern Ireland and some justice matters are reserved in Wales. Whilst we endeavoured to learn from the experiences of the UK as a whole, our recommendations focus on the jurisdiction of England and Wales.

12. The members of the Committee are listed in Appendix 1, alongside their declared interests. We are grateful for the support of Kathryn Westmore, Senior Research Fellow, Royal United Services Institute (RUSI) and Sam Thomas, barrister and author (2 Bedford Row) as Specialist Advisers to the Committee. We would also like to thank the staff team who supported our inquiry: Mark Gladwell (Committee Operations Officer), Francesca Crossley (Policy Analyst) and Alastair Taylor (Clerk).

---

28 Q 32 (Lord Agnew of Oulton); see also 'UK taxpayer on hook for billions lost on Covid business loans', *Financial Times* (5 September 2022): https://www.ft.com/content/a8addc5d-0e20-4e5b-aa71-c145e22ec5e0 [accessed 1 November 2022]. While his comments referred to the issue of COVID-19 relief loans, we understood Lord Agnew's comments to reflect a wider culture.

29 HL Deb, 19 January 2022, cols 1167–1168

30 HL Deb, 12 May 2022, cols 109–111

13. We have chosen to focus our inquiry on two specific areas that we felt required urgent attention: authorised push payment (APP) fraud and the impact of digital fraud on individual consumers.

14. The vast majority of fraud victims over the past 13 months are individuals (89%) rather than organisations or businesses.[31] Criminals may target individuals in several ways, for example credit card theft and account takeover, which does not necessarily require direct contact with the victim.

15. In cases of APP fraud, individuals are targeted by fraudsters directly in order to coerce them into making a payment. This is because individuals are seen as the most vulnerable link in the fraud chain. Katy Worobec, Managing Director of Economic Crime at UK Finance told us:

> "The most common business model from the frauds we are seeing in the industry is that of targeting the individual as the weakest link in the chain … through social engineering, often on online platforms or by phone, to get the personal information in the first place, and then use that information to dupe the customer into making payments from their account into another account."[32]

16. APP scams occur when a person or business is tricked into sending money or data to a fraudster posing as a genuine payee so that the business or person has authorised the transfer. There are two types of APP scam; 'malicious payee' scams happen when someone is tricked into purchasing goods that don't exist or are not received, and 'malicious redirection' scams happen when a scammer impersonates someone, such as a member of bank staff, to direct a victim to transfer funds.[33] APP fraud losses stood at £583.2 million in 2021 (up from £479 million in 2020), with £505.8 million lost by scammed individuals (up from £387.8 million) and the rest lost by non-personal accounts or businesses.[34]

The scale of fraud in the UK

17. Data from the Office for National Statistics (ONS) Crime Survey for England and Wales (CSEW) shows that there were 4.5 million fraud offences in the year to March 2022, an increase of 25% on the pre-pandemic year ending March 2020. Computer misuse offences increased by 1.6 million, an 89% increase. In contrast, crime excluding fraud and computer misuse decreased by 18% compared with the year ending March 2020.[35] Computer misuse differs from fraud because it takes place "when fraudsters hack or use computer viruses or malware to disrupt services, obtain information illegally or extort individuals or organisations", whereas fraud involves a person

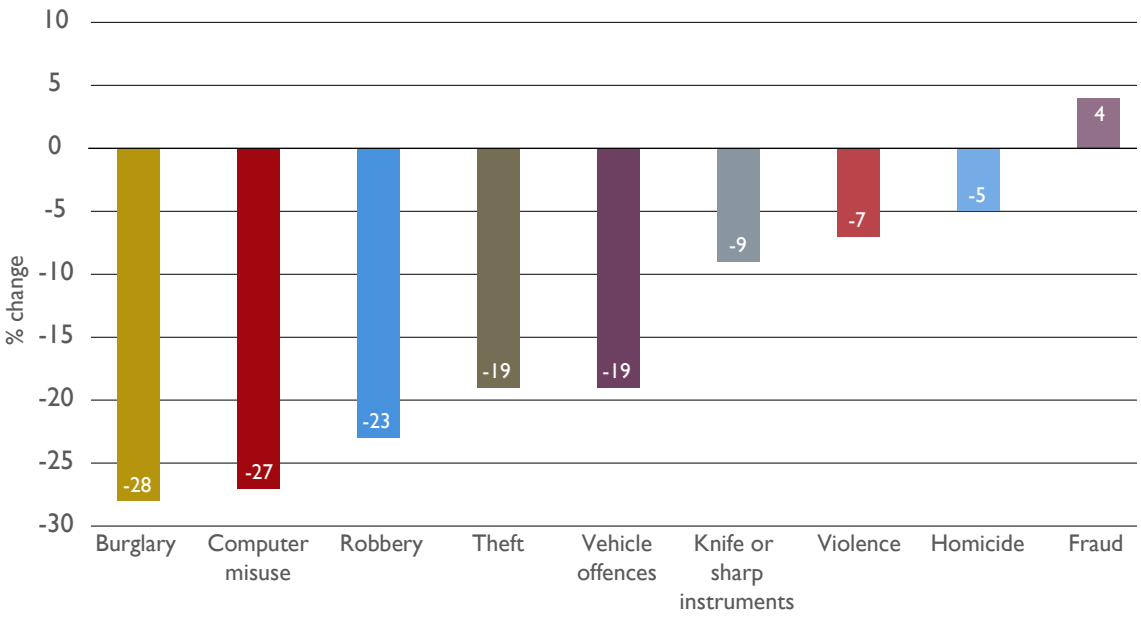
31 City of London Police, 'NFIB Fraud and Cyber Crime Dashboard: 13 months of data': https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46 [accessed 1 November 2022]
32 Q 14 (Katy Worobec)
33 House of Commons Library, *Banking fraud*, Briefing Paper CBP8545, 23 February 2021
34 UK Finance, Annual fraud report (July 2022), p 47: https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022_FINAL_.pdf [accessed 1 November 2022] and UK Finance, *Fraud: the facts 2021* (June 2021): https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf [accessed 1 November 2022]
35 ONS, 'Crime in England and Wales: year ending March 2022' (21 July 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2022 [accessed 1 November 2022]

dishonestly or deliberately deceiving a victim for personal gain or to cause a loss to another.[36]

18. This trend does appear to have stabilised in recent months, with the latest figures indicating that fraud has returned to pre-pandemic levels. ONS data shows that there were 3.8 million fraud offences in the year to June 2022, only a slight increase on the 3.7 million offences in the year to March 2020. However, advance fee fraud increased tenfold to 611,000 offences compared with the year ending March 2020 (60,000 offences). [37] The ONS defines advance fee fraud as when a payment is made to fraudsters, who claim to be in a position of authority, to transfer money or for a promise of employment, wealth or gifts. This includes some types of APP scams, for example lottery scams or where victims transfer funds to a fraudster posing as a delivery company.[38] Despite this stabilisation, fraud remains the only main crime type in the CSEW that is increasing (see Figure 2).

19. This trend may continue. Commander Nik Adams, Economic Crime Portfolio Lead at the City of London Police, recently told the House of Commons that the force predicts there could be anywhere from 25% to 65% growth in fraud over the next four to five years.[39]

Figure 2: Percentage change in main crime types for the year ending June 2022 compared to year ending March 2020, England and Wales



Source: ONS, 'Crime in England and Wales: year ending June 2022' (27 October 2022), Table 1: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2022#fraud [accessed 1 November 2022]

36 *Ibid.*

37 ONS, 'Crime in England and Wales: year ending June 2022 (27 October 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2022#fraud [accessed 1 November 2022]

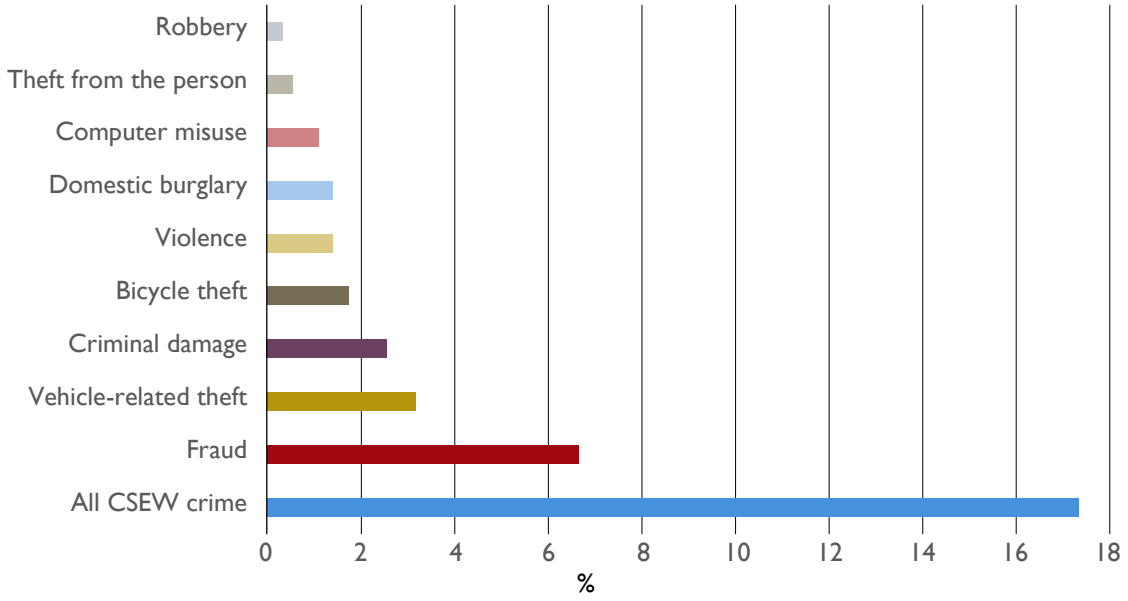
38 ONS, 'Nature of fraud and computer misuse in England and Wales: year ending March 2022' (26 September 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022 [accessed 1 November 2022]

39 Public Bill Committee on the Economic Crime and Corporate Transparency Bill, (Second sitting), 25 October 2022, col 54

20. Fraud can be reported in several ways, which leads to challenges when making an assessment of the true scale of fraud in the UK. Action Fraud is the UK's national fraud reporting service based in the City of London Police. Other groups also record fraud, such as UK Finance and Cifas, a not-for-profit fraud prevention service.[40] The CSEW has been used to collate information on fraud and computer misuse since 2015.[41]

21. What is clear is that a person aged 16 or over is more likely to be a victim of fraud than other individual crime types (7%) (see Figure 3).[42]

Figure 3: The likelihood of being a victim of different crime types



Source: ONS, 'Crime in England and Wales: year ending June 2022' (27 October 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2022#fraud [accessed 1 November 2022] Percentages show the proportion of adults who experienced a crime.

22. The difficulties in analysing the scale of fraud are compounded by under-reporting, and result in the likely under-estimation of the true extent of the problem. Mike Haley, CEO of Cifas, told us:

> "It is not a crime that people speak to others about because there is this embarrassment and shame about being a victim of fraud. Therefore, it is underreported."[43]

23. As of October 2022, Action Fraud data shows that over the past 13 months there have been 357,129 reports of fraud, totalling reported losses of £4 billion. 89% of victims are individuals (316,520 reports totalling £1.9 billion losses) and 68% of these reports were recorded as cyber-enabled (see Box 1).[44]

---

40 Written evidence from the City of London Police (FDF0031)

41 Office for National Statistics, 'Crime in England and Wales: year ending March 2022' (21 July 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2022#fraud [accessed 1 November 2022]. The CSEW became the telephone-operated TCSEW during the pandemic.

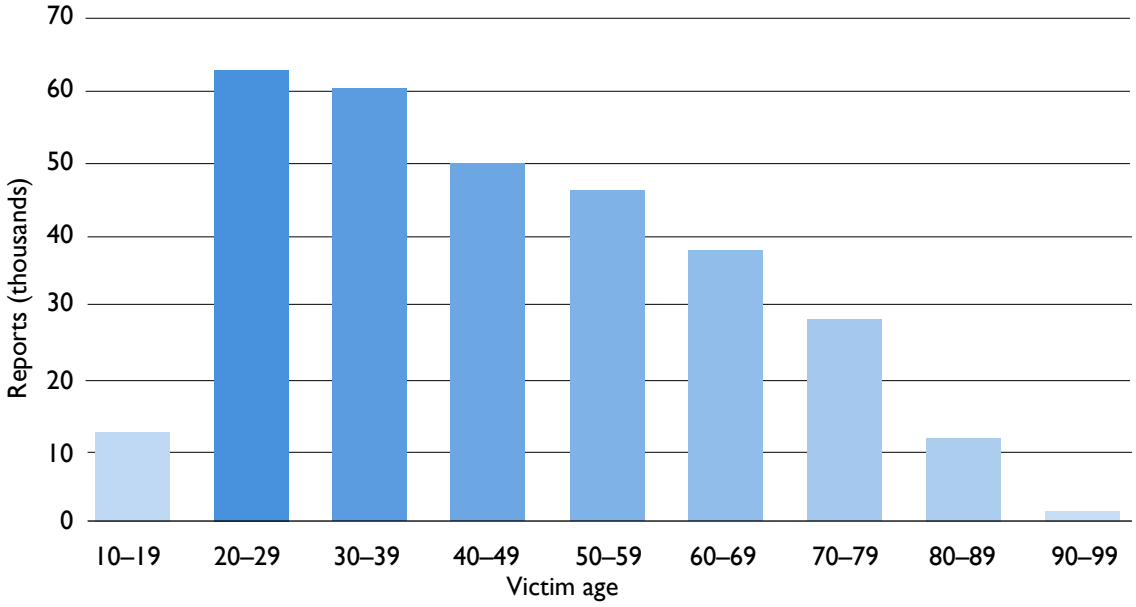
42 ONS, 'Crime in England and Wales: year ending June 2022' (27 October 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2022#fraud [accessed 1 November 2022]

43 Q 15 (Mike Haley)

44 City of London Police, 'NFIB fraud and cybercrime dashboard: 13 months of data': https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46 [accessed 1 November 2022]

24. Within this group of individuals, there are no typical victims of fraud and all people, regardless of age, gender, education or financial situation are vulnerable.[45] In the past 13 months, 44% of individual victims were female, 43% were male and the rest did not identify their gender.[46] Contrary to popular opinion, the likelihood of being a victim is generally lower in the older age groups. By age, most individual victims were aged 20 to 29 as shown in Figure 4.

Figure 4: Victims of fraud by age group



Source: City of London Police, 'NFIB fraud and cybercrime dashboard: 13 months of data': https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46 [accessed 1 November 2022]

25. The ONS recognises that there is "considerably less variation in fraud victimisation rates across different demographic groups than with other crime types."[47] Joe Lycett, presenter of the consumer programme *Joe Lycett's Got Your Back*, told us that "anyone can be caught out by it, and it can completely ruin your life".[48]

26. However, there are some features that may make a person more likely to become a victim of fraud. Examples of such variations include:

    - Income: Adults living in higher income households are more likely to become victims.[49] This is considered to include those earning £50,000

45 Victim's Commissioner, 'Bold and ambitious action on fraud will help victims'(13 October 2021): https://victimscommissioner.org.uk/news/blog-who-suffers-fraud/ [accessed 1 November 2022] and Q 199 (Karl Laird)

46 City of London Police, 'NFIB fraud and cybercrime dashboard: 13 months of data': https://colpolice.maps.arcgis.com/apps/opsdashboard/index.html#/604993045650 45b0bce05d2ca7e1e56c [accessed 1 November 2022]

47 ONS, 'Nature of fraud and computer misuse in England and Wales: year ending March 2019': https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019#fraud-characteristics-of-victims [accessed 1 November 2022]

48 Q 99 (Joe Lycett)

49 House of Lords Library, 'Financial fraud and vulnerable people' (29 November 2021): https://lordslibrary.parliament.uk/financial-fraud-and-vulnerable-people/ [accessed 1 November 2022]; See also House of Commons Library, *Consumer protection: online scams*, Briefing Paper CBP9214, 20 May 2021.

or more, and correlates with adults with degrees, diplomas, or those in managerial and professional jobs.[50]

- Digital exclusion: Those who are digitally excluded or who lack digital skills or cyber security awareness may be more vulnerable.[51] Around a third (37%) of the UK's workforce are thought to lack the skills needed for safe and legal online behaviour.[52]

- Mental health: Reports show those who have experienced mental health problems are three times more likely (23%) than the wider population (8%) to have fallen victim to an online scam.[53]

- Disability: Adults with a disability were more likely to be a victim of fraud (9.1%) in the year ending March 2022 than those without a disability (7.4%).[54]

Why has digital fraud increased?

27. A range of long and shorter-term factors have made the UK a centre for digital fraud. We heard evidence that long term factors include globalisation, the position of the UK as an English language hub, and rapid digitalisation. Short-term drivers include the COVID-19 pandemic, the recent cost of living crisis, and the emergence of cryptoassets. A further significant factor has been the UK's leading adoption of the Faster Payments service.

The UK's position as an English language hub

28. Rapid globalisation and the increasing use of the English language globally is believed to make the UK uniquely vulnerable to digital fraud. Duncan Tessier, Director of Economic Crime at the Home Office, argued that London's place as a global financial centre and the international prevalence of the English language presented criminal gangs with an ease of access which is not afforded by other countries.[55] While we recognise that this may factor into the fraud rates in other English-speaking nations such as the USA, groups including UK Finance and the National Crime Agency (NCA) recognise the English language as one compounding factor in the UK's unique attraction to fraudsters.[56]

29. The National Economic Crime Centre (NECC), an arm of the NCA which holds responsibility for coordinating the UK's response to economic crime, told us that: "Globally, the UK is disproportionately targeted by criminals

50 ONS, 'Nature of fraud and computer misuse in England and Wales: year ending March 2019': https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019#defining-fraud-and-computer-misuse [accessed 1 November 2022]

51 Parliamentary Office of Science and Technology, 'COVID-19 and the digital divide' (17 December 2020): https://post.parliament.uk/covid-19-and-the-digital-divide/ [accessed 1 November 2022]

52 Lloyds Bank, *UK Consumer Digital Index 2020* (2020), Appendix 44: https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/211109-lloyds-consumer-digital-index-2020-eds.pdf [accessed 1 November 2022]

53 Money and Mental Health Policy Institute, *Caught in the web: online scams and mental health* (December 2020): https://www.moneyandmentalhealth.org/wp-content/uploads/2020/12/Caught-in-the-web-full-report.pdf [accessed 1 November 2022]

54 ONS 'Nature of fraud and computer misuse in England and Wales: year ending March 2022' (26 September 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022 [accessed 1 November 2022]

55 Q 1 (Duncan Tessier) and written evidence from RUSI (FDF0036)

56 Q 14 (Katy Worobec) and written evidence from NECC (FDF0044)

engaged in fraud due to widespread use of English as a second language and the high uptake of digital banking and shopping in the UK, accelerated by COVID-19."[57]

Digitisation and the rise of online services

30. The digitisation of the global economy has been matched by a growing threat from economic criminals. As technology develops, there has been a proportionate increase in online and technology-enabled scams. Digitalisation has allowed fraud to become "industrialised".[58] According to Action Fraud, the UK's national reporting centre for fraud and cyber-crime, 80% of fraud is cyber-enabled (see Box 1).[59] TechUK, a technology sector trade association, said: "As we have moved our lives online and increased our digital footprint, fraudsters have found ways to adapt their sophisticated techniques to prey on the vulnerabilities of society."[60]

Box 1: Cyber-dependent and cyber-enabled fraud

ONS statistics show that there were 1.6 million computer misuse offences in the year ending March 2022, an increase of 89% on the year ending March 2020.[61] Between November 2020 and 2021, the UK lost £2.5 billion in fraud and cyber-crime cases.[62] Dr Alice Hutchings, Director of the Cambridge Cybercrime Centre at the University of Cambridge, told us:

> "The question as to where offenders are based is a really difficult one if they have good operational security skills. Often, the location where it appears the attack is coming from is the location of a compromised device or server that is being used as a proxy by the attacker. It can be quite difficult if you do not have the resources to do proper in-depth investigations to find out where attackers are based."[63]

There is a distinction between cyber-dependent and cyber-enabled fraud. Cyber-dependent fraud can only be committed using ICT devices, and in such cases the devices are both the tool for committing the crime and the target.[64] For example, the so-called FluBot attack was a type of malware spread via SMS text in 2021. When the victim clicked on an embedded link, malware was downloaded to harvest data and forward the message to contacts held in the phone. The malware prevented newly contacted numbers from re-contacting the sending device, limiting users' ability to report it.[65]

57 Written evidence from NECC (FDF0044)
58 Written evidence from ONBORD (FDF0013)
59 Action Fraud, *Fraud Crime Trends 2020–21*: https://data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/2020–21-Annual-Assessment-Fraud-Crime-Trends.pdf [accessed 1 November 2022]
60 Written evidence from techUK (FDF0059)
61 ONS 'Nature of fraud and computer misuse in England and Wales: year ending March 2022' (26 September 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022 [accessed 1 November 2022]
62 City AM, 'UK loses £2.5bn in fraud and cyber-crime cases during 2021' (20 January 2022): https://www.cityam.com/uk-loses-2-5bn-in-fraud-and-cyber-crime-cases-during-2021/ [accessed 1 November 2022]
63 Q 63 (Dr Alice Hutchings)
64 Cabinet Office, 'National Cyber Strategy 2022' (7 February 2022): https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 [accessed 1 November 2022]
65 ThreatMark, 'FluBot Malware' (20 May 2021): https://www.threatmark.com/flubot-banking-malware/ [accessed 1 November 2022]

Cyber-enabled fraud can be committed without ICT devices, but its scale and reach are altered by ICT technology e.g., romance fraud using an app.[66]In 2021, 80% of fraud was cyber-enabled.[67] Kathryn Westmore, Senior Research Fellow at RUSI, told us that the response to cyber-enabled crime has not caught up with the response to cyber-dependent crime:

> "On the cyber dependent-type attacks, I think the strategy and the work of the National Cyber Security Centre is pretty good. Some of the weaknesses are on cyber-enabled frauds, which are the ones that as consumers we tend to notice more because we are being attacked through scam text messages, adverts or emails, for example. I think there is a lack of centralised response to dealing with those kinds of frauds that falls somewhere between the cyber world and the broader fraud world."[68]

The Motion Picture Association, a trade association for the UK's film and television sector, told us that cyber-crime has become a cottage-industry due to the emergence of 'cyber-crime as a service'.[69] Using the dark web, fraudsters can access a way to pay for the skills and tools (such as ransomware and other 'crimeware') needed to perform cyber-crime.[70] Dr Alice Hutchings explained how this works in action:

> "We can see people creating crimeware. People use that to compromise credentials. Those credentials may then be traded, and other actors use the credentials to monetise them and cash out. There is a whole level of different services being provided at different points in the supply chain."[71]

Europol has identified cybercrime as a service as a key challenge, noting its role in helping fraudsters to increase the technical complexity of their attacks.[72] Furthermore, Dr Hutchings explained that its existence adds complexity to the challenge of locating and identifying fraudsters.[73]

While cybercrime as a service is illegal under Section 7 of the Fraud Act, under which a person is guilty if they make or supply articles designed for use in frauds, it is particularly difficult to identify those who are offering such services online due to the challenges of the dark web.[74] Nevertheless, it is clear that more should be done to work with overseas law enforcement agencies to stamp out this threat.

66 Cabinet Office, 'National Cyber Strategy 2022' (7 February 2022): https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 [accessed 1 November 2022]
67 Action Fraud, *Fraud Crime Trends 2020–21*: https://data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/2020–21-Annual-Assessment-Fraud-Crime-Trends.pdf [accessed 1 November 2022]
68 Q 65 (Kathryn Westmore)
69 Written evidence from the Motion Picture Association (FDF0068)
70 Q 61 (Dr Konstantinos Mersinas)
71 Q 62 (Dr Alice Hutchings)
72 Europol, *Internet Organised Crime Threat Assessment 2020* (2020): https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf [accessed 1 November 2022]
73 Q 62 (Dr Alice Hutchings)
74 Fraud Act 2006, section 7

31. The UK has the eighth highest online banking penetration in Europe, with 76% of adults using such services, up from 30% in 2007.[75] Research published in September 2022 shows that people in the UK are nearly twice as likely as other Europeans to prefer applying for financial products online.[76] UK Finance expects this trend to continue; while 86% of UK adults used remote banking in 2021 (65% used online banking and 57% used mobile banking), it is forecast that this will rise to 93% by 2031.[77]

32. The Security Minister told us that the widespread availability of instantaneous payments in the UK is a critical feature in the UK's attraction to fraudsters over and above other jurisdictions. He said:

> "We are one of the very few jurisdictions in the world that allows for pretty much instantaneous transfers; very few others do. That means that you can do two things. One is that obviously you can defraud somebody quickly and therefore have access to the cash immediately, but you can then do the second thing, which is so important, which is to pass it on to 20 or 30 other bank accounts and then other bank accounts and so on, so that by the time the law enforcement authorities are involved, the money has long since left the country, or at least left the jurisdiction."[78]

33. While digitalisation has been advancing at pace over the last 20 years, recent short-term drivers, such as the onset of the COVID-19 pandemic, have impacted on how fraudsters have manipulated their victims.

COVID-19

34. There has been an increase in fraud because of the COVID-19 pandemic and the impact it has had on consumer behaviour. Unlike other crime types, fraud rose during lockdowns. ONS data shows that there were 5.1 million fraud offences in the year ending September 2021, a 36% increased on the previous year.[79] UK Finance told us that: "The pandemic environment has provided rich pickings for fraudsters, in the form of new-to-digital consumers, heightened vulnerabilities and anxieties, as well as new channels to exploit."[80] The City of London Police said that the increase in fraud was primarily due to the increased use of online services, most notably shopping and dating.[81]

35. Impersonation scams saw the biggest increase during the pandemic, with fraudsters impersonating trusted services like the NHS or government departments.[82] At the onset of the pandemic, Google reported blocking

---

75 'Nordic countries dominate European online banking take up', *Computer Weekly* (2 February 2021): https://www.computerweekly.com/news/252495736/Nordic-countries-dominate-European-online-banking-take-up [accessed 1 November 2022]

76 'City exclusive: Brits leave Europeans trailing in digital banking as UK soaks up fintech inflows', *City AM* (12 September 2022): https://www.cityam.com/city-exclusive-brits-leave-europeans-trailing-in-digital-banking-as-uk-soaks-up-fintech-inflows/ [accessed 1 November 2022]

77 UK Finance, *UK Payment Markets Summary 2022* (August 2022): https://www.ukfinance.org.uk/system/files/2022–08/UKF%20Payment%20Markets%20Summary%202022.pdf [accessed 1 November 2022]

78 Q 262 (Tom Tugendhat MP)

79 ONS, 'Crime in England and Wales: year ending September 2021': https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2021#fraud [accessed 1 November 2022]

80 UK Finance, *Fraud: the facts 2021* (June 2021): https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf [accessed 1 November 2022]

81 Written evidence from City of London Police (FDF0031)

82 UK Finance, *Fraud: the facts 2021* (June 2021): https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf [accessed 1 November 2022]

18 million hoax emails about COVID-19 every day.[83] The City of London Police in their evidence raised the fear that the same predatory behaviour may be replicated during the developing cost of living crisis.[84]

36. An example of the increase in technology-linked scam attempts during the pandemic can be seen in the 86% increase in screen sharing scams. Screen sharing scams occur when a victim is prompted to download software that allows a fraudster to take control of the victim's screen, allowing them access to the user's personal details. The pandemic led to greater use of online video-sharing platforms and screen-sharing facilities. The Financial Conduct Authority (FCA), the UK's financial services regulator, saw 2,142 cases of this between July 2020 and May 2022, with over £25 million lost between 1 January 2021 and 31 March 2022.[85]

37. The pandemic increased the rate of online shopping, and this was matched by a rise in fraud relating to e-commerce activity. The West Midlands Police and Crime Commissioner told us that in the past year, 89% of all fraud in the West Midlands was cyber-enabled, with online shopping appearing most frequently.[86] This was supported by Will Semple, Director of Global Information Security Group at eBay, who described an uptick of fraudulent attacks on the platform during the pandemic but also the wider long-term trend of a "major transition from high street retail-type crime to cybercrime."[87] Cifas told us:

> " … [Online] platforms are exploited at scale, whether through the posting of fraudulent adverts, social engineering via direct messaging, or the sale of data, documents and guidance on how to commit fraud."[88]

38. The use of online dating platforms and subsequent rates of romance fraud both increased during the pandemic.[89] Romance fraud occurs when a person is duped into sending money to a fraudster who has gained their trust and convinced them their relationship is genuine. Action Fraud identified that scammers often manipulate, persuade and exploit their victims using emotive methods, such as claiming they need money for medical care.[90] 38% of people who have dated online in the past year have been asked for money.[91] Romance scams often prey on individuals at their most vulnerable using aggressive social engineering tactics. Mark Shelford, Police and Crime Commissioner for Avon and Somerset, told us that victims can be too embarrassed to tell family or friends about the fraud, which sustains feelings of isolation, increasing the likelihood of becoming a repeat victim.[92]

---

83 BBC, 'Google blocking 18m coronavirus scam emails every day' (17 April 2020): https://www.bbc.co.uk/news/technology-52319093 [accessed 1 November 2022]
84 Written evidence from City of London Police (FDF0031)
85 FCA, ''Sharing my screen cost me £48,000': half of investors would miss signs of screen sharing scam as FCA warns of 86% increase' (5 May 2022): https://www.fca.org.uk/news/press-releases/investors-miss-screen-sharing-scam-signs [accessed 1 November 2022]
86 Written evidence from the West Midlands Police and Crime Commissioner (FDF0035)
87 Q 119 (Will Semple)
88 Written evidence from Cifas (FDF0015)
89 Written evidence from City of London Police (FDF0031)
90 Action Fraud, 'Romance fraud': https://www.actionfraud.police.uk/a-z-of-fraud/dating-fraud [accessed 1 November 2022]
91 UK Finance, 'Romance Fraud: a human issue': https://www.ukfinance.org.uk/news-and-insight/blogs/romance-fraud-human-issue [accessed 1 November 2022]
92 Q 219 (Mark Shelford)

39. COVID-19 was a catalyst for the growth of fraud, however the impact of the pandemic is unlikely to be short-term, nor is there likely to be a return to 'normal' as we emerge from the crisis. This is due to a range of factors including changed habits and the role of other emerging and longstanding trends.

The emergence of cryptoassets

40. The emergence of cryptoassets presents new challenges to the counter-fraud landscape. Cryptocurrencies are a form of cryptoasset which can be defined as cryptographically secured digital representations of value or contractual rights that can be transferred, stored or traded electronically".[93] There are two major kinds of cryptoassets; unbacked assets like Bitcoin that are considered speculative and volatile, and stablecoins, which are tied to another asset like Pound Sterling.[94]

41. Cryptocurrency uses blockchain technology to form a transactional database. Blockchain is a type of distributed ledger technology, which is a means of recording and sharing data across multiple data stores. Blockchain is encrypted and uses algorithms to create a growing data structure. Data cannot be removed from this structure.[95]

42. Fraud is the most frequently identified predicate offence in the illegal use of cryptocurrencies.[96] There are multiple ways in which crypto-fraud can be committed, including 'rug pull' scams in which scammers persuade investors to put money into a new crypto token before disappearing with their money.[97] A similar process is followed during an Initial Coin Offering scam in which the 'latest' token is promoted by someone offering an investment that is essentially worthless. These are often facilitated by fraudulent advertising including false celebrity endorsements on social media.[98]

43. A core issue surrounding fraud and cryptocurrency is the lack of regulatory oversight of the sector. Cryptoasset scams are the type of fraud most frequently reported to the FCA alongside new types of boiler room and recovery scams. However the regulator told us it does not have the "power to tackle" many of these cryptoasset frauds.[99] Boiler room fraud is a type of investment fraud run out of an office where criminals contact victims to convince them to invest in bogus schemes.[100]

44. We have heard that, despite the use of blockchain technology, cryptocurrency provides an outlet for fraudulent finance that is harder to trace than payments made via traditional banking infrastructure.[101] While not necessarily the case for simple crypto transactions that are accessible on the blockchain, the use of technology such as crypto mixers, which disguise transactions by shuffling

---

93 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692)

94 Bank of England, 'What are cryptoassets?' (19 May 2020): https://www.bankofengland.co.uk/KnowledgeBank/what-are-cryptocurrencies [accessed 1 November 2022]

95 Europol, *Cryptocurrencies: tracing the evolution of criminal finances* (December 2021): https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf [accessed 1 November 2022]

96 *Ibid.*

97 'Record $14bn flowed into crime-linked crypto wallets in 2021', *Financial Times* (6 January 2022): https://www.ft.com/content/3c171512-7c58-4dc9-950f-28e2f75b03d9 [accessed 1 November 2022]

98 For an example see BBC News, 'Harry and Meghan misused in fake investment endorsement' (20 January 2022): https://www.bbc.co.uk/news/uk-60040937 [accessed 1 November 2022]

99 Written evidence from the FCA (FDF0069)

100 Action Fraud, 'Boiler room fraud': https://www.actionfraud.police.uk/a-z-of-fraud/boiler-room-fraud [accessed 1 November 2022]

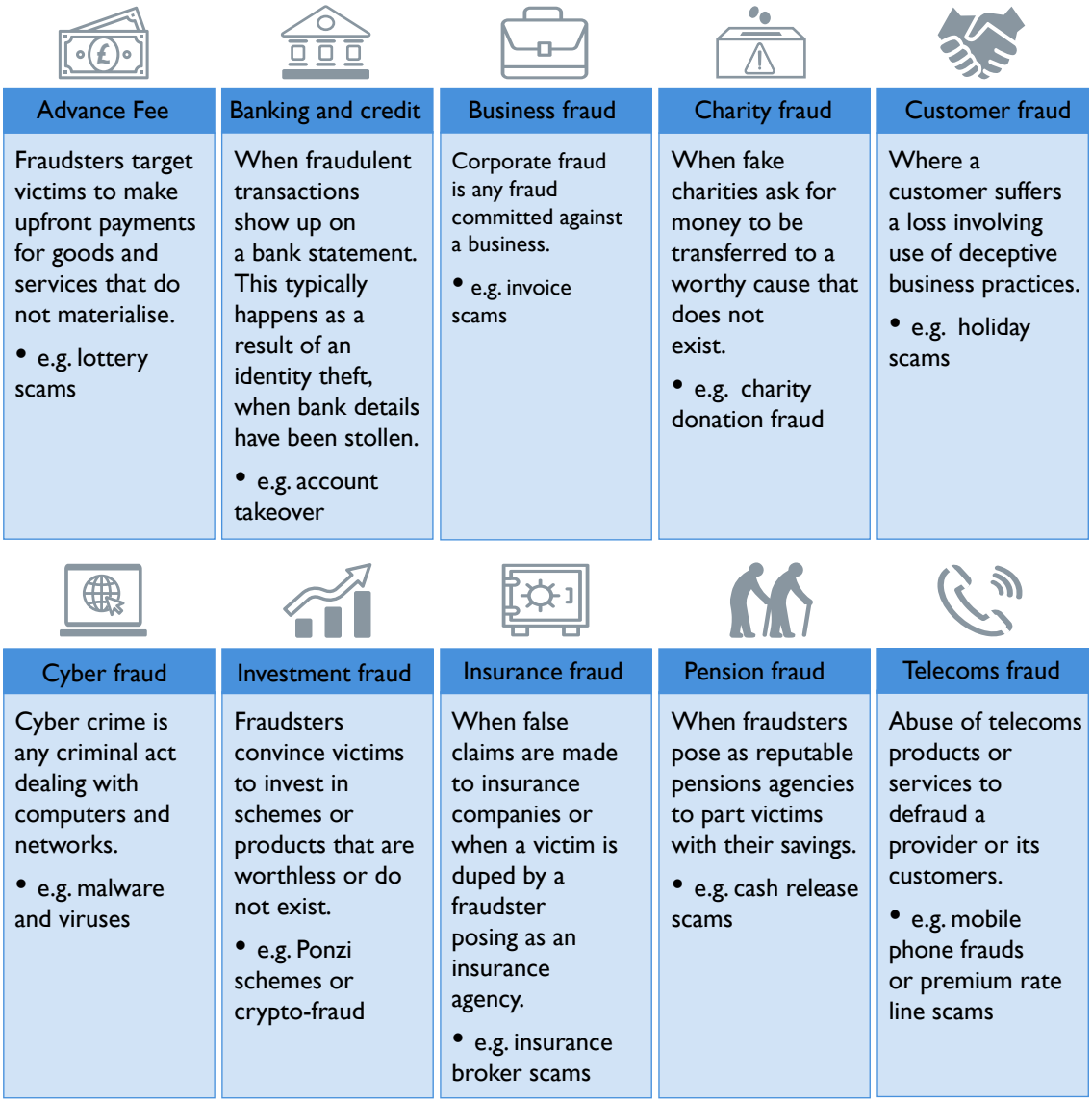
101 See Q 177 (Markko Künnapu) and Q 194 (Gerard Pollock).

coins, may create anonymity. Around 15% of all proceeds of crime were routed through mixers in 2021. In March, the NCA called for regulation of mixers to force organisations operating them to comply with money laundering laws, which would include customer checks and audit trails.[102]

The business model of digital fraud

45. There are hundreds of different fraud 'business models' that are operated by fraudsters, and several different ways that they are categorised by fraud authorities and law enforcement agencies. Common examples are categorised by Action Fraud as follows (excluding 'Other'):

Figure 5: Common fraud typologies

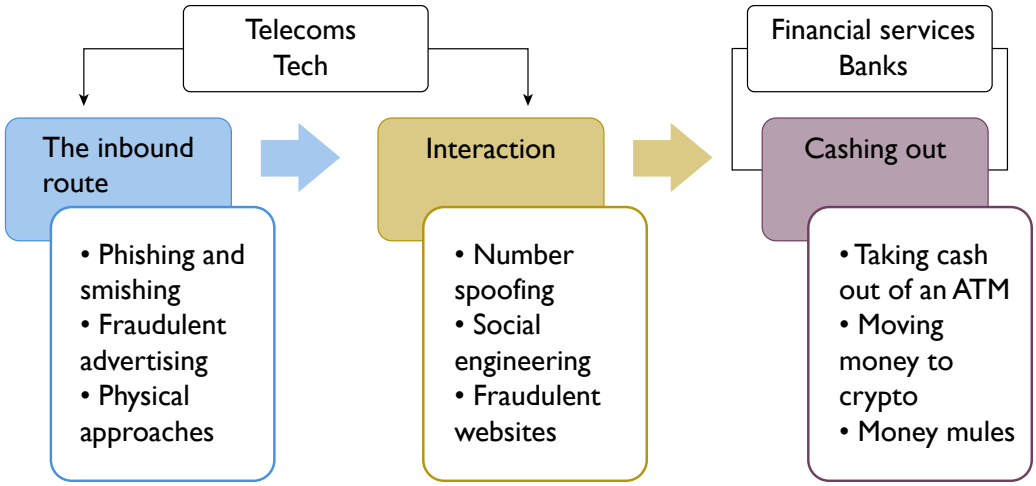


Source: Action Fraud, 'A-Z fraud': https://www.actionfraud.police.uk/a-z-of-fraud-category/business [accessed 1 November 2022]; Action Fraud, 'What is fraud and cyber crime?': https://www.actionfraud.police.uk/what-is-fraud [accessed 1 November 2022]; Investopedia, 'The most common types of consumer fraud': https://www.investopedia.com/financial-edge/0512/the-most-common-types-of-consumer-fraud.aspx [accessed 1 November 2022] ;The Pensions Regulator, 'Avoid pensions scams': https://www.thepensionsregulator.gov.uk/en/pension-scams [accessed 1 November 2022] and Europol, 'Telecommunications Fraud'(6 December 2021): https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/telecommunications-fraud [accessed 1 November 2022]

102 Q 71 (Katie Martin) and 'NCA calls for regulation of crypto mixers used in 'churning criminal cash'', *Financial Times* (15 March 2022): https://www.ft.com/content/c6df2b68-a244-4560–9911–88cc1fa61576 [accessed 1 November 2022]

46. The interaction between a fraudster and a victim can be analysed in a step-by-step process that we have called the 'fraud chain'. We prefer this to the 'kill chain' that has been used elsewhere.[103] The fraud chain tracks the development of fraud from the first approach by the fraudster through to the point when a criminal 'cashes out'. There are different ways in which this can take place. A simplified version of the chain is shown in Figure 6.

Figure 6: The Fraud Chain



Source: Q 14 (Katy Worobec) and written evidence from CCSG (FDF0063)

Who is responsible for the response to fraud?

47. The Home Office have overall responsibility for the Government's response to fraud against individuals and businesses. As noted, fraud against the public purse is outside the scope of this Inquiry. However, there are multiple departments, regulators and law enforcement agencies who contribute to the counter-fraud landscape.

48. Eight different departments have a key role in mitigating fraud. The Ministry of Justice has overall responsibility for the Fraud Act 2006. Other departments with a role include His Majesty's Treasury (HMT), the Department for Digital, Culture, Media and Sport (DCMS), the Department for Business Energy and Industrial Strategy (BEIS), Attorney General's Office (AGO), Foreign, Commonwealth and Development Office (FCDO) and the Department of Work and Pensions (DWP) (see Figure 7).

103 Q 14 (Katy Worobec)

Figure 7: Departmental responsibility for counter-fraud policy

Home Office	HM Treasury	Dept for Digital, Culture, Media & Sport	Dept for Business, Energy & Industrial Strategy
• Works with law enforcement and MI5 • Overall response to fraud against the individual and businesses • Economic crime • Serious and organised crime	• Works with the FCA, PSR and HMRC • Regulation of financial and banking sectors • Economic crime (regulations) • Insurance • Payments	• Works with Ofcom and the Information Commissioner's Office • Tech and Online • Data • Digital Identity • Telecomms	• Works with Comapnies House and National Trading Standards • Consumer policy • Corporate transparency • Trading standards
Ministry of Justice	**Attorney General's Office**	**Foreign, Commonwealth and Development Office**	**Dept for Work and Pensions**
• Works with HM Courts, Tribunal Service and Victim Support • Fraud Act 2006 • Victim strategy overall (victim support is managed by the Home Office)	• Works with Serious Fraud Office and Crown Prosecution Service • Disclosure • Criminal procedure rules	• Works with GCHQ, National Cyber Security Centre and MI6 • International relationships	• Works with the Pensions Regulator • Pensions fraud

Source: Home Office, 'Fraud Act 2006 and Digital Fraud Committee paper on cross departmental fraud responsibilities': https://committees.parliament.uk/publications/23100/documents/169176/default/

49. A number of law enforcement bodies have responsibility for tackling fraud. In England and Wales, these include the City of London Police who act as the lead force for fraud, Action Fraud, the National Fraud Intelligence Bureau (NFIB), the NCA and the NECC. Regional Organised Crime Units (ROCUs) are specialist policing units that provide capabilities at regional level (see Chapter 5).

50. To co-ordinate economic crime policy across the public and private sector, the Government convenes the Economic Crime Strategic Board (ECSB) (see Box 9). The ECSB, chaired by the Home Secretary and Chancellor, is a ministerial-level public-private board to oversee the Economic Crime Plan. The Economic Crime Plan 2019–22 set out plans to understand better the threat from fraud while at the same time promoting information-sharing, better victim reimbursement, and enhancing the overall response to economic crime.[104] In April 2021, a Statement of Progress set out further action to tackle fraud, including the delivery of a Fraud Action Plan, measures to improve the effectiveness and efficiency of the whole system response to economic crime, and to develop legislative proposals to tackle fraud, seize more criminal assets, and reform Companies House.[105]

51. Overseen by the ECSB, the Joint Fraud Taskforce (JFT) was relaunched in October 2021 by the then Home Secretary and is chaired by the Security

104 HM Treasury and Home Office, 'Economic Crime Plan, 2019 to 2022' (updated 4 May 2021): https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version [accessed 1 November 2022]

105 HM Government, *UK Finance, Economic Crime Plan: Statement of Progress: July 2019–February 2021* (April 2021): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/983251/Economic_Crime_Plan_Statement_of_Progress_May_2021.pdf [accessed 1 November 2022]

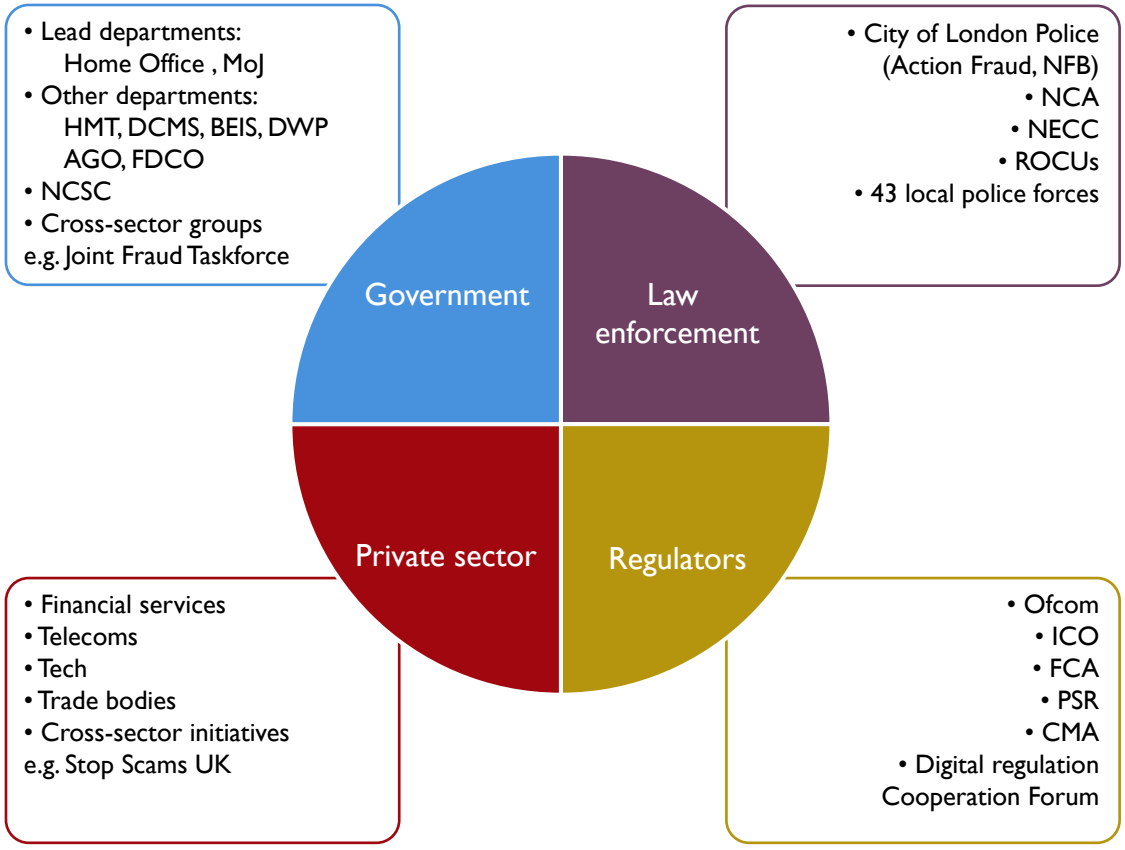
Minister.[106] The Taskforce is a partnership between the Government, the private sector and law enforcement, which is designed to foster collaboration (see Box 10).[107]

52. The two bodies suffer from a lack of transparency and infrequent meetings. The last set of publicly available minutes from the Economic Crime Strategic Board date from 2019.[108] It is understood that the JFT will continue under the new Security Minister Tom Tugendhat, however it has not yet met. [109] The Home Office confirmed to us that the JFT will meet in Autumn 2022 and the ECSB will meet in the new year.[110]

53. In addition to Government and law enforcement agencies, a number of regulators have a key role in fraud. These include the FCA, which regulates the financial service industry and the Payment Systems Regulator (PSR), which regulates payment systems like bank transfers and contactless payments. Ofcom regulates the telecommunications industry including tech platforms. The Competition and Markets Authority (CMA) is the regulator with responsibility for competition regulation and has recently established a Digital Markets Unit to oversee a new regulatory regime for digital firms that includes protecting consumers from unfair practices.[111] The Information Commissioner's Office (ICO) regulates data controllers and has responsibility for the Data Protection Act 2018 and the General Data Protection Regulations (GDPR), legislation critical to the efficacy with which fraud data can be shared.[112] These regulators are members of the Digital Regulation Cooperation Forum (DRCF) which was formed in July 2020 and fosters collaboration in tackling challenges posed by online regulation.[113] The PSR works alongside the forum but is not a member.[114]

106 Treasury Committee, *Economic Crime* (Eleventh Report, Session 2021–22, HC 145)
107 Home Office, 'Joint Fraud Taskforce' (updated 10 May 2022): https://www.gov.uk/government/collections/joint-fraud-taskforce [accessed 1 November 2022]
108 Available at gov.uk, 'Economic crime' (updated 21 September 2021): https://www.gov.uk/government/collections/economic-crime#economic-crime-strategic-board-minutes- [accessed 1 November 2022].
109 Q 255 (Tom Tugendhat and Duncan Tessier)
110 Confirmed in a private email dated 25 October 2022.
111 Competition and Markets Authority, 'Digital Markets Unit' (updated 20 July 2021): https://www.gov.uk/government/collections/digital-markets-unit [accessed 1 November 2022]
112 See regulator websites for more information.
113 Competition and Markets Authority, Information Commissioner's Office, Ofcom, and Financial Conduct Authority, 'The Digital Regulation Cooperation Forum' (10 March 2021): https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum [accessed 1 November 2022]
114 Competition and Markets Authority, 'Digital Regulation Cooperation Forum: Plan of work for 2021 to 2022' (10 March 2021): https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022 [accessed 1 November 2022]

Figure 8: Key stakeholders active in the response to fraud



54. The efficacy of the Government's multi-agency approach to tackling fraud is detailed in Chapter 5.

Legislative background

55. There are several pieces of legislation that are important when analysing the fraud landscape. The Social Market Foundation said that there is a "panoply of laws" relevant to the economic crime, cyber-crime and organised crime space, and they called for greater consolidation.[115] The key legislative tools are outlined in brief below. Chapter 6 contains more detail on the legislative instruments outlined below.

56. **The Fraud Act 2006** (see paragraph 426) came into force in 2007 with the objectives of clarifying and modernising the law surrounding fraud and to make fraud law more straightforward for juries and legal practitioners.[116]

115 Written evidence from the Social Market Foundation (FDF0026)

116 Ministry of Justice, *Post-Legislative Assessment of the Fraud Act 2006*, CP 680 (June 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1081360/fraud-memo-2022.pdf [accessed 1 November 2022]

Under the Act, a person is guilty of fraud if they are in breach of any of the following means of committing the offence:

(1) By false representation (Section 2): A representation may be express or implied. It is false if untrue or misleading and the person making it knows that this is or may be so. Most incidents fall within this category.[117]

(2) By failing to disclose information (Section 3): This applies where there is a legal duty to disclose it.

(3) By abuse of position (Section 4): Abuse of position applies where a person occupies a position in which they are expected to safeguard, or not to act against, the financial interests of another person. A person may abuse that position through an act or omission.[118]

57. The Fraud Act contains further offences relating to the possession, manufacture or supply of articles for use in frauds and obtaining services dishonestly.[119]

58. **The Computer Misuse Act 1990** (see paragraph 440) is the main UK legislation relating to offences using computer systems. Computer misuse covers any unauthorised access to computer material. The Act sets out the following key offences:

(1) Unauthorised access to computer material

(2) Unauthorised access with intent to commit or facilitate commission of further offences

(3) Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer

- 3ZA: Unauthorised acts causing, or creating risk of, serious damage
- 3A: Making, supplying or obtaining articles for use in offence under Section 1, 3 or 3ZA.[120]

59. **The Proceeds of Crime Act (POCA) 2002** covers the recovery and confiscation of proceeds derived from criminal activities and money laundering, and came into force on the 24 March 2002.[121] It provides the legal framework for freezing or seizing criminally obtained assets. The Crown Prosecution Service (CPS) has a specialist unit dedicated to asset recovery, the CPS Proceeds of Crime (CPSPOC) team. This works with

117 ONS, 'Nature of fraud and computer misuse in England and Wales: year ending March 2019': https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019#defining-fraud-and-computer-misuse [accessed 1 November 2022]

118 Thompson Reuters Practical Law, 'Financial crime in the UK (England and Wales) overview' (1 March 2020): https://uk.practicallaw.thomsonreuters.com/8-520-4390 [accessed 1 November 2022]

119 Fraud Act 2006, sections 2–4

120 CPS, 'Computer Misuse Act': https://www.cps.gov.uk/legal-guidance/computer-misuse-act [accessed 1 November 2022]

121 St Pauls Chambers, 'The Proceeds of Crime Act Explained', (2 November 2020]: https://www.stpaulschambers.com/the-proceeds-of-crime-act-explained/ [accessed 1 November 2022]

law enforcement agencies and multiple cross-government departments to recover assets.[122]

60. **The Data Protection Act 2018** (see paragraph 460) implemented EU General Data Protection Regulations (GDPR) into UK law. The Act controls how personal information is used by organisations, businesses or the government.[123]

61. **The Telecommunications (Security) Act 2021** (see paragraph 483) introduced a general duty for public electronic communications network and service providers to identify and reduce the risk of security compromises and prepare for their occurrence, as well as a duty on them to prevent, remedy or mitigate any adverse effects.[124]

62. In addition, there are a number of forthcoming Bills that are directly relevant to counter-fraud policy. These include the following:

    (a) **The Economic Crime and Corporate Transparency Bill** aims to tackle economic crime through reforms to empower Companies House, the companies registrar, with greater verification, investigation and enforcement powers (see Box 11). The Bill will also give law enforcement powers to seize and recover suspect cryptoassets and introduce new powers to bolster information sharing and intelligence gathering.[125] This Bill is the second of two Acts aiming to strengthen the UK's approach to economic crime. The Economic Crime (Transparency and Enforcement) Act 2022 came into force in March 2022.[126] It sets out measures to mandate the creation of a beneficial ownership register for overseas entities holding UK real estate, to strengthen unexplained wealth orders (UWOs), and to make it easier to prosecute individuals involved in "sanction-busting."[127]

    (b) **The Online Safety Bill** (see paragraph 528) will set new rules for firms that host user-generated content and search engines all to improve online safety. The Online Safety Bill includes a legal duty (in clauses 34, 35 and 36) for large online platforms (Category 1) and search engines (Category 2A) to take steps to prevent paid-for fraudulent adverts appearing on their services. It also includes further measures, including the requirement for in scope companies to conduct risk assessments in relation to the likelihood of illegal content appearing on their sites of platforms.[128]

    (c) **The Draft Digital Markets, Competition and Consumer Bill** (see paragraph 565) intends to tackle fake online reviews, boost competition by limiting the market power of big tech firms, empower the Digital

122 CPS, 'Proceeds of Crime': https://www.cps.gov.uk/crime-info/proceeds-crime [accessed 1 November 2022]
123 HM Government, 'Data protection': https://www.gov.uk/data-protection [accessed 1 November 2022]
124 Telecommunications (Security) Act 2021, Chapter 31
125 Economic Crime and Corporate Transparency Bill, Parts 1–6 [Bill 154 (2022–23)]
126 Economic Crime (Transparency and Enforcement) Act 2022, section 1
127 The Law Society, 'Economic Crime Act: what does it mean for law firms?' (5 August 2022): https://www.lawsociety.org.uk/topics/anti-money-laundering/economic-crime-act [accessed 1 November 2022]
128 House of Commons Library, *Analysis of the Online Safety Bill*, Research Briefing CBP9506, April 2022

Markets Unit and give greater powers to the CMA including to issue fines for breaches of consumer law.[129]

(d) **The Data Protection and Digital Information Bill** (see paragraph 480) plans to reform the UK's data protection regime. The Bill makes provision for the implementation of agreements on sharing information for law enforcement purposes.[130] The Bill is currently on hold, with Culture Secretary Michelle Donelan MP suggesting that the UK will introduce its own replacement for GDPR.[131]

(e) **The Financial Services and Markets Bill** was introduced to Parliament on 20 July 2022.[132] The Bill clarifies regulatory provisions that enable the PSR to use its powers to require mandatory reimbursement by payment services providers (PSPs) in cases of APP fraud. It will also bring some types of cryptoassets within the UK regulatory perimeter. The Bill also makes changes to the authorisation of financial promotions.[133]

129 HM Government, *The Queen's Speech 2022* (10 May 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1074113/Lobby_Pack_10_May_2022.pdf [accessed 1 November 2022]

130 Data Protection and Digital Information Bill, [Bill 143 (2022–23)]

131 'Britain to replace GDPR data privacy regime with own system', *Reuters* (3 October 2022): https://www.reuters.com/legal/litigation/britain-replace-gdpr-data-privacy-regime-with-own-system-2022–10-03/ [accessed 1 November 2022]

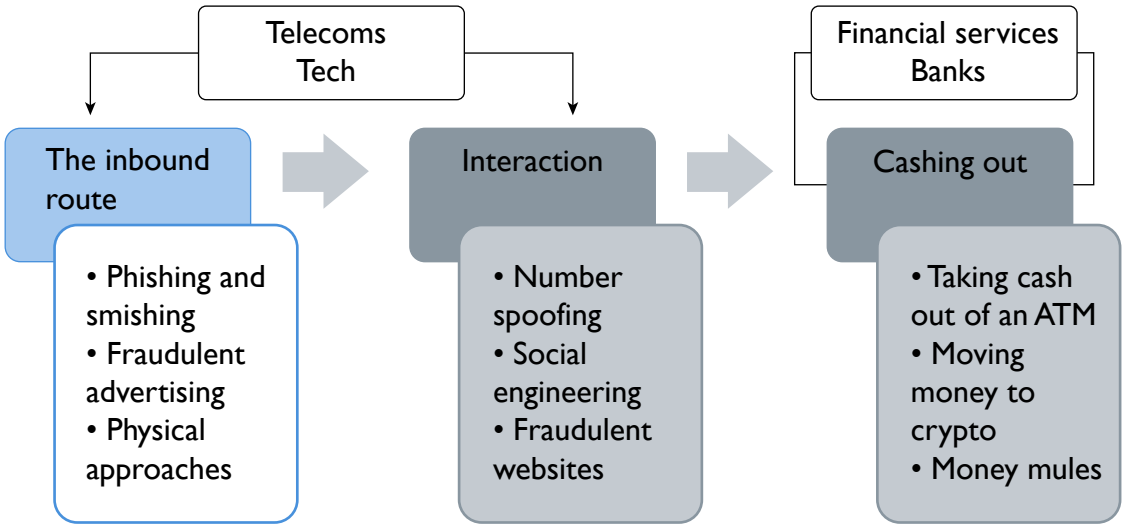
132 HM Treasury, 'Financial Service and Markets Bill': https://www.gov.uk/government/collections/financial-services-and-markets-bill [accessed 1 November 2022]

133 *Ibid.*, and explanatory notes to the Financial Services and Markets Bill [Bill 146 (2022-3)-EN]

CHAPTER 2: THE INBOUND ROUTE

63. During APP scams, criminals trick their victims into sending money directly from their account to an account that the criminal controls.[134] The inbound route is the first step in the fraud chain and describes the process by which a fraudster makes initial contact with a chosen victim or victims. There are several common ways in which a criminal may do this. Historically, a scam may have started with a knock at the door or flyer on the street. These methodologies are still used, but now most fraudulent approaches use technology due to the ready availability and reach of systems of mass communication such as bulk texting and online advertising.

Figure 9: The Fraud Chain: The inbound route



Source: Q 14 (Katy Worobec) and written evidence from CCSG (FDF0063)

Phishing and smishing

64. Phishing is the practice of sending fraudulent communication that appears to come from a reputable source. Smishing is the same practice but refers to the use of SMS text messages to defraud victims.[135] The ONS recognises phishing as one of the main methods used to commit fraud, however it only began including questions on phishing into the TCSEW October 2021 and therefore data is limited.[136] We attempted to source external statistics on the prevalence of phishing in the UK but as a result of our efforts believe that no comprehensive data on the scale of the problem exists.

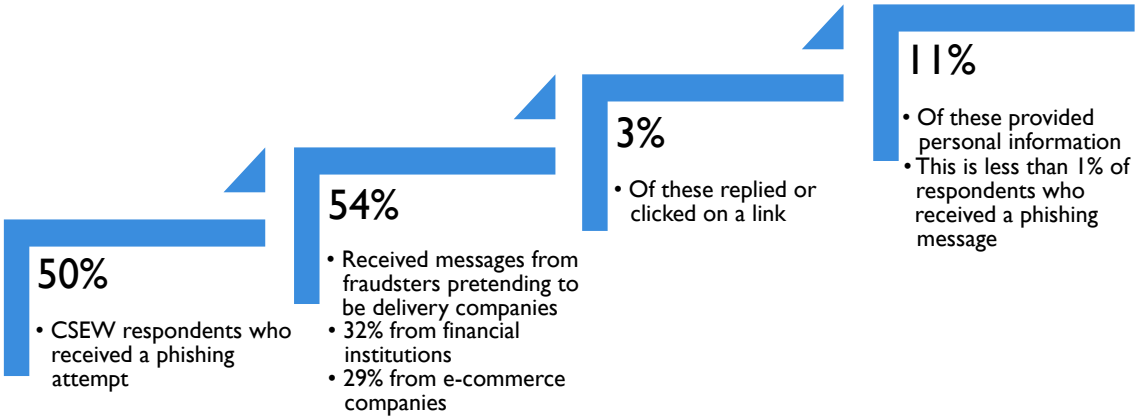
> *"It's a bit like the wild west at the moment, virtually on a daily basis we all get scamming texts and phone calls from scammers who are able to use the actual bank telephone numbers … such*

134 House of Commons Library, *Banking fraud*, Briefing Paper CBP8545, 23 February 2021
135 Cisco, 'What is Phishing?': https://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html [accessed 1 November 2022] and written evidence from BT Group (FDF0067)
136 ONS, 'Nature of fraud and computer misuse in England and Wales: year ending March 2022' (26 September 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022 [accessed 1 November 2022]

hijacking needs to be tackled and stopped at the engineering digital system level." - Graham [137]

65. ONS data from July 2022 shows that 50% (around 6,000) of respondents reported receiving an email, text, or social media message that may have been a phishing attempt in the previous month. Fraudsters were most likely to pretend to be from delivery companies (54%).

Figure 10: The prevalence of phishing attempts in England and Wales



Source: ONS, 'Crime in England and Wales: year ending March 2022' (21 July 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2022 [accessed 1 November 2022]

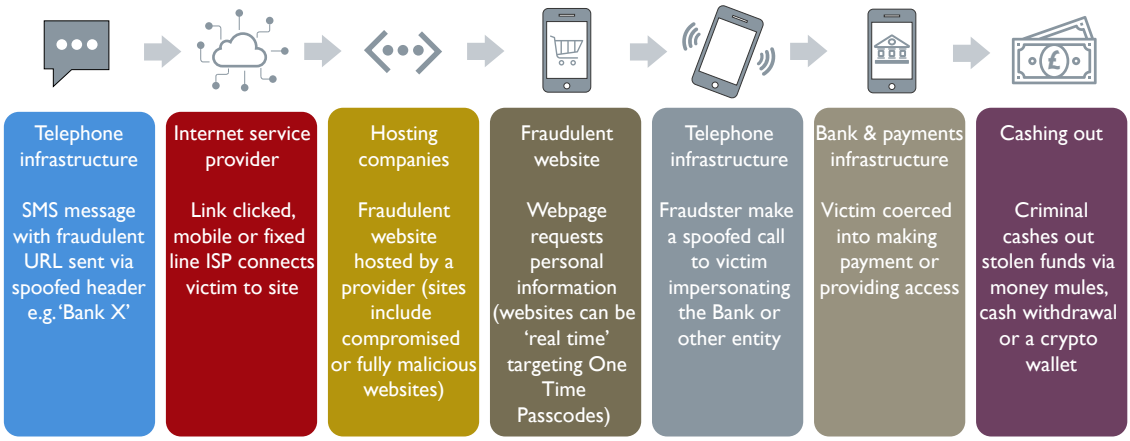
66. The prevalence of smishing can be explained in part by the widespread availability of SIM cards and the limited checks placed on those who purchase them. Professor Feng Hao, Professor of Security Engineering at the University of Warwick, told us that the process of catching fraudsters using smishing is akin to a game of 'cat and mouse' because, even when detected and shut down, the loss for criminals is relatively small and they are able to buy new SIM cards quickly and cheaply. He added that the lack of identity checks exacerbates this issue.[138] It is clear to us that more should be done to prevent such abuse. However, we recognise that greater identity checks at the point of purchase of a single SMS card for legitimate use may limit access to technology to some groups of people. Hamish MacLeod, Chief Executive of Mobile UK, told us:

> "Some countries insist on ID before you buy SIM cards; some do not. There is no evidence that that makes a difference in reducing this type of crime, but we worry a lot that it might create barriers to the socially excluded in accessing telephony."[139]

67. Additional checks on individual SIM card purchases may also have little beneficial effect because of the availability of bulk messaging services such as SIM farms (see paragraph 71) and SMS gateways in other countries.

137 Anonymous written evidence (FDF0102)
138 Q 233 (Prof Feng Hao)
139 Q 49 (Hamish MacLeod)

Figure 11: A phishing/smishing fraud chain



Source: Adapted from a UK Finance model shared via email

68. Criminals use smishing to obtain personal information and socially engineer the victim. The sophistication of cyber-enabled attacks such as phishing or smishing are growing.[140] Smishing messages may contain a URL and purport to be from a recognised authority such as a bank or the Government. This link will take victims to a fake website where the fraudsters will harvest data or seek to gain access to a person's financial accounts. In a second step, the fraudster may engage in number spoofing in order to make the scam seem more realistic as it appears to come from a trusted number. This step will be explored in Chapter 3.[141]

Box 2: Dale's story

In April 2022, Dale was a victim of digital fraud. Dale, who owned a building company, heard from his clients that they had received phishing emails from his BT email address requesting money transfers.

> *"Someone had broken into my email account, snooped around, looked to see who my current clients were, and sent out emails asking for payment. Fortunately, all recipients were suspicious, as I had never asked for any payments during face-to-face discussions."*

Dale's email account had been hacked by a fraudster. The criminal had used social engineering tactics to convince a BT call operator that they were Dale and they had forgotten his password, in order to allow them into Dale's account. The operator said they would send the scammer a four-digit code to Dale's mobile number to allow the password to be updated. The scammer convinced the operator that they had changed their mobile number, and the operator updated all the details accordingly to the scammer's phone number.

> *"That is all he needed to access my email account. I am still seething on how BT could do this without checking more deeply about passwords, mobile numbers etc."*

140 Cifas, 'This is Fraudscape 2022': https://www.fraudscape.co.uk/ [accessed 27 July 2022]

141 Home Office, 'Fraud sector charter: telecommunications (accessible version)' (updated 26 October 2021): https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version [accessed 1 November 2022]

Once the scammer had access to the account the criminal constructed believable phishing emails that were sent to clients. As with many APP frauds, the messages contained external links intended to draw individuals into transacting data or finances in a separate location. One of their phishing messages read:

> "Hi Adam, can you email my accounts team and get the 50% deposit paid so they can book in a provisional date as we are almost fully booked for the year the email for them is accounts2@[redacted].com. The deposit will need to be paid directly to them to the supplies manager for him to place the order. Cheers, Dale"

> *"The scammer even mimicked my signing off. When clients are new, I sign off with, 'Kind Regards'. Once we have met a couple of times I change to, 'Cheers'. The scammer had copied this to look genuine."*

Dale quickly got in touch with BT to find out what had happened and stop any further activity. In this case, the fraud was not successful because his customers recognised the warning signs and did not make payments to the fraudster.

In response to Dale's experience, BT said:

> "Our process involves asking a caller a number of security questions. In case of Dale, the scammer was able to provide an acceptable answer to a security question which we can only assume he guessed - that allowed the scammer to complete the verification process… We regret that our current customer verification process was not able to prevent a scammer from gaining access to Dale's BT and email account. However, we are in the process of strengthening this process to help prevent this type of fraud."[142]

Source: Written evidence from Dale (FDF0104)

69. The efficacy of smishing messages often relies on their connection to real-life situations and events. For example, Katy Worobec identified an uptick in fraudsters using the Ukraine crisis to manipulate victims, adding that "[fraudsters] use world events all the time to add credibility to the way in which they operate."[143]

70. The pandemic provided ample opportunities for fraudsters. The CPS told us that cyber criminals exploited the COVID-19 pandemic through the use of phishing, smishing and fake websites. For example, in August 2021, a criminal was prosecuted and jailed for sending fake smishing messages that purported to be from HM Revenue and Customs (HMRC). The messages were designed to trick victims into providing personal banking details after claiming that the recipient was eligible for a COVID-19 grant.[144]

71. The proliferation of smishing texts is exacerbated using so-called SIM farms. SIM farms are technological devices that can send thousands of texts an hour by connecting to multiple pay-as-you-go sim cards that do not require proof of identity unlike mobile phone contracts.[145] Hamish MacLeod

142 Additional supplementary written evidence from BT Group (FDF0098)
143 Q 14 (Katy Worobec)
144 Written evidence from the CPS (FDF0004)
145 'Text that could cost you THOUSANDS: The fake Royal Mail message that's snaring victims across the UK using cheap Chinese technology', *This is Money* (30 March 2021): https://www.thisismoney.co.uk/money/beatthescammers/article-9418729/Text-cost-THOUSANDS-fake-Royal-Mail-message-snaring-victims-UK.html [accessed 1 November 2022]

explained that there are two ways of routeing text messages: person to person (P2P) or application to person (A2P). A2P involves messages being sent from organisations, such as the NHS, to individuals. SIM farms are used by fraudsters to send out mass text messages by P2P routing. Macleod said SIM farms "are extremely hard to detect."[146] Superintendent Gerard Pollock told us how SIM farms are used in practice:

> "There are criminals … who are being allowed, on an ongoing basis, to buy hundreds of SIM cards, plug them into SIM farms and use them to pump out thousands of text messages every day to potential victims without any regulatory or compliance steps."[147]

Figure 12: A SIM farm device

Source: 'Covid fraud: £34.5m stolen in pandemic scams', BBC Click (24 March 2021): https://www.bbc.co.uk/news/technology-56499886. Image by Matt Quinton

72. The telecoms sector is vulnerable to manipulation by fraudsters located across the globe. The Fraud Advisory Panel, a counter-fraud charity, told us that "fraud often involves criminals (including organised crime groups) operating from overseas 'hard-to-reach' jurisdictions".[148] TrueCall Ltd, a telecoms technology company, added that this can compound the difficulties of catching fraudsters:

> "A lot of mass marketing fraud either originates or has links to criminals abroad. Fraudulent telemarketing and mailshots often originate from international centres, some of which are in jurisdictions that are difficult to gain local enforcement cooperation, or to trace individuals."[149]

Action to tackle phishing and smishing

73. We recognise that there is work being done, across both the public and private sectors, to mitigate the reach of smishing and phishing messages. However, the current approaches are uneven with counter-fraud policies being introduced inconsistently across the telecommunications sector. This is not a new problem and it has been allowed to continue for too long. We

146 Q 47 (Hamish Macleod)
147 Q 194 (Superintendent Gerard Pollock)
148 Written evidence from Fraud Advisory Panel (FDF0048)
149 Written evidence from trueCall Ltd (FDF0012)

believe much swifter and firmer action needs to be taken. Prof Hao said: "The telecom companies have some solutions, but they should do a lot more. So far, what they have done is the minimum and driven entirely by revenue."[150]

74. The main formal mechanism for coordinated telecommunications action on fraud is the Telecommunications Sector Charter created by the Government's Joint Fraud Taskforce. The charter committed signatories to tackling the impact of scam calls on customers, coordinating to tackle smishing, and more technical pledges such as using real-time checking to tackle SIM swap and Mobile Number Porting fraud. Signatories were BT, EE, Sky, Three, Tesco Mobile, Virgin Media & O2 and Vodafone.[151]

75. The Telecommunications Sector Charter sets nine key actions to help the sector to tackle fraud. The full charters, including others relating to Retail Banking and Accountancy, are provided in Appendices 4, 5 and 6. The nine key actions are as follows:

    (1) Identify and prevent scam calls

    (2) A coordinated approach to tackle smishing

    (3) Use of Dynamic Direct Debit (a pilot system to facilitate three-way authentication and authorisation at the point of sale between a customer, their bank and the telecommunications provider) in order to tackle identity theft and subscription fraud

    (4) Use of real-time checking to tackle SIM swap and Mobile Number Porting fraud

    (5) Sector information sharing

    (6) Systematic sector analysis of shared fraud and other intelligence

    (7) Engagement by law enforcement to investigate significant/repeated fraud against customers and providers

    (8) Improve support to victims

    (9) Increase fraud awareness

76. Under Action 2, signatories committed to block smishing by identifying and implementing new counter-smishing mechanisms. These included a review of the 7726–reporting service (see Box 16) and better information sharing with the National Cyber Security Centre (NCSC) and NFIB.[152] The Communications Crime Strategy Group (CCSG), a telecommunications sector body focussing on crime, told us that three out of four UK mobile network providers have now implemented SMS filters while others have applied additional technical controls on bulk SMS and financial controls on SIM use.[153]

150 Q 237 (Prof Feng Hao)
151 Home Office, 'Fraud sector charter: telecommunications (accessible version)' (updated 26 October 2021): https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version [accessed 1 November 2022]
152 *Ibid.*
153 Written evidence from the CCSG (FDF0063)

77. Hamish MacLeod told us that the telecommunications charter created five lines of defence within the industry. These include safety by design processes to encourage telecoms providers to make sure that they use reliable routes for buying text messaging and incorporate fraud defence technology into the mobile phones. As an example, MacLeod told us that Android phones now use text filtering and awareness functions to flag fraudulent text messages.[154]

78. To counter the threat of SIM farms, some firms are putting in place measures to prevent the ease with which SIM cards can be abused by such technology. Alex Towers, Director of Policy and Public Affairs at BT, told us that BT has introduced limits on the number of text messages any one SIM can send in a day (although the limit continues to remain high at around 2,000 per day) and BT have stopped selling low-cost bundles of mobile data that allow people to abuse SIMs for as low as £5.[155]

79. Given the global nature of the threat from phishing and smishing, private sector companies must work together. Will Semple said that eBay works with telecoms companies across the US, the UK and Europe to identify the senders of phishing/smishing texts operated from across the world and then take down the numbers.[156]

80. Alex Towers told us that BT had instituted a "Spam Shield" across the EE network to try to block out, at source, spam text messages.[157] According to Towers, since the creation of the shield, 80% of spam texts are blocked from the system and the numbers of reported scams and spam messages fell by over 90%.[158] In written evidence, BT said that since 2021, 120 million SMSs have been blocked and that collaboration between EE with other operators to collate data from the 7726 spam reporting mechanism allows the company to block numbers generating spam on their network.[159] Hamish Macleod added:

> "All service providers are doing something towards spam shields: All the operators are at some phase of implementing their spam text filters. We have three operational now and one in the phase of becoming operational."[160]

81. These strategies do have weaknesses. Action to tackle phishing and smishing is hampered by the lack of a comprehensive assessment of the scale of telephony-fraud. The CCSG suggested that the NECC could not estimate the amount of telephony-enabled fraud and, as a result, "it seems hard to direct private sector or law enforcement resources effectively unless there is better understanding of inbound fraud routes."[161]

82. The telecoms industry has not implemented existing counter-phishing measures with enough consistency. The Association of Chief Trading Standards Officers (ACTSO) told us that telecommunications providers can do more to prevent the spoofing of numbers and shut down numbers that are

154 Q 45 (Hamish MacLeod)
155 Q 47 (Alex Towers)
156 Q 125 (Will Semple)
157 Q 44 (Alex Towers)
158 *Ibid.*
159 Written evidence from BT Group (FDF0067)
160 Q 45 (Hamish MacLeod)
161 Written evidence from the CCSG (FDF0063)

being used to commit fraud.[162] This is particularly the case with the disjointed implementation of spam blocking technology. Adrian Gorham, Chair of the CCSG, told us that all the major operators now have the technology to roll out spam protections on their networks but that "it is just a question of going through the processes of tuning and so on."[163]

83. In addition to informal engagement with communications providers, Ofcom has several enforcement powers to tackle nuisance calls, including fraudulent calls:

- Ofcom has the power to request that telecommunications providers block access to numbers or services where they have been misused, including to facilitate fraud.[164] The most recent information on how often this has been used was published in December 2016 and shows that Ofcom issued directions against communication providers to prevent consumers receiving millions of nuisance calls from calls presenting certain 084 numbers. However, it is not clear whether these calls were considered fraudulent.[165] Ofcom was unable to provide more recent publicly available information on how often this measure has been used. These figures are now six years out of date.

- Since 2018, it can also withdraw number allocations from providers if they have been used to cause harm and the provider has not taken adequate steps to prevent this. Ofcom confirmed that it has not yet withdrawn numbers from a provider under these conditions.[166]

- Under sections 128 to 130 of the Communications Act 2003, Ofcom can take enforcement action against a person who has persistently misused a communications network or service. Ofcom has consulted on new proposals to develop a good practice guide to prevent scammers from accessing valid phone numbers. The regulator expects to publish a statement in Autumn 2022.[167]

84. The increased use of online messaging platforms has created a new threat. Fraudsters are able to circumvent filters placed on SMS services by using new internet-based messaging services to contact victims. Services such as WhatsApp, Skype, Zoom and Microsoft Teams all use internet technology called Voice over the Internet Protocol (VoIP). This technology allows telephone calls to be made via the internet.[168]

---

162 Written evidence from ACTSO (FDF0018)
163 Q 237 (Prof Feng Hao)
164 Ofcom, General Conditions of Entitlement: Unofficial consolidated version (17 June 2022): https://www.ofcom.org.uk/__data/assets/pdf_file/0030/238962/unofficial-consolidated-general-conditions-june-2022.pdf [accessed 1 November 2022] Nb. the GC was previously GC 20.3
165 Ofcom, *Tackling nuisance calls and messages: update on the ICO and Ofcom Joint Action Plan* (December 2016): https://www.ofcom.org.uk/__data/assets/pdf_file/0017/96110/ICO-Ofcom-joint-action-plan-2016.pdf [accessed 1 November 2022]
166 Ofcom, *General Conditions of Entitlement: Unofficial consolidated version* (17 June 2022): https://www.ofcom.org.uk/__data/assets/pdf_file/0030/238962/unofficial-consolidated-general-conditions-june-2022.pdf [accessed 1 November 2022] B1.18 (d), (e); Ofcom confirmed this in a private email dated 14 September 2022.
167 Ofcom, *Tackling scam calls and texts: Ofcom's role and approach* (23 February 2022): https://www.ofcom.org.uk/__data/assets/pdf_file/0018/232074/statement-tackling-scam-calls-and-texts.pdf [accessed 1 November 2022]
168 See BBC News, 'Internet revamp for the humble landline' (16 August 2021): https://www.bbc.co.uk/news/technology-58233420 [accessed 1 November 2022]

85. BT told us that the incorporation of encrypted VoIP services, such as WhatsApp, into the telecommunications system limits the ability of telecoms providers to police fraudulent communication. They said:

> "The rise of encrypted services creates new opportunities for fraudsters, about which telecoms companies can do nothing… if a user is deceived into contact with a fraudster on an encrypted platform such as WhatsApp or Apple's iMessage (the way many Apple phone users message each other) then telcos have no visibility of any aspect of these communications …"[169]

86. WhatsApp is an encrypted instant messaging service owned by Meta. It offers VoIP services although it requires a cellular mobile number to operate. In February 2021, Lloyds Bank found that WhatsApp scams have surged by more than 2,000% in a year, with this type of crime being recognised as the fastest growing form of impersonation fraud. This type of fraud often involves criminals posing as family members or friends in difficulty, claiming that they have had to change their number due to a lost phone.[170]

Box 3: Graham's story

Graham's daughter was tricked into an APP fraud and sent money to a scammer's bank account. The scammer convinced her that he was a trusted family member by 'hijacking' a telephone number in a WhatsApp group that she was a member of.[171]

> *"My daughter didn't see any reason to question the source particularly because the fraudster had not initially asked her for money but had managed to continue a relevant conversation."*

When she realised the scam, Graham's daughter quickly got in touch with her bank, which told her that she should have asked more questions of the person claiming to be her brother. The family also contacted the fraudster's bank and Graham argues that it was a "major failure" that the bank did not freeze the account at that point.

Graham makes the case that more should be done to enable banks to use their powers to recover funds, freeze transactions and track payments more closely when they appear suspicious. He said that the inability or unwillingness of banks to act is leading to billions of pounds in losses for many people and suggests that more needs to be done to improve preventative technology.

Graham argues for a 'guardian angel' system, whereby a trusted third party can be appointed to watch over transactions if they appear suspicious.

169 Written evidence from BT Group (FDF0067)

170 Lloyds Bank, 'Fraud Warning: number of WhatsApp scams has surged by more than 2000% in a year' (31 January 2022): https://www.lloydsbankinggroup.com/assets/pdfs/media/press-releases/2022-press-releases/lloyds-bank/31.01.2022-whatsapp-scams-surge-over-200-per-cent-in-a-year.pdf [accessed 1 November 2022]

171 Anonymous written evidence (FDF0102)

> *"Many of us do realise that we may be vulnerable either because of age or simply not being tec savvy and would support a system whereby we could designate a trusted third party to our bank. This would enable the bank to check with the third party, a Guardian Angel, independently to check out any suspicious transactions before proceeding."*

Graham's daughter has since received full reimbursement, however Graham expressed frustration at the hurdles it took to achieve this outcome.

Meta told us that they were "sorry to hear of the distressing situation [Graham] and his family have experienced" but said that the company was unable to comment on the specific case without more details. It noted Meta's ambition for WhatsApp to be the "safest place for private, personal communication" and raised the importance of encrypted messaging, simple number blocking and reporting tools, and two-step verification. WhatsApp also operates machine learning systems, which are used to detect bulk and automated messaging. It said that more than 70% of bans for suspected spam or scam behaviour is made before a user reports to WhatsApp.[172]

Source: Written evidence from Anonymous (name has been changed) (FDF0102) and supplementary written evidence from Meta (FDF0099)

87. Given that WhatsApp and other online messenger services are encrypted, they are harder to police than other SMS based messaging services, even by the owners of the platform. Rob Jones, Director General of the NECC, said: "WhatsApp has been end-to-end encrypted since 2014. If WhatsApp wanted to go after content that is fraudulent on that platform, it could not do it, because it has locked itself out of its own content."[173] We recognise the abuse of end-to-end encrypted platforms such as WhatsApp as an issue that must be urgently addressed by tech companies, however we also appreciate that policing such messages would require significant intrusion of privacy.

88. Meta, the owner of WhatsApp, acknowledged that their ability to identify variations in IP address is undermined by the use of Virtual Private Networks (VPNs) which can falsify the locational appearance of a device.[174] As variations in location and country code are a hallmark of fraudulent phishing messages, WhatsApp's vulnerability to VPN manipulation is a concern in relation to counter-fraud policy. Meta has built-in protections that aim to mitigate fraudulent phishing activity including two-factor authentication and warnings displayed when a WhatsApp user receives a call or message for the first time from another user who is not in their contact list.[175]

89. Concerns have been raised about two other Meta owned online messaging platforms, Instagram and Facebook Messenger. Research by TSB found that between January and March 2022, 70% of cases of investment fraud reported to them (where a platform was recorded) started on Facebook or Instagram, either through adverts or direct messaging.[176] Katie Martin, Markets Editor at the Financial Times, told the Committee that at the time

172 Supplementary written evidence from Meta (FDF0099)
173 Q 218 (Rob Jones)
174 Written evidence from Meta (FDF0052)
175 *Ibid.*
176 Written evidence from TSB (FDF0066)

of giving evidence a scammer was impersonating her on Instagram and direct messaging people to con them into APP crypto-frauds.[177]

90. The current regulatory system does not impose sufficient leverage or incentives on digital platforms to combat fraudulent online messaging, particularly in comparison with the liability placed on the banking sector. TSB concluded:

> "Tech firms and social media companies have huge power and resources but are regulated as if they did not. The financial services industry is heavily regulated by bodies with enormous power to enforce and penalise banks and rightly so. However, the largest social media firms and tech companies (who are some of the largest companies in the world) are regulated as if they have no power or responsibility to their users."[178]

91. In-app messaging services are in scope of the Online Safety Bill, and thus subject to the same duties in relation to user-generated fraud and to prevent fraudulent advertising as tech platforms. However, SMS and email are not.[179] The Committee's analysis of the Online Safety Bill is found in paragraph 528.

92. It is clear that Ofcom needs to do more to enforce the powers it has to bring the tech and telecoms companies it regulates in line. The regulator is due to receive expanded powers under the Online Safety Bill and should face greater scrutiny as a result. The National Audit Office (NAO) is described by the regulator as its external auditor and the NAO has reported on Ofcom in the past, most recently in 2019.[180] We consider that an updated review may be in order given Ofcom's expanded remit and powers however that is a decision for the NAO to make.

93. **Phishing and smishing techniques are among the most prolific business models operated by fraudsters. Sending scam emails and texts is a simple and effective tactic, conductible speedily and in volume. While steps have been taken by telecoms companies to prevent such tactics, fraudsters continually evade these efforts and exploit new avenues to reach victims. The Committee believes much swifter and firmer action by telecoms companies needs to be taken to reduce the quantity of fraudulent communications slipping through the net. Ofcom has a broad remit and increasing powers. The level of accountability for Ofcom's regulation of telecoms companies must therefore increase accordingly.**

94. ***Ofcom must carry out a comprehensive assessment of telephony fraud in order to tackle the worrying information deficit on the scale of the problem. It must bolster its use of, and report on how often it uses, its enforcement powers to hold telecoms and tech companies to account for telephony-based scams. For example, it should report the frequency with which it has used its General Conditions to request***

177 Q 70 (Katie Martin)
178 Written evidence from TSB (FDF0066)
179 Ofcom, *Online Safety Bill: Ofcom's Road to Regulation* (6 July 2022): https://www.ofcom.org.uk/__data/assets/pdf_file/0016/240442/online-safety-roadmap.pdf [accessed 1 November 2022]
180 See Ofcom, *Annual report and accounts 2021/22* (2022): https://www.ofcom.org.uk/__data/assets/pdf_file/0022/240727/annual-report-2021–22.pdf [accessed 1 November 2022] and NAO, *Regulating to protect consumers in utilities, communications and financial services markets* (20 March 2019) https://www.nao.org.uk/wp-content/uploads/2019/03/Regulating-to-protect-consumers-in-utilities-communications-and-financial-service-markets.pdf [accessed 1 November 2022]

that numbers are blocked due to fraudulent activity being detected. It should publish this information as part of an annual fraud report presented to Parliament.

95. ***The ever-increasing role and powers of Ofcom and wider digital regulation should be subject to enhanced parliamentary scrutiny. We add our voice to that of the Communications and Digital Committee in supporting the recommendation of the Joint Committee on the Online Safety Bill that digital regulation requires dedicated parliamentary oversight and therefore a Joint Committee of both Houses should be established to perform this role.***

96. ***In addition, we suggest that Ofcom should face further oversight as part of wider scrutiny of the DRCF (see paragraph 563) and that Ofcom should be part of the NECC (see paragraph 284).***

Romance fraud

97. Online dating is commonplace in the UK. Use of dedicated dating apps such as Bumble, Tinder, Hinge as well as social media platforms including Facebook and Instagram have joined websites including Match.com and eHarmony in providing opportunities to meet people online. Research shows that a third (32%) of relationships that began between 2015 and 2019 started online, compared to only 19% between 2005 and 2014.[181]

98. The pandemic encouraged many people to turn to internet services. In the year to April 2021, consumer group Which? found that romance fraud had increased by 40%, with over 7,500 reported scams.[182] This trend has not changed in the time after the pandemic. At the time of writing, the previous 13 months have seen 8,848 reports of dating fraud, with reported losses totalling £99.7 million. 100% of these cases were cyber-enabled.[183]

99. While young people typically might be expected to use online dating services more frequently, as many people aged 50 to 59 fell victim to a dating scam in the last 13 months as those aged 20 to 29 (1,600).[184]

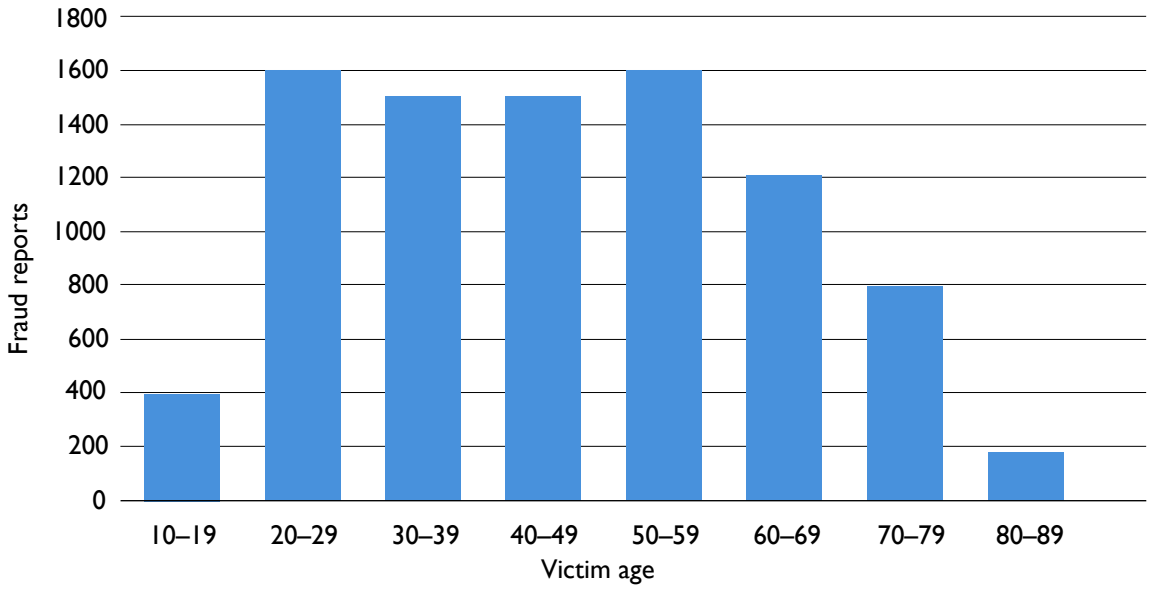
181 Sky News, 'Finding love online: more than half of couples set to meet via the internet' (27 November 2019): https://news.sky.com/story/finding-love-online-more-than-half-of-couples-set-to-meet-via-the-internet-11871341 [accessed 1 November 2022]

182 Which?, 'Romance fraud soared by 40% during the pandemic, Which? warns' (11 June 2021): https://press.which.co.uk/whichpressreleases/romance-fraud-soared-by-40-during-the-pandemic-which-warns/ [accessed 1 November 2022]

183 City of London Police, 'NFIB Fraud and Cyber Crime Dashboard: 13 months of data': https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46 [accessed 1 November 2022]

184 *Ibid.*

Figure 13: Romance fraud victims by age



Source: City of London Police, 'NFIB Fraud and Cyber Crime Dashboard: 13 months of data' [accessed 1 November 2022]

100. Furthermore, while online dating platforms are often used for the purpose of forming relationships online, other online messaging and social media platforms may also be used to date online. Which? identified romance scammers operating on platforms such as LinkedIn or even online gaming platforms.[185]

101. The Online Dating Association, a dating app trade association, told us that those who are most vulnerable to fraud are "those that are lonely or isolated and looking for connection".[186] It typically involves a victim being duped into sending money to a criminal who has convinced them, sometimes over significant periods of time, that they are a genuine romantic partner. Criminals gain their victims' trust using social engineering techniques (see paragraph 161).[187]

185 Which? 'Online dating 'romance' scams up 40% through the pandemic' (11 June 2021): https://www.which.co.uk/news/article/online-dating-fraud-up-40-through-pandemic-aKHlv5M09iYX [accessed 1 November 2022]

186 Written evidence from the Online Dating Association (FDF0028)

187 Action Fraud, 'Romance fraud': https://www.actionfraud.police.uk/a-z-of-fraud/dating-fraud [accessed 1 November 2022]

Box 4: Rachel's story

In 2021, Rachel was the victim of a romance scam that originated on Facebook and led to the loss of £113,000. After experiencing a break-up, Rachel connected with the fraudster online. He told her that his wife had died of breast cancer and that his daughter was encouraging him to meet someone new. The two began to message via text, and it appeared the scammer was using a UK number.

During the fraud the two never met in person. He then told Rachel that he had secured an engineering contract in Ukraine. On allegedly arriving in Ukraine, the scammer asked her for £250 to cover a tax issue with his business. Rachel trusted the fraudster and conducted due diligence, confirming the details of the supposed company on Companies House (see Box 11).

Rachel believes that this small initial payment was intended to "suck her in" to a spiral of increasing payments. The fraudster used manipulative social engineering techniques to pressurise the victim into borrowing more money. This included claiming that his passport had been stolen and that he was being held hostage until he could pay to get it back.

> *"He sent me pictures of himself locked in a cellar with only a bucket to wash in."*

Over a period of three months, Rachel borrowed £90,000 and spent £20,000 in personal savings to send payments to Ukraine.

When the police were eventually alerted by the banks, Rachel misled the police about her spending because she believed the fraudster was going to be murdered if he could not raise the money to pay back the loan sharks. This demonstrates how effective social engineering can be.

Rachel realised that she had been defrauded when she visited the address that the fraudster had given her as his home. After Rachel disclosed the reality of the situation to the police, she felt that she had experienced victim shaming. She claimed that she was told by police that the fraud was her fault, and that officers could not be held responsible given the falsified information she had declared. This was compounded by letters from Santander and HSBC, which said that they could not refund her as she had willingly transferred the funds.

> *"The police told me it was my fault, but a person who is a victim of burglary is not asked by the police if they put up a fight, and a victim of theft is not asked why they don't have CCTV. When you are a victim of fraud, you are made to feel as if you are the criminal."*

The impact on Rachel has been financially and emotionally devastating. Rachel experienced a mental breakdown and described the trauma of her experience. She told us that she felt stupid and had lost trust in the police and other people, including friends.

In response to Rachel's experience, Santander called for greater incentivisation- and accountability for fraud enablers including social media and telecoms companies. The bank said:

> "Unfortunately, despite repeatedly warning her of the dangers of transferring money to someone she hadn't met and directly raising our concerns that this was a scam with Rachel and the police, she confirmed that she wanted to proceed with payments … Due to the strength of the social manipulation by the scammer, Rachel hadn't accepted that she was being scammed when she decided to transfer funds to HSBC. Consequently, we did not have her required consent to raise a scam claim or to contact HSBC."[188]

HSBC said it noted its commitments under the CRM Code and confirmed that it had "fulfilled our responsibilities under the CRM code" as the customer was provided with fraud warnings and still proceeded with the payments. It added that "we work hard to ensure fair and reasonable outcomes for all customers who fall victim to scams".[189]

Source: Rachel spoke to the Committee at an engagement event on 7 July 2022.

Action to tackle romance fraud

102. There are several strategies that can be used to reduce the ability of fraudsters to commit digital fraud that relies on impersonation of others or concealing a true identity, such as in the case of romance fraud. These include the implementation of stringent user verification policies, referred to as know-your-customer (KYC) checks.

103. Identity verification has already been adopted by some online dating platforms. Fluttr was launched on Valentine's Day 2022 emphasising the unique pledge to root out romance fraudsters. The app was launched in the wake of renewed interest in the issue of romance fraud thanks to documentaries including Netflix's *The Tinder Swindler*. Graham Pullan, CEO of Fluttr, told us that the app relied on biometric identity verification:

> "This means that all our customers are verified at the very start of the process. We do it by matching the image of the user's face to their photo ID or their chosen photo ID, which in the UK is typically a passport or a driving licence. That is done using biometric face-matching technology."[190]

104. Biometric testing involves matching a user of an online service, such as a dating platform, to a known characteristic. Examples include retina scans, fingerprints, facial and voice recognition. HSBC reports a reduction by 50% of telephone banking fraud since the introduction of biometric security using voice identification.[191]

105. While biometrics may have significant benefits in reducing fraud risks, we have also heard concerns that they are intrusive. Prof Hao told us that increased use of biometrics might require a central database of biometrics,

188 Written evidence from HSBC (FDF0106)
189 *Ibid.*
190 Q 135 (Graham Pullan)
191 Computer Weekly, 'HSBC blocks £249m in UK fraud with voice biometrics' (6 May 2021): https://www.computerweekly.com/news/252500302/HSBC-blocks-249m-in-UK-fraud-with-voice-biometrics [accessed 1 November 2022]

raising further privacy concerns.[192] Professor Victoria Nash, Director at the Oxford Internet Institute cautioned that, as a guiding principle, society should "only ever require the minimum amount of information needed to carry out whatever the activity is in a risk-reducing way."[193]

106. In February 2021, DCMS published a draft UK Digital Identity and Trust Framework setting out plans to make it easier for people to verify their identity online.[194] This follows the rollout of the Government's previous Verify platform, which faced criticism due to its low success rate and high cost, and was terminated in 2021.[195] The beta version of the new framework was published in June 2022 and will undergo additional testing in collaboration with industry, civil society and the public.[196] The Data Protection and Digital Information Bill currently is on hold. However, it is expected to establish the regulatory framework for the provision of digital identity verification services in the UK.[197] The Minister for Tech and the Digital Economy told us that creating a robust digital identity framework is an ongoing piece of work.[198]

107. The Online Safety Bill will also introduce new measures requiring Category 1 companies to ensure adult users are given the option to verify their identity.[199] Identity theft is tackled in more detail in paragraph 453.

108. There are tools that individual consumers can use to minimise their fraud risk. For example, a 'catfish'—someone who uses a false identity and fake images to lure victims towards their profile—can be tested for through use of reverse image search, however the onus is on the user to use and operate this technology to detect prospective romance fraudsters. Joe Lycett said:

> "Then there are things such as reverse image search … It is a very simple thing you can do. If you get a message from somebody and it has an image—let us say on their WhatsApp—you can take that image and put it into Google image search and it will look to see if that image has been used anywhere else. Often that will reveal that it has been used millions of times … "[200]

109. The Online Dating Association said that despite the availability of new technologies, background checks and ID verification, "dating services will continue to be vulnerable to romance and investment fraud, as it is a convenient way for fraudsters to attempt to meet victims."[201]

---

192 Q 235 (Prof Feng Hao)
193 Q 57 (Prof Victoria Nash)
194 DCMS, 'The UK digital identity and attributes trust framework' (11 February 2021): https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework [accessed 1 November 2022]
195 Cabinet Office, Government Digital Service and Julia Lopez MP 'Julia Lopez speech to The Investing and Savings Alliance' (2021): https://www.gov.uk/government/speeches/julia-lopez-speech-to-the-investing-and-savings-alliance [accessed 1 November 2022]
196 DCMS, 'UK digital identity and attributes trust framework: beta version' (13 June 2022): https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version [accessed 1 November 2022]
197 Explanatory Notes to the Data Protection and Digital Information Bill [Bill 143 (2022–23)-EN]
198 Q 271 (Damian Collins MP)
199 DCMS, 'Online Safety Bill: Factsheet' (updated 19 April 2022): https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet [accessed 1 November 2022]
200 Q 100 (Joe Lycett)
201 Written evidence from the Online Dating Association (FDF0028)

110. **Online dating is now a common means by which many seek to meet new people. Easy access to potentially vulnerable, isolated or lonely people makes these platforms prime targets for exploitation by fraudsters. Furthermore, as continued technological developments proliferate, fraudsters will find new ways to perpetuate false identities online. We are aware of the wider privacy issues surrounding debate on identity verification, particularly in light of the Data Protection and Digital Information Bill. However, in the context of online dating it is clear that identity verification is a crucial first step in stamping out romance fraudsters.**

111. ***The Online Safety Bill must be amended to ensure that dating platforms are subject to mandatory identity verification processes in order to establish that their users are genuine.***

112. ***As part of platforms' efforts to design-out fraud (see paragraph 131), online dating platforms must be required to implement checks such as proactively deploying reverse image search, rather than placing the onus on users to do so.***

Fraudulent advertising

113. Fraudulent advertising is another key method used by criminals to reach their victims. Using this business model, victims are scammed after clicking on fraudulent adverts that appear on online platforms and search engines.

114. The nature of advertising varies across platforms. Some major internet services such as Facebook. Instagram or Google use advertising as a central revenue stream. Other platforms including eBay and Amazon host and publish material for e-commerce purposes and integrate advertising within their websites.[202] There is currently no legal duty imposed upon internet platforms and social media companies compelling them to run KYC checks on their advertising customers.[203]

Box 5: Crypto investment scams

As noted, the cryptoasset market has grown at rapid pace since its inception over a decade ago. Investment in cryptoassets has drawn a huge number of backers following the success of the first crypto coin known as Bitcoin. Katie Martin, explained why investing in crypto is so popular:

> "There is the idea that the price of bitcoin, the earliest crypto coin, shot to the moon, so that if you get in at an early stage on a lot of other tiny little crypto coins, perhaps you could enjoy those sorts of riches too. It is rarely made clear enough in the advertising around that that you are taking a huge risk with your money and that you could lose all of it."[204]

202 Q 123 (Will Semple)
203 Treasury Committee, *Economic Crime* (Eleventh Report, Session 2021–22, HC 145)
204 Q 70 (Katie Martin)

While many crypto investment advertisements may be legitimate, albeit risky, fraudsters have capitalised on this avenue in order to scam would-be investors. Crypto investment scams are on the rise. In 2021, crypto crime amounted to a $14 billion industry.[205] Tom Mutton, Director for Central Bank Digital Currency at the Bank of England, broke this down, explaining that two thirds of crypto thefts related to decentralised finance (De-Fi) protocols, which is an umbrella term for cryptoasset projects that do not have a traditional, centralised intermediary (like a bank).[206] He added that "the majority were crypto scams, including things like rug pulling and other fake investment scams. They were worth $7.8 billion, up 82%."[207]

Many investment scams are advertised cheaply and easily online. The Advertising Standards Authority (ASA), the UK's independent, voluntary and self-regulatory advertising body, told us that the majority of Scam Ad Alerts it sent over the last 12 months have been for scams relating to cryptocurrency. However, it also sent alerts for other scam types, including fake energy saving devices and diet pill subscription scams.[208] The NCSC has reportedly removed over 74,000 online scams and 90,000 URLs specifically associated with cryptocurrency investment scams between April 2020 and March 2022.[209]

Katie Martin suggested that while regulating cryptoassets is a complex task, regulation could be introduced relatively quickly in order to control how these adverts reach the public because, at present, "anybody can launch a coin … anybody can advertise that coin."[210] She also suggested that the Government should work with industry and regulators to launch an awareness campaign around the dangers of investing in cryptocurrency.[211]

While cryptoasset scams are the most frequently reported scam to the FCA, the regulator may have limited power to tackle this threat as often these scams are not linked to genuine cryptoasset firms. To tackle this, the FCA runs campaigns to inform speculative investors about the risks of investing (see 'InvestSmart', Box 12). In August 2022, the FCA set out new rules for high-risk investments subject to financial promotion rules, however it noted that "cryptoasset promotions are currently outside our remit." The FCA intends to publish rules for crypto promotions after legislation has been introduced to bring qualifying cryptoassets within the financial promotions regime under Chapter 2 of the Financial Services and Markets Bill.[212]

115. Given the pace of technological change, it is highly likely that new technologies will provide new opportunities for fraudsters to reach consumers. For example, there is a risk that an increased uptake in smart devices may lead

205 Chainalysis, *The 2022 Crypto Crime Report* (February 2022): https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf [accessed 1 November 2022]
206 'The FT crypto glossary', *Financial Times* (21 October 2021): https://www.ft.com/content/df9f5795-2aaf-4088-a76e-304056db61ef [accessed 1 November 2022]
207 Q 161 (Tom Mutton)
208 Written evidence from the ASA (FDF0022)
209 Money Saving Expert, 'Over 74,000 scams axed after 10 million-plus reports to the Government: what to do if you've been scammed' (18 March 2022): https://www.moneysavingexpert.com/news/2022/03/over-90-000-scams-involving-cryptocurrencies-and-more-have-been-/ [accessed 1 November 2022]
210 Q 71 (Katie Martin)
211 Q 79 (Katie Martin)
212 FCA, 'PS22/10: Strengthening our financial promotion rules for high-risk investments and firms approving financial promotions' (1 August 2022): https://www.fca.org.uk/publications/policy-statements/ps22-10-strengthening-our-financial-promotion-rules-high-risk-investments-firms-approving-financial-promotions [accessed 1 November 2022]

to new avenues for fraudsters to contact and manipulate victims. Prof Nash said:

> "For example, the role of smart speakers, non-screen-based technologies. What does it mean, for example, if I ask my smart speaker at home to give me information about a financial product? Are we sure that the sorts of cues and information we rely on platforms to provide will work in that context? Equally, with IoT—internet of things—devices, such as navigation systems, is there any way your navigation system can be hacked to push you towards particular garages? There could be new forms of mobile phone scams."[213]

116. The Government has recognised the cyber-security threat posed by the rise in smart technology through the Product Security and Telecommunications Infrastructure Bill, which will provide for minimum security requirements in consumer connectible products, place compliance duties on the makers, importers and distributors of these products, and introduce powers to allow breaches to be punished.[214]

117. Without sufficient futureproofing, technology will most likely continue to create new opportunities for fraudsters to target victims. For example, the metaverse—a digital world in which experiences and interactions occur within a virtual space—may be open to abuse by fraudulent advertisers.[215] Callsign Ltd, a digital identity company, told us that the metaverse "will create additional avenues for existing fraud methods to be applied."[216] The FCA warned that it is not clear whether KYC checks applicable in the real world will apply in the metaverse, nor is it clear who will have responsibility for the oversight of such spaces. It cautioned that "the jurisdictional issues regarding 'where' misconduct in the metaverse occurs, and how regulators and law enforcement can engage effectively, must be tackled now rather than when harm occurs".[217]

Action to tackle fraudulent advertising

118. Online advertising is regulated by the ASA. Its Scam Ad Alert System was launched in June 2020 in partnership with online platforms and digital advertising companies. It resulted in 1,251 reports and 67 alerts from March 2021 to 2022. This information is then shared with platforms, which reported that 765 ads and/or accounts had been removed as a direct result of alerts.[218] While we welcome efforts to tackle fraudulent advertising via collaboration, we consider the number of alerts to be considerably out of proportion to the scale of the issue.

---

213 Q 59 (Prof Victoria Nash)

214 DCMS, 'Product Security and Telecommunications Infrastructure (PSTI) Bill: Factsheets' (24 November 2021): https://www.gov.uk/government/collections/the-product-security-and-telecommunications-infrastructure-psti-bill-factsheets [accessed 1 November 2022]

215 BBC News, 'Apparently, it's the next big thing. What is the metaverse?' (18 October 2021): https://www.bbc.co.uk/news/technology-58749529 [accessed 1 November 2022]

216 Written evidence from Callsign Ltd (FDF0038)

217 Written evidence from the FCA (FDF0069)

218 Written evidence from the ASA (FDF0022) and DCMS, 'Online Advertising Programme consultation': https://www.gov.uk/government/consultations/online-advertising-programme-consultation/online-advertising-programme-consultation [accessed 1 November 2022]

119. In written evidence to the Committee, the ASA acknowledged that the current regulatory approach is not properly equipped to deal with online advertising fraud. They said:

> "While we play an active role in seeking to disrupt scam ads, as a non-statutory body that was not established for and is not equipped to tackle fraud, we do not investigate them because criminals, who have little regard for the law, clearly have no incentive to comply with the UK advertising rules."[219]

120. In addition to self-regulatory action, there are several additional activities either in train or being planned to tackle fraudulent advertising.

The Online Safety Bill

121. The Government is working to enhance digital safety through the Online Safety Bill. At the time of writing, its passage has been subject to further delays. The information in our report will reflect the Online Safety Bill that was published prior to the Parliamentary summer recess.

122. Fraud is designated as 'priority illegal content' under the Online Safety Bill. It includes a legal duty (in clauses 34, 35 and 36) for large online platforms (Category 1) and search engines (Category 2A) to take steps to prevent paid-for fraudulent adverts appearing on their services. Under clause 34(1), large social media platforms (Category 1) must put into place proportionate systems and processes to:

    (a) Prevent individuals from encountering fraudulent advertising,

    (b) Minimise the amount of time that fraudulent advertising is present, and

    (c) Swiftly remove fraudulent advertising once they are made aware of it through any means.[220]

123. We have identified several issues with the Online Safety Bill. In brief, these include:

- The inadequacy of metrics used to categorise companies in-scope
- The status of intermediary platforms
- The role of identity verification
- The role of a joined-up regulatory system for enforcing the legislation
- The applicability of principles to the telecoms sector
- The position of organic and influencer content

124. The Committee's full assessment of the Online Safety Bill is found in paragraph 528, and some of these issues may soon be addressed in the Government's forthcoming Online Advertising Programme.

---

219 Written evidence from the ASA (FDF0022)

220 House of Commons Library, *Analysis of the Online Safety Bill*, Research Briefing. CBP 9506, 8 April 2022

Online Advertising Programme

125. The Government is in the process of finalising its review of the Online Advertising Programme (OAP). The Programme is being led by DCMS with the aim of reviewing the regulatory framework for paid-for online advertising and tackling "the evident lack of transparency and accountability across the whole supply chain."[221] While the Online Safety Bill only covers platforms and search engines, the OAP is likely to include advertisers, media agencies, intermediaries, and publishers (see Table 1).

Table 1: Inexhaustive list of actors in the advertising supply chain in scope of the Online Safety Bill (OSB) and Online Advertising Programme (OAP)

Actor	In scope of OSB	In scope of OAP
Advertisers (including agencies)	No	Yes
Ad servers (intermediary)	No	Yes
Demand-side platforms (intermediary)	No	Yes
Supply-side platforms (intermediary)	No	Yes
Platforms	Yes	Yes
Publishers (other hosts of online ads)	No	Yes

Source: DCMS, 'Online Advertising Programme consultation' (updated 30 September 2022): https://www.gov.uk/government/consultations/online-advertising-programme-consultation/online-advertising-programme-consultation [accessed 1 November 2022]

126. We have heard support for the programme, particularly for its potential to crack down on fraudulent advertising. TSB said that the Government should "Pursue a robust approach to online advertising through the Online Advertising Programme—which places significant and meaningful requirements on firms to limit fraudulent adverts and which imposes severe consequences on those who fail to comply."[222]

127. Cifas suggested that the Programme may be used to tackle some of the intermediary platforms that the Online Safety Bill appears to ignore. Cifas said: "it is important that the Online Advertising Programme effectively tackles fraudulent abuse of adverts across other channels, such as job sites, which are so often exploited to advertise jobs that simply do not exist."[223]

Private sector initiatives

128. In order to tackle fraudulent advertising, platforms can try to limit the ability of fraudsters to relocate consumers away from their service and onto a malicious website. The social media platform TikTok bans content that contains links to other websites. However, some fraudsters continue to manage to subvert the system, with Elizabeth Kanter, Director of Government Affairs and Public Policy Manager at TikTok, saying:

> "What they do underneath is put a different landing page, so that when a user clicks through to the landing page there might be a QR code in

221 DCMS, 'Online Advertising Programme consultation' (updated 17 March 2022): https://www.gov.uk/government/consultations/online-advertising-programme-consultation/online-advertising-programme-consultation [accessed 1 November 2022]
222 Written evidence from TSB (FDF0066)
223 Written evidence from Cifas (FDF0015)

the landing page that tries to take the user out of our app into another space that may contain fraudulent activity … That is fraudulent activity that is not allowed on the platform. We banned over 10 million ads in 2021 containing that and other types of ads that violate our policies."[224]

Box 6: Google's action on fraudulent ads

In July 2021, the FCA set out that it "believes that search and social media platforms may be breaching section 21 of the Financial Services and Markets Act 2000 (FSMA) if they provide optimised or value-added services in relation to a financial promotion that is not approved by an FCA authorised firm or that is not otherwise exempt".[225]

Following this intervention in 2021, Google introduced a new verification policy to ensure that financial promotions hosted through Google Ads are only made by firms authorised by the FCA.[226] Where categories of financial services advertisers are not FCA authorised, such as crypto, some SME lenders or gold, these adverts are now prohibited.[227]

Didi Denham, Government Affairs and Public Policy Manager at Google, said the move had "a very significant impact" with reports suggesting that the move had "almost all but eliminated scams on Google Search."[228]

Google has since followed this action with several steps including integrating and automating the FCA Alert List which prevents ads linking to more than 5000 websites featured on the FCA's Warning List. It is rolling out an advertiser identity verification process using both dual use of state-issued ID verification and business operation verification, in which business operations are checked to investigate unlawful activity.

Other social media sites have already or are in the process of taking the same steps. TikTok told us that it was the first platform to adopt the steps in 2020.[229]Meta said that the process of integrating this into their services is "ongoing", with completion expected by the end of 2022.[230] However, Mark Steward, outgoing Director of Enforcement and Market Oversight at the FCA, told us that Meta has made only "noises" and the FCA is at risk of 'losing patience' with the process.[231] We echo these sentiments.

Former Minister for Tech and the Digital Economy Damian Collins told us that Google has seen positive results from its actions in driving down fraud, while "on Meta, in particular on Instagram, they seem to have increased quite dramatically". He told us that it would be proper for Ofcom to consider this when developing its forthcoming codes of practice under the Online Safety Bill.[232]

224 Q 135 (Elizabeth Kanter)
225 Letter from Mark Steward, FCA Executive Director of Enforcement and Market Oversight to Chair, 'Assessment of Corporate Fraud Through Online Promotion' (14 July 2021): https://committees.parliament.uk/publications/6817/documents/72272/default/
226 Oral evidence taken before the Treasury Committee on 21 September 2021 (Session 2021–22), QQ 267–278
227 Oral evidence taken before the Treasury Committee on 21 September 2021 (Session 2021–22), Q 343
228 Q 119 (Didi Denham)
229 Q 135 (Elizabeth Kanter)
230 Q 142 (Philip Milton)
231 Q 155 (Mark Steward)
232 Q 258 (Damian Collins MP)

The Financial Services and Markets Bill will introduce measures to allow for greater regulation of financial promotions. At present, most financial promotions have to be undertaken by authorised firms, but these firms are able to approve third party promotions. Clause 20 will strengthen oversight of such promotions.[233]

Source: QQ 119–120 (Didi Denham) and written evidence from Google (FDF0072)

129. In tandem with the OAP, the ASA has started a year-long pilot programme with online services such as Amazon, TikTok, Google and Meta.[234] As part of the pilot, participating companies will introduce a set of principles covering how they will raise advertisers' awareness of the rules that apply to their ads and they will also help the ASA to secure compliance in cases when an advertiser is unwilling to follow the rules.

130. **Online advertising is a favoured tool in the fraudsters' toolkit. Scam ads are prominent across a range of online platforms and services and have the potential to expand further as technologies develop. We welcome new legislation to try to tackle this issue via the Online Safety Bill and Online Advertising Programme, but regulations must go further to ensure that the full suite of tools are used to tackle fraudulent ads wherever they appear online. Recommendations relating to the Online Safety Bill are contained in Chapter 6.**

131. ***The Government should ensure that the terms and conditions of all social media platforms expressly prohibit fraudulent user-generated content and advertising and that platforms should be held accountable for all fraudulent material that appears thereafter. We urge Meta and other large social media companies to take action more quickly and ensure that safety is considered at design level in all future product developments.***

132. ***By Autumn 2023, all online platforms including Meta should be mandated to only allow online adverts for financial services from companies authorised by the FCA. Financial promotions should not carry the words 'FCA authorised' unless they are authorised for the specific activity or product advertised. The FCA should strive towards enforcing this principle of specificity more widely in future.***

Analogue fraud

133. While the focus of our inquiry is the rise of digital fraud, physical or in-person approaches are still used by criminals and should not be ignored by policymakers. Methods of fraud constantly evolve and it is conceivable that as law enforcement improves its response to online scams, fraudsters may return to targeting individuals outside of the digital realm. This is why we are covering physical approaches by fraudsters in this report on digital fraud. ACTSO said:

> "It is important not to overlook the traditional frauds (e.g. doorstep crime, rogue traders, counterfeiting, used cars, aggressive sales practices etc). These frauds continue to be carried out through traditional means, including face-to-face (often on the doorstep), by telephone, and by mail. These frauds are just as serious as online scams, and are often targeted at individuals who are made vulnerable by their circumstances."[235]

233 Financial Services and Markets Bill, clause 20 [Bill 146 (2022–23)]
234 Written evidence from the ASA (FDF0022)
235 Written evidence from the ACTSO (FDF0018)

134. Some victims are targeted specifically by these methods. The East of England Trading Standards Authority said that "doorstep crime related fraud is still the method of choice for a small percentage of the criminal community who often prefer to target elderly, vulnerable and infirm persons in their homes, using aggression and coercion to elicit monies for poor or non-existent work."[236]

135. There is a correlation between physical isolation and a victim's susceptibility to digital fraudsters. The Good Things Foundation, a charity working to reduce digital exclusion, said:

> "the experience of digital fraud may reduce their [victims] motivation, trust and confidence in continuing to use the internet… Where this results in people making decisions to avoid online banking or the NHS App - wider risks arise for commercial and public sector service provision and inequalities."[237]

136. The Committee has heard arguments for reorganising the counter-fraud policing model given that the majority of fraud is cyber-enabled and perpetrated by fraudsters who are often far from where the victim lives (see paragraph 302). Andy Cooke, HM Inspector of Constabulary, proposed a central tasking model sitting within the NCA that is fully linked into regional economic crime investigators and those involved in local economic crime.[238] However, we are conscious that retaining a local approach to fraud investigation may have benefits in instances of traditional fraud, where fraudsters may rely on local knowledge to execute their crimes. Andy Cooke also told us that a move away from the localised approach could result in loss of 'local touch' to support investigations.[239]

137. **While digital fraud is increasing, 'analogue' approaches continue to be used by some fraudsters to target victims, particularly those who are digitally excluded. The local policing model has some value in supporting these vulnerable individuals and should be kept in these cases.**

138. ***The Government's forthcoming Fraud Strategy should not ignore the threat of 'analogue' fraud as well as focussing on the increasing risk of digital fraud. Counter-fraud strategies should be varied to tackle analogue tactics including leafletting and door-stepping, and it must support those who are typically targeted by them.***

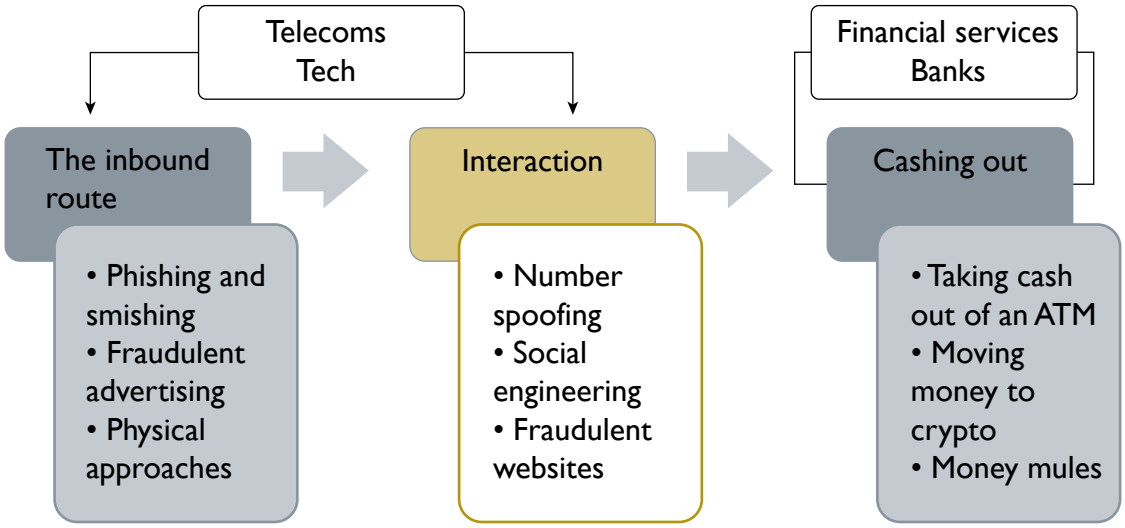
236 Written evidence from East of England Trading Standards Authority (FDF0024)
237 Written evidence from the Good Things Foundation (FDF0045)
238 Q 226 (Andy Cooke)
239 Q 226 (Andy Cooke)

CHAPTER 3: INTERACTION

139. The second step in the fraud chain is typically marked by interaction between fraudsters and their victims. Phone calls, texts, physical meetings or other means of communication may be used to convince a victim to handover money or data. These interactions lean heavily on social engineering techniques and often manufacture pressure, anxiety and stress to force an individual into a "hot state" in which they are more likely to transfer money to a fraudster, who will rapidly 'cash out' their stolen funds.[240]

140. This chapter will provide an assessment of number spoofing, fraudulent websites and social engineering to analyse how digital fraudsters interact with their victims.

Figure 14: The Fraud Chain: Interaction



Source: Q 14 (Katy Worobec) and written evidence from CCSG (FDF0063)

Number spoofing

141. Number spoofing is used by fraudsters to convince their victims that they are calling them from a legitimate organisation. Overseas fraudsters are able to use technology to convince victims that calls are coming from UK numbers. This increases the likelihood that victims will buy into the scams and commit to transferring funds or data to fraudulent depositories. It often takes place following a smishing or phishing attempt.[241]

142. Number spoofing is prolific in the UK. In 2021, Ofcom found that 8 in 10 (82%) people surveyed had been targeted with scam texts or phone calls, which were intended to convince them that they were from trusted organisations such as banks, the NHS or government departments.[242]

240 Q 34 (Brian Dilley)
241 Written evidence from BT Group (FDF0067)
242 Ofcom. '45 million people targeted by scam calls and texts this summer' (20 October 2021): https://www.ofcom.org.uk/news-centre/2021/45-million-people-targeted-by-scams [accessed 1 November 2022]

Box 7: Paul's story

Paul is a pensioner in his mid-70s who suffers from a history of heart attacks. His income outside savings is a state pension of £817. In February 2022, Paul fell victim to a sophisticated malicious misdirection APP scam that cost him £65,000. The fraud was conducted through smishing and number spoofing with the bulk of the interaction being conducted by phone.

> *"He was very well spoken and with a soft Scottish accent. He identified himself as 'Clive' and then said he needed to take me through some security questions … I had no doubt that he was who he said he was, and so I co-operated."*

Initially, Paul received a smishing text claiming to be from Royal Mail. Because he was expecting a delivery, Paul did not consider the text unusual and paid a redirection fee of £2.99 using his debit card. Two days later, he received a spoofing call claiming to be 'Clive' from his bank's fraud department.

The fraudster then personalised the scam by confirming Paul's local bank branch in his town's shopping centre. Paul said that he took this as a subliminal confirmation that the scammer was who they said they were. The scammer then went on to use sophisticated social engineering techniques. He isolated Paul by instructing him to drive home and collect his passport. He then convinced Paul that he needed Paul to assist him in catching other alleged fraudsters at the bank, cutting him off further from reaching out for assistance.

The fraudster asked Paul to transfer money to 'dummy accounts' and for him to speak to the payment verification department via phone so that he could monitor the bank's responses. The fraudster explained how to set up a shared call, and said he was recording the calls. By the end of this process, the scammer had moved £65,000 from Paul's bank account into three 'dummy' accounts, controlled by the fraudster. The fraudster said that the police would be visiting Paul to receive a witness's statement from him regarding fraud at Santander. When this didn't happen and the criminal stopped communicating with him, Paul realised it was a scam.

> *"He also said there had been 14 attempts to fraudulently move money involving this bank branch in the past month and he was leading an internal investigation to discover who might be colluding at the bank, and he needed my help."*

Paul has now been fully reimbursed by Santander. However, the effects of the scam are longstanding.

> *"I feel that the scam of which I am a victim was extremely sophisticated—they played on my anxiety and this whole experience has left me feeling violated. It's as if someone took control of my brain and manipulated me."*

In response to Paul's experience, Santander said:

> "Our dedicated fraud contact centre contacted Paul, but despite specific conversations around potential scams Paul chose to provide inaccurate information to us regarding the reason for the payments, which resulted in them being released… Santander had initially agreed to reimburse Paul 50% of the first payment, but not the second and third payment based on the interaction and questions asked by the Bank prior to them being sent. Upon receiving more information regarding the customer's individual circumstances during the Financial Ombudsmen review, we refunded the customer in full, alongside paying 8% interest on his loss from the date of the transactions until the date of the refund and a further £500 compensation."[243]

Source: Written evidence from Paul (FDF0103)

143. When spoofing happens, scammers make it appear that a phone call or text is coming from a trusted telephone number, for example that of a delivery company. Scammers are able to do this because of the telephone identification protocol, SS7. This tells the network what 'presentation number' or 'calling line identification' (CLI) a user is calling from on both mobile and landline phones. Fraudsters can steal this presentation number. SS7 is a core part of 2G and 3G networks and is still used in telecoms networks globally.[244]

144. Prof Hao used the analogy of a letter to describe how number spoofing works:

> "First, number spoofing is always possible. From the day the telephone system was designed you could modify the caller ID … You can think of it as posting a letter. You write the receiver's address, and you can also write the sender's address on the envelope. You can arbitrarily write a sender's address. It is your choice. Sometimes, if you post a letter from home, for example, you may want to write a different sender's address because you want the receiver to return the letter to a different address, maybe to your work address."[245]

145. The UK is particularly vulnerable to the international trend of number spoofing. Brian Dilley, Group Director of Economic Crime Prevention at Lloyds Banking Group, said that the inability for telecoms companies to block international scam calls and fraudulent number spoofing was the largest fraud vulnerability for the bank.[246] Part of the high degree of susceptibility seen in the UK may be a product of the historical pattern of communication between service provider and their customers. Transpact.com, an escrow service company, said:

> "Individuals and businesses have been 'groomed' by UK banks and UK utilities to receive a phone call from the bank/utility and for the bank/utility to ask the call recipient to divulge confidential information … to prove the call receiver's identity. This is disastrous practice, as neither an individual (nor a business) can know whether they are being called by the genuine bank/utility or by a fraudster impersonating them."[247]

243 Written evidence from Santander (FDF0094)
244 BBC News 'Why phone scams are so difficult to tackle' (23 August 2021): https://www.bbc.co.uk/news/business-58254354 [accessed 1 November 2022]
245 Q 232 (Prof Feng Hao)
246 Q 42 (Brian Dilley)
247 Written evidence from Transpact.com (FDF0061)

146. This process, conducted by many different types of companies from broadband operators to energy companies, has had the effect of 'grooming' customers into divulging information when asked by a person who claims to represent a trusted authority via telephone, despite the fact that they do not have to identify themselves in any meaningful capacity. While there are some legitimate uses of this practice, we believe that it should be phased out in favour of a more effective solution.

147. Spoofing technology is readily available to fraudsters. Police Scotland's DCI Stevie Trim told us about the availability of number spoofing applications provided by multiple companies. DCI Trim said: "From my experience, a lot of these are independent companies. There are spoofing apps that people can download. They were originally used to play jokes: I could put in a phone number and pretend to my mum that I was from a particular organisation."[248]

148. Action to tackle number spoofing is made much harder by VoIP technology. Prof Hao argues that the ability to falsify your CLI is getting easier because of "the deregulation of the market, more and more telecommunication companies use VoIP-based technology. With those kinds of companies, the service is in the cloud, so it is much easier to modify a number."[249]

149. For example, as well as online messaging, WhatsApp (see Chapter 2 and 3) permits calls through the use of VoIP, although it blocks attempts to register an account on WhatsApp using a VoIP provider specifically. Meta recognises that WhatsApp only has a "limited ability to identify when a call or message is originating from a location that differs from the country code assigned to the registered phone number, using identifiers like a user's IP address for example." This leaves it open to abuse.[250]

150. All voice calls, regardless of the use of encryption, are undermined in their ability to mitigate number spoofing by the design of their service. Adrian Gorham told us: "voice calls which are, by policy and technical design, 'any-to-any' so can be originated by any customer in the UK/internationally to any customer in the UK and cannot be subject to prior filtering by content"[251]

Action to tackle spoof calls

151. Action to tackle and prevent scam calls is listed in Action 1 of the Telecommunications Fraud Sector Charter. The Charter sets out measures including implementing enhanced call blocking solutions, working with Ofcom and the Information Commissioner's Office (ICO), as well as data sharing on the sources of scam calls with law enforcement, banking and the industry.[252] According to the CCSG, this work is "on track."[253]

152. Ofcom has taken several steps to tackle number spoofing. In October 2021, Ofcom asked phone networks to block internet calls coming from overseas if they pretend to be from UK numbers. When TalkTalk implemented the

248 Q 194 (DCI Stevie Trim)
249 Q 232 (Prof Feng Hao)
250 Supplementary written evidence from Meta (FDF0082)
251 Supplementary written evidence from the CCSG (FDF0088)
252 Home Office, 'Fraud sector charter: telecommunications' (updated 26 October 2021): https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version [accessed 1 November 2022]
253 Written evidence from the CCSG (FDF0063)

measure it claimed to see a 65% reduction in complaints about scam calls.[254] Different operators are now rolling out their own solutions to this issue.[255] EE has launched new firewall technology to block international scam calls that use a UK CLI and claims to have blocked up to a million a day since its inception in July 2022, benefitting BT, Plusnet and EE customers.[256]

153. In February 2022, Ofcom published a consultation on improving the accuracy of CLI data. The consultation set out plans to strengthen its existing General Condition C6, which introduced CLI measures—to require providers, where technically feasible, to identify and block calls with CLI data that is either invalid, non-dialable or does not uniquely identify the caller. It will provide guidance on what it expects providers to do to meet the new obligations. We understand that Ofcom expects to publish a statement on these plans in Autumn 2022.[257]

154. The 'Do Not Originate' list is a key measure being used to tackle number spoofing. Created by Ofcom and UK Finance, the list details numbers that are allocated to financial institutions, but which are never used for outbound customer service calls. Huw Saunders, Director of Network Infrastructure and Resilience at Ofcom, told us that the list now comprises "over 12,500 numbers, which, if they are seen in the network, are known to be malicious or known to be a scammer and therefore should be blocked." Saunders also added that from Ofcom's perspective the list "has proven very effective".[258] When HMRC implemented the measure, it reduced the amount of phone scams spoofing genuine inbound HMRC numbers "to zero".[259]

155. Part 4 of the Data Protection and Digital Information Bill, which is currently on hold, is set to increase fines for nuisance calls and texts by extending the reach of the Privacy and Electronic Communications Regulations (PECR). Clause 80 will enable the ICO to investigate and act against organisations responsible for unwanted direct marketing.[260] The PECR are not aimed at fraud and it appears that these measures will need to be directed towards fraudulent calls unless there is clear guidance that this should apply.

156. We have taken evidence that highlights how international best practice can be followed by UK regulators. For example, in 2022 the US Federal Trade Commission (FTC) took action against a VoIP service provider for facilitating the transmission of pre-recorded scam robocalls, many relating to the pandemic, several of which originated overseas and used spoofed numbers.[261] The case was the FTC's third action against a VoIP provider.

---

254 'Ofcom plans crackdown on fake number fraud', *The Independent* (23 February 2022): https://www.independent.co.uk/news/uk/ofcom-talktalk-government-consumers-companies-house-b2021235.html [accessed 1 November 2022]

255 Q 237 (Adrian Gorham)

256 EE, 'EE takes a stand against scammers with latest international call-blocking technology' (18 August 2022): https://newsroom.ee.co.uk/ee-takes-a-stand-against-scammers-with-latest-international-call-blocking-technology/ [accessed 1 November 2022]

257 Ofcom, Improving the accuracy of Calling Line Identification (CLI) data: Consultation on changes to our General Conditions and supporting guidance on the provision of CLI facilities (23 February 2022): https://www.ofcom.org.uk/__data/assets/pdf_file/0015/232071/consultation-improving-cli-data-accuracy.pdf [accessed 1 November 2022]

258 Q 152 (Huw Saunders)

259 Take Five, 'Criminals exploit Covid-19 as fraud moves increasingly online': https://www.takefive-stopfraud.org.uk/news/criminals-exploit-covid-19-as-fraud-moves-increasingly-online/ [accessed 1 November 2022]

260 Data Protection and Digital Information Bill, Part 4, clause 80 [Bill 143 (2022–23)]

261 Written evidence by the FTC (FDF0093)

The court action included an order permanently stopping the defendants from such illegal conduct, forcing them to introduce technology to block such calls and screen new customers, and included a suspended civil penalty of more than $3 million.[262]

157. Also in the US, technology has been created termed 'Stir and Shaken' protocols which will enable networks to authenticate CLI numbers. At present, this cannot be implemented on EU phone networks and Ofcom says that UK providers cannot implement such technology until networks and the technology that supports voice services are upgraded. The Government is switching off the public switched telephone network (PSTN) in order to make all phone lines digital by December 2025. In practice, this means that landlines will be connected by broadband connections (like in VoIP) rather than copper phone lines. This means that CLI authentication likely will not be fully available in the UK until that point.[263]

158. **Number spoofing is fundamental to convincing victims that they are being contacted by a genuine, trusted authority. We endorse the valuable work being undertaken by Ofcom and the industry to tackle number spoofing, however efforts to address CLI spoofing must not be watered down or delayed.**

159. ***Ofcom must expedite its work on number spoofing. It must ensure that technologies that prevent CLI abuse are rolled out as soon as possible, and take all available steps to require the mandatory use of these technologies immediately when possible. Updates to the core network should be made urgently to stamp out fraud, ideally prior to 2025. Where such reasonable steps are not taken, companies must face penalties.***

160. ***Companies should phase out the process of identifying consumers via telephone by confirming personal information with them. A more effective solution to this requirement must be sought.***

Social engineering

161. Social engineering is the process by which criminals groom and manipulate people into divulging personal and financial details or transferring money.[264] Fraudsters use social engineering to bring a victim into what Brian Dilley called a "hot state".[265] This is the point at which individuals stop thinking clearly and often feel rushed, anxious and mistrustful.

162. Highlighting the risks of romance fraud and the vulnerability characteristics of victims, the Online Dating Association said: "Fraudsters are extremely adept at emotional manipulation and recognising the signs of those who are

262 Federal Trade Commission, 'FTC takes action to stop voice over internet provider from facilitating illegal telemarketing robocalls, including scams relating to the pandemic' (26 April 2022): https://www.ftc.gov/news-events/news/press-releases/2022/04/ftc-takes-action-stop-voice-over-internet-provider-facilitating-illegal-telemarketing-robocalls [accessed 1 November 2022]

263 BBC News, 'Ofcom asks phone networks to block foreign scam calls' (25 October 2021): https://www.bbc.co.uk/news/business-59032795 [accessed 1 November 2022]; BBC News, 'Why phone scams are so difficult to tackle' (23 August 2021): https://www.bbc.co.uk/news/business-58254354 [accessed 1 November 2022] and Which?, 'Digital Voice and the landline phone switch-off: what it means for you' (7 October 2022): https://www.which.co.uk/reviews/broadband/article/digital-voice-and-the-landline-phone-switch-off-what-it-means-for-you-aPSOH8k1i6Vv [accessed 1 November 2022]

264 Written evidence from Amazon (FDF0073)

265 Q 34 (Brian Dilley)

vulnerable and easy targets."[266] For example, isolation, reduced digital literacy or mental health illness may contribute to higher levels of vulnerability.[267]

163. Social engineering is not only successful against victims who are predisposed to scammers by existing vulnerabilities. Dr Konstantinos Mersinas, Senior Lecturer at Royal Holloway, explained that anyone can fall for social engineering saying: "The fact that security professionals might fall for social engineering attacks, and phishing, indicates that it is not a matter of knowledge or of providing the information."[268]

164. Social engineering reduces the efficacy of counter-fraud warning signs. Attempts to fight back against social engineering may be undermined by the lack of trust created by the criminal. Brian Dilley told us that this often leads to the victim believing that the person trying to contact them genuinely is trying to help them because they have created a compelling narrative.[269] TSB acknowledged that social engineering helps criminals circumvent warnings and public information campaigns created by stakeholders within the fraud chain:

> "Given the scale of fraud in the UK and the sophistication of many scams, the technologies that are used, and the complex social engineering tactics used it is not credible to suggest that educating people about fraud is particularly effective … Fraudsters will always find ways to explain away a customer's concern."[270]

165. Social engineering can prevent individuals from asking for help and it can leave victims with residual feelings of shame. Mike Haley explained this issue by its parallel with the experience of burglary and fraud:

> "I could be burgled, and everyone would have sympathy for me. I would not feel shame or embarrassment about it, and other people would have some empathy. With a fraud, there is a degree to which people will feel ashamed and embarrassed to even speak about it. They feel, as do others, that they have brought it on themselves in some way, they were not very savvy, and they were taken in by social engineering."[271]

166. See Box 7 for Paul's experience of being socially engineered to transfer £65,000 into a fraudster's account. The fraud was predominantly based on the high degree of trust Paul placed in the fraudster.[272]

Action to tackle social engineering

167. In September 2021, Stop Scams UK a cross-sector industry body, launched a pilot scheme called 159, a memorable short code phone service that connects the retail banking customers directly with their bank, should they receive an unexpected or suspicious call on a financial matter. Stop Scams UK told us that the average bank impersonation scam costs consumers more than £4,500. By spring 2022, 80,000 calls had been made to 159 and the

266 Written evidence from Online Dating Association (FDF0028)
267 Written evidence from Liz Eden (FDF0089)
268 Q 64 (Dr Konstantinos Mersinas)
269 Q 34 (Brian Dilley)
270 Written evidence from TSB (FDF0066)
271 Q 15 (Mike Haley)
272 Written evidence from Paul (FDF0103)

service has now been expanded to accommodate other banks including the Co-operative Bank, the Nationwide Building Society, and TSB.[273]

168. Initiatives like the 159 initiative are vitally important in shaking a victim out of the 'hot state'. Stop Scams UK said that the initiative can help to "break the scam journey at that critical moment when the consumer is at most risk of being socially engineered and making a payment."[274]

169. Education is a central component of helping people recognise and response to social engineering. Brian Dilley said that whilst attaining reliable metrics for studying the success of awareness messaging is challenging, education is "the first line of defence" because it can help a victim to understand when to hang up the phone.[275] More information regarding consumer education can be found at paragraph 402.

170. **Social engineering is a cruel tactic used by fraudsters to manipulate their victims. It has longstanding impacts on victims, who may find it difficult to trust organisations in future because of the tactics used by fraudsters to manoeuvre them into the 'hot state' in which they make a payment.**

171. ***Financial institutions, whether banks or building societies, must be encouraged to participate in the 159 initiative, and should be mandated to provide information on the service to their customers if the initiative is extended beyond pilot stage.***

Fraudulent websites

172. Fraudsters incorporate fraudulent websites or domains into phishing messages to draw victims into the interaction phase of a fraud. Domain registration to set up a website is cheap and easy, often only costing between $10 and $30 a year.[276] This enables some fraud to be carried out with relative ease. The ease with which fraudsters create these domains means that identifying and closing them down becomes a game of "whack-a-mole".[277]

173. Fake websites often link to real life scenarios or contemporary events that are exploited to help social engineering of victims. The COVID-19 pandemic provided a rich opportunity for phishing attacks. Texts often relocated victims to fake website pages about vaccinations or COVID-19 passes. Websites were designed to collect personal and financial information from victims. They offered vaccine booking appointments in return for a fee.

174. There are a number of ways in which fraudsters aim to spoof websites. For example:

- TLD squatting happens when a fraudster registers an identical brand-owned domain name with a different Top Level Domain e.g. Facebook.co instead of Facebook.com.

273 Written evidence from Stop Scams UK (FDF0057)
274 *Ibid.*
275 Q 35 (Brian Dilley)
276 Allen & Overy, 'Domain names, online fraud and UDRP proceedings': https://www.allenovery.com/en-gb/global/blogs/digital-hub/domain-names-online-fraud-and-udrp-proceedings [accessed 1 November 2022]
277 Q 150 (Mark Steward)

- Typosquatting/URL hijacking happens when a fraudster registers a site close to an entity's brand or copyright e.g. faceb0k-login.com.
- A fraudster might use a lookalike in order to replace letters with similar looking characters e.g. royaimaii.com rather than royalmail.com.[278]

175. Prof Hao's research shows that fraudulent domain names often work best on mobile devices because users are less likely to notice that a website is different to the original on their phones because of the smaller screen size and user interface.[279]

176. The use of fraudulent websites presents a significant challenge to counter-fraud agencies because domains can be made quickly with very few identity checks. Prof Hao said: "Often, phishing websites are short-lived. They do not last long, because it takes time for the activities to be detected. After a day or two, they get the fraudulent transactions and make enough money, and if it is detected and blocked, they just open another domain."[280]

177. New software makes finding and removing fraudulent websites even harder. Proxy servers can be used to guide users to websites that are blocked in other countries via domain hopping (the practice of relocating to new domains to prevent being penalised). An example of this kind of site is Unblockit. In addition, IP masking services disguise the IP address of the hosting server through software like Cloudfire. The Motion Picture Association told us that these pieces of software offer criminals the ability to evade shutdowns through 'domain hopping'. It said:

> "When enforcement activities are implemented—be it ISP blocking, search engine delisting or otherwise—Unblockit and sites like it simply move to a new domain."[281]

Action to tackle fraudulent domains

178. Action to tackle fraudulent domains is spearheaded by the NCSC. In 2021, the NCSC took down 2.7 million campaigns amounting to 3.1 million URLs. This was an increase on the 700,595 campaigns and 1.4 million URLs taken down in 2020. Overall, since the takedown service began in June 2016 it has taken down 3.7 million campaign groups (5.8 million URLs covering more than 2 million IP addresses).[282]

179. The Motion Picture Association has argued that more should be done to tackle fraudulent domains by know your business customer (KYBC) checks. It suggested that a new KYBC obligation should be placed on online service providers such that checks "would require commercial entities to establish

278 Techradar, 'Why criminals spoof your domain name' (7 November 2019): https://www.techradar.com/news/why-criminals-spoof-your-domain-name [accessed 1 November 2022]

279 Mohammed Aamir Ali, Muhammad Ajmal Azad, Mario Parreno Centeno, Feng Hao, Aad van Moorsel, 'Consumer-facing technology fraud: economic, attack methods and potential solutions', *Future Generation Computer Systems*, vol 100 (2019), pp 408–427 (November 2019): https://www.dcs.warwick.ac.uk/~fenghao/files/Consumer_Facing_Technology_Fraud.pdf [accessed 1 November 2022]

280 Q 240 (Prof Feng Hao)

281 Written evidence from the Motion Picture Association (FDF0068)

282 National Cyber Security Centre, *Active Cyber Defence: The fifth year*: https://www.ncsc.gov.uk/files/ACD-The-Fifth-Year-full-report.pdf [accessed 1 November 2022]

the true identity of their business customers as a precondition for selling, and receiving payment for, digital services."[283]

180. Will Semple suggested that KYC checks could help to prevent criminals registering new domains and encrypting the traffic between a web server and the customer's browser. He said:

> "They have to register a domain. Often, they have to register what we call an SSL certificate, which encrypts the traffic between the web server and the customer's browser … my view is that it is too easy to register, and some simple know your customer-type techniques would probably introduce a major speedbump into the entire process. They would not stop it, but they would definitely make it harder for bad actors to carry out these activities."[284]

181. However, Prof Hao told us that this is more difficult than it sounds because domain hosts can only monitor traffic on a website and deduce whether it is likely to be fraudulent by the type of traffic it attracts. While it is possible to look up the owner of a domain, this is not common practice. In addition, Prof Hao said:

> "Criminals never use their real identity; they always use a stolen identity to register the domain. They do not register it in the UK; they register it overseas. They use a stolen credit card to make payments, or bitcoin or an anonymous payment method."[285]

182. The Association of British Insurers said that there must be more effort to deter fraudsters from registering fraudulent domains given that "the issue moves so quickly that simply listing domains will always be outpaced by new domains emerging." They argue that prosecution is vital to deter future fraudulent activity.[286] However, Michael Skidmore, Senior Researcher at the Police Foundation, cautioned that policing these domains would be challenging because we are "dealing in this regard with quite technical and cross-border offenders."[287]

183. Will Semple argued that action against fraudulent domains must be cross-sectoral. Noting that "everyone has a role to play", He identified eBay's collaboration with PSPs, financial services institutions, software providers and domain name registrars as an example.[288] The efficacy of this approach can be seen in the work of Stop Scams UK who said that through collaboration BT, TalkTalk and others had put online a URL Blocking Proof of Concept service that blocked 33,000 phishing domains as of February 2022.[289] These partnerships must stretch to law enforcement.

283 Written evidence from the Motion Picture Association (FDF0068)
284 Q 127 (Will Semple)
285 Q 240 (Prof Feng Hao)
286 Written evidence from the Association of British Insurers (FDF0051)
287 Q 90 (Michael Skidmore)
288 Q 129 (Will Semple)
289 Written evidence from Stop Scams UK (FDF0057)

Box 8: The role of the National Cyber Security Centre (NCSC)

The NCSC was launched in 2017 as part of the Government Communications Headquarters (GCHQ). Its role is to act as a bridge between industry and Government and it is the UK's national authority on the cyber security environment.[290] The National Cyber Strategy 2022 set out that the NCSC's key priorities are to take direct action to reduce cyber harms, support the UK in protecting itself, provide technical input to government policy and regulation, provide UK sovereign capabilities, and to support growth in cyber skills and investment. [291]

The NCSC has a key role in preventing fraud. In April 2020, the NCSC launched the Suspicious Email Reporting Service, inviting people to share suspicious emails or websites with report@phishing.gov.uk or by reporting directly online. Since the launch, the NCSC have shut down over 76,000 scams across 139,000 websites.[292]

It works in partnership with the ASA on the Scam Ad Alert System; if a post is suspected of being fraudulent, an Alert is sent to the NCSC (and participating social media platforms), which scans the alert for URLs and remove the website if found to be malicious.[293] The NCSC has a key role in taking down scams reported to the 7726 service (see Box 16).

It also runs the Cyber Security Information Sharing Partnership, a public-private information sharing service that allows organisations to share cyber threat information securely and confidentially.[294] In addition, under Action 2 of the Telecommunications Fraud Sector Charter, telecoms providers will share reported URLs and phone numbers linked to smishing with the NCSC. Under Action 7, the NCSC (along with the City of London Police and NECC) is required to appoint a telecommunications fraud point of contact.[295] The Centre also provides guidance for individuals, SMEs, large organisations and public and private sector professionals as part of its Cyber Aware campaign.[296]

290 HM Government, 'National Cyber Security Centre': https://www.gov.uk/government/organisations/national-cyber-security-centre [accessed 1 November 2022]

291 Cabinet Office, 'National Cyber Strategy 2022' (updated 7 February 2022): https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#the-national-cyber-security-centre [accessed 1 November 2022]

292 DCMS, 'Major law changes to protect people from scam adverts online' (8 March 2022): https://www.gov.uk/government/news/major-law-changes-to-protect-people-from-scam-adverts-online [accessed 1 November 2022]

293 Written evidence from the ASA (FDF0022)

294 National Cyber Security Centre, 'CiSP': https://www.ncsc.gov.uk/section/keep-up-to-date/cisp [accessed 1 November 2022]

295 Home Office, 'Fraud sector charter: telecommunications' (26 October 2021): https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version [accessed 1 November 2022]

296 See National Cyber Security Centre, 'New web tool to test your cyber risk as survey exposes 80% of British people fear online attacks' (March 2021): https://www.ncsc.gov.uk/news/consumer-cyber-action-plan [accessed 1 November 2022].

We have heard that the NCSC fosters positive collaboration with the private sector. BT Group told us that it has worked with the NCSC on the development of its security education and advice for customers.[297]Stop Scams UK is currently working on how it can better share data from its 159 project with the NCSC.[298] Will Semple told us that "we see very strong leadership in our ecosystem from agencies such as the NCSC and GCHQ", noting regular collaboration with eBay.[299]However, we are concerned that collaboration with ISPs is lacking, particularly given their role in domain hosting and the creation of fraudulent websites.

We recognise that more can be done, particularly at a local level. Fighting Fraud and Corruption Locally, a working group connected to Cifas, told us that there should be better communication between local authorities, the police and the NCSC to encourage joint working at a local level.[300] The National Anti-Fraud Network (NAFN) told us that while content to support businesses' awareness of fraud is valuable, it should be more widely publicised and supported with a focus on local implementation.[301]

184. Finally, we note the lack of current focus on the role that Internet Service Providers (ISPs) play in the fraud chain. ISPs supply individuals with access to the web and supply hosting facilities for websites.[302] Dr Mersinas called for a collective effort that included getting "the technological giants, the ISPs and the platforms on board" and not relying on law enforcement efforts alone."[303] At the moment, membership of the CCSG does not include ISPs despite their role in domain hosting and the Telecommunications Sector Charter does not explicitly mention cooperation or data sharing with ISPs.[304]

185. We understand that the Government is considering fraudulent domain names as part of its review of the Computer Misuse Act, including potential powers to seize internet domain names so that fraudsters cannot register a domain to "lure people down a fraudulent path".[305]

186. We also understand that the issue of fraudulent domains is not considered to be within Ofcom's regulatory perimeter. Furthermore, it is arguably inconceivable to bring it within its territorial perimeter due to the overseas nature of this activity. We recognise that any efforts to bring this issue within Ofcom's regulatory perimeter might result in domain hosts using overseas services.

187. **Fraudulent websites have become a common means by which fraudsters can convince their victims that they are interacting with a genuine organisation or authority. At present, it is too easy to set up a spoof website. Domain hosts and ISPs have been left out of the debate on how to tackle fraud. This oversight has left them without**

297 Written evidence from BT Group (FDF0067)
298 Written evidence from Stop Scams UK (FDF0057)
299 Q 122 (Will Semple)
300 Written evidence from Fighting Fraud and Corruption Locally (FDF0030)
301 Written evidence from the National Anti-Fraud Network (FDF0055)
302 Carphone Warehouse, 'What is an Internet Service Provider (ISP)?': https://www.carphonewarehouse.com/broadband/guides/what-is-an-isp.html [accessed 1 November 2022]
303 Q 66 (Dr Konstantinos Mersinas)
304 Home Office' Fraud sector charter: telecommunications' (26 October 2021): https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version [accessed 1 November 2022]
305 Q 264 (Tom Tugendhat MP)

due scrutiny. These services must be subject to the same stringent counter-fraud controls that should apply across the board.

188. ***The Government must clarify within whose regulatory perimeter domain hosts and other ISPs sit and explore whether bringing this issue within Ofcom's regulatory remit would materially benefit its counter-fraud function. The responsible regulator should consult on new regulations requiring domain name providers to enforce greater KYC checks on those registering domain names, and on codes of practice to establish protocols that prohibit domains from being used if it is believed that the intention is to deceive users.***

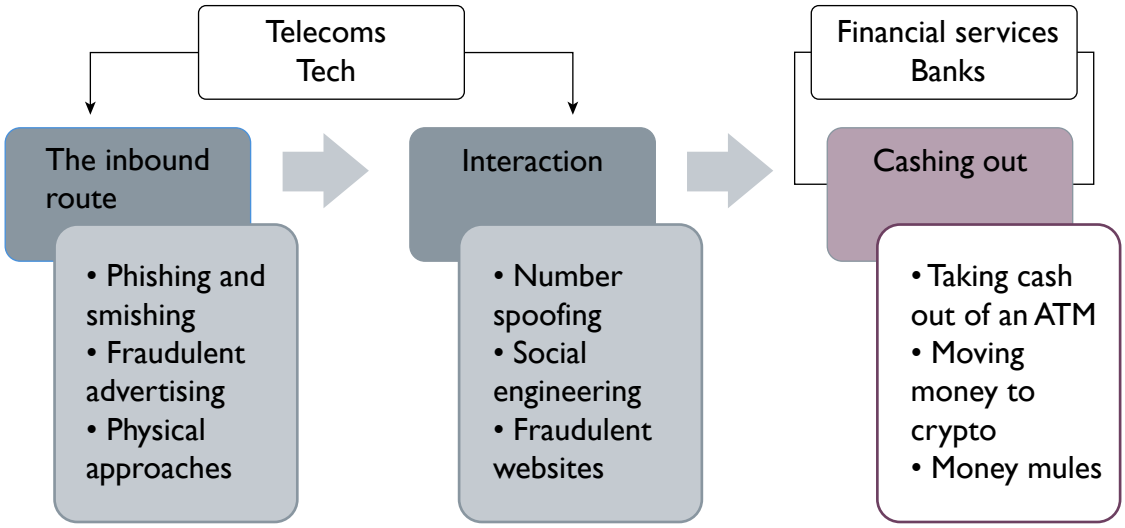
189. ***The Government must expedite the forthcoming Tech Sector Charter and include ISPs within its scope.***

CHAPTER 4: CASHING OUT

190. The process by which fraudsters withdraw their criminally obtained funds is known as 'cashing out'. This is a common feature of all frauds. There are a number of ways in which criminals can cash out their stolen funds once a payment has been made, for example via withdrawal at an ATM machine, transferring the money into cryptocurrency to be withdrawn later or by laundering it, often by using money mules, sometimes to overseas accounts.

191. This chapter explores the various intervention points at which the process of cashing out could be interdicted so that criminals cannot walk away from their attempted fraud with a victim's money. It is preferable that intervention should take place prior to this stage given the earlier in the chain a fraud is halted, the less the impact on the victim.

Figure 15: The Fraud Chain: Cashing out



Source: Q 14 (Katy Worobec) and written evidence from CCSG (FDF0063)

Payments infrastructure

192. Fraudsters exploit the speed and ease with which digital and online banking users can make payments. As noted, individuals are seen as the 'weak link' in the fraud chain due to their capacity to be taken in by social engineering techniques to make authorised payments to fraudsters. Due to the current payments infrastructure, these payments happen at pace.

193. The payments ecosystem is comprised of all parties that interact during the process of a transaction. Payment systems, such as Bacs, the Image Clearing System for cheques, CHAPS, LINK (cash) and Faster Payments, are run by payment systems operators.[306] The New Payments Architecture programme is due to be introduced in 2024 and will replace BACS and Faster Payments with updated payment systems intended to respond better to changes in

306 Pay.UK, 'Faster Payment System': https://www.wearepay.uk/what-we-do/payment-systems/faster-payment-system/ [accessed 11 March 2022]

technology.[307] PSPs are third-party companies that help businesses to accept online payments.[308]

194. Three key regulators have responsibility for this ecosystem. The PSR was set up in 2015 to promote effective competition, innovation in payment systems, and to ensure that such systems are operated and developed to promote consumers' interests. The FCA has responsibility for day-to-day supervision of payment services, and the Bank of England regulates systemic payment systems.[309]

195. Digital transfers are a widespread and growing means of payment in the UK. While cash remains the second most commonly used form of payment at 15%, behind debit card payments (48%), UK Finance expects that by 2031 cash will account for just 6% of all payments made in the UK while remote banking methods will continue to rise to a point where it is used by 93% of adults.[310] Digital payments can be received by anyone with a bank account.

Know-your-customer

196. It is relatively easy to open a bank account in the UK today. This leaves the banking system vulnerable to fraudsters opening and closing bank accounts to launder the proceeds of fraud with relative ease. Under anti-money laundering (AML) regulations, regulated financial institutions are required to carry out due diligence on customers and companies when they open an account and on an ongoing basis—although the nature of checks varies given different types of customer, risk and product type—to check that they are who they say they are and to understand the customer's expected behaviour. However, there are clearly flaws in the system. For example, synthetic identities can be created using a combination of real and fake information to create an entirely new identity.[311] During the filming of his consumer rights programme, Joe Lycett opened a new bank account using a false name:

> "I managed to open a bank account in someone else's name, with their permission, and that felt concerning to me—that you could open accounts without too many questions being asked. It is quite easy to funnel money in that way."[312]

197. Digital identity verification is a crucial step in banks' counter-fraud approach. Biometric Know Your Customer (KYC) checks are used by some banks in order to confirm that a payment is being authorised by the account

---

307 'New regulatory framework set for New Payments Architecture', Linklaters (13 December 2021): https://financialregulation.linklaters.com/post/102hede/future-regulatory-framework-set-for-new-payments-architecture [accessed 7 January 2022] and PSR, 'New Payments Architecture (NPA)': https://www.psr.org.uk/our-work/new-payments-architecture-npa/ [accessed 7 January 2021]

308 FCA, 'Using payment service providers' (9 March 2022): https://www.fca.org.uk/consumers/using-payment-service-providers [accessed 1 November 2022]

309 HM Treasury, *Payments Landscape Review: Response to the Call for Evidence* (October 2021): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1024174/HMT_Payments_Landscape_Review_-_The_Government_s_Response__October_2021_.pdf [accessed 1 November 2022]

310 UK Finance, *UK Payment Markets Summary 2022* (August 2022): https://www.ukfinance.org.uk/system/files/2022–08/UKF%20Payment%20Markets%20Summary%202022.pdf [accessed 1 November 2022]

311 'Faces are the next target for fraudsters', Wall Street Journal (7 July 2021): available at https://www.wsj.com/articles/faces-are-the-next-target-for-fraudsters-11625662828 [accessed 1 November 2022] and LexisNexis Risk Solution, 'What is Synthetic Identity Fraud?': https://risk.lexisnexis.com/insights-resources/article/synthetic-identity-fraud [accessed 1 November 2022]

312 Q 93 (Joe Lycett)

holder, for example by using facial identification on smartphones. However, some fraudsters are able to bypass these methods. Deepfake technology is a process that uses deep learning, a sub-field of artificial intelligence, to make fake pictures or voices and this can be used to fake an image or voice of a real-life user in order to convince a bank that they are the genuine customer.[313]

198. Dr Hutchings has cautioned against overstating the risks currently presented by such technology:

> "I do not think we are seeing deepfakes so much as people trying to imitate genuine customers in some ways, such as by having an IP address that is in the same region as the customer. We are seeing less technical means that are just as effective at overcoming those types of algorithms. The more complicated technical approaches are not likely to be used in favour of relatively straightforward, non-technical attacks."[314]

199. Transpact told us that fraudulent driving licences are frequently used to open bank accounts. Many banks allow driving licences as proof of ID to accommodate individuals who do not have a passport (usually alongside another form of proof of address). However, Transpact suggested that the security of driving licences is not as good as passports due to the lack of a cryptographically viable, encrypted chip. As a result, they argue that driving licences are "relatively easy to forge". They also suggested that driving licences should include a cryptographically verifiable chip, similar to new passports, to ensure that the individual presenting the document can be verified.[315]

200. The on-hold Data Protection and Digital Information Bill will establish in law a framework for the provision of digital identity verification services in the UK and enable public authorities to disclose personal information to trusted digital identity providers for identity and eligibility verification.[316] We are supportive of this work, however we are concerned that the framework and authentication systems must be watertight in order to avoid concerns that have been raised about digital identity theft, which could lead to fraud.[317]

201. Finally, AI and machine learning have a role in preventing fraudsters from opening accounts. For example, this technology can be used to understand customer behaviour better and flag characteristics that might be indicative of higher risk, such as several accounts being opened in a particular postcode where fraudsters are known to be in operation.

202. While we have heard that the process of opening a bank account may be too easy, we are equally aware that efforts to make opening bank accounts more difficult may have a negative impact on financial inclusion. The need to prevent financial crime must be balanced with this consideration in support of a society that champions access to financial services. A balance must

313 'What are deepfakes: and how can you spot them?' *The Guardian* (13 January 2020): https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them [accessed 1 November 2022]

314 Q 63 (Dr Alice Hutchings)

315 Written evidence by Transpact.com (FDF0061)

316 Explanatory Notes to the Data Protection and Digital Information Bill [Bill 143 (2022–23)-EN]

317 Eversheds Sutherland, 'UK Government aims to lead on trust in Digital IDs' (23 March 2022): https://www.eversheds-sutherland.com/global/en/what/articles/index.page?ArticleID=en/tmt/UK-Government-aims-to-lead-on-trust-in-Digital-IDs [accessed 1 November 2022], see comments by Philip James.

be struck between preventing fraud and introducing new AML or KYC procedures that may create unnecessary obstacles for honest customers to open bank accounts.

Transaction monitoring

203. A key part of AML requirements is transaction monitoring. In a retail bank, this usually takes place via a system—either built in-house or purchased from a third party—based on 'rules' that flag transactions for review. This might include a balance limit being reached in a particular account, or the identification of transactions that appear 'abnormal' for an account or group of customers, and may require the use of AI and Machine Learning technologies to improve the 'rules' applied.

204. We have heard that transaction monitoring systems can lead to a large number of 'false positive alerts', which require extensive resources to review. In some cases, accounts may be frozen or closed if a bank suspects that it is being used for fraud, which can lead to customers being denied access to cash.[318] In 2018, e-money service Revolut contacted the FCA to inform it of its failure to comply with AML procedures by switching off an automated system designed to stop suspicious money transfers. It told the regulator it did this after 8,000 false positives incorrectly identified legitimate transactions as being suspicious and blocked them as a result.[319]

205. Dr Mersinas told us that technology has not yet caught up with the scale of the issue:

> " … machine learning can, of course, be used for the legitimate purposes of marketing and entertainment, in coping with fraud, and with the opposite goals in mind. We are at the stage where the technology still has many false positives and many false negatives. Incidents are incorrectly marked as real incidents and vice versa. We are still bound by historical data. We are still bound by simulations and exercises. In that sense, we are not there yet."[320]

206. Nicholas Taylor, former Head of Policy and Public Affairs at Revolut, told us that Revolut tackles fraud and money laundering through a two-pronged approach based on working with former law enforcement officials and financial crime experts, alongside engineers and technologists.[321]

207. The scope for improvement in transaction monitoring is made clear when looking at the FCA's enforcement actions in recent years, which have largely focussed on failures in transaction monitoring rather than KYC processes. For example, in 2021, NatWest was fined £264.8 million in the first example of the FCA pursuing criminal charges for AML failures. It was found that NatWest was "responsible for a catalogue of failures in the way it monitored

318 See "It's my money, not theirs': Account closures exposed at Pockit, Revolut, Monese and Monzo', *The i* (18 May 2021): https://inews.co.uk/inews-lifestyle/money/saving-and-banking/customers-pockit-revolut-monese-complain-unexpected-account-closures-1008448 [accessed 1 November 2022].

319 'Digital bank Revolut's sanctions screening issue revealed', *Daily Telegraph* (28 February 2019): available at https://www.telegraph.co.uk/technology/2019/02/28/revolut-failed-block-suspicious-transactions/ [accessed 1 November 2022]

320 Q 63 (Dr Konstantinos Mersinas)

321 Q 36 (Nicholas Taylor)

and scrutinised transactions that were self-evidently suspicious".[322] Also in 2021, HSBC was fined £63.9 million for deficient transaction monitoring processes over a period of eight years up to 2018.[323]

Enforcement of the AML regime

208. We have heard that supervision and enforcement of AML regulations is patchy. Ghela Boskovich, Regional Director of the Financial Data and Technology Association, told us that more action must be taken by banks receiving payments to ensure that they comply with KYC and AML requirements.[324] Nicholas Taylor told us that "AML compliance is something that everyone needs to improve".[325]

209. The FCA told us that it "prolifically enforced" the AML regime. Since 2018 it has taken action against 11 firms for inadequate AML, anti-bribery and corruption controls, culminating in £655 million in penalties.[326] Far from being 'prolific', this figure seems startlingly low.

210. Transparency Task Force argued that given low enforcement activity by the FCA, more pressure should be put on the FCA to take more action to stop fraud reaching consumers. It suggested that patchy enforcement of rules may even 'attract' fraudsters to the financial services sector. The group argue that the FCA should lose what it terms its "broad exemption from civil liability" under Part 4(25) of the Financial Services Act 2012 and require it to pay redress for regulatory failure via changes to its Complaints Scheme.[327]

211. However, we recognise that the FCA's capacity to bring prosecutions against corporations for failures to comply with AML regulations may be a by-product of inadequate resourcing. The FCA is funded by the institutions that it regulates. Its budget in 2020 (£632.6 million) was around a third of the US Securities and Exchange Commission (SEC) ($1.815 billion), the federal regulatory agency responsible for maintaining the fair and orderly function of the US securities markets.[328]

212. Furthermore, the measures introduced in the Financial Services and Markets Bill may increase oversight of the FCA and Prudential Regulation Authority's (PRA) rules. For example, Clause 27 will introduce a requirement that the rules are kept under review, and the Treasury will be able to direct regulators to review certain rules if in the public interest. Clause 28 would give the Treasury powers to direct the regulators to make rules on certain issues. The

322 FCA, 'NatWest fined £264.8 million for anti-money laundering failures' (13 December 2021): https://www.fca.org.uk/news/press-releases/natwest-fined-264.8million-anti-money-laundering-failures [accessed 1 November 2022]; Southwark Crown Court, R -v- National Westminster Bank, Sentencing Remarks of Mrs Justice Cockerill (13 December 2021)

323 FCA, 'FCA fines HSBC Bank plc £63.9 million for deficient transaction monitoring controls' (17 December 2021): https://www.fca.org.uk/news/press-releases/fca-fines-hsbc-bank-plc-deficient-transaction-monitoring-controls [accessed 1 November 2022]; see also FCA, Decision Notice: https://www.fca.org.uk/publication/decision-notices/hsbc-bank-plc.pdf [accessed 1 November 2022].

324 Q 74 (Ghela Boskovich)

325 Q 36 (Nicholas Taylor)

326 Written evidence by the FCA (FDF0091)

327 Financial Services Act 2012, Schedule 3, Part 4(25) and written evidence by Transparency Task Force (FDF0092)

328 Macfarlanes, 'Is the United States more effective than the United Kingdom at prosecuting economic crime?' (7 May 2021): https://www.macfarlanes.com/what-we-think/in-depth/2021/is-the-united-states-more-effective-than-the-united-kingdom-at-prosecuting-economic-crime/ [accessed 1 November 2022]

legislation will also introduce greater measures to require reimbursement in cases of APP fraud (see paragraph 386).[329]

Faster Payments

213. Thanks to new banking technologies such as Open Banking and Faster Payments, payments can be made with speed and efficiency. Open Banking was introduced in 2018 to enable the sharing of transaction data with third parties more easily, to allow third parties to initiate payments directly from an account as a bank transfer, and to share firms' product information and customer indicators more openly.[330] Faster Payments is a payment system offering near-instant payments.[331]

214. The Committee has heard that the speed with which payments are processed has made it easier for fraudsters to quickly cash out stolen money. Last year, 3.4 billion transactions were processed via the Faster Payments System, up 20% on the figure for 2020.[332] It was the method of payment used to facilitate 96% cases of APP fraud in 2020, an increase of 34% since 2019 according to UK Finance.[333] Pay.UK, which operates the system, cautioned that APP fraud affects less than 1% (0.0066%) of payments made via this system.[334] The Building Societies Association told us:

> "Implementation in the UK concentrated solely on delivering speed of transaction and chose to ignore risks that too much speed did not give time for customers to consider fraud risk or PSPs to recover funds paid to fraudsters."[335]

215. An increase in reports of fraud following the implementation of quicker payment systems has also been reported in other jurisdictions. Australia introduced the New Payments Platform in February 2018. At the time, the Reserve Bank of Australia raised concerns about fraud given the increase in speed of payments.[336] The Australian Competition and Consumer Commission (ACCC) reported record levels of scam activity in 2021. $324 million was reported lost to Scamwatch, the ACCC's reporting centre, up 84% since 2019. The ACCC recognised new payment methods and faster payment transfers as a means by which scammers can quickly move money between accounts before a victim realises that they are being scammed.[337]

---

329 House of Commons Library, *Financial Services and Markets Bill 2022–23*,Research Briefing, CBP 9594, 1 September 2022 and Financial Services and Markets Bill, clauses 27 and 28

330 House of Commons Library, *Open Banking: banking but not as we know it?*, Briefing Paper CBP 08215, 26 January 2018

331 Pay.UK, 'How Faster Payments works': https://www.wearepay.uk/what-we-do/payment-systems/faster-payment-system/how-faster-payments-work/ [accessed 1 November 2022]

332 Pay.UK, 'Faster Payment System': https://www.wearepay.uk/what-we-do/payment-systems/faster-payment-system/ [accessed 1 November 2022]

333 UK Finance, *Fraud: the facts 2021* (June 2021): https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf [accessed 1 November 2022]

334 Written evidence from Pay.UK (FDF0014)

335 Written evidence from the Building Societies Association (FDF0023)

336 'Australia Central Bank Acknowledges Faster Payments' Risk Challenge', *PYMNTS.com* (20 March 2018): https://www.pymnts.com/news/b2b-payments/2018/australia-banking-faster-payments-fraud/ [accessed 1 November 2022]

337 Australian Competition and Consumer Commission, *Targeting scams: Report of the ACCC on scams activity 2021* (July 2022): https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scams%20activity%202021.pdf [accessed 1 November 2022]

The ACCC has since recommended the take up of Confirmation of Payee (see paragraph 220), based on the UK's example, to mitigate losses.[338]

Action to tackle fraud at the payment stage

216. There are a number of steps that banks can take if they have reason to suspect that a payment might be fraudulent. Indicators of a suspicious payment might include an abnormally large payment, often to a new payee, or money being quickly transferred in and out of an account.

217. The Banking Protocol is a best-practice initiative introduced to help bank staff spot these 'red flags' and to alert police. The Protocol comes into effect when a bank suspects that a person making a payment in branch is being scammed. At this point they will speak to the customer to try to explain that a fraud could be taking place. If the customer wants to proceed with the payment, the bank can call the police if they still believe that criminal activity is taking place. This may help to shake the victim out of a so-called 'hot state'.[339] We have heard that the Banking Protocol has been considered highly effective. The Building Societies Association told us that between 2016 and 2021, the scheme stopped fraud estimated at a value of £142 million and led to 900 arrests. The Building Societies Association said:

> "The most successful recent fraud policy intervention has been the Banking Protocol. This private/public initiative involving UK police forces, building societies and banks gives building societies and banks the option to bring in guaranteed police intervention where there are concerns that a customer might be being targeted for fraud."[340]

218. Although UK Finance are working to expand it to telephone and online banking, the Protocol is not mandatory and is only best practice and it only applies in branch.[341] We heard from members of the Midlands Fraud Forum that the Protocol is not applied evenly by all banks and staff require greater training in order to ensure it is effective.

> *"I met six of the nine red flags that banks should be looking out for under the Banking Protocol. Why didn't banks immediately stop me from transferring money if they thought it was fraudulent?" - Rachel*

219. Banks are also subject to the Quincecare duty. This places an onus on banks to refrain from executing payment instructions if there are reasonable grounds to believe that the instruction may be an attempt to misappropriate customer funds.[342]

220. Customers of some banks are required to go through the Confirmation of Payee (CoP) process when making online payments. CoP is a name-checking service that was introduced in 2020. It warns customers if a payee's name

338 "People are losing a fortune': ACCC urges banks to act as scam losses surge', *Sydney Morning Herald* (4 July 2022): https://www.smh.com.au/business/consumer-affairs/people-are-losing-a-fortune-accc-urges-banks-to-act-as-scam-losses-surge-20220704-p5ayvy.html [accessed 1 November 2022]

339 Q 36 (Brian Dilley)

340 Written evidence from the Building Societies Association (FDF0023)

341 UK Finance, 'Expanding the Banking Protocol Scheme': https://www.ukfinance.org.uk/news-and-insight/blogs/expanding-banking-protocol-scheme [accessed 1 November 2022]

342 See Thomson Reuters Practical Law, *Barclays Bank Plc v Quincecare Ltd [1992] 4 All E.R. 363* (24 February 1988): available at https://uk.practicallaw.thomsonreuters.com/Document/ID61FA820A39B11ECAA9B8E16236A2AFE/View/FullText.html [accessed 1 November 2022].

does not match the account number they provide. More than 1 million CoP requests are made every day covering over 90% of Faster Payments volumes.[343]

221. While many of the major banks have implemented CoP, some of the smaller players in the market have not. Brian Dilley told us that the introduction of CoP was followed by a migration of fraudsters to banks that do not implement the measure.[344] Nicholas Taylor said that "there is no reason why any firm operating in the UK should not have confirmation of payee".[345]

222. We have heard arguments for and against slowing down the speed with which payments can take place. The arguments for retaining higher speed payments are about the convenience to customers, who value a smooth customer journey. Former Economic Secretary to the Treasury John Glen MP told the Treasury Committee that consumers do not want to see their payments slowed down.[346]

223. However, we found the evidence of Security Minister Tom Tugendhat compelling. He told us that the speed of transactions in the UK is one of the key reasons underpinning the high rate of fraud in the UK. We understand from the Minster that such discussions are now being held with the Treasury and fully support these discussions.[347]

224. Furthermore, in the PSR's November 2021 consultation, the regulator expressed concern that slowing of payment services could disproportionately affect those with protected characteristics given that they might be perceived as more at risk of scams. They suggest that this may limit access to banking and payment services and result in poorer outcomes for certain demographic groups such as the elderly and those with serious mental health conditions.[348] While we recognise this argument, it has been made abundantly clear to us that all people have the capacity to become victims of fraud, regardless of perceived vulnerability. Therefore, this measure should apply across the board.

225. We have heard that there would be value in slowing some payments to give more time to analyse suspicious payments. Rob Jones told us that slowing down a small number of Faster Payments would be beneficial as it would allow time for analysis of fraudulent payments and ultimately prevent APP fraud.[349] Chris Hemsley, Managing Director of the PSR, told us:

> "Most customers would agree that, if I am using my bank account to pay for something like a coffee, it needs to go through quickly. If I am moving potentially life-changing sums of money, a delay of what might be five minutes is not a return to the bad old days of five days to clear funds. It buys a bit of time for the prevention mechanisms to kick in."[350]

---

343 UK Finance, *Fraud: the facts 2021* (June 2021): https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf [accessed 1 November 2022]
344 Q 36 (Brian Dilley)
345 Q 36 (Nicholas Taylor)
346 Oral evidence given taken before the Treasury Committee on 29 November 2021 (Session 2021–22), Q 430 (John Glen)
347 Q 262 (Tom Tugendhat MP)
348 PSR, *Authorised Push Payment (APP) Scams: Consultation paper* (November 2021): https://www.psr.org.uk/media/kg0bx5v3/psr-cp21-10-app-scams-consultation-paper-nov-2021.pdf [accessed 1 November 2022]
349 Q 221 (Rob Jones)
350 Q 158 (Chris Hemsley)

226. The FCA has introduced the New Consumer Duty, a principles-based duty that comes into effect and firms will have to implement by July 2023. It stipulates that firms should consider building 'positive friction' into processes to deliver good outcomes. It suggests that additional steps in the customer journey that are designed to prevent fraud, "would not amount to an unreasonable barrier" and can help to prevent poor decisions. The Duty is outcomes-based rather than led by prescriptive rules. This means that it can be applied more flexibly as technology changes.[351]

227. Finally, information sharing may have a significant impact on reducing fraudulent transfers at the time of payment if shared in real-time. For example, Chris Hemsley told us that the regulator is working to improve information sharing between payment firms to ensure that they can share information around how long an account has been open, which impacts understanding of how risky the account might be.[352]

228. **The speed with which payments are able to be executed, while beneficial for legitimate customers, is helping fraudsters to get their hands on stolen money at pace. Current provisions in place to help to prevent fraud are welcome but must be strengthened to stop payments reaching fraudsters before they are able to cash out stolen money.**

229. ***To stop fraudulent payments slipping through the net, the speed with which certain payments can be made should be subject to a delay lasting no more than several hours. This might include high-value payments made by personal customers to new payees, with an option to extend this to existing payees in the case of high-value payments. The PSR should consult with industry on the introduction of such a measure and the value threshold to be set. Implementation of this measure must not impact the application of other measures such as AI-assisted transaction monitoring.***

230. ***Approval of a banking and/or e-money licence in the UK must be made conditional upon signing up to Confirmation of Payee.***

231. ***The Banking Protocol should be made mandatory and expanded to telephone and online banking. Banks should be required to provide more training to ensure compliance and to help staff to spot 'red flags'.***

232. ***The FCA should conduct a thematic review of retail banks to understand how easy it is for fraudsters to open accounts and consult with industry on the possible solutions, including potential reforms to AML procedures. It should encourage the regular stress-testing of KYC procedures in order to address emerging threats such as deepfake technology.***

233. ***The FCA and PSR should work with PSPs to increase transparency and customer understanding about measures in place to prevent fraud, including possibly slowing the pace of transactions and KYC***

351 FCA, *FG22/5 Final non-Handbook Guidance for firms on the Consumer Duty* (July 2022): https://www.fca.org.uk/publication/finalised-guidance/fg22-5.pdf [accessed 1 November 2022] and FCA, *A new Consumer Duty: Feedback to CP21/36 and final rules* (July 2022): https://www.fca.org.uk/publication/policy/ps22-9.pdf [accessed 1 November 2022]

352 Q 158 (Chris Hemsley)

checks. This work should feed into the Government's centrally led public awareness campaign (see paragraph 418).

Cryptoassets

234. A cryptoasset is a cryptographically secured digital representation of value or contractual rights that can be transferred, stored or traded electronically".[353] There are two major kinds of cryptoassets; unbacked assets like Bitcoin that are considered speculative and volatile, and stablecoins, which are tied to another asset like Pound Sterling.[354]

235. Europol recognises that "criminals involved in frauds strongly rely on the use of cryptocurrencies".[355] Since 2008, the emergence of cryptoassets has provided fraudsters with new opportunities to defraud people, for example through cryptoasset investment scams (see Box 5), and also to cash out their stolen funds. Mark Taber, an anti-fraud campaigner, told us that crypto is used by criminals because it "bypasses traditional banks and the anti-fraud and consumer protection measures they have in place."[356]

236. Katie Martin explained how the process works:

> "Money laundering on the wholesale side is relatively straightforward. You take ill-gotten gains from whatever it is—people trafficking or the drug trade [or fraud]—and convert those proceeds into cryptocurrencies and then pull them out of the financial system at the other end in currencies that you can actually use for day-to-day life, such as sterling, dollars or euros."[357]

237. Cryptoassets can be held anonymously in crypto wallets based anywhere in the world, and the owners of such assets are hard to identify. This is due to difficulties matching blockchain addresses to real users.[358] Issues with blockchain identification are compounded by traditionally poor KYC processes at the point of sign-up. Katie Martin told us that such checks are "often not there", despite claims made by large crypto exchanges.[359] For example, some cryptoasset exchanges do not require or provide identification or verification of those participating in it, nor do they generate historical records of transactions associated with real identities.[360]

Action to regulate cryptoassets

238. TSB has argued that greater use of KYC processes should be built into the cryptoasset ecosystem. It argued that crypto exchanges, which have typically suffered from poor security and KYC processes, should take steps to "tighten up their standards and to accept responsibility for reimbursing

353 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692)
354 Bank of England, 'What are cryptoassets' (19 May 2020): https://www.bankofengland.co.uk/KnowledgeBank/what-are-cryptocurrencies (accessed 1 November 2022]
355 Europol, Cryptocurrencies: tracing the evolution of criminal finances (2021): https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf [accessed 1 November 2022]
356 Written evidence from Mark Taber (FDF0056)
357 Q 70 (Katie Martin)
358 *Ibid.*
359 *Ibid.*
360 2 Bedford Row, 'Money laundering and virtual cryptocurrencies' (27 February 2018): https://www.2bedfordrow.co.uk/money-laundering-virtual-cryptocurrencies-sam-thomas/ [accessed 1 November 2022]

users suffering fraud on their accounts".[361] The Motion Picture Association took this further, arguing that all commercial entities should be required to establish the true identity of their customers as a precondition of doing business.[362]

239. In addition to KYC checks, we have heard that there should be greater scrutiny of on and off ramps within the cryptocurrency system. These are the points at which individuals move their money on and off cryptocurrency platforms. This would be beneficial because, in contrast to some other parts of the cryptoasset ecosystem, these ramps are usually regulated entities such as banks.[363] Furthermore, regulating the process by which money is transferred from traditional banking into crypto might prove an easier task than regulating crypto itself, which is proving a complex challenge for regulators globally.

240. In the USA, the Chair of the Securities and Exchange Commission (SEC) has called on Congress for more powers to police crypto trading, lending and De-Fi platforms, which they described as a "Wild West".[364] The EU has set out its proposed principles in the Markets in Crypto Asset (MICA) directive, which is expected to come into force in 2024.[365] MICA is intended to "protect consumers against some of the risks associated with the investment in cryptoassets, and help them avoid fraudulent schemes".[366]

241. Some nation states have gone further, for example the Estonian Government has implemented additional obligations for cryptoasset service providers to implement KYC checks, which are similar to those that are placed on other types of financial services.[367] The measure was implemented in March 2022 and it is too soon to analyse its impact.

242. The UK has also taken steps to regulate crypto. As of 2020, crypto exchanges and wallet providers must comply with AML obligations and register with the FCA. In March 2021, the FCA launched the Unregistered Crypto Currency Businesses List, which lists firms operating in the UK without registration and that do not appear to be seeking regulation. The list has helped to identify potential scam investments and has led to intervention and subsequent removal of such websites. There are 230 firms on the list as of May 2022.[368]

243. However, as noted, cryptoassets are not within the regulatory perimeter at present. The FCA intends to publish rules for crypto promotions when

361 Written evidence from TSB (FDF0066)
362 Written evidence from the Motion Picture Association (FDF0068)
363 QQ 71–75 (Katie Martin)
364 'U.S. SEC Chair Gensler calls on Congress to help rein in crypto 'Wild West', Reuters (3 August 2021): https://www.reuters.com/technology/us-sec-chair-gensler-calls-congress-help-rein-crypto-wild-west-2021-08-03/ [accessed 1 November 2022]
365 'Borderless crypto markets show need for global rules', *Financial Times* (28 February 2022): https://www.ft.com/content/0e0dc602-af91-4253-a230-c1598781b3b4 [accessed 1 November 2022]
366 European Council, Council of the European Union, ' Digital finance: agreement reached on European crypto-assets regulation (MiCA)' (30 June 2022): https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/ [accessed 1 November 2022]
367 Q 177 (Markko Künnapu). See also 'Crypto bears the brunt of Estonia's war against dirty money', *Politico* (11 March 2022): https://www.politico.eu/article/crypto-finance-estonia-dirty-money/ [accessed 1 November 2022].
368 Written evidence from the FCA (FDF0091) and the FCA (FDF0069)

legislation has been introduced to bring qualifying cryptoassets within the financial promotions' regime.[369]

244. HM Treasury has set out its approach to regulation, including the regulation of stablecoins.[370] It confirmed its plans to legislate to bring certain stablecoins, where used for payment, into the regulatory remit of UK regulators. Under the Financial Services and Markets Bill, the Government will be able to bring newly classified 'digital settlement assets' including stablecoins and other cryptoassets within the regulatory perimeter.[371] The Government intends to consult on the regulatory approach to other types of cryptoasset outside stablecoins (such as Bitcoin) later this year.[372]

245. The Economic Crime and Corporate Transparency Bill will provide additional powers to law enforcement to help them to seize and recover cryptoassets more easily. It will do this by amending criminal confiscation powers in Parts 2, 3 and 4 of POCA and civil recovery powers in Part 5.[373] Whilst we welcome this step, the Committee is concerned that these efforts may be hampered by the difficulties associated with cross-jurisdictional civil orders.

246. Melissa Hodgman, Associate Director in the Enforcement Division at the SEC, told us about the importance of cross-border working given the decline of the 'national market' in favour of international, fast moving payments ecosystems including crypto.[374] Katie Martin agreed that the global nature of cloud-based transactions presents opportunities for multilateral working:

> "It is crucial that the UK is extremely plugged into what the international community is doing on [crypto] … it does not matter if one country manages to do it well. The bad actors can simply move somewhere else. International communication is key."[375]

247. Finally, further technological developments in how digital money is used may present further opportunities for fraudsters. The Committee has heard that the Bank of England is in the early stages of discussing the future of a central bank digital currency, a type of digital bank note. Tom Mutton told us that identity verification was key to the security of any future such digital currency:

> "If we have a central bank digital currency, we want it to have very strong financial crime controls. We want, as far as possible, to make sure that it is reducing financial crime such as fraud. Most of that comes to the question of identity verification. At the same time, if we are to

369 FCA, 'PS22/10: Strengthening our financial promotion rules for high-risk investments and firms approving financial promotions' (1 August 2022): https://www.fca.org.uk/publications/policy-statements/ps22-10-strengthening-our-financial-promotion-rules-high-risk-investments-firms-approving-financial-promotions [accessed 1 November 2022]

370 HM Treasury, *UK regulatory approach to cryptoassets, stablecoins, and distributed ledger technology in financial markets: Response to the consultation and call for evidence* (April 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1088774/O-S_Stablecoins_consultation_response.pdf [accessed 1 November 2022]

371 Financial Services and Markets Bill, Chapter 2(22)

372 Explanatory Notes to the Financial Services and Markets Bill [Bill 146 (2022–23)-EN]

373 HM Government, 'Fact sheet: Economic Crime and Corporate Transparency Bill' (22 September 2022): https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/fact-sheet-economic-crime-and-corporate-transparency-bill-overarching [accessed 1 November 2022]

374 Q 183 (Melissa Hodgman)

375 Q 79 (Katie Martin)

have trust and confidence in the money, we need to make sure that it is upholding society's reasonable expectations of privacy."[376]

248. **Alongside the threat of cryptoasset investment scams, cryptoassets are increasingly being used by fraudsters to syphon off their stolen funds, allowing them to disappear without trace. Regulators must focus more tightly on the 'on and off-ramps' that facilitate the transfer of funds from traditional banks into and out of crypto-based wallets. Regulators must use their existing powers to tackle this challenge and support the work of the global regulatory community as it continues to create an aligned approach to cryptoasset regulation.**

249. ***The Government should work with the private sector to integrate better KYC checks into the cryptoasset account set-up process. This should include designing systems that ensure cryptoassets and crypto-wallets can be traced to an identified individual.***

250. ***HM Treasury should urgently bring forward the measures in the Financial Services and Markets Bill to enable the FCA to regulate cryptoassets, as well as its forthcoming consultation on other types of cryptoassets.***

251. ***The Home Office should urgently bring forward measures in the Economic Crime and Corporate Transparency Bill to allow the seizure of cryptoassets using civil recovery powers as well as the existing criminal powers.***

Money mules

252. A money mule is someone who receives money from a third party in their bank account and transfers it somewhere else, or who withdraws it as cash and gives it to someone else, obtaining a commission for it or payments in kind. These individuals are targeted by 'mule herders', who recruit money mules, often using social media or gaming platforms.[377] Mules may be promised a cut of the money that they are asked to transfer. The City of London Police told us:

> "The continued use of 'money mule networks' to receive, move and conceal the proceeds of fraud is an ongoing and persistent threat evidenced across many fraud types and continues to facilitate the movement of fraudulent funds as well as access to victims across domestic and international jurisdictions. The recruitment of money mules for use in fraud has continued over the past year on both digital messaging services and social media platforms."[378]

253. Criminals may also use more traditional tactics to recruit young people to act as money mules. Research from Cifas in the pre-pandemic year 2019

376 Q 165 (Tom Mutton)
377 Q 37 (Brian Dilley) and HSBC, *Get to know gaming: spending*: https://www.hsbc.co.uk/content/dam/hsbc/gb/pdf/video-transcripts/hsbc-transcript-spending.pdf [accessed 1 November 2022]
378 Written evidence from City of London Police (FDF0031)

showed that the number of cases of 14 to 18 year olds acting as money mules grew by 73% (5,819 cases) in the previous two years.[379] Mike Haley told us:

> "There are certain areas and schools where we know that there are young people called 'fraud stars' who will hang around the gates and recruit people—we call them mule herders—into money mule activity … If you do not realise that this is criminal activity, and what the repercussions and consequences are to protect yourself, we will end up … sleepwalking not just into an epidemic of fraud but into our young people seeing it as a legitimate way of getting a new pair of trainers or a bit of cash."[380]

254. We have also heard that overseas students' bank accounts are often targeted once they have left the UK.[381] The Devon and Cornwall Police told us that these students may have been recruited when they enter the UK and make their UK bank accounts available for money laundering once they have returned overseas.[382] It is clear that banks should increase monitoring on such accounts and ensure that they are closed once the students leave the UK in a timely fashion once activity on the account has ceased.

255. Many of these young people are unaware of the consequences of being a money mule, which can include, bank account closure, limited access to loans or credit cards, difficulty obtaining a phone contract, and/or a prison sentence of up to 14 years.[383] Philip Milton, Public Policy Manager at Meta, told us about the importance of education to tackle this threat:

> "I point to education in this piece as well, because often you find that money mules do not actually know that that is what they are. It is often a crime that people commit unknowingly. The mule herders know exactly what they are doing, but often it is a get-rich-quick scheme for people who might not necessarily know the implications of what they are doing. It is effectively money laundering."[384]

256. Geraldine Lawlor, Global Head of Financial Crime at KPMG, cautioned that there is a distinction between money mules who are unknowingly facilitating crime, and those that wilfully ignore advice:

> " … Sometimes individuals do not take heed, and they still allow access to their accounts. There is a point where you can determine that they have been reckless and have ignored all the attempts to prevent them going down that route and have gone ahead regardless. That is assessed in how you determine whether they should be treated as a criminal or a victim."[385]

379 BBC News, 'Rise in teenage money mules prompts warnings' (16 September 2019): https://www.bbc.co.uk/news/business-49717288 [accessed 1 November 2022]
380 Q 21 (Mike Haley)
381 Q 37 (Geraldine Lawlor)
382 Written evidence from Devon and Cornwall Police (FDF0009)
383 Cifas, UK Finance, 'Don't be fooled': https://www.moneymules.co.uk/ [accessed 1 November 2022]
384 Q 138 (Philip Milton)
385 Q 37 (Geraldine Lawlor)

Action to tackle money muling

257. Tackling money muling is listed as a priority in the Retail Banking Fraud Sector Charter under Action 4, which sets out the need for more effective deterrents for such activity, and for these to be applied consistently.[386]

258. There are a number of procedures in place by banks to prevent and detect money muling. The Mule Insights Tactical Solution (MITS) was developed to track suspicious payments and identify mule accounts. It is a network-level solution that traces funds through the financial system.[387] MITS works through algorithms, which alert financial institutions to suspect mule accounts within their portfolios. It is superior to manual tracking processes that cannot keep up with Faster Payments and allows financial institutions to see the whole payments network.[388]

259. The West Midlands Police and Crime Commissioner, Simon Foster, has funded a project to educate schoolchildren on the risks of being a money mule. The PCC told us that early intervention and preventative action are underused tools in the counter-fraud response, arguing that education increases fraud awareness within these groups.[389] Mike Haley argued that education on the dangers of muling should be a mandatory part of the PSHE curriculum."[390]

260. Transpact told the Committee that banks should do more to educate their customers on the risks of muling, arguing that too many mules claim they did not know what they were doing is wrong. It suggests that the payee bank (the mule's account) should be held responsible for warning its customers of accepting such payments for the purposes of transferring illegally obtained money.[391]

261. Former Minister for Tech and the Digital Economy Damian Collins told us that the Government already funds several programmes to tackle media literacy in order to educate citizens with the "basic information they need to try to keep themselves safe and question the sources of information they see".[392]

262. **Money muling is a serious form of money laundering, yet not enough people are alert to the dangers and risks that can follow from allowing their bank account to be used to launder the proceeds of crime. The Committee is concerned that cost of living pressures could force more people from a range of demographic groups towards money muling.**

263. ***Building on the work of Cifas and UK Finance, the Government should roll out a national campaign in partnership with schools and universities focussed on raising awareness of the dangers of***

386 Home Office, 'Fraud sector charter: retail banking' (updated 26 October 2021): https://www.gov.uk/government/publications/joint-fraud-taskforce-retail-banking-charter/fraud-sector-charter-retail-banking-accessible-version [accessed 1 November 2022]

387 See written evidence submitted by Mastercard to the Treasury Committee inquiry on Economic Crime (ECC0074)

388 Vocalink, 'Mule Insights Tactical Solution': https://www.vocalink.com/newsroom/success-stories/case-study-mits/ [accessed 1 November 2022]

389 Written evidence from the West Midlands Police and Crime Commissioner (FDF0035)

390 Q 21 (Mike Haley)

391 Written evidence from Transpact.com (FDF0061)

392 Q 269 (Damian Collins MP)

money muling. It should also consider awareness campaigns for demographic groups that are not typically targeted by mule herders.

264. ***In partnership with industry, the Government must explore the functionality of a mechanism akin to Confirmation of Payee that alerts a payee about the dangers of money muling and requests authorisation when they receive a payment from an unknown bank account.***

CHAPTER 5: THE GOVERNMENT RESPONSE TO FRAUD

265. The responsibility to catch and prosecute fraudsters is held by various authorities including law enforcement and the courts. The Government's response to counter-fraud policy shapes how this looks and feels in practice. Its response is made up of Government departments and bodies, law enforcement agencies including the police and CPS, and it involves a range of stakeholders in the process of supporting victims and making the public aware of current threats.

266. This chapter will explore how the Government's organisational response to fraud could be improved in England and Wales.

The Government's multi-agency approach

267. Multiple government departments, regulatory and law enforcement agencies are responsible for enacting the Government's multi-agency approach to tackling fraud. In response to a request by this Committee, the Home Office set out the responsibilities of the various agencies involved as outlined in Figure 7.[393]

268. Concerns have been raised that this fragmented departmental approach has led to a "responsibility vacuum" within fraud policy and the low prioritisation of fraud by the Government.[394] Speaking to the Committee following his resignation as Minister for Efficiency and Transformation at HM Treasury, Lord Agnew of Oulton told us about his frustration around the lack of cross-departmental working:

> " … there is painfully little join-up of departments to collaborate on issues that are complex, such as this. It applies on things like adult social care and homelessness. There are a whole range of interventions today that government needs to make to improve citizens' lives, where it does not sit tidily in one department. Fraud is one of those examples."[395]

269. The result of such fragmentation is de-prioritisation of fraud as a policy issue. The lack of priority given to fraud by senior members of the Government was highlighted earlier this year. Speaking in February 2022, former BEIS Secretary and now former Chancellor Kwasi Kwarteng commented that fraud was not a crime that people experience in their "day-to-day lives".[396] This is plainly not the experience that we have heard from victims of fraud. Nor is it borne out by the statistics, with levels of fraud and computer misuse offences increasing 17% in the year ending March 2022 compared to the previous year.[397] Furthermore and as noted, according to the Home Office, fraud is the most commonly experienced crime.[398]

393 Home Office, 'Fraud Act 2006 and Digital Fraud Committee paper on cross departmental fraud responsibilities': https://committees.parliament.uk/publications/23100/documents/169176/default/
394 Written evidence from RUSI (FDF0036)
395 Q 24 (Lord Agnew of Oulton)
396 BBC, 'Sunday Morning' (6 February 2022): https://www.bbc.co.uk/iplayer/episode/m00149kt/sunday-morning-06022022 [accessed 1 November 2022]
397 See Home Office, 'Crime outcomes in England and Wales 2021 to 2022' (22 July 2021): https://www.gov.uk/government/statistics/crime-outcomes-in-england-and-wales-2021-to-2022/crime-outcomes-in-england-and-wales-2021-to-2022 [accessed 1 November 2022].
398 Home Office, 'Beating Crime Plan': https://www.gov.uk/government/publications/beating-crime-plan/beating-crime-plan#fn:16 [accessed 1 November 2022]

270. We recognise that the new Security Minister has set out his intention to place greater emphasis on tackling fraud. Tom Tugendhat told us that fraud was raised immediately in discussions with the former Prime Minister Liz Truss MP, and he described it as a "matter of national security".[399]

271. The Government has sought to overcome the fragmented nature of counter-fraud policymaking via two key working groups, the Economic Crime Strategic Board (ECSB) and its Joint Fraud Taskforce (JFT), which, as noted, have not yet met under the new Security Minister. Membership of these groups are shown in Box 9 and Box 10.

272. At present, the ECSB contains representatives of individual telecoms sector companies but does not have the same level of representation from the tech sector beyond the inclusion of techUK and Google. However, we understand that many of these companies are members of the Online Fraud Steering Group (OFSG), an offshoot of the ECSB (see below).

Box 9: Membership of the ECSB

- Home Office—Home Secretary, Minister for Security and Borders, Director General for Homeland Security, Director, Economic Crime
- HMT—Chancellor of the Exchequer, Economic Secretary to the Treasury, Director, Economic Crime
- AGO—Attorney General
- DCMS—Minister for Tech and the Digital Economy
- FCDO - Minister for South and Central Asia, North Africa, UN and the Commonwealth
- SFO—Director
- CPS—Director of Public Prosecutions
- HMRC—Director, Fraud Investigation Service
- Prime Minister's Anti-Corruption Champion
- Governor of the Bank of England
- Regulators—Solicitors Regulation Authority, Financial Conduct Authority
- National Crime Agency
- City of London Police
- Representative bodies—UK Finance, techUK, Association of British Insurers, ICAEW, Law Society of England and Wales
- Financial services—HSBC, Lloyds, Natwest, Barclays, Standards Chartered, Nationwide, Revolut, Santander, Vocalink
- Google
- Vodafone UK

399 Q 250 (Tom Tugendhat MP)

Box 10 Membership of Joint Fraud Taskforce

- Home Office
- DCMS
- HMT
- Serious Fraud Office
- National Cyber Security Centre
- Victims Commissioner
- City of London Police
- National Economic Crime Centre
- National Trading Standards
- Ofcom
- Financial Conduct Authority
- Cifas
- UK Finance
- techUK
- Citizens Advice
- Victim Support
- British Retail Consortium
- Institute of Chartered Accountants in England and Wales (ICAEW)
- Association of British Insurers
- Law Society of England and Wales
- Communications Crime Strategy Group

Source: Home Office, 'Fraud Act 2006 and Digital Fraud Committee paper on cross departmental fraud responsibilities': https://committees.parliament.uk/publications/23100/documents/169176/default/ [accessed 1 November 2022] Note: John Penrose, the Prime Minister's Anti-Corruption Champion resigned in June 2022 and the Government has not confirmed a replacement.

273. We welcome the re-launch of the JFT in 2021 following soaring rates of fraud during the pandemic. We are pleased to see that some private companies are engaged with these working groups and have heard positive feedback on their output. Security Minister Tom Tugendhat highlighted that the Joint Fraud Taskforce has "the intention of coming up with strategies and policies that will make a difference."[400] Katy Worobec agreed that the ECSB is a "force for good", however she cautioned that "they must be active and lead to action as opposed to being talking shops".[401] Worobec praised the creation of the OFSG, saying:

> "That move from the Economic Crime Strategic Board to the setting up of the Online Fraud Steering Group is a real example of how the convening power of bringing senior people from government, law enforcement and the private sector together with a general focus on economic crime can really make a difference."[402]

274. We have also heard criticisms about the functionality and output of the ECSB. Brian Dilley told us that the ECSB has met "irregularly" due to changing political circumstances, albeit making a positive contribution when it does.[403]

275. The Joint Fraud Taskforce has published three charters setting out steps that signatories should take to tackle fraud (see Appendix 4). These focus on the three areas of accountancy, retail banking and telecommunications. We

400 Q 255 (Tom Tugendhat MP)
401 Q 19 (Katy Worobec)
402 *Ibid.*
403 Q 40 (Brian Dilley)

understand that a fourth Tech Sector Charter is due to be published in the near future.[404] At present, the Fraud Sector charters remain voluntary.

276. In addition to these bodies, the National Economic Crime Centre was set up by the Home Office to take on the operational leadership on economic crime and to bring together government departments with law enforcement, regulatory bodies and the private sector.[405] The NECC also receives Suspicious Activity Reports (SARs), which detail the knowledge of suspicion of money laundering or terrorist financing, via its UK Fraud Intelligence Unit (UKFIU), which makes them available to law enforcement. The NECC includes representatives from a range of Government and law enforcement agencies, as shown in Figure 16.

Figure 16: Membership of the National Economic Crime Centre

Source: NCA, 'National Economic Crime Centre': https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre [accessed 1 November 2022]

277. The NECC co-chairs the OFSG with UK Finance and techUK. Mark Steward told us that the coordinating focus of the NECC works well but that it is hampered by a lack of funding. This has been addressed in Chapter 5.[406] Duncan Tessier told us that the NECC could do more to coordinate counter-fraud communication to citizens.[407] Dr Hawley suggested that fraud

404 Treasury Committee, *Economic crime: responses to the Committee's Eleventh Report* (Eighth Special Report, Session 2021–22, HC 1261)
405 Q 3 (Duncan Tessier)
406 Q 147 (Mark Steward)
407 Q 10 (Duncan Tessier)

is not prioritised within the organisation because it does not have a specific mandate to tackle fraud.[408]

278. The Government is expected to set out its approach to fraud in a forthcoming long-term Fraud Strategy. Security Minister Tom Tugendhat explained that the strategy will be led by the minister and coordinated by the Economic Crime Strategic Board. It will focus on three core pillars:

(1) 'Stop and block' measures to stop fraudulent advertising and outreach from fraudulent individuals

(2) Empowering people by giving them the information they need to respond to and report phishing

(3) Pursue fraudsters.[409]

Box 11: Reforming Companies House

Companies House is an executive agency sponsored by BEIS. Its responsibilities are to incorporate and dissolve limited companies, examine and store company information and to make information available to the public. More than four million limited companies are registered in the UK and over half a million are set up every year.[410]

However, Companies House has no statutory powers, and it cannot verify information provided to it. The Government has boasted that incorporation of companies by the registrar is "among the fastest and cheapest in the world".[411] Companies can be registered at pace for a fee as low as £12 and 99% of applications are processed within 24 hours.[412] This leaves it open to abuse by unscrupulous individuals who can use fake details to establish fraudulent or non-existent companies.

Following his resignation from office, Lord Agnew told us that the Government had dragged its feet over reforms to Companies House. He put this delay down to "a mixture of naivety, complacency, ignorance and stupidity".[413] The former Cabinet Office and Treasury minister suggested it was a weak argument to suggest that reforms might place more burdens on new business creation.[414]

408 Q 84 (Dr Susan Hawley)
409 Q 254 (Tom Tugendhat MP)
410 Companies House, 'About us': https://www.gov.uk/government/organisations/companies-house/about [accessed 1 November 2022]
411 HM Government, *The Queen's Speech 2022* (10 May 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1074113/Lobby_Pack_10_May_2022.pdf [accessed 1 November 2022]
412 'Overhaul of Companies House is long overdue', *Financial Times* (29 September 2021): https://www.ft.com/content/6fd92a72-e457-4d32-a5a5-c44ec2b76e20 [accessed 22 July 2022]; HM Government, *The Queen's Speech 2022* (10 May 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1074113/Lobby_Pack_10_May_2022.pdf [accessed 1 November 2022] and Q 26 (Lord Agnew of Oulton)
413 Q 26 (Lord Agnew of Oulton)
414 *Ibid.*

Furthermore, there is widespread misunderstanding about the role of Companies House. Victims we spoke to told us that they believed that Companies House was the go-to source to assess the legitimacy of a company and its directors. The general public do not receive enough information and advice on the role and remit of the registrar, and as a result are being misguided by the information published on it.

> *"I researched the company on Companies House because I thought it would tell me if it was legitimate. When I later found out it was a fake company I felt angry and silly. Companies House needs reform." - Bill*

The Treasury Committee called for reform of the registrar in its February 2022 report, calling specifically for more rigorous identity checks and higher incorporation fees.[415] The forthcoming Fraud Action Plan is expected to contain plans to reform Companies House further, in particular by introducing greater corporate transparency.[416]

The Economic Crime and Corporate Transparency Bill delivers several improvements to Companies House, including the following reforms:

- new powers to allow Companies House to check, remove and/or decline incorrect or fraudulent information submitted to or already on the register
- the introduction of identity verification for new and existing company directors, People with Significant Control and those delivering documents
- a tightening of registration and transparency requirements for limited partnerships
- upgrading investigation and enforcement powers, enabling it to cross-check data with public and private sector bodies and proactively share suspicious activity with security agencies and law enforcement.[417]

We remain concerned about how these reforms will be funded. Campaign groups such as Transparency International UK have raised the lack of assurances given as of yet that the reforms will be accompanied by additional funding. Spotlight on Corruption have recommended increasing registration fees in order to fund enforcement of the registrar's new powers.[418] The Security Minister confirmed that this option is being discussed, while we understand that funds from the Economic Crime Levy will also be used to fund the reforms.[419] It will be essential that alongside any such funding, adequate resources are given to upskilling the workforce Companies House to support the growth in investigative capacity.

279. The lack of central government leadership to guide fraud policy has led some to suggest that a Minister for Fraud should be appointed. BT Group made the case that putting counter-fraud policy under the ownership of one

415 Treasury Committee, *Economic Crime* (Eleventh Report, Session 2021–22, HC 145)
416 HM Government, *UK Finance, Economic Crime Plan: Statement of Progress: July 2019–February 2021* (April 2021): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/983251/Economic_Crime_Plan_Statement_of_Progress_May_2021.pdf [accessed 1 November 2022]
417 HM Government, 'Fact sheet: Economic Crime and Corporate Transparency Bill overarching' (22 September 2022): https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/fact-sheet-economic-crime-and-corporate-transparency-bill-overarching [accessed 1 November 2022]
418 BBC News, 'Economic Crime Bill: Plan to tackle dirty money in UK set out' (22 September 2022): https://www.bbc.co.uk/news/uk-politics-62996876 [accessed 1 November 2022]
419 Q 255 (Tom Tugendhat MP and Duncan Tessier)

department with one minister responsible for ownership would bring clarity and enable more joined up working.[420] TSB recommended the establishment of a cabinet level, cross-departmental minister for fraud, with oversight over the entire fraud landscape, to act as a single point of accountability and to "join up the different and competing elements that are the current fraud landscape.[421]

280. Given the cross-departmental nature of the fraud policy landscape, it is unclear in which department such a minister would sit. The cross-departmental working groups including the ECSB and the Joint Fraud Taskforce are providing an effective forum for this activity, and should continue to be led by a Home Office minister with a clear focus on fraud within their portfolio.

281. Others including RUSI, Spotlight on Corruption and Meta suggested a statutorily appointed Commissioner for Fraud might be best placed to hold the Government to account for its record.[422] However, we remain concerned that any such Commissioner or counter-fraud oversight body must have sufficient 'teeth' and a requirement to report to Parliament once a year.[423]

282. **We welcome the re-launch of the Joint Fraud Taskforce and other public-private forums for discussion and cross-sector information sharing. However, we remain concerned that these bodies remain voluntary 'talking shops' and do not maximise their potential for effective leadership in the counter-fraud landscape. While we recognise the merits of appointing a sole point of accountability, this is challenging given that fraud sits across departmental boundaries. We do not wish to add more acronyms to the alphabet soup of stakeholders responsible for economic crime, however it is clear the current approach is not working. Fraud is a national risk and must be treated as a national priority.**

283. ***The Government should bring forward the Economic Crime and Corporate Transparency Bill to ensure that Companies House becomes a more active and transparent gatekeeper of company information to protect consumers. Companies House must be provided with appropriate resources to achieve the ambitions set out in the Economic Crime and Corporate Transparency Bill.***

284. ***Membership of the NECC should be broadened to include Ofcom given its remit for digital communications and the rapid increase in fraud by exploitation of digital communications. In addition, we recommend that the NCA join the DRCF (see recommendation 86).***

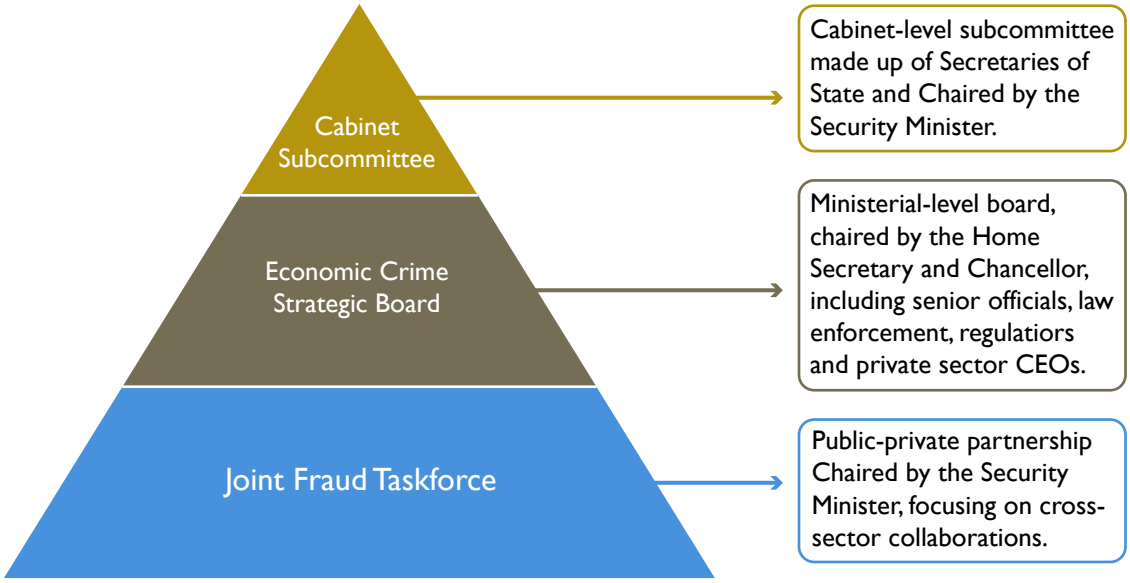
285. ***The NCA must treat fraud as a crucial part of its responsibility to address serious crime under the Crime and Courts act 2013. The Secretary of State should explore whether they could encourage more co-operation between the NCA and Ofcom to combat fraud by determining this as a strategic priority under Section 3 of the Crime and Courts Act 2013. Consultation with Ofcom and a direction that the NCA and Ofcom work more closely together should underline and strengthen more proactive enforcement activity by Ofcom.***

---

420 Written evidence from BT Group (FDF0067)
421 Written evidence from TSB (FDF0066)
422 Q 84 (Dr Susan Hawley), Q 145 (Philip Milton) and written evidence from RUSI (FDF0036)
423 Q 27 (Lord Agnew of Oulton)

286. ***A cabinet sub-committee with a clear mandate to tackle fraud should be established, chaired by and accountable to the Security Minister. The sub-committee should bring together more effectively all departments with a portfolio that spans fraud. To ensure transparency, its membership and terms of reference should be made public.***

Figure 17: Suggested structure for oversight of fraud policymaking



Law enforcement

Policing

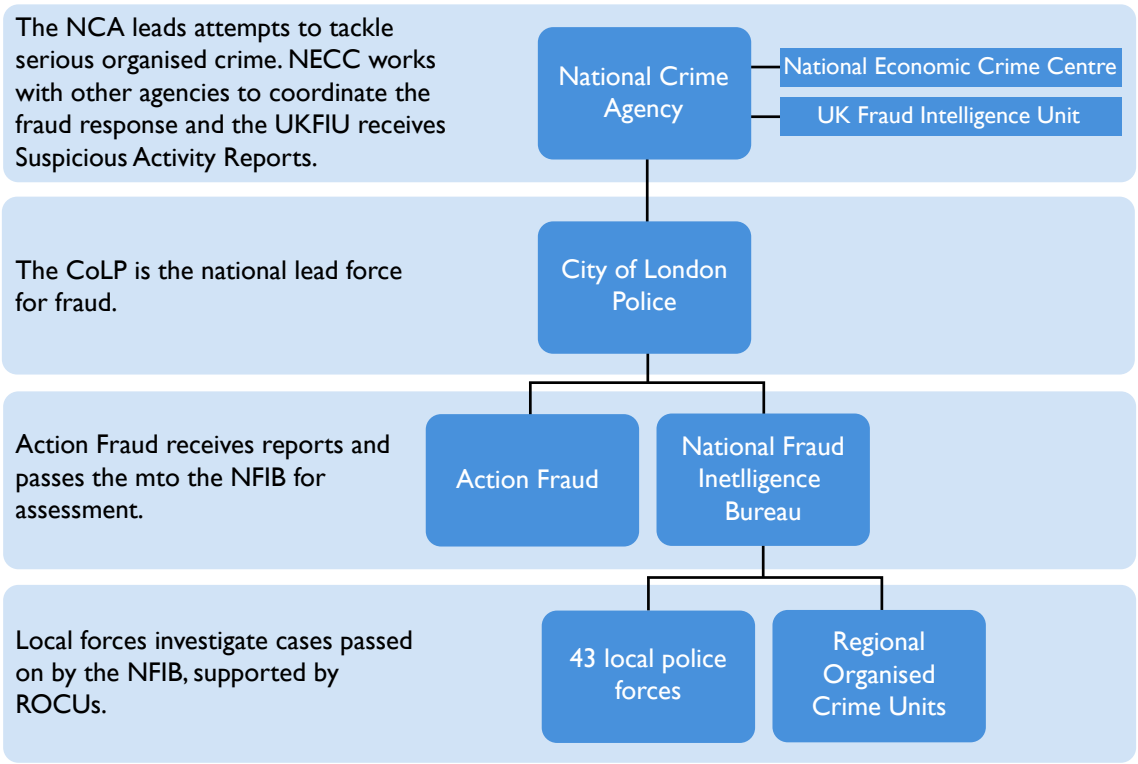
287. Law enforcement plays a critical role in tackling fraud. At present, the Government advocates for a multi-agency approach to law enforcement.[424] This means that England and Wales' response to fraud consists of several different bodies, including non-ministerial government departments such as the NCA, co-ordinating bodies such as the NECC, and front-line police officers and staff in 43 local forces. The current approach to policing fraud was raised several times in evidence as ineffective. Reasons to be explored in this chapter include:

- The myriad of bodies involved in the law enforcement response
- Structural challenges related to the organisation and responsibilities of police force areas
- Challenges due to the international nature of fraud
- The under-prioritisation of fraud vs other crime types
- A chronic lack of financial resources to employ and train law enforcement staff and police officers in speciality areas such as digital and cyber-crime.

424 Treasury Committee, *Economic crime: responses to the Committee's Eleventh Report* (Eighth Special Report, Session 2021–22, HC 1261)

288. In England and Wales, the response to serious and organised crime is led by the NCA and coordinated by the NECC, which brings together law enforcement and other relevant agencies including the Home Office, HMRC, the CPS, the Serious Fraud Office (SFO), the FCA, and the City of London Police. The City of London Police is the national lead force to fraud and is responsible for Action Fraud, the national reporting centre, and the NFIB, which analyses the reports received by Action Fraud. The key elements of the law enforcement response to fraud in England and Wales are shown in Figure 18.

Figure 18: The law enforcement structure for policing fraud



289. In addition to these bodies, a range of other stakeholders are involved in the counter-fraud response. These include the SFO, which investigates and prosecutes serious or complex fraud, Trading Standards, which investigates unfair trading and illegal business activity including rogue traders and scams, and the Financial Ombudsman Service, which settles complaints between consumers and financial service businesses.

290. This "alphabet soup" of agencies involved in the counter-fraud response has been criticised by a variety of organisations, with Spotlight on Corruption arguing that this approach increases the fragmentation of efforts to tackle fraud.[425] Mark Shelford told us that this can exacerbate the impact on victims:

> "From a victim's perspective, the landscape is very confusing. If they ring the local police, the local police will say, "You need to ring Action Fraud". They ring or write to Action Fraud, and they may or may not get a response, so they feel that there is a black hole there. Then, confusingly, it might be allocated from Action Fraud to the regional investigation—the ROCUs—or allocated back to the original force, in

425 Written evidence from Mark Taber (FDF0056) and Spotlight on Corruption (FDF0053)

my case Avon and Somerset. They find that whole process extremely confusing."[426]

291. The Government has defended its multi-agency approach to law enforcement, however the Security Minister has recognised the need to streamline and tighten the various elements that make up the response to fraud, and told us that the Government is keeping the structure under review.[427]

292. Attempts to reorganise and simplify the law enforcement approach to economic crime have been put forward, which we welcome. Recent proposals are detailed in the table below.

Table 2: Recent proposals to reorganise the structural policing model

Author	Detail
Treasury Committee, Economic Crime (February 2022)	The Treasury Committee recommended the introduction of a single law enforcement agency with clear responsibilities and objectives to fight economic crime. The Government dismissed this in favour of a multi-agency approach.
The Police Foundation, Strategic Review of Policing in England and Wales (March 2022)	The 'Barber Review' recommended the creation of a new Crime Prevention Agency and the expansion and strengthening of the NCA in control of regional serious and organised crime capabilities under its control. Fraud investigations would be carried out by economic crime specialists in Regional Organised Crime Units (ROCUs). Local forces would lose their responsibility for fraud but would retain supervision of vulnerable victims.
Social Market Foundation (March 2022)	The think tank called for local forces to lose their responsibility for economic crime. An expanded NCA would absorb the economic crime functions of the City of London Police and the SFO. The review called for a review of pay to ensure that the law enforcement agencies can compete with the private sector for talent.
Policy Exchange (August 2022)	Policy Exchange recommended that the Home Office should reorganise the response to fraud by including it in the SPR and giving responsibility for investigation to appropriately-resourced ROCUs under the NCA's leadership.

Source: Treasury Committee, Economic Crime: (Eleventh Report, Session 2021–22, HC 145); Treasury Committee, Economic Crime: responses to the Committee's Eleventh report (Eighth Special Report, Session 2021–22, HC 1261); The Police Foundation, A new mode of protection: Redesigning policing and public safety for the 21st century (March 2022): https://www.policingreview.org.uk/wp-content/uploads/srpew_final_report.pdf [accessed 1 November 2022]; Social Market Foundation, 'Fraud is now Britain's dominant crime, but policing has failed to keep up' (4 March 2022): https://www.smf.co.uk/commentary_podcasts/fraud-is-britains-dominant-crime/ [accessed 1 November 2022] and Policy Exchange, 'What do we want from the next Prime Minister?' A series of policy proposals for new leadership: Crime & Policing - a force fit for the future (31 August 2022): https://policyexchange.org.uk/wp-content/uploads/2022/09/Crime-Policing-What-do-we-want-from-the-next-Prime-Minister.pdf [accessed 1 November 2022]

426 Q 213 (Mark Shelford)
427 Q 255 (Tom Tugendhat MP)

293. The Committee recognises calls for a new overarching agency, however we were concerned that any such agency would be vulnerable to significant disruption, which could result in lulls in enforcement and 'brain drain' of expertise as individuals move from one agency to another.[428] Assistant Commissioner Pete O'Doherty at the City of London Police argued that the best outcomes would be achieved by building on current systems, arguing that this should focus on "evolution, not revolution".[429]

294. Police Scotland has taken a different approach to command control. The Scottish Crime Campus was established in 2015 and comprises 27 law enforcement agencies, co-located on the campus.[430] It is characterised as a 'national force' as opposed to the multi-agency approach taken in England and Wales. The model places specialist resource at the centre, with less complex frauds tackled by front-line police officers.[431] In his Independent Review of Serious and Organised Crime, Sir Craig Mackey QPM argued for the creation of a UK Crime Campus to allow for collaboration within a shared working environment, complemented by Regional Crime Campuses.[432] However, while the campus model benefits from a centralised focus, we also recognise that a national model may result in lost impact at a local level, which is crucial for victim support.[433]

295. Some elements of the present system in England and Wales do appear to be effective. At present, local forces are tasked with investigating fraud in their police force areas. This localised response has benefits for victims (see Chapter 5) as it allows for a tailored response. However, its effectiveness is limited by the geographical spread of fraudsters, both nationally and internationally, who are able to reach victims in another police force areas via the internet. The City of London Police estimated that 78% of frauds involve offences where suspects and victims do not live in the same force's jurisdiction.[434]

Prioritisation

296. We received evidence that fraud is under-prioritised compared to other crime types by law enforcement, both at the local level and more widely. Michael Skidmore told us that the cross-border nature of fraud means that it requires strong "national leadership, direction and governance to steer the ship". He suggested that the NCA is able to do this effectively in some areas such as drug-related organised crime, however outside the City of London Police, fraud is not considered a priority.[435]

297. In part, this is due to local police forces being overburdened. Michael Skidmore told us that police may be assigned an investigation without a local victim, which means that it is outcompeted by other types of local

428 Written evidence from Spotlight on Corruption (FDF0053)
429 Q 213 (Pete O'Doherty)
430 Oral evidence taken before the Treasury Committee on 25 January 2021 (Session 2019–21), Q 47 (Patrick Campbell)
431 Q 189 (DCI Stevie Trim)
432 Home Office, 'Independent Review of Serious and Organised Crime' (16 March 2021): https://www.gov.uk/government/publications/independent-review-of-serious-and-organised-crime/independent-review-of-serious-and-organised-crime-accessible-version [accessed 1 November 2022]
433 Q 189 (DCI Stevie Trim)
434 Written evidence from City of London Police (FDF0031)
435 Q 81 (Michael Skidmore)

crime when it comes to public demand for response.[436] The Social Market Foundation added:

> " … fraud is not a priority for most local forces, who face squeezed budgets, competing priorities and a lack of sufficient skilled officers and civilian staff to investigate complex crimes, that are time and labour intensive to deal with. The result is that the parts of the police service of England and Wales that are worst placed to deal with fraud are ultimately the ones that—in most cases—are expected to deal with it. Consequently, they fail to do so."[437]

298. The under-prioritisation of fraud as a crime type has wider social and ideological causes. In 2019, HM Inspectorate of Constabulary, Fire and Rescue Services (HMICFRS) noted that "fraud does not bang, bleed or shout".[438] As a result, it is de-prioritised in comparison to other violent crime types. This common misconception underestimates the impact of fraud on its victims, which is explored further from paragraph 359. Former Victims' Commissioner Dame Vera Baird suggested that fraud is prey to assumptions including the suggestion that victims have taken risks with their own money, are affluent, or have been "stupid".[439] We were dismayed to read a recent investigation by The Times, which showed that some police forces were using victim conduct, for example whether they ignored warnings, to de-prioritise fraud cases.[440]

299. While these assumptions may not permeate law enforcement's assessment of fraud, these views may impact public perceptions of what the police should prioritise.

300. One suggestion to address the lack of priority given to fraud is to make fraud part of the Strategic Policing Requirement (SPR). The SPR sets out the Home Secretary's assessment of the national threats that police must prioritise in England and Wales. The Committee received support for the inclusion of fraud within the SPR from groups including the City of London Police, RUSI and the Association of Police and Crime Commissioners.[441] Rob Jones told us that inclusion within the SPR would help to "shift the dial" on prioritising fraud.[442] However, we recognise concerns raised by Andy Cooke that continuously adding more to the SPR results in de-prioritisation of other areas, potentially those within the SPR at present.[443]

International law enforcement

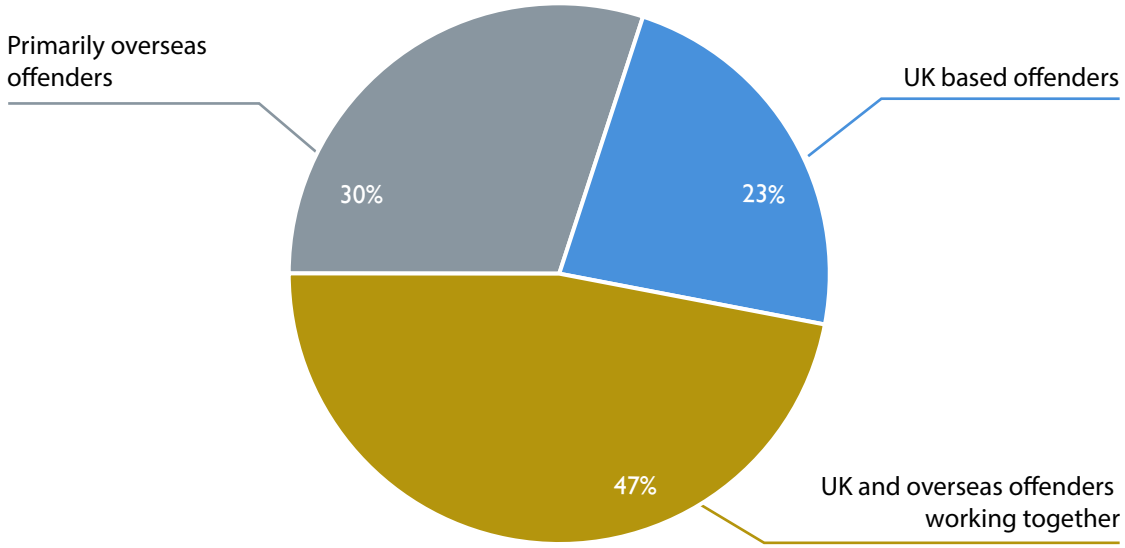
301. In addition to the divergence of fraudsters and their victims across the UK, many victims are defrauded by criminals based overseas. There are several processes by which international agencies can cooperate with one

436 Q 81 (Michael Skidmore)
437 Written evidence from the Social Market Foundation (FDF0026)
438 His Majesty's Inspectorate of Constabulary and Fire & Rescue Services, *Fraud: Time to Choose* (April 2019): https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/fraud-time-to-choose-an-inspection-of-the-police-response-to-fraud.pdf [accessed 1 November 2022]
439 Q 111 (Dame Vera Baird)
440 'Fraud victim? The police won't help if you were warned about it', *The Times* (20 August 2022): https://www.thetimes.co.uk/article/fraud-victim-the-police-wont-help-if-you-were-warned-about-it-2xns9jn2z [accessed 1 November 2022]
441 Written evidence from City of London Police (FDF0031), RUSI (FDF0036), and the Association of Police and Crime Commissioners (FDF0064)
442 Q 212 (Rob Jones)
443 Q 223 (Andy Cooke)

another. These include Mutual Legal Assistance treaties—obtained through a process that RUSI describes are "cumbersome"—as well as international agreements such as the 2001 Budapest Convention on Cybercrime and the UN Convention Against Transnational Organised Crime.[444] In addition, international law enforcement agency Interpol launched a new Financial Crime and Anti-Corruption Centre in March 2022.

302. Despite these agreements and partnerships, fraudsters based overseas are still able to reach UK shores. In 2021, the NCA estimates that approximately 30% of fraud is committed by offenders who are predominantly based overseas.[445]

Figure 19: The share of fraud in the UK by offender location



Source: Written evidence from the NECC (FDF0044)

303. RUSI told us that more needs to be done to disrupt the channels used by overseas fraudsters to reach UK victims. This is challenging due to a lack of intelligence in relation to who the fraudsters are and the scale of the international threat from fraud.[446] We were surprised by how little intelligence appears to exist about who fraudsters are and where they operate from. While noting efforts by the NCA and Foreign Office, the Security Minister told us that "the reality is that most of this is very difficult to be certain of".[447] Improving this intelligence should be a priority for law enforcement and this should be done in collaboration with the private sector. Tom Tugendhat told us:

> "A lot of the best analysis is done, or rather could be done, by the private sector. After all, it is Meta that knows who paid for the advert that went on to Instagram, and it is Meta that knows where the person who constantly comments under my Instagram stories offering to do financial exchanges at extraordinarily bizarre rates is raising those comments from."[448]

444 Written evidence from RUSI (FDF0036)
445 Written evidence from the NECC (FDF0044)
446 Written evidence from RUSI (FDF0036)
447 Q 263 (Tom Tugendhat MP)
448 Q 263 (Tom Tugendhat MP)

304. Damian Collins told us that the provisions in the Online Safety Bill will go some way to improving this situation by ensuring that tech platforms use their AI capabilities better to train models to prevent fraud. He said:

> "The systems-based approach in the Online Safety Bill means that the regulator can say, 'Come on, there are some learned characteristics of these fraud ads that we know are happening now. You should be using your AI to identify all those things in real time and get rid of them'. That is the kind of change in approach that we will see, I think."[449]

305. Others made the case for more cooperation between international law enforcement partners. The Social Market Foundation argued for a strengthened international law enforcement network and for the pursuit of an international framework for cooperation that goes further than current international conventions in place.[450] The Fraud Advisory Panel summarised the challenge as follows:

> " … our police forces are constrained by national police boundaries. Fraudsters are not. This makes the effective policing of fraud difficult (if not impossible). The inadequacy of existing resources (both people and money) compounds this."[451]

Financial resources

306. A lack of financial resources was noted as a barrier to an effective law enforcement response. Spotlight on Corruption estimates that the UK spends the equivalent of 0.042% of GDP on resourcing core national economic crime enforcement bodies, despite that fraud is estimated by the group to cost the UK 14.5% of GDP.[452] Speaking to the Treasury Committee, the former director of the NECC, Graeme Biggar, told MPs that they requested an additional £80 million to fund law enforcement activity; they received just £42 million in the 2021 Spending Review.[453] Reflecting on this, Andy Cooke told us "you could probably times the £80 million by five and you would start to make a small dent in relation to the scale of the problem".[454]

307. The disparity in resourcing for UK agencies is made starker when it is compared with overseas agencies. For example, the FBI in the United States has a budget 15 times higher than that of the UK's NCA.[455]

308. This lack of resources presents challenges for staffing across law enforcement. The Social Market Foundation told us that across the 43 local constabularies of England and Wales in 2021, just 1,753 staff (0.8%) are focussed on economic crime, equivalent to 2.1 officers and other staff per every 1000 fraud offences.[456] The Police Uplift Programme intends to recruit an additional 20,000 officers by March 2023 and appears to be on track to meet

---

449 Q 263 (Damian Collins MP)
450 Written evidence from Social Market Foundation (FDF0026)
451 Written evidence from Fraud Advisory Panel (FDF0048)
452 Written evidence from Spotlight on Corruption (FDF0053)
453 Oral evidence taken before the Treasury Committee on 25 January 2021 (Session 2019–21), QQ 43–46 (Graeme Biggar) and HM Treasury, *Autumn Budget and Spending Review 2021: A Stronger Economy for the British People* (October 2021): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1043689/Budget_AB2021_Web_Accessible.pdf [accessed 1 November 2022]
454 Q 227 (Andy Cooke)
455 Written evidence from Spotlight on Corruption (FDF0053)
456 Written evidence from Social Market Foundation (FDF0026)

this target according to the National Audit Office.[457] However, Spotlight on Corruption told us that just 5.9% of these new resources will be dedicated for economic crime.[458] The Social Market Foundation suggests that 30,000 additional officers should be focussed on economic crime to redress this imbalance at a cost of £3.5 billion per year.[459]

309. This presents a huge cost to the taxpayer. In light of this, a number of proposals have been put forward to redress the imbalance in funding for law enforcement agencies. Spotlight on Corruption has suggested the creation of an economic crime fighting fund that would see funds raised by agencies reinvested on top of their core budgets. It found that between 2016 and 2021, law enforcement bodies fighting economic crime raised £3.9 billion via fines, confiscation, forfeiture and civil recovery orders.[460] The SFO, for example, generated £1.6 billion through deferred prosecution agreements, on top of that collected in fines and penalties. These funds are returned to the Treasury, rather than being recycled into law enforcement activity.[461]

310. We recognise concerns that this approach risks encouraging agencies to focus on the most potentially financially advantageous, high-value cases to the detriment of individuals who may have lost a relatively small amount of money.[462] This approach would not reflect concerns about the harm caused by fraud irrespective of actual financial loss and may result in the de-prioritisation of high-volume but low-value individual cases. For example, two thirds of fraud incidents (64%) resulted in a financial loss in the year ending March 2022. The majority of victims that suffered a loss lost less than £250 (77%), whereas a smaller proportion (9%) lost £1,000 or more.[463] While resources to fight fraud are desperately needed, this approach may therefore not be the most appropriate solution.

311. The Government has said it has committed £400 million through a combination of the Spending Review settlement and Economic Crime Levy to support law enforcement over the next three year period.[464] The Economic Crime Levy is intended to bring in £100 million of this, per year from 2023/24. However, it cannot be spent on fraud and will only be used to fight money laundering. We recognise that within the Government's response to its consultation on the levy, it did not receive support for the inclusion of fraud. The Government noted that responsibility for fraud sits across society

457 National Audit Office, 'The Police Uplift Programme' (25 March 2022): https://www.nao.org.uk/press-release/the-police-uplift-programme/ [accessed 1 November 2022]
458 Written evidence from Spotlight on Corruption (FDF0053)
459 Written evidence from Social Market Foundation (FDF0026)
460 Spotlight on Corruption, Closing the UK's economic crime enforcement gap: Proposals for boosting resources for UK law enforcement to fight economic crime (January 2022): https://drive.google.com/file/d/1wTR2zvs1sfq3BqidmAiBTdc6qj-Umyf4/view [accessed 1 November 2022]
461 'UK 'overstretched' and 'outgunned' in economic crime fight, says report', *Financial Times* (24 January 2022): https://www.ft.com/content/aa43fe76-4f1d-49d1-be62-f78d17e982f2 [accessed 1 November 2022]
462 See Wilmer Hale, 'The UK's economic crime enforcement gap: the merits of a new funding proposal' (23 February 2022): https://www.wilmerhale.com/en/insights/blogs/WilmerHale-W-I-R-E-UK/20220223-the-uks-economic-crime-enforcement-gap-the-merits-of-a-new-funding-proposal#page=1 [accessed 1 November 2022].
463 ONS, 'Nature of fraud and computer misuse in England and Wales: year ending March 2022' (26 September 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022 [accessed 1 November 2022]
464 Commons written statement, UIN HCWS300, Session 2022–23

and other sectors.[465] The Security Minister argued that the private sector has a valuable tole to play in resourcing:

> "The amount of resource that the private sector puts in here will dwarf what the Government do, and rightly so. That is going to make the biggest difference."[466]

312. Elsewhere, RUSI has argued in a recent paper that consideration should be given to reinvesting the proceeds of asset recovery action, regulatory fines or deferred prosecution agreements (DPAs) into the law enforcement system.[467] In addition, the Government should consider reinvesting fines levelled as a result of action taken under the forthcoming Online Safety Bill to support law enforcement activity.

313. Furthermore, while an injection of resources would be welcome, we have taken evidence that it must be sustained in order to avoid 'cliff-edge' funding patterns that do not allow for long-term planning. Andy Cooke told us that short-term funding for specialist units such as Action Fraud and ROCUs, based on a 12 month cycle, is a barrier to investment in better technology.[468] The Government's latest Spending Review committed to a three-year settlement for police forces in contrast to the previous model of annual grants.[469] Considering the forthcoming publication of the fraud strategy Pauline Smith, Director of Action Fraud, told us that funding should reflect this extended period of time:

> "Action Fraud has three years funding for our economic crime victim care unit, and we want to deliver a national standard for victims of this sort of crime … I would certainly like to see the funding for our unit to reflect the 10-year fraud strategy rather than three years and what is going to happen after three years."[470]

Skills deficit

314. This lack of resources also impacts skills within law enforcement and the retention of civilian staff and police officers. The Committee has heard that law enforcement struggles to attract and retain staff, particularly those with advanced digital and cyber skills. This is primarily due to salary competition with the private sector and results in 'brain drain' out of the sector.[471] A 2021 report of the NCA's Remuneration Review Body found that it struggled to fill 'hard-to-fill' posts and faced a turnover of more than a quarter (28%) in its cyber capacity every year. Many of these skilled individuals turned to the banking sector, where they would be able to receive substantial salaries.[472]

---

465 HM Treasury, Economic Crime (Anti-Money Laundering) Levy: Response to the Consultation (September 2021): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1019454/HMT_ECL_Consultation_Response_final__21.09.21_.pdf [accessed 1 November 2022]

466 Q 256 (Tom Tugendhat MP)

467 RUSI, 'Five problems with economic crime policing: and how to solve them' (11 July 2022): https://rusi.org/explore-our-research/publications/commentary/five-problems-economic-crime-policing-and-how-solve-them [accessed 1 November 2022]

468 Q 224 (Andy Cooke)

469 Commons written statement, UIN HCWS503, Session 2021–22

470 Q 118 (Pauline Smith), Q 230 (Andy Cooke) and Q 221 (Pete O'Doherty)

471 Written evidence from Spotlight on Corruption (FDF0053)

472 NCA Remuneration Review Body, Seventh Report 2021, CP 467 (July 2021): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004935/NCARRB_2021_report_-_web_accessible.pdf [accessed 1 November 2022] and written evidence from Spotlight on Corruption (FDF0053)

315. A lack of resourcing for law enforcement agencies is clearly damaging its capacity to attract and retain frontline police and specialist staff. RUSI told us that there must be targeted approach to investing any additional resources. They said:

> "It is clear that many law enforcement and other Government organisations are under resourced compared to the volume of fraud. Increased funding is vital, but this should not simply be a 'more of the same' approach, but part of a clear strategy for funding the right skills, in the right places, under a new set of clearly defined roles and responsibilities of different agencies involved with targets and measurable outputs."[473]

316. Mark Shelford told us that law enforcement agencies are turning to other agencies to support them and even working with military reserves in some specialist areas due to the inability to attract staff. Some law enforcement agencies have chosen to partner with private sector companies to enable them to share expertise and capabilities that may help to prevent and tackle fraud. The City of London Police works with Microsoft's industry experts, who sit in their intelligence department to analyse computer service software frauds. It then explores how its own platform could be updated to prevent that crime in future.[474]

317. Furthermore, we believe the resources of the private sector can be utilised to better effect given the skills readily available to private businesses and the inability of law enforcement to carry out all the required activities in house due to what Mark Shelford called a 'failure to recruit'.[475] A positive example of such activity is the Card and Dedicated Cheque and Plastic Crime Unit (CDCPCU), which is partnered with and funded by UK Finance. To take this further, law enforcement should be given the appropriate resources to contract those with specialised skills and resources to complement its own efforts, for example in data analytics. DCI Stevie Trim told us that "it is incredibly expensive to go to some of the big financial private companies to assist with complex financial and highly specialised investigations".[476]

318. In addition to outsourcing, there is clearly a need for greater capability development within law enforcement. Rob Jones told us:

> "As for being able to access industry, yes, I absolutely agree, but there needs to be a balance, because what this whole threat area—dealing with all online threats—has suffered from is not investing, digging in and creating digital skills in law enforcement. That needs addressing, which means that we need to focus on growing our own talent as well as accessing other areas for support."[477]

319. The Justice Committee recently recommended a review of the training offered to front-line staff to reflect better changes in the fraud landscape. We have identified this training as insufficient, and would go further in encouraging proactive upskilling now.[478] For example, a recent report by Policy Exchange suggested the development of a new corps of skilled data

473 Written evidence from RUSI (FDF0036)
474 Q 214 (Pete O'Doherty)
475 Q 214 (Mark Shelford)
476 Q 195 (DCI Stevie Trim)
477 Q 214 (Rob Jones)
478 Justice Committee, *Fraud and the Justice System* (Fourth Report, Session 2022–23, HC 12)

scientists, programmers and hackers to be recruited into policing to meet some of the shortfall, in addition to the uniformed officers being recruited under the Government's existing Police Uplift Programme.[479]

Box 12: Recruiting graduates with cyber and digital skills

Teach First is a well-known charity that operates a training programme for teachers. Participants achieve Qualified Teacher Status via a two-year training programme. Those on the programme are placed at schools made up of disadvantaged students across the country, where participants must stay for two years. It the ninth top graduate recruiter according to The Times Top 100 Graduate Employers 2021.

Similarly, Police Now offers graduates two years conducting front-line policing as neighbourhood police officers. Police Now is ranked as a top 30 graduate recruiter (28). However, in light of a lack of skills in digital and cyber, we have heard that more could be done to recruit and train graduates with these specific skills.

Pete O'Doherty told the Committee that it would be unrealistic for law enforcement to match industry salaries, particularly in cyber or digital roles. However, in conversation with the NECC's Rob Jones, he suggested that law enforcement agencies could benefit from a more targeted approach to encourage socially-minded young graduates with skills in digital and cyber to take up the opportunity for training within law enforcement before moving on to an industry role:

> "Say we know that this really great graduate in cybersecurity is looking for a job in industry in five years. If they get the job in industry, we could provide the training in law enforcement. They give two- or three-years' return service and then they begin their role in industry. That is great for industry, because they are fully trained, they have police and threat experience, and they have work and life experience. Equally, we get five years from that person."

Source: The Times, 'Top 100 Graduate Employers 2021' (2021): https://www.top100graduateemployers.com/employers [accessed 1 November 2022] and Q 214 (Pete O'Doherty)

320. Taken together, the under-resourcing of law enforcement, the siloed approach to policing, and the lack of prioritisation of fraud by law enforcement has actively encouraged career criminals to turn to fraud. The Fraud Advisory Panel told us:

> "The reluctance of the successive governments to invest adequately in counter fraud activity means that the risk of detection, investigation, and prosecution is so low that fraud has become an attractive and lucrative career choice for many criminals."[480]

321. **Fraud is the most commonly experienced crime in England and Wales today and represents a substantial national threat. If this were any other type of crime, this would be a matter of national importance. The woeful under-prioritisation from the NCA to local police forces**

479 Policy Exchange, ''What do we want from the next Prime Minister?' A series of policy proposals for new leadership: Crime & Policing: A force fit for the future' (30 August 2022): https://policyexchange.org.uk/wp-content/uploads/2022/09/Crime-Policing-What-do-we-want-from-the-next-Prime-Minister.pdf [accessed 1 November 2022]

480 Written evidence from the Fraud Advisory Panel (FDF0048)

is in part due to public misconceptions about the impact of fraud on victims—it doesn't "bang, bleed or shout"—and competing pressures on already-stretched law enforcement resources, compounded by a fundamental lack of capacity and skills amongst law enforcement staff. More funding is clearly needed, however we recognise the difficulty of securing this from the public purse.

322. **Furthermore, the structure of the model for policing in England and Wales is complex and results in siloed thinking that does not effectively serve victims of fraud. However, a wholesale reconfiguration of this approach would not be in the best interests of victims. Therefore, we suggest an approach of evolution rather than revolution.**

323. ***To address the siloed approach to policing in England and Wales, we recommend an expanded and empowered central command unit to coordinate and steer efforts to tackle fraud with a focus on improving intelligence. Local police forces should retain their responsibility to support victims and tackle 'analogue' fraud.***

324. ***To support recruitment and upskilling efforts, the Government should develop a national policing workforce strategy. It must work with law enforcement and the private sector to support the secondment of specialist private sector civilian staff to complement and bolster law enforcement's skills pool through contracting specialist private sector services. It should explore the establishment of a Teach First-style model for recruiting law enforcement officers with specialisms in cyber and digital investigation. Further, we endorse the recommendations made by Policy Exchange to develop greater cyber capabilities specifically focussing on online crime within the police force.***

325. ***To support the forthcoming fraud strategy with adequate resources, the Government must commit to a long-term funding strategy with an increased offer for law enforcement agencies, focussed primarily on recycling revenue collected by law enforcement agencies back into law enforcement activity.***

326. ***The Government should broaden the scope of the Economic Crime Levy to cover fraud and it must widen the remit for companies in scope in order to share the load with those in the tech and telecoms sectors.***

327. ***To tackle under-prioritisation, we agree with the Justice Committee that fraud should be written into the Strategic Policing Requirement.***

The Crown Prosecution Service

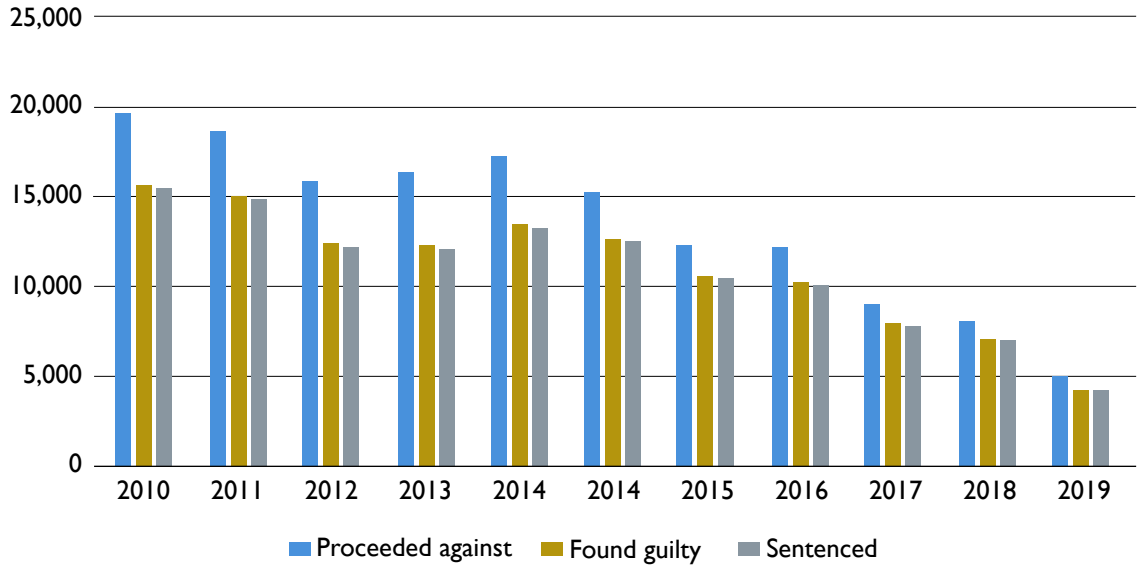
328. The CPS is the principal public agency for conducting criminal prosecutions in England and Wales. It is independent of the police and Government.[481] In recognition of the growth of fraud, the CPS recently merged its specialist fraud, organised crime and international headquarter divisions into one new directorate called the Serious Economic, Organised Crime and International Directorate (SEOCID).[482]

481 CPS, 'About CPS': https://www.cps.gov.uk/about-cps [accessed 1 November 2022]
482 Written evidence from the CPS (FDF0004)

329. In the year 2020/21, there were 59,838 recorded outcomes for fraud cases referred for investigation, but just 11.5% (nearly 6,900) of these were judicial. This is less than 1% of the 875,622 reports received by Action Fraud during that period.[483]

330. The total value of alleged fraud reaching UK Crown Courts in the first half of 2022 was £532.6 million. This was an increase of up 288% from £137.4 million in the same time period in 2021. However, the volume of cases that reached the courts fell 13% from 149 to just 129.[484] Criminal prosecutions for fraud have declined significantly since 2010. The graph in Figure 20 shows the decline in prosecutions, convictions and subsequent sentencing in fraud cases in England and Wales since 2010.[485]

Figure 20: Decline in criminal prosecutions of fraud since 2010



Source: MoJ figures available at Commons written answer, UIN 120774 Session 2021–22

331. Whilst the Committee recognises the efficacy of the Fraud Act as a piece of legislation to prosecute fraud (see paragraph 426), we have identified several barriers hindering the prosecutorial process.

Court capacity

332. The CPS told us that it faced limits to investigative and court capacity. In part, this is due to the effects of COVID-19. The CPS' caseload of the most complex frauds in the Crown Court has increased by 56% since March 2020.[486]

333. The City of London Police is in the process of establishing the City of London Law Courts with 18 dedicated court rooms. This may help to lighten the load, however the CPS cautions that it will not resolve capacity

483 Action Fraud, Fraud crime trends 2020/21: https://data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/2020–21-Annual-Assessment-Fraud-Crime-Trends.pdf [accessed 1 November 2022]

484 KPMG, 'Rampant fraud shows no sign of slowing, putting sustained pressure on UK Courts' (31 August 2022): https://home.kpmg/uk/en/home/media/press-releases/2022/08/rampant-fraud-shows-no-sign-of-slowing-putting-sustained-pressure-on-uk-courts.html [accessed 1 November 2022]

485 Available at Commons written answer, UIN 120774 Session 2021–22.

486 Written evidence from the CPS (FDF0004)

issues in the system.[487] The Justice Committee recently argued that the Government should pilot the establishment of more economic crime courts and, if successful, should roll these out around the country.[488]

334. We heard other arguments in favour of such an approach. Arun Chauhan told us that the complexity of offences means that it is difficult for prosecutors to make the case to a jury and supported consideration of specialist courts.[489]

335. The APPGs on Fair Business Banking and Anti-Corruption and Responsible Tax, have argued that more specialist judges could enhance nationwide expertise.[490] Southwark Crown Court was raised in evidence as one such court that has benefitted from the utilisation of such specialist judges. Dr Susan Hawley, Executive Director of Spotlight on Corruption, supports the need for more economic crime judges, noting that the Court "has almost played the role more of an economic crime court, with some judges who hear economic cases again and again".[491]

336. While we recognise these arguments, we suggest that issues within the courts are less to do with a lack of expertise or jury understanding due to the complexity of cases, and more to do with a lack of resources. Mark Fenhalls KC told us that "there is no comprehension issue" but rather issues within the criminal justice system were related to "a resource issue of space and time".[492]

Resources

337. It is clear that constraints on the CPS' capacity to prosecute fraudsters are due to a lack of resources. The Bar Council wrote that "the fundamental problem with the investigation and prosecution of fraud offences is the lack of adequate funding in the criminal justice system as a whole".[493]

338. The Spending Review 2021 provided an £80 million cash increase in resource funding for the CPS by 2024–5.[494] However, figures show that the CPS has faced real-terms budget cuts of 33% between 2010 and 2019.[495] Campaign group Spotlight on Corruption argue that the Government would have had to increase CPS funding by a further £184.8 million in order to restore funding to 2010 levels.[496]

---

487 Written evidence from the City of London Police (FDF0031) and the CPS (FDF0004)
488 Justice Committee, *Fraud and the Justice System* (Fourth Report, Session 2022–23 HC 12)
489 Q 16 (Arun Chauhan)
490 APPG on Fair Business Banking and APPG on Anti-Corruption & Responsible Tax, Economic Crime Manifesto (May 2022): https://static1.squarespace.com/static/5e4a7793b0171c0e2321f308/t/627d25b7db612b1ed95559de/1652368831698/Economic+Crime+Manifesto+-+Final-compressed.pdf [accessed 1 November 2022]
491 Q 88 (Dr Susan Hawley) see also Q 208 (Mark Fenhalls KC).
492 Q 208 (Mark Fenhalls KC)
493 Written evidence from The Bar Council (FDF0054)
494 HM Treasury, *Autumn Budget and Spending Review 2021: A Stronger Economy for the British People* (October 2021): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1043689/Budget_AB2021_Web_Accessible.pdf [accessed 1 November 2022]
495 Channel 4 News, 'FactCheck: extra funding for CPS comes after long-term cuts' (23 June 2021): https://www.channel4.com/news/factcheck/factcheck-extra-funding-for-cps-comes-after-long-term-cuts [accessed 1 November 2022]
496 Spotlight on Corruption, *Closing the UK's economic crime enforcement gap: proposals for boosting resources for UK law enforcement to fight economic crime* (January 2022): https://drive.google.com/file/d/1UzymaDZZSVF8By1WYGtahRN-gvBI2R-_/view [accessed 1 November 2022]

339. This is not an isolated problem. We also recognise a lack of resourcing for other prosecuting agencies such as the SFO. Sir David Calvert-Smith KC recently told the Justice Committee that there was an "endemic lack of resources" with which to prosecute large cases.[497]

The disclosure regime

340. Disclosure is the process of providing the defence with copies or access to material in their possession that might reasonably be considered capable of undermining the prosecution case and/or assist the defence.[498] Disclosure obligations are set out under the Criminal Procedure and Investigations Act (CPIA) 1996.

341. Rapid developments in technology since 1996 have caused a shift in the volume of information that is required to be produced as part of disclosure obligations. The Code of Practice under Section 23(1) of the CPIA identifies a general duty to "pursue all reasonable lines of inquiry".[499] This duty has resulted in a need to generate huge volumes of data.[500] The City of London Police told us that disclosure "typically adds six months to a medium-size investigation".[501] Decisions about disclosure are taken on a case-by-case basis and are subject to interpretation, with any disclosure schedules completed and signed prior to charging.[502] Mark Fenhalls KC told us that the CPIA was essentially created to solve a "pre-digital" problem.[503] He said:

> "When I began and phones were first downloaded, the average phone download was 70 pages of just text messages and a list of calls. Now your average phone download is between 10,000 and 30,000 pages. That is because people live their lives on their phones. So there is plenty of grief around doing it, but there is no human way to search any of this stuff. The truth is that we have to work through an awful lot more thought about how issues are narrowed, how phones and computers are searched, in order to give people a chance to have a fair process."[504]

342. In September 2022, Director of the Serious Fraud Office Lisa Osofsky also called for reforms to the disclosure regime due to the volume of data that investigators and prosecutors have to deal with.[505] The City of London Police argued that more guidance was needed to aid legal counsel on decision-making on what is reasonable and necessary for the disclosure process. It argued that this should take place earlier in the prosecutorial process to enhance the prospect of a successful prosecution.[506]

---

497 Oral evidence taken before the Justice Committee on 19 October 2022 (Session 2022–23), Q 2 (Sir David Calvert-Smith KC)

498 CPS, 'Disclosure': https://www.cps.gov.uk/about-cps/disclosure [accessed 1 November 2022]

499 Ministry of Justice, *Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice* (March 2015): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/447967/code-of-practice-approved.pdf [accessed 1 November 2022]

500 See NECC response to Ministry of Justice, *Post-legislative assessment of the Fraud Act 2006: Memorandum to the House of Lords Select Committee on the Fraud Act 2006 and Digital Fraud*, CP 680 (June 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1081360/fraud-memo-2022.pdf [accessed 1 November 2022]

501 Written evidence from City of London Police (FDF0031)

502 *Ibid.*

503 Q 204 (Mark Fenhalls KC)

504 *Ibid.*

505 'Osofsky calls for reform of disclosure rules', *Law Society Gazette* (6 September 2022): https://www.lawgazette.co.uk/news/osofsky-calls-for-reform-of-disclosure-rules/5113590.article [accessed 1 November 2022]

506 Written evidence from City of London Police (FDF0031)

343. The problem of volume is compounded by the complexity of analysing and storing digital data. Karl Laird, a Senior Lecturer and Tutor in Law at the University of Oxford, told us that "technology … is part of the problem, but it also can be part of the solution", noting the use of artificial intelligence (AI) to sift through data.[507] While the Attorney General's Office has cautioned against reliance on technology as a "panacea" to solve the problem, the Ministry of Justice has welcomed greater use of technology to support the storage and review of digital evidence and its presentation in court. [508] The FCA implied that the Government's policy remained unclear, and called for a clear endorsement of the use of AI and technology to review of material and thereby shorten the investigation length.[509]

344. There is a more general need to raise awareness and standards of training within law enforcement agencies as to the requirements and importance of the disclosure regime.[510] In a recent review of disclosure, the Attorney General's Office found that "investigative officers can lack the basic skills to effectively comply with their statutory disclosure obligations". More widely, the Attorney General's Office found a "deeply held culture which views disclosure as merely bureaucratic or tick-box exercise".[511] We agree with the Justice Committee that the AGO should look again at its disclosure guidelines to address some of these issues, however we suggest that a review of the entire disclosure process is required to address the range of issues we have heard.[512]

GDPR

345. We have also heard that GDPR presents a significant hurdle to law enforcement. GDPR requirements increase the burden surrounding disclosure due to the need for personal information to be redacted before providing police files to the CPS for a charging decision. Mark Fenhalls KC told us that data protection concerns presented a "spectacular burden".[513] He welcomed the idea of a working group between both the CPS and ICO to provide a forum for discussion on the implementation of GDPR within a criminal justice context and asked for greater flexibility and understanding between the Home Office and the ICO about the rigorous application of

507 Q 204 (Karl Laird)

508 Attorney General's Office, *Annual review of disclosure* (26 May 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1078195/Annual_Disclosure_Review_Publication_Copy.pdf [accessed 1 November 2022] and Ministry of Justice, *Post-legislative assessment of the Fraud Act 2006: Memorandum to the House of Lords Select Committee on the Fraud Act 2006 and Digital Fraud,* CP 680 (June 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1081360/fraud-memo-2022.pdf [accessed 1 November 2022]

509 Written evidence from the FCA (FDF0069)

510 See comments by City of London Police's National Lead Force Fraud Investigation Team in Ministry of Justice, *Post-legislative assessment of the Fraud Act 2006: Memorandum to the House of Lords Select Committee on the Fraud Act 2006 and Digital Fraud,* CP 680 (June 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1081360/fraud-memo-2022.pdf [accessed 1 November 2022]

511 Attorney General's Office, Annual review of disclosure (26 May 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1078195/Annual_Disclosure_Review_Publication_Copy.pdf [accessed 1 November 2022]

512 Justice Committee, *Fraud and the Justice System* (Fourth Report, Session 2022–23, HC 12)

513 Q 199 (Mark Fenhalls KC)

GDPR in the criminal justice process.[514] However, Max Hill KC, Director of Public Prosecutions, cautioned against taking this approach:

> "A GDPR-free corridor strikes me as very difficult. It would be a wholesale opt-out from the law that applied to us all."[515]

346. In addition, courts already have GDPR exemptions in the case of materials being prepared for courts like witness statements and exhibits. These materials do not need to be redacted due to exemptions for the court processing documents in their judicial capacity. Article 9(2)(f) of the GDPR allows for special categories of data to be processed for the defence of a claim or when a court is acting in its legal capacity.[516] This does not mean that the CPS cannot be held liable if it commits a GDPR breach under different circumstances—indeed it has been fined by the ICO in the past for such breaches—and we would argue that these measures should remain in place.[517]

347. The Government has paused its Data Protection and Digital Information Bill, which was introduced to design a "more flexible, outcomes-focused approach to data protection that helps create a culture of data protection, rather than 'tick box' exercises".[518] It remains to be seen how the legislation may impact law enforcement and the criminal justice system.

348. **Various issues including resourcing and the disclosure regime hinder how effectively the Crown Prosecution Service can bring fraudsters to justice under the Fraud Act 2006. Over time, these developments have resulted in a declining rate of prosecutions for fraud, in stark contrast to the rising number of cases.**

349. ***The Government should work with the CPS on specialist training for personnel within the criminal justice system, including police officers, prosecutors and judges to expedite cases of complex fraud.***

350. ***As part of the Government's reconsideration of the UK Data Protection and Digital Information Bill, the Government should:***

    (a) ***Endeavour to establish a formal working group between the CPS and the ICO on the issue of GDPR (or its replacement) and its use in criminal prosecutions, and to publish guidance and protocols on redaction for police and prosecutors, subject to regular review.***

    (b) ***Require the ICO to work with the College of Policing to support police staff with resources and training to improve their understanding of data protection legislation and use their enforcement powers where needed to support this.***

---

514 QQ 200–201 (Mark Fenhalls KC)

515 Q 246 (Max Hill KC)

516 European Union, 'General Data Protection Regulations, Article 9(2)(f)': https://gdpr.eu/article-9-processing-special-categories-of-personal-data-prohibited/ [accessed 1 November 2022]

517 'CPS breached Data Protection Act for 12 years, ICO reveals' *Law Society Gazette* (4 November 2015): https://www.lawgazette.co.uk/news/cps-breached-data-protection-act-for-12-years-ico-reveals/5051988.article#commentsJump [accessed 1 November 2022]

518 HM Government, *The Queen's Speech 2022* (10 May 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1074113/Lobby_Pack_10_May_2022.pdf [accessed 1 November 2022]

351. ***We agree with the Justice Committee that the AGO should review the disclosure guidelines and consider new guidelines on disclosure in digital fraud cases. More widely, the Government should review the CPIA and in particular how the disclosure regime impacts the efficacy and speed with which fraudsters can be prosecuted.***

352. ***The Government should endorse the use of AI and technology-assisted review of material gathered in criminal investigations to shorten the length of investigations, with a mechanism for judicial approval of use pre-charge in individual cases.***

Civil proceedings

353. Civil proceedings are typically brought by victims to seek recovery of assets stolen from them or to receive compensation. These cases are decided by a judge rather than a jury.[519] Civil action does not result in custodial sentences, but it may result in a range of outcomes including recovery of assets and/or damages. A judge can make an interim order to freeze a defendant's assets so that they cannot move their assets during the case.

354. While civil and criminal proceedings can take place simultaneously or one after the other, the Committee has heard evidence that there is a case for increased use of civil remedies to tackle rising cases of fraud. The Social Market Foundation told the Committee that the civil route is currently under-utilised and could be used more widely to compliment provisions in criminal law.[520]

355. Civil Recovery Orders enable enforcement to recover property obtained through unlawful conduct under the Proceeds of Crime Act 2002. Civil Recovery orders recouped a total value of £12.7 million for the financial year 2020/21.[521] While a 42% increase from 2019/20, the Building Societies Association noted that this is still low compared to losses of nearly £500 million for the same period.[522] Furthermore, Max Hill KC told us that civil recovery should not be seen as an alternative to prosecution but as one of a number of tools.[523]

356. Injunctions, court orders requiring a company or person to stop doing (prohibitory injunction) or to do (mandatory injunction) something, were raised in evidence.[524] Melissa Hodgman noted that injunctions that limit what fraudsters can do can constitute a deterrent in pursuit of behaviour change and preventative action:

> "One way that we think we can be very effective in keeping people out of the US markets is deterrence, by sending a message to people: 'If you

519 Kingsley Napey, 'Fraud: Civil vs. Criminal FAQs': https://www.kingsleynapley.co.uk/services/department/dispute-resolution/civil-fraud-and-investigations/fraud-civil-vs-criminal-faqs [accessed 1 November 2022]

520 Written evidence from the Social Market Foundation (FDF0026)

521 Home Office, 'Asset recovery statistical bulletin: financial years ending 2016 to 2021' (9 September 2021): https://www.gov.uk/government/statistics/asset-recovery-statistical-bulletin-financial-years-ending-2016-to-2021/asset-recovery-statistical-bulletin-financial-years-ending-2016-to-2021 [accessed 1 November 2022]

522 Written evidence from Building Societies Association (FDF0023)

523 Letter of 18 July 2022 to the Committee from the CPS: https://committees.parliament.uk/publications/23168/documents/169435/default/

524 Ashfords, 'Guide to injunctions' (5 March 2018): https://www.ashfords.co.uk/news-and-media/general/guide-to-injunctions [accessed 1 November 2022] and written evidence from the Social Market Foundation (FDF0026)

engage in this behaviour and you are caught, this is what is going to happen'."[525]

Box 13: A hybrid approach to criminal and civil prosecution

In the USA, enforcement agencies take a 'hybrid approach' to law enforcement involving both a regulatory and criminal law response to financial crime.[526]

Speaking to the Committee, Melissa Hodgman told us that the regulator works "in parallel" with the criminal authorities and is seeking to work increasingly closely with them.[527] In particular, Hodgman noted the role of access requests, a process by which other agencies can be granted access to SEC files.[528] The SEC coordinates with its criminal law enforcement counterparts by working with US Attorneys' Offices around the country.[529]

For example, Russian businessman Denis Georgiyevich Sotnikov was involved in a fraudulent scheme to lure investors into buying fictitious Certificates of Deposit (CDs) with high rates. Sotnikov did this through internet advertising and the creation of fraudulent spoof websites that resembled reputable financial institutions. Since their establishment in 2014, the scheme led to over $26 million in investor losses, many of which resulted from older investors who had used their retirement savings.

The SEC charged Sotnikov with violating antifraud provisions of the federal securities laws and aiding and abetting. It sought a permanent injunction and the return of the ill-gotten gains with interest and penalties. At the same time, the US Attorney's Office for the District of New Jersey charged Sotnikov with wire fraud in pursuit of criminal charges and asset seizures.[530]

357. **There is scope to increase the use of civil remedies to take action against fraudsters and achieve justice for victims.**

358. ***The Government should launch a review into the use of civil remedies to tackle fraud, including an examination of obstacles, for example, fees to commence civil proceedings, to the use of civil remedies such as asset recovery and injunctions.***

Responding to victims of fraud

The impact of fraud

359. The impact of fraud on victims has long been underestimated. In addition to financial loss, victims of fraud may experience significant emotional distress. In the financial year 2020/21, Action Fraud identified 28 risk-to-life incidents and 234 individuals at risk of suicide or self-harm.[531] The City of London Police told us that in October 2020, an individual who suffered from mental

525 Q 181 (Melissa Hodgman)
526 Nicholas Ryder. 'Too Scared to Prosecute and Too Scared to Jail?' A Critical and Comparative Analysis of Enforcement of Financial Crime Legislation Against Corporations in the USA and the UK', *Journal of Criminal Law, vol 82(3)* (1 June 2018): https://journals.sagepub.com/doi/abs/10.1177/0022018318773209?journalCode=clja [accessed 1 November 2022]
527 Q 182 (Melissa Hodgman)
528 *Ibid.*
529 SEC, *Division of Enforcement: 2020 Annual Report*: https://www.sec.gov/files/enforcement-annual-report-2020.pdf [accessed 1 November 2022]
530 *Ibid.* See also SEC, 'SEC Charges Russian National for Defrauding Older Investors of Over $26 Million in Phony Certificates of Deposit Scam' (13 March 2020): https://www.sec.gov/news/press-release/2020–61 [accessed 1 November 2022]
531 Written evidence from City of London Police (FDF0031)

health issues committed suicide after communication with criminals who used a spoofed number to convince them that they owed HMRC £18,000. The individual referenced the scam in their suicide note.[532]

> *"At my lowest, I experienced a mental breakdown and have even considered suicide." - Rachel*

360. The impact of this emotional distress has been given as a reason for increasing the maximum sentence under the Fraud Act, which is explored in paragraph 430. The City of London Police told us that fraud is seen as "financial violence", and results in loss of trust and isolation.[533] In addition, the impacts of fraud can result in multiple negative consequences for victims, such as a loss of confidence or trust in institutions. For example, the Good Things Foundation explained that the experience of digital fraud may reduce motivation, trust and confidence in continuing to use the internet.[534]

> *"I feel angry and silly. I will not trust banks in future and will put my money back under the mattress." - Bill*

> *" … I no longer feel safe ordering goods online and I'm fearful of this happening again." - Naomi*

361. Liz Eden, a student support worker at a Russell Group university, told us that young students face feelings of shame following a scam:

> "We hear students expressing deep feelings of guilt and shame when they realise that they have been defrauded. They are angry at themselves for having trusted someone they shouldn't, and they are also afraid other people will be angry with them for having been so gullible. In some cases, students have turned first to their parents for support. They are then further distressed by their parents' reaction which might be intense anger or disappointment."[535]

362. These feelings of shame may lead to under-reporting. Figures show that only 15% of victims report their experience to the police or Action Fraud.[536] However, in the year ending March 2022, there was a 17% increase in fraud reported to the police compared to the previous year.[537]

363. There are other reasons why victims might not report crime to authorities. Home Office figures from 2016 show that a lack of awareness of Action Fraud is a driver of low reporting rates. 66% of those who said they were a victim of fraud in response to the Crime Survey for England and Wales but did not

532 *Ibid.*
533 Written evidence from City of London Police (FDF0031)
534 Written evidence from the Good Things Foundation (FDF0045)
535 Written evidence from Liz Eden (FDF0089)
536 Victim's Commissioner, 'Fraud surged by 24% under Covid. Now a new study reveals around 700,000 victims a year are likely to be highly vulnerable to fraudulent crime and seriously harmed by it' (13 October 2021): https://victimscommissioner.org.uk/news/who-suffers-fraud/ [accessed 1 November 2022]
537 ONS, 'Nature of fraud and computer misuse in England and Wales: year ending March 2022' (26 September 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022 [accessed 1 November 2022]

report it to Action Fraud said they had never heard of the organisation. 15% said that they thought the fraud would be reported by another authority.[538]

364. It is clear more needs to be done to support reporting. The Security Minister told us:

> "We should be supporting those who have become victims and making sure that they feel able to report. Only if we get the reports in are we able to deal with it—and, of course, in reporting, victims protect others."[539]

365. While we recognise efforts to improve awareness of Action Fraud have increased, stakeholders continue to recognise the inadequacy of the service. Dame Vera Baird told us that pathways to get help remain unclear, and that "most people think they need to report to the police". Dame Vera also said that, faced with reporting to Action Fraud as well as their bank and potentially other institutions involved, victims may suffer from reference 'fatigue':

> "People may hear about all these things, but the pathway is not clear and they can get what is called referral fatigue. You go to the police and they send you to Action Fraud. If you get some contact from Action Fraud, they may send you back to the police unless they are going to deal with the case themselves, by which time you may be a bit worn out with this kind of Alphabetti spaghetti. There are a lot of places to go, which I think makes it very difficult for victims of fraud to know what they are supposed to do to get help."[540]

366. Victims that do report fraud to the authorities typically report it to trained call handlers at Action Fraud. In 2019, the service came under significant criticism due to an investigation by The Times into its response to victims.[541] We recognise that improvements to the service have been made following the subsequent review of the service led by Sir Craig Mackey QPM. These include reduced call waiting times and the introduction of new technologies such as chatbots.[542] Once a report is made, a victim is given the opportunity for their contact details to be passed to Victim Support, a charity offering free emotional support and practical help.[543]

367. The NECC Victim Care Unit was established in 2014 to support vulnerable victims of fraud. The City of London Police told us that the service assesses the needs of around 80,000 victims a year, supporting those victims whose cases do not lead to investigation. It reports that only 24 service users became repeat victims in the year to April 2022 and since January 2021, the unit has helped victims to secure £2.2 million in reimbursement.[544]

368. Despite improvements to the service provided by Action Fraud, the Social Market Foundation told us that "quite simply, Action Fraud is failing to deliver the kind of service required if the public are to have confidence in and

538 Home Office, The scale and nature of fraud: a review of the evidence: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720772/scale-and-nature-of-fraud-review-of-evidence.pdf [accessed 1 November 2022]
539 Q 269 (Tom Tugendhat MP)
540 Q 109 (Dame Vera Baird)
541 The Times, 'Action Fraud investigation: victims misled and mocked as police fail to investigate' (15 August 2019): https://www.thetimes.co.uk/article/action-fraud-investigation-victims-misled-and-mocked-as-police-fail-to-investigate-wlh8c6rs6 [accessed 1 November 2022]
542 Written evidence from City of London Police (FDF0031)
543 House of Commons Library, *Banking Fraud,* Briefing Paper CBP 8545, 23 February 2021
544 Written evidence from City of London Police (FDF0031)

use it."[545] HM Inspector Andy Cooke told us that "there is still a long way to go in relation to victims of fraud". He noted that fraud victims are not given enough information, even about whether their case will be investigated.[546]

369. We received evidence from victims that corroborated these views. Tricia, a member of a Facebook group dedicated to tackling fraud, told us that despite providing evidence to Action Fraud, "mostly, we have been ignored".[547] A lottery scam victim told us that victims are forced to turn to other avenues to seek justice such as the media or social media as they feel they have been ignored by official channels.[548]

> *" … there is nobody who is prepared to stop the fraudsters or help us in any way, shape or form." - Tricia*

370. Action Fraud is due to be replaced with an improved national fraud and cyber-crime reporting system as announced in the Government's Beating Crime Plan.[549] It is understood that this will be in place by 2025.[550] It remains unclear what the new service will be called. Members of the Midlands Fraud Forum told the Committee that at the very least, Action Fraud should be renamed to reflect more accurately its remit as a fraud reporting hotline. It was argued that this may help victims to understand better what they can expect from the service.[551] Tricia told us that Action Fraud should be renamed, removing the word 'Action' as this overstates the role of the reporting service.[552]

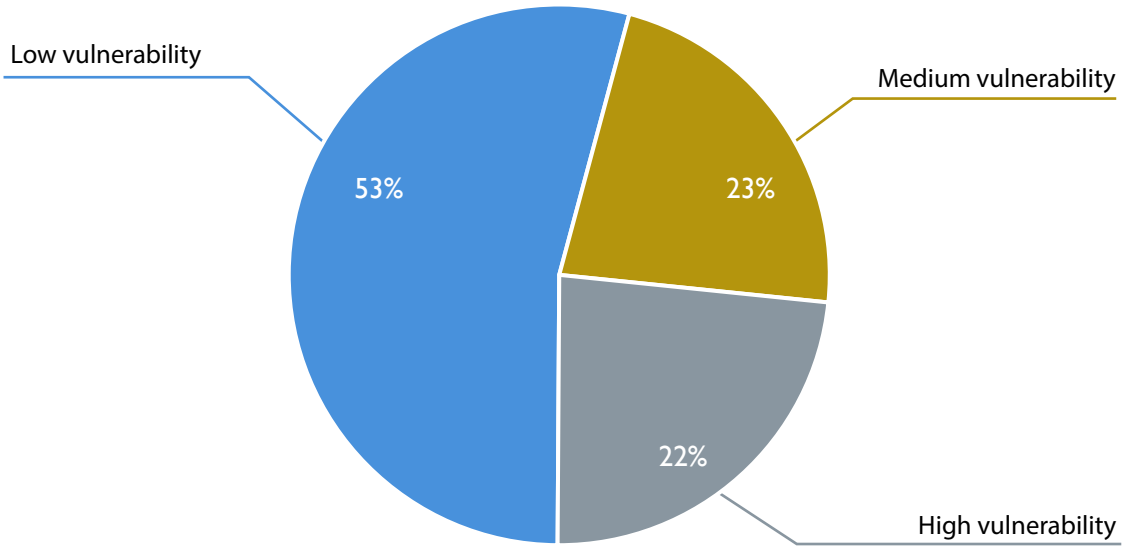
371. The Government published the draft Victims Bill in May 2022. The Victims Bill will place the principles of the Victims' Code—a statutory document setting out how victims of crime must be treated—into primary legislation and ensure criminal justice agencies keep their delivery of the Code under review. It also seeks to place victims at the heart of the criminal justice system, improve support, and strengthen transparency.[553] While the aims of the Victims Bill are welcome, Pete O'Doherty told us that it does not specifically mention victims of economic crime, who require tailored support and care depending on their circumstances.[554]

372. Dame Vera Baird defined vulnerability as the level of risk and harm to victims, with the underlying assumption that the more vulnerable a person is, the higher their risk of victimisation. In October 2021, the former Victims' Commissioner published research that segmented victims of fraud into clusters of vulnerability, looking at factors including whether they were a repeat victim or whether they were of a certain age that made them more

545 Written evidence from Social Market Foundation (FDF0026)
546 Q 229 (Andy Cooke)
547 Written evidence from Tricia (FDF0105)
548 Anonymous written evidence (FDF0010)
549 Home Office, 'Beating Crime Plan': https://www.gov.uk/government/publications/beating-crime-plan/beating-crime-plan#fn:16 [accessed 1 November 2022]
550 Cabinet Office, 'National Cyber Strategy 2022' (7 February 2022): https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 [accessed 1 November 2022]
551 Engagement session with the Midlands Fraud Forum (7 July 2022)
552 Written evidence from Tricia (FDF0105)
553 Ministry of Justice, *Draft Victims Bill*, CP 687 (May 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1079189/draft-victims-bill.pdf [accessed 1 November 2022]
554 Q 220 (Pete O'Doherty)

likely to be at risk from the fraud. It also segmented them into high, medium and low vulnerability groups, as shown below.

Figure 21: Analysis of the vulnerability of fraud victims



Source: Victims' Commissioner, Who suffers fraud? Understanding the fraud victim landscape (October 2021): https://s3-eu-west-2.amazonaws.com/jotwpublic-prod-storage-1cxo1dnrmkg14/uploads/sites/6/2021/12/VC-Who-Suffers-Fraud-Report-1.pdf [accessed 1 November 2022]

373. The research showed a variety of different groups within these degrees of vulnerability. For example, high vulnerability victims were more likely to have experienced financial loss and to have experienced severe or multiple reactions. 6% were elderly vulnerable victims who were more likely to live alone or be disabled. 10% in this group were younger, high harm victims who were more likely than other groups to be from an ethnic minority background. In the medium harm group, 9% were younger, urban, less affluent victims who had the highest probability of multiple victimisation. In the low-risk group, 8% of victims were categorised as low vulnerability and harm and were very likely to say that the incident had no impact on them. The Victims' Commissioner concluded that the need for support for victims is not necessarily commensurate with the amount of money lost, with some victims requiring more support even if they have not lost money, and others requiring limited support when they have.[555]

374. The FCA have produced guidance for firms about the fair treatment of vulnerable customers. This recommends steps to ensure that staff understand the needs of vulnerable customers, that they have the skills and capability to respond effectively, and that firms can take practical action to ensure their services are tailored to support vulnerable customers.[556] However, more work needs to be done to assess the risks of sharing data on customers considered

555 Victims Commissioner, *Who suffers fraud? Understanding the fraud victim landscape* (October 2021): https://s3-eu-west-2.amazonaws.com/jotwpublic-prod-storage-1cxo1dnrmkg14/uploads/sites/6/2021/12/VC-Who-Suffers-Fraud-Report-1.pdf [accessed 1 November 2022]; Victims Commissioner, 'Fraud surged by 24% under Covid. Now a new study reveals around 700,000 victims a year are likely to be highly vulnerable to fraudulent crime and seriously harmed by it': https://victimscommissioner.org.uk/news/who-suffers-fraud/ [accessed 1 November 2022] and Q 118 (Dame Vera Baird)

556 FCA, 'Guidance for firms on the fair treatment of vulnerable customers' (19 July 2021): https://www.fca.org.uk/publications/finalised-guidance/guidance-firms-fair-treatment-vulnerable-customers [accessed 1 November 2022]

vulnerable to fraud, and to train those working in frontline financial services to recognise such customers.

375. This is a considerable challenge. As we have heard, everyone is vulnerable to fraud and vulnerability may change throughout different periods in a person's life.[557] While metrics for assessing vulnerability do exist, these are relatively broad provisions and require the collection of significant personal information. Furthermore, it is unclear what the impact on the customer of being labelled vulnerable might be, and what this might result in, for example restrictions on their access to funds. The Justice Committee recently recommended that Action Fraud's replacement system should be more effectively trained to assess the needs and vulnerabilities of victims and to direct them to appropriate resources.[558]

376. The CPS has also analysed the needs of victims within the criminal justice system. It found that victims want to be recognised as individuals, to receive personalised, regular and clear communications including about how the process works, and to be supported with information.[559] In June 2022, the CPS outlined four areas of improvement to improve its support for a victim throughout the prosecutorial process, including taking action to:

- Improve the support to all victims by increasing the level of communication and support of its universal service offer
- Enhance the service provided to victims with the greatest need
- Innovate and pilot new ways to strengthen engagement with victims
- Build an organisational and leadership culture around better victim engagement.[560]

377. Finally, it has been argued that any reorganisation of the police response to fraud must take into consideration the needs of victims. Police and Crime Commissioners currently commission victims' services for their force areas. For example, the London Victims and Witness Service is commissioned by the Mayor's Office for Policing and Crime.[561] The Local Government Association has argued for the retention of this local approach, "which provides local areas with the flexibility and resources to identify local priorities and take action".[562] Models for policing fraud are discussed in more depth in paragraph 287.

378. **While efforts are being made to protect and support victims of fraud, support pathways remain unclear and there are gaps in provision. This is leading to a loss of trust between victims and the systems in place. It remains unclear how the Victims Bill will support victims of**

557 Written evidence by the Fraud Advisory Panel (FDF0048)
558 Justice Committee, *Fraud and the Justice System* (Fourth Report, Session 2022–23, HC 12)
559 CPS, 'Delivering Justice for victims: A consultation on improving victims' experiences of the justice system: CPS response' (4 February 2022): https://www.cps.gov.uk/publication/delivering-justice-victims-consultation-improving-victims-experiences-justice-system [accessed 1 November 2022]
560 CPS, 'Transforming our service to victims at the CPS' (27 June 2022): https://www.cps.gov.uk/stories/transforming-our-service-victims-cps [accessed 1 November 2022]
561 House of Commons Library, 'Support for victims of crime' (7 December 2020): https://commonslibrary.parliament.uk/support-for-victims-of-crime/ [accessed 1 November 2022]
562 Local Government Association, 'LGA responds to the publication of the Draft Victims Bill' (25 May 2022): https://www.local.gov.uk/about/news/lga-responds-publication-draft-victims-bill [accessed 1 November 2022]

fraud and the recent resignation of the Victims' Commissioner has highlighted the lack of due attention provided to victims across the board. We trust a replacement will be appointed soon.

379. ***The Government must specifically include victims of fraud and economic crime in the Victims Bill and consider the recommendations of the former Victims' Commissioner that support for victims of fraud is tailored to the three high-vulnerability groups identified.***

380. ***The Government must consider the local needs of victims as part of any future review of the policing structure for fraud.***

381. ***As part of the process of replacing Action Fraud, and to provide clarity for victims, Action Fraud should be renamed to reflect more accurately its role as a reporting service. We agree with the Justice Committee that the new system should be victim-focussed to improve the flow of information about the progress of fraud cases to victims. The new system must be coupled with increased training for fraud call handlers to ensure that vulnerable victims are identified and treated appropriately, and to ensure that cases that are solvable are passed to the NFIB for investigation.***

Reimbursement

382. In the year to March 2022, victims of fraud who suffered a financial loss were fully reimbursed in around three fifths (62%) of cases, although this proportion varied across different fraud types; the figure was higher in cases of bank and credit account fraud (73%) than for advance fee fraud (64%) and consumer and retail fraud (46%).[563]

383. The committee appreciates how important reimbursement of victims of fraud can be to securing justice for them. We appreciate that a focus on reimbursement alone ignores the causes of fraud and focusses on symptoms rather than bringing the perpetrators to justice. For this reason, a balanced approach to fraud risks is required across the system and throughout the fraud chain. Nicholas Taylor told us:

> "Focusing on reimbursement is important, but ultimately reimbursement is treating the symptom. We need to tackle the root cause. Ultimately, payment service providers are the final step in all of this. We need to drill down and focus on those who bring risk into the system."[564]

384. Often victims of APP fraud struggle to recoup their losses through reimbursement, depending on with whom they bank. Banks have different policies on reimbursement. The most widespread reimbursement model is the Contingent Reimbursement Model (CRM) Code, which was introduced in 2019. PSPs who signed up to the Code agree that victims of APP fraud should be reimbursed if it wasn't reasonable to expect them to have protected themselves. The Code does not apply to payments made using cash, cheque, credit or debit cards and it is not compulsory.[565]

---

563 ONS, 'Nature of fraud and computer misuse in England and Wales: year ending March 2022' (26 September 2022): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022 [accessed 1 November 2022]

564 Q 39 (Nicholas Taylor)

565 House of Commons Library, *Banking fraud*, Briefing Paper CBP8545, 23 February 2021

385. To date, the Code has currently been signed by ten banking groups and covers 90% of relevant transactions.[566] Figures from UK Finance show that £117.2 million of losses were returned to victims under the Code (60%) in the first half of 2022.[567]

386. In May 2022, the Government announced its intention to legislate in the Financial Services and Markets Bill to clarify that the PSR may use existing regulatory powers to require reimbursement in cases of APP scams in some payment systems, including Faster Payments.[568] The Bill amends the Payment Services Regulations 2017 to clarify that regulation 90 does not affect the liability of a PSP where the regulator has exercised regulatory powers in relation to APP scams. This will enable the PSR to use its powers to require mandatory reimbursement. The Financial Services and Markets Bill will also place a duty on the PSR to take regulatory action on APP scam reimbursement by participants using Faster Payments, by requiring it to consult on a draft regulatory requirement, and impose a regulatory requirement, within two and six months respectively of the legislation coming into force.[569] The Committee recognises the complexities of regulatory perimeters but is unclear why this measure should apply to Faster Payments alone.

387. In September 2022, the PSR published a consultation in which it emphasised its support for mandatory reimbursement in cases totalling losses of over £100 in all but exceptional cases. However, "exceptions will include scams where the customer is involved in the fraud themselves, or where they have acted with gross negligence". The specific definition of 'gross negligence' is yet to be set out. The PSR also set out that from 2023, the largest PSPs will be required to publish data on their performance on APP scams and reimbursement.[570]

388. We heard that the CRM Code should be made mandatory for all PSPs. Richard Emery criticised the "shockingly low level of reimbursement by the banks", suggesting that banks are not applying the Code effectively.[571] Since April 2019 TSB has implemented its own Fraud Refund Guarantee, refunding 97% of fraud claims compared to an industry average of 42%. It argues that obligations to refund victims should be mandated across the financial services industry. The bank has not signed up to the CRM code because it believes that the approach under the Code encourages victim blaming, with banks able to reject claims if they believe a customer is at fault for the fraud.[572]

---

566 HM Treasury, 'Government approach to authorised push payment scam reimbursement' (10 May 2022): https://www.gov.uk/government/publications/government-approach-to-authorised-push-payment-scam-reimbursement/government-approach-to-authorised-push-payment-scam-reimbursement [accessed 1 November 2022]

567 UK Finance, *2022 half year fraud update* (13 October 2022): https://www.ukfinance.org.uk/system/files/2022–10/Half%20year%20fraud%20update%202022.pdf [accessed 1 November 2022]

568 HM Treasury, 'Government approach to authorised push payment scam reimbursement' (10 May 2022): https://www.gov.uk/government/publications/government-approach-to-authorised-push-payment-scam-reimbursement/government-approach-to-authorised-push-payment-scam-reimbursement [accessed 1 November 2022]

569 Explanatory Notes to the Financial Services and Markets Bill [Bill 146 (2022–23)-EN]

570 PSR, *Authorised Push Payment (APP) scams: Requiring reimbursement* (September 2022): https://www.psr.org.uk/media/kzlncenx/psr-cp22-4-app-scams-reimbursement-september-2022-v6.pdf [accessed 1 November 2022]

571 Written evidence from Richard Emery (FDF0040)

572 Written evidence from TSB (FDF0066)

389. We asked TSB if they had seen any significant change in fraud being reported to them since they introduced their Fraud Refund Guarantee, which might signal a shift in consumer behaviour. TSB told us that its policy did not create an additional moral hazard and it had not seen any significant change in the amount of fraud being reported.[573]

390. We also heard arguments to the contrary. Some PSPs argue that the Code is not applicable to their services. Klarna, a fintech company, told us that, in addition to offering protections against fraud, its business model differs so far from other PSPs that any proposed extension of the Code without revision would be disproportionate.[574] Steve Buck, a former law enforcement officer, told us that the Code was designed for current accounts, and is not practically applicable for savings accounts that operate as what are known as closed or semi-closed loop accounts, whereby the account is set up for a single purpose.[575] In addition, the Lending Standards Board (LSB), which has responsibility for governance and oversight of the Code, told us that there is a "regulatory gap" in relation to cryptocurrency, which is out of the Board's remit. The LSB told us that it has "no immediate plans to extend the scope of the CRM Code, for instance to capture crypto asset service providers", however it is considering further guidance to firms on how the Code applies in cases relating to cryptoassets.[576]

391. The Building Societies Association asked the Committee to consider whether making reimbursement mandatory could lead to it being considered a "victimless crime".[577] The Committee's attention was drawn to a range of potential outcomes should reimbursement become mandatory including that:

- Consumers may change their behaviour if the risk element is removed, removing the need to take precautionary steps
- Fraud may be considered a "victimless crime" and thus increase
- Law enforcement may be disincentivised to tackle fraud if all victims are reimbursed
- Fraud-enabling sectors may also be disincentivised to tackle fraud on their services and platforms.[578]

392. The Government recognises some of these concerns. Speaking to the Treasury Committee in October, the Financial Secretary to the Treasury, Andrew Griffith, told MPs that the regulator must work with the industry on the assessment of whether victims should be compensated or not, recognising "there is a moral hazard piece and we have to get that right balance".[579] The Security Minister told us that he did not want to encourage an avenue "in which companies can prove victim to a different form of fraud where you

573 This was confirmed in a private email from TSB (21 October 2022)
574 Written evidence from Klarna (FDF0049)
575 Written evidence from Steve Buck (FDF0084). Also see Investopedia, 'Closed Loop Card' (updated 24 June 2021): https://www.investopedia.com/closed-loop-card-definition-4683996 [accessed 1 November 2022].
576 Written evidence from the Lending Standards Board (FDF0050)
577 Written evidence from the Building Societies Association (FDF0023)
578 Written evidence from the Building Societies Association (FDF0023), Nottingham Building Society (FDF0025) and Steve Buck (FDF0084)
579 Oral evidence taken before the Treasury Committee on 11 October 2022 (Session 2022–23), Q 75 (Andrew Griffith)

have the impression of a victim but the victim is actually a participant", however he recognised this might happen in only a tiny minority of cases.[580]

393. We heard calls for greater transparency in reporting about the CRM Code. TSB suggested that all PSPs should be required to report their fraud refund rate and display this information prominently both in physical spaces and online.[581] However, Geraldine Lawlor told us that there may be unintended consequences from such an approach:

> "Measurement is always helpful in a system, because at least you have something tangible to reflect on and can look at trends year on year, but there are sometimes unintended consequences with measurement, particularly as numbers in and of themselves lack context for cases that were reimbursed and, more importantly, cases that were not. If you look at pure numbers, sometimes people compare across institutions. It may not give you the full context and it could drive the wrong outcome and behaviours. It could also lead to people wanting to drive up more or even down, or even question their own framework if the numbers do not compare."[582]

394. The extent to which the bank receiving the fraudulent payment should be involved in reimbursing the customer was also raised in evidence. At present, the bank receiving a fraudulent payment has limited liability for the fraud, even if fraudsters were able to open a bank account with relative ease. The PSR is consulting on proposals to incentivise PSPs to prevent APP scams, whether they are the sending or receiving bank. The PSR proposes that, as a default, the sending and receiving PSP should share the cost of reimbursement (over £100) 50:50.[583] We endorse this measure.

395. Brian Dilley, told us that reforms to the Code were needed to hold the recipient bank to account for fraudulent payments it had accepted.[584] Chris Hemsley told us that there was a need to get a better balance between both parties in the payment transaction:

> "One of the next steps we need to take is to make sure all firms participate. This issue of mandatory involvement is really important. We need to get the receiving firms in the system. When we have that mandatory involvement, exactly as you said, it allows us to share the liability between the sender and receiver. Over time, I would like to do that in a smarter and more sophisticated way."[585]

396. In addition, the Committee has heard that the costs of reimbursement should be shared more evenly amongst fraud-enabling sectors. The Lending Standards Board (LSB) told us that "this cannot be a fight for the financial services industry alone".[586] Prof Hao gave the example of the telecoms sector:

---

580 Q 266 (Tom Tugendhat MP)
581 Written evidence from TSB (FDF0066)
582 Q 39 (Geraldine Lawlor)
583 PSR, *Authorised push payment (APP) scams: Requiring reimbursement* (September 2022): https://www.psr.org.uk/media/kzlncenx/psr-cp22-4-app-scams-reimbursement-september-2022-v6.pdf [accessed 1 November 2022]
584 Q 39 (Brian Dilley)
585 Q 158 (Chris Hemsley)
586 Written evidence from the Lending Standards Board (FDF0050)

> "In the telecommunications system at the moment, when someone receives a spoofed phone call claiming to be from a bank or HMRC and is tricked into making a payment, the telecommunication companies are not liable. There is also a lack of incentive for the telecom companies to address these problems aggressively, partly because the telcos are driven by revenues. To stop these kinds of attacks, they need to invest, and that does not bring in additional revenue, so there is a misalignment of incentives."[587]

397. TSB called for a new cost sharing mechanism whereby banks can seek to recover the costs of reimbursement of fraud victims from the platforms which enabled customers to be targeted. The Committee is concerned that any such mechanism ought to ensure a single point of contact for the victim seeking reimbursement. TSB argued that without such a mechanism:

> "Social media firms, tech firms and telcos have almost no financial or regulatory incentive to prevent fraud. While this remains the case these firms will have no reason to cooperate or to take the issue seriously."[588]

398. The Lending Standards Board told us that it believes the introduction of the Code in 2019 has led to the detection and prevention of APP scams becoming a "key priority" for most major UK banks. The proportion of APP scam losses reimbursed to victims rose from 25.4% to 43.2% between 2019 and 2020, resulting in a decrease in the loss to customers. The LSB concludes that the Code has "clearly raised protection for customers and put the UK banking industry in a much stronger position to tackle APP scams".[589]

399. **Reimbursing victims cannot be the seen as the primary focus of counter-fraud policy, yet it is a fundamental part of securing justice for victims. While we recognise the case for mandatory reimbursement of victims of APP fraud, we are concerned that a blanket reimbursement policy may lead to increased levels of moral hazard and fraud, and the perception that it is a 'victimless crime'. In some cases, it may even lead directly to new avenues for APP-reimbursement frauds. We also recognise how much banks have done to reimburse their customers. However, banks are the last link in the fraud chain and cannot be expected to foot the fraud bill alone. Furthermore, the inconsistency in the application of the CRM code across the sector demonstrates the need for uniformity.**

400. ***The Government must revise its proposals to legislate to allow the PSR to mandate blanket reimbursement of APP fraud conducted via Faster Payments. The Committee suggests that further exploration on the long and short-term risks of this approach is required and recommends that the Government seek a solution that achieves a level playing field for all customers.***

401. ***To incentivise companies to act on fraud and more accurately reflect the balance of responsibility for fraud, the Government must establish a mechanism by which fraud-enabling sectors—in addition to the outgoing and recipient PSP—are required to contribute to the costs of reimbursement in cases where their platforms and***

587 Q 234 (Prof Feng Hao)
588 Written evidence from TSB (FDF0066)
589 Written evidence from the Lending Standards Board (FDF0050)

services helped to facilitate the fraud. In making these changes, the Government must ensure that these reforms do not complicate the victims' experience of reimbursement; they should retain a single point of contact.

Consumer awareness campaigns

402. Awareness and consumer education campaigns play a critical role in informing the public about the dangers of fraud and how to respond to them. There are two main types of counter-fraud awareness campaign. The first is deployed by financial services companies and typically may be displayed at the point of payment. The second is a broader awareness campaign typically run by counter-fraud bodies and promoted on social media, as in Figure 22.

Figure 22: Examples of fraud awareness campaigns

Source: UK Finance Cifas

403. The Take Five campaign, run by UK Finance, is one of the most recognisable anti-fraud campaigns. Brian Dilley told us that data showed that a quarter of the public recognise the current campaign, which is 'Stop, Challenge, Protect', and two fifths recognise the 'Take Five' banner. Lloyds Banking Group displays the banner on all its ATMs, apps and in-branch.[590]

404. Some digital-first banks have gone further to educate a customer base that primarily is app-based.[591] Nicholas Taylor told us that Revolut worked with behavioural scientists and deploys Instagram-style 'stories' on its app that customers cannot skip through ahead of payments are deemed to be riskier than most. This is coupled with email campaigns and push notifications published on the banking app.[592]

405. The efficacy of such warnings and education campaigns is difficult to assess. Nicholas Taylor told us that Revolut's machine learning models correctly identify over 90% of attempted APP fraud, but 85% of customers warned directly, ignore the warnings. Even after direct intervention when a customer is required to speak with an agent, 80% still go on to make the payment.[593] Callsign suggested that current warnings are often "generic and easily ignored" due to being deployed too frequently. It said that alerts delivered

590 Q 35 (Brian Dilley)
591 Sifted, 'Neobanks' biggest challenge isn't growth. It's fraud' (8 February 2022): https://sifted.eu/articles/fraud-neobanks-challenge-fintech-paypal/ [accessed 1 November 2022]
592 Q 35 (Nicholas Taylor)
593 Q 34 (Nicholas Taylor)

during legitimate payments create undue friction in the payment journey and are perceived as common in the payment process. Callsign says that "this ultimately decreases users' sense of the importance of warnings, encouraging them to click through without due consideration of the message's contents."[594]

406. We have heard that there is a pressing need for greater awareness and understanding of the nature of fraud risks to individuals. It is clear that there is a need for such campaigns to be targeted at specific at-risk groups. Markko Künnapu, Legal Adviser at the Estonian Ministry of Justice, told us that different frauds target different population groups, and as such counter-fraud campaigns must be targeted similarly with clear messages on the key trends, threats and risks. He called for a focus on increasing levels of "cyber hygiene" across the board.[595]

Box 14: Examples of international awareness campaigns

The US SEC's Office of Investor Education and Advocacy (OIEA) is responsible for helping investors to invest wisely and avoid fraud. It develops campaigns about emerging threat areas, working in partnership with other offices in the SEC. This leads to coordinated press releases and public statements, including speaking events, intended to help the public to understand the threat landscape in a "user friendly" way.[596]

In June 2022, the OIEA released a gameshow-themed public service campaign to help investors to avoid fraud. The 'Investomania' campaign was intended to replicate the feeling of investing when it looks and feels like a game. The campaign included a 30-second TV advertisement, a 15-second video on cryptoassets and other types of investment, and interactive quizzes with the goal of reaching "existing, new and future investors of all ages". It encourages these investors to research their investments before parting with their money, leading them to the SEC's resource for investor education, Investor.gov.[597]

594 Written evidence from Callsign (FDF0038)
595 Q 171 (Markko Künnapu)
596 Q 187 (Melissa Hodgman)
597 US Securities and Exchange Commission, 'SEC launches gameshow-themed public service campaign' (1 June 2022): https://www.sec.gov/news/press-release/2022–95 [accessed 1 November 2022]

The FCA has its own equivalent, InvestSmart, which is designed to inform newer, younger investors who might be tempted to buy complex, higher-risk products that do not reflect their risk tolerance. The campaign is not specifically about fraud prevention but aims to help consumers make better investment decisions. It is promoted on TikTok and the FCA has partnered with influencers.[598]

407. The Committee has heard that the landscape for fraud awareness campaigns is too cluttered. The Security Minister told us:

> "I am told that one of the things we have found with this is that the multiplicity of voices has actually led to confusion, not reporting. Having a simpler form of information is an important element; this is where we really need to be focused rather than multiplying the number of voices."[599]

408. Commentators have argued for a centrally led approach. This has precedent and was taken by the Government during the COVID-19 public health campaign. The Fraud Advisory Panel told us that there was a need for a well-funded and sustained public education campaign led by the government at a national level to inform consumers about protecting themselves.[600] Geraldine Lawlor, called for government-coordinated action on messaging to establish a "common voice" on consumer protection.[601] Despite its ScamSmart and InvestSmart campaigns, which are limited to investment fraud, the FCA argues:

> "There is no single Government-sponsored site or campaign dedicated to helping the public avoid scams and frauds. There is a risk that individual initiatives by different organisations fragment or dilute the preventative message. Funding for individual campaigns is limited. The cost of a publicly funded permanent centralised campaign would be justified by the savings to consumers and would ramp up prevention efforts substantially."[602]

598 Written evidence from the FCA (FDF0069)
599 Q 267 (Tom Tugendhat MP)
600 Written evidence from the Fraud Advisory Panel (FDF0048)
601 Q 43 (Geraldine Lawlor)
602 Written evidence from the FCA (FDF0069)

409. The Justice Committee has recently argued that the upcoming publication of the Fraud Strategy might be accompanied by such a national awareness campaign.[603]

410. Given the common misconception that older people are the target of scams, there is clearly a need for young people to be taught about the risk of fraud through financial education. The APPG on Financial Education for Young People concluded in 2021 that "those leaving school without an effective financial education are at high risk of financial abuse", including being exploited by fraudsters and at the hands of mule herders. It suggested that the present offering was "patchy".[604]

411. Financial education does feature in the national curriculum, however it is a non-statutory subject.[605] Recent Bank of England research showed that the largest challenge faced by teachers in delivering financial education was curriculum time (63%).[606] The Bank of England has developed a set of materials to support financial education, chiefly through its Money and Me resource for Key Stage 1 and 2 PSHE lessons, and through EconoME for those at Key Stages 3 and 4.[607] However, we recognise the need to go further. The Fraud Advisory Panel told us that fraud and cyber education should be mandatory within the national curriculum for all school children with the Department for Education actively involved in such discussions."[608]

412. Joe Lycett provided examples of what might be covered in the classroom:

> " … There are some really basic things, such as changing the privacy settings on your apps, never using the default settings on things like smart devices in your house. If you buy a wi-fi camera, always change the settings to make sure that the password is not the basic password … If people have these basic tools and are taught about them in school, it will help."[609]

603 Justice Committee, *Fraud and the Justice System* (Fourth Report, Session 2022–23, HC 12)
604 APPG on Financial Education for Young People, Inquiry on primary-school aged financial education (2021): https://www.young-enterprise.org.uk/wp-content/uploads/2021/07/Inquiry-on-primary-school-aged-financial-education-Report.pdf [accessed 1 November 2022]
605 Bank of England, 'Financial education in a digital world' (29 March 2022): https://www.bankofengland.co.uk/quarterly-bulletin/2022/2022-q1/financial-education-in-a-digital-world [accessed 1 November 2022]
606 *Ibid.*, Chart 1
607 Bank of England, 'Money and ME': https://www.bankofengland.co.uk/education/education-resources/money-and-me [accessed 20 July 2022] and Bank of England, 'EconoME': https://www.bankofengland.co.uk/education/econome [accessed 1 November 2022]
608 Written evidence from the Fraud Advisory Panel (FDF0048)
609 QQ 99–100 (Joe Lycett)

Box 15: Digital literacy in Estonia

Estonia along with Finland, Sweden, Denmark and the Netherlands is one of the highest performing EU member states in the European Commission's Digital Economy and Society Index (DESI).[610] Their Government believes that the proportion of Estonians that trust its digital systems is around 80%.[611]

Estonia operates a baseline national digital identity including national ID cards and additional tokens including mobile ID, residence card, digital ID and e-resident card. It says that this "ensures the uniformity of a person's identity on the internet and allows for authentication and digital signing". There is no central database and communication between databases is encrypted via the X-road, the infrastructure backbone of the e-Estonia system.[612]

Estonia has high rates of digital literacy. Students in Estonia begin learning about online services and safety in primary school. There are partnerships with the country's Ministry of Defence and Ministry of Education and Research that increase awareness of digital threats, alongside initiatives by private companies to educate people about the risks.[613]

Markko Künnapu told us that Estonia's cyber-crime response is built on education and population level resilience:

> "You need to have dedicated, responsible cyber-crime units with the necessary capacity, but you also need to pay attention to overall awareness and education. It is very important to reach out to different categories of people, not only young people and children but the elderly, because these fraud schemes may target and address different population groups. Therefore, countries need to be ready. They need to provide clear messages on what to expect and what the key trends, threats and risks are."[614]

He also said: "It is important that people understand or realise that this [a scam] is too good to be true, that it is suspicious and fraudulent. It is about awareness raising, education and what we like to call proper cyber hygiene—how to behave online, what to do and what one should not do."[615]

Source: QQ 171–178 (Markko Künnapu)

413. Alongside classroom education, the importance of lifelong learning and adult education cannot be forgotten. Data from Lloyds Banking Group shows that 21% of the population (11 million) are digitally disadvantaged, with around 10 million of them lacking foundation level digital skills.[616] The Good

610 European Commission, 'Digital Economy and Society Index (DESI) 2020 Questions and Answers' (11 June 2020): https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1022 [accessed 1 November2022]

611 'How Estonia created trust in its digital-forward government', Security Intelligence (17 September 2021): https://securityintelligence.com/articles/estonia-trust-digital-government/ [accessed 1 November 2022]

612 E-Estonia, *Factsheet: Cyber security*: https://e-estonia.com/wp-content/uploads/cyber-security-factsheet-sept2021.pdf [accessed 1 November 2022]

613 Security Intelligence, 'How Estonia created trust in its digital-forward government' (17 September 2021): https://securityintelligence.com/articles/estonia-trust-digital-government/ [accessed 1 November 2022]

614 Q 171 (Markko Künnapu)

615 *Ibid.*

616 Lloyds Banking Group, *Essential Digital Skills Report 2021* (September 2021): https://www.lloydsbank.com/assets/media/pdfs/banking_with_us/whats-happening/211109-lloyds-essential-digital-skills-report-2021.pdf [accessed 1 November 2022]

Things Foundation highlighted that digital exclusion means lacking access to devices, data and the digital skills to participate safely online, including what to do if things go wrong. It called for sustained education campaigns and resources on digital fraud as well as sustained community infrastructure to act as a national safety net for digital inclusion in society.[617]

414. In February 2022, the Government launched 'Cyber Explorers' as part of the National Cyber Strategy, a free interactive learning platform rolled out across secondary schools and aimed at young people aged 11 to 14. It is intended to teach students essential digital skills to meet future skills demands.[618] Furthermore, the Government's Digital Strategy was published in the summer of 2022 and set out plans to tackle the digital skills gap, including supporting lifelong digital learning that will enable adults to participate in a digitalised world.[619]

415. There is clearly a role for online platforms in public service advertising given the volume of fraud that takes place on these services. We welcome the news that the OFSG, including Google, Meta and Amazon recently gave the FCA advertising credits worth $1 million to support the Take Five campaign.[620] Google has also provided $1 million advertising credit to the FCA to support industry awareness campaigns, however we understand that there is no offer to continue the partnership beyond the credit shared so far, nor have other platforms made any offer.[621] The NAFN suggested that Ofcom should be directly responsible for ensuring that media platforms promote such awareness.[622]

Box 16: The 7726 service

The 7726 service is a number by which UK mobile customers can report unwanted texts or calls. Once reported, mobile providers are alerted to investigate the number and potentially block it. The service does not automatically block the number. 7726 was chosen because it spells out 'SPAM' on an alphanumeric telephone keyboard.[623] During the pandemic, it is believed that a rise in scam texts defrauded consumers of £2.35 billion in 2021.[624]

The Telecoms Fraud Sector Charter sets out that the sector must make a coordinated effort to review the use of the service to explore how it can be utilised more effectively to prevent smishing.[625]

617 Written evidence from Good Things Foundation (FDF0045)
618 DCMS, 'Cyber Explorers' (23 February 2022): https://www.gov.uk/guidance/cyber-explorers [accessed 1 November 2022]
619 DCMS, *UK Digital Strategy* (6 July 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1089103/UK_Digital_Strategy_web_accessible.pdf [accessed 1 November 2022]
620 Q 19 (Katy Worobec)
621 Q 156 (Mark Steward)
622 Written evidence from the NAFN (FDF0055)
623 Ofcom, 'How to report scam texts and mobile calls to 7726': https://www.ofcom.org.uk/phones-telecoms-and-internet/advice-for-consumers/scams/7726-reporting-scam-texts-and-calls [accessed 1 November 2022]
624 Mobile UK, 'Industry implemented strengthened customer protections result in substantial reduction in scam texts' (20 July 2022): https://www.mobileuk.org/news/industry-implemented-strengthened-customer-protections-result-in-substantial-reduction-in-scam-texts [accessed 1 November 2022]
625 Home Office, 'Fraud sector charter: telecommunications' (26 October 2021): https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version [accessed 1 November 2022]

When the 7726 service is used, the results can be positive. The NCSC has removed 12,000 scams reported by 7726 in the past two years.[626] Other public bodies such as the ICO have access to the service and can pursue persistent offenders.[627] Reports to the service have dropped by 90% (500,000 reports to 50,000) since August 2021, which Mobile UK claims shows the reduction in scam messages reaching customers.[628]

However, awareness of 7726 is not widespread. Research by Ofcom showed that eight in 10 people (79%) are unaware that 7726 exists.[629] Others may not feel motivated to use the service. Alex Towers told us:

> "Every week, BT and EE get roughly 20,000, when you add together calls to our contact centres and things reported to the 7726 line. That is a lot lower than what we know the scale of the problem is. That is largely because for lots of people, and I certainly include myself, it is very easy to ignore it and move on, knowing that it is something you should not pay any attention to."[630]

Evidently, there is a need to promote the 7726 service. Ofcom's General Conditions of Entitlement are the regulatory conditions that providers of electronic communications networks and services must adhere to. Consumer protection conditions are detailed in Part C. The latest General Conditions were published in June 2022 and there is no general condition that providers must provide education and raise awareness amongst customers of the risks of fraud nor on how to report including by existing services like 7726.[631]

Further restricting the impact of the 7726 service is its limitation to mobile networks. Online messenger platforms have their own systems in place to report scam messages. As closed user groups, these platforms are subject to different regulatory oversight and, while Ofcom can set out guidance for these platforms, the divergence in reporting systems is unhelpful. Furthermore, while Meta told us that it uses such reports made on its platforms to train its AI systems to detect fraud in future, a more publicly transparent system underpinned by a 'duty to report' placed on companies themselves (see paragraph 523) may help to ensure that action is taken when fraud is reported to a company.[632]

416. We recognise the tensions between the argument for greater consumer education and the impact that this has on victim blaming. TSB argued that, despite the positive effects of education campaigns, the scale of fraud and the adeptness with which fraudsters can "explain away" a target's concern mean that their efficacy is limited. It said:

> " … It is not possible, or reasonable to expect, people to maintain an advanced level of knowledge about the current modus operandi of

626 'Don't delete scam texts: send them to 7726 and become a scambuster: Around 500 a month are being removed' *This is Money* (1 June 2022): https://www.thisismoney.co.uk/money/beatthescammers/article10872575/Dont-delete-scam-texts-send-7726-scambuster.html [accessed 1 November 2022]

627 Q 45 (Hamish MacLeod)

628 Mobile UK, 'Industry implemented strengthened customer protections result in substantial reduction in scam texts' (20 July 2022): https://www.mobileuk.org/news/industry-implemented-strengthened-customer-protections-result-in-substantial-reduction-in-scam-texts [accessed 1 November 2022]

629 Ofcom, '45 million people targeted by scam calls and texts this summer' (20 October 2021): https://www.ofcom.org.uk/news-centre/2021/45-million-people-targeted-by-scams [accessed 1 November 2022]

630 Q 47 (Alex Towers)

631 Ofcom, General Conditions of Entitlement: Unofficial consolidated version (17 June 2022) [accessed 1 November 2022]

632 Written evidence by Meta (FDF0052)

every type of fraud that they may fall victim to. Fraud is one of the only crimes in the UK where it is acceptable to immediately question the degree to which the victim is responsible for having been the victim. This means fraud victims are often met with less sympathy, support and understanding than the victims of other crimes. It also creates a false distinction in the minds of the public."[633]

417. **Public awareness campaigns are a crucial part of the fight against fraud. The Committee recognises that, while personal responsibility and awareness have a role, this should not be an excuse for fraud-enabling sectors to shirk their responsibilities to do more to tackle fraud via systems design.**

418. ***The Government should oversee the introduction of a single, centrally funded consumer awareness campaign in partnership with industry. This should align with the priorities established in the forthcoming Fraud Strategy and should provide clear guidance on how fraud can be reported.***

419. ***The Government must work with the tech sector to establish free advertising credits for the FCA and law enforcement to promote counter-fraud messaging as public service advertising.***

420. ***The Government urgently must bring forward the measures outlined in the UK Digital Strategy to strengthen the digital education and digital skills pipeline and ensure that these measures extend to lifelong learning for adults without essential digital skills.***

421. ***The Government must support the meaningful inclusion of financial education in the National Curriculum as part of teaching about online safety within primary and secondary schools.***

422. ***Ofcom should introduce a measure under part C of its General Conditions of Entitlement that providers of telecommunications services should do more to educate consumers about the risks of fraud, and how to report it via 7726. Ofcom must apply pressure to online messenger platforms to ensure that they make their equivalent scam reporting services more transparent to encourage user reporting. Online messenger platforms must be encouraged to begin piloting their proposed approach under the Online Safety Bill by conducting transparent risk assessments of their services and reporting mechanisms.***

423. ***The Government should commission a review of how users respond to warning messages linked to potentially fraudulent payments as part of the customer journey, and whether such messages change their behaviour.***

633 Written evidence from TSB (FDF0066)

CHAPTER 6: THE FRAUD ACT 2006 AND THE LEGISLATIVE FRAMEWORK

424. Part of this Committee's remit was to analyse the efficacy of the Fraud Act 2006, the principle legislative tool used for the prosecute fraud in England and Wales. In addition, we considered other legislative tools that are used either to prosecute fraudsters or are used in the process of bringing them to justice, including the Computer Misuse Act 1990, data protection regulations and those that govern corporate criminal liability.

425. This chapter explores our assessment of these legislative mechanisms and considers possible areas for reform.

The Fraud Act 2006

426. The Fraud Act 2006 applies in England, Wales and Northern Ireland and is the key piece of legislation used to prosecute fraud. For a summary of the provisions of this legislation see paragraph 56.

427. In response to a request from the Committee, the Ministry of Justice provided a memorandum on the Fraud Act, which gathered views about the efficacy of the Act from those with responsibility for enforcing and applying it. The Act was passed to clarify and modernise the law and make fraud law more straightforward for law enforcers and prosecutors. It was drafted with rapid technological advances in mind. The department concluded that fifteen years on from its introduction, the Fraud Act "continues to deliver on its objectives and is still regarded as an incredibly useful piece of legislation".[634]

428. We received similar sentiments in our evidence. Cifas told us:

> "The Fraud Act 2006 provided the required clarity around what constitutes fraud, by removing the confusing barrier of conspiracy and introducing a general offence covering false representation, failing to disclose information and abuse of position. Our assessment is that the Act has provided police and law enforcement with the legal clarity they require to tackle fraud more effectively, including for prosecution. It is therefore not deficiencies in the Fraud Act that has led to shortfalls in the Government and policing response to fraud, but a lack of focus, prioritisation and investment … "[635]

429. Security Minister Tom Tugendhat described the Fraud Act 2006 as "remarkably resilient", however he added:

> " … there is evidence that there are things that need to be reviewed. The reality, from my perspective, is that it is more to do with bringing prosecutions that can get to the Fraud Act rather than reforming the Fraud Act itself."[636]

430. While we agree that upstream prevention is better than focussing on punitive action, we recognise that there are areas where the Fraud Act could

634 Ministry of Justice, *Post-legislative assessment of the Fraud Act 2006: Memorandum to the House of Lords Select Committee on the Fraud Act 2006 and Digital Fraud*, CP 680 (June 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1081360/fraud-memo-2022.pdf [accessed 1 November 2022]

635 Written evidence from Cifas (FDF0015)

636 Q 264 (Tom Tugendhat MP)

be strengthened. Sentencing powers under the Act were raised in evidence. The Fraud Act carries a maximum sentence of 10 years imprisonment and/or a fine.[637] This compares to a maximum sentence for money laundering of 14 years. The City of London Police argued that, given the harm caused by fraud to individuals, the maximum sentence should be raised in order to bring the two offences in line. The force argues that the legislation places too much reliance on financial 'gain' and 'loss', which often is not commensurate with the emotional harm caused to the victims of fraud, because "losing £5,000 to one person can be as impactful as the impact of losing £50,000 to another".[638] Neil Postins, Service Delivery Manager at the NECC Victim Care Unit, said:

> "The maximum sentence for fraud is 10 years. Money laundering, which inevitably falls out of fraud, is 14 years, and I think even burglary is 14 years. We need the opportunity to review the sentencing and, while we do that, to take into account the emotional and physical effect of that fraud, as opposed to the value of it, because sometimes sentencing is geared to the value of loss. We take a person's emotional and mental state into account with other crimes, and perhaps it is a consideration with sentencing for fraud."[639]

431. In addition to a custodial sentence, convicted fraudsters may face additional ancillary orders, for example compensation or confiscation orders.[640] Similar mechanisms can also be employed in civil cases.

432. Concerns about the extent to which the Act can be applied to complex cyber fraud was raised by policing bodies including the Association of Police and Crime Commissioners and the West Midlands Police and Crime Commissioner, who argued for updated legislation to reflect the threat more clearly.[641] In addition, the extent to which it applies to cryptoasset fraud was raised by Nottingham Building Society.[642] However, we consider that the Act is broad enough to address these threats and flexible enough to adapt to modern forms of digital fraud. In addition, such offences could be prosecuted under the Computer Misuse Act 1990.

433. For example, a criminal that used a password to access a computer system, without authorisation, could be prosecuted under section 1 of the Computer Misuse Act 1990 or under Sections 1 and 2 of the Fraud Act 2006.[643] In the latter case, a prosecutor would need to prove an intention to cause a gain or loss. Section 2(5) of the Fraud Act 2006 sets out:

> 2(5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention).[644]

---

637 Explanatory Notes to the Fraud Act 2006
638 Written evidence from City of London Police (FDF0031)
639 Q 118 (Neil Postins)
640 Sentencing Council, 'Ancillary orders': https://www.sentencingcouncil.org.uk/sentencing-and-the-council/types-of-sentence/ancillary-orders/ [accessed 1 November 2022]
641 Written evidence from West Midlands Police and Crime Commissioner (FDF0035) and the Association of Police and Crime Commissioners (FDF0064)
642 Written evidence from Nottingham Building Society (FDF0025)
643 Dean Armstrong KC, Dan Hyde and Sam Thomas, *Cyber Security Law and Practice* (London: Lexis Nexis, 2019), para 1.76
644 Fraud Act 2006, section 2(5)

434. Equally, under Section 6 of the CMA, a person is guilty if they have in their possession or under control any "article for use in the course of or in connection with any fraud".[645] The Dedicated Card and Payment Crime Team at the City of London Police argued that the broad definition of the term 'article' allows for a wide interpretation, covering the use of hardware like SIM farms, and software such as phishing kits.[646]

435. The Fraud Act is also sufficiently broad to capture cryptoassets as "property". Under the Fraud Act Section 5(2), references to 'gain' and 'loss' are defined as follows:

> (2) "Gain" and "loss"
>
> (a) extend only to gain or loss in money or other property;
>
> (b) include any such gain or loss whether temporary or permanent; and "property" means any property whether real or personal (including things in action and other intangible property).[647]

436. There are several wider concerns that hinder the efficacy of the Act, including the disclosure regime and corporate criminal liability, which will be explored in the next section.

437. Finally, we have heard that the Fraud Act is not sufficiently wide enough in scope so as to be applicable to or address fraud-enabling sectors. TSB told us that the focus of the Act on fraudsters failed to capture the companies that fraudsters rely on to carry out their fraud:

> "While the Fraud Act 2006 covers participation in a fraudulent business it does not cover a business ignoring, enabling or facilitating the use of its technology or platform to systematically target people for the purposes of fraud."[648]

438. **The Fraud Act 2006 is a sound piece of legislation that is not in need of substantial reform. However, its efficacy is hindered by wider issues relating to its use in the prosecution of fraud cases and shortfalls in the prevention and detection of fraud, and enforcement of the legislation. Reform of corporate criminal liability will be essential in order to maximise the impact of the Fraud Act and other legal tools going forward.**

439. ***We agree with the Justice Committee that sentencing guidelines should be amended to reflect fully the financial, emotional and psychological harms caused by fraud. The Government should review the sentencing powers for fraud offences to bring sentences for fraud offences in line with money laundering offences. This should be followed by a review of the Sentencing Council's guidelines.***

---

645 Fraud Act 2006, section 6

646 Ministry of Justice, *Post-legislative assessment of the Fraud Act 2006: Memorandum to the House of Lords Select Committee on the Fraud Act 2006 and Digital Fraud*, CP 680, (June 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1081360/fraud-memo-2022.pdf [accessed 1 November 2022]

647 Fraud Act 2006, section 5(2)

648 Written evidence from TSB (FDF0066)

The Computer Misuse Act 1990

440. The Computer Misuse Act 1990 is used to prosecute cases of fraud. The Act was introduced long before many of the online platforms and services we are now familiar with were developed. Updated in 2010, the Act has been overtaken by the proliferation of social media firms.[649] Pauline Smith told us that the Act should be updated again so that it reflects "where we are now."[650]

441. The Home Office recognises concerns about the Act. Duncan Tessier told us that the Department's view is that "the Act is fundamentally not working."[651] Security Minister Tom Tugendhat agreed. He told us:

> "The Computer Misuse Act, as you know, is now about 30 years old, and although it has proven remarkably adaptable it still needs updating and we need to be quite clear that that is becoming ever more important."[652]

442. In recognition of concerns about the Act, the Home Office announced a review of the Act and held a consultation in Spring 2021.[653] The outcome has not yet been published and in September 2022, the Home Office published a new Call for Information on the Act as the first step in a new package of measures to be called the Cyber Duty to Protect.[654] Tom Tugendhat told us that a range of measures and reforms are being considered as part of this review including in the following areas:

- Powers to seize internet domain names
- Powers to require the preservation of data
- The new offence of illegally copied data
- Sentence levels
- The introduction of defences for activity that might breach offences under the Act.[655]

443. We have taken evidence that the Act requires reform to protect cybersecurity professionals acting in the public interest. The CyberUp campaign, a non-profit organisation representing cybersecurity professionals, told us that these individuals face prosecution under the Act. For example, Section 1 of the CMA forbids unauthorised access to any programme or data held in any

649 Cifas, 'Why we need to re-think online defences to combat fraud' (14 April 2021): https://www.cifas.org.uk/insight/fraud-risk-focus-blog/re-think-online-defences-to-combat-fraud [accessed 1 November 2022]
650 Q 118 (Pauline Smith)
651 Q 2 (Duncan Tessier)
652 Q 264 (Tom Tugendhat MP)
653 Home Office, 'Computer Misuse Act 1990: call for information' (9 August 2021): https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information [accessed 1 November 2022]
654 Home Office, 'Call for information: Unauthorised access to online accounts and personal data' (1 September 2022): https://www.gov.uk/government/consultations/unauthorised-access-to-online-accounts-and-personal-data/call-for-information-unauthorised-access-to-online-accounts-and-personal-data#background--why-we-are-holding-this-call-for-information [accessed 1 November 2022]
655 Q 264 (Tom Tugendhat MP)

computer. Defensive security activities frequently involve the interrogation of compromised systems.[656] The CyberUp Campaign told us:

> "This creates the perverse situation where cyber security professionals, acting in the public interest to prevent and detect crime, are held back by legislation that seeks to protect computer systems."[657]

444. The CyberUp Campaign have called for a statutory defence to be written into the Computer Misuse Act to protect cyber security professionals acting in the public interest.[658] However, Max Hill KC has suggested that the public interest test enshrined in the Code for Crown Prosecutors should mitigate such concerns. The two elements of this test are evidential sufficiency and public interest. He said that "in every crime, every prosecutor will need to apply his or her mind to public interest factors."[659]

445. Despite these reassurances, Dr Hutchings told us that such guidelines do not sufficiently reassure professionals:

> "There are some issues—things like the possession of hacking tools used by penetration testers to test networks, the possession of which is a crime. We have guidelines in the Crown Prosecution Service saying that people will not be prosecuted for their possession, but it creates some stress for people in those industries that they could be prosecuted. Technically, it is a crime."[660]

446. This has some international precedent. In May 2022, the US Department of Justice announced a revision of its policy, stating that under the Computer Fraud and Abuse Act, "good-faith security research should not be charged".[661]

447. Support for this position was not universal. Mark Fenhalls KC noted that whilst it might be a "theoretical issue", he was not aware of any prosecutions of cybersecurity professionals under the Act. He also told us that permission granted to cyber-security professionals by their employer would cover them from prosecution.[662] Karl Laird, agreed, adding:

> "The offences in the Computer Misuse Act are focused on unauthorised access and unauthorised acts. I struggle to see how those offences would impact cybersecurity professionals who are acting in the interests of their clients."[663]

448. There is some evidence that the law has been used to prosecute individuals in the past. In 2012, a student at York University was sentenced to eight months in prison—later halved—for accessing Facebook's internal systems to try to discover bugs.[664]

---

656 Computer Misuse Act 1990, section 1
657 Written evidence from CyberUp Campaign (FDF0005)
658 *Ibid.*
659 Q 244 (Max Hill KC)
660 Q 68 (Dr Alice Hutchings)
661 US Department of Justice, 'Department of Justice announces new policy for charging cases under the Computer Fraud and Abuse Act' (19 May 2022): https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act [accessed 1 November 2022]
662 Q 202 (Mark Fenhalls KC)
663 Q 202 (Karl Laird)
664 'Tear up decades-old law to save Britain from hackers, say cyber experts', *Daily Telegraph* (5 September 2022): https://www.telegraph.co.uk/business/2022/09/05/tear-decades-old-law-save-britain-hackers-say-cyber-experts/ [accessed 1 November 2022]

Box 17: Protection for whistleblowers

We have taken evidence that whistleblowers are not adequately supported or incentivised to come forward. The Fraud Advisory Panel told us that "incentives should be provided to whistleblowers to come forward, in order that more cases can be brought to light".[665]

The Protection for Whistleblowing Bill was introduced by Baroness Kramer as a private members bill in June 2022. It sets out provisions to protect whistleblowers, including by the establishment of an independent Office of the Whistleblower. Under the legislation, a person would be defined as a whistleblower if "that person has made, makes or is intending to make a protected disclosure or is perceived by a relevant person to have made, be making or intend to make a protected disclosure".[666] This definition differs from the current definition under the Public Interest Disclosure Act, which stipulates a whistleblower must be a 'worker' in the place where wrongdoing occurs.[667]

Transparency Task Force supported the measures and said that the treatment of whistleblowers and their evidence should be overhauled in order to increase the number of whistleblowers in the financial services sector with the goal of preventing and punishing investment frauds.[668]

Some witnesses including Onbord and Spotlight on Corruption praised the US' rewards regime for whistleblowers.[669] Baroness Kramer described the approach of the US as valuing whistleblowers as a "citizens' army".[670] Melissa Hodgman told us about the SEC's whistleblower rewards programme:

> "We have a tremendously good whistleblower programme, which has been extraordinarily helpful and allows us to give money to people if they give us information that allows us to obtain at least $1 million. We gave away almost $1 billion dollars last year as a result of this."[671]

It appears to us that more could be done to follow the example of the approach being taken in the US. The Security Minister told us that he was cautious of an approach that he felt focussed on financial gain by the whistleblower. We understand that legislation to offer whistleblower protection will be introduced in Parliament separately from the Online Safety Bill. We welcome measures setting out that protection will be offered to those who come forward in breach of a non-disclosure agreement to share information with a regulator.[672]

449. Finally, we heard that the Act is overly complex, which hinders its efficacy. Karl Laird told us that given efforts to keep pace with technological change, the Act has undergone many amendments. He suggested that this has overcomplicated the legislation and noted that understanding the territorial application of the Act required one to "wrap a cold tea towel around one's head". Laird suggested that the Act was being underutilised due to its complexity.[673]

665 Written evidence by the Fraud Advisory Panel (FDF0048)
666 Protection for Whistleblowing Bill, Part 1 (2) [HL Bill 27 (2022–23)]
667 Public Interest Disclosure Act 1998, Chapter 23, Part IVA, 43(A)
668 Written evidence by Transparency Task Force (FDF0092)
669 Q 88 (Dr Susan Hawley) and written evidence by Onbord (FDF0013)
670 HL Deb, 2 December 2021, col 311GC
671 Q 181 (Melissa Hodgman)
672 Q 261 (Tom Tugendhat MP and Damian Collins MP)
673 Q 202 (Karl Laird)

450. **The review of the Computer Misuse Act is welcome, however it cannot be delayed further.**

451. ***The Government must publish its review of the Computer Misuse Act 1990 with urgency, and consider immediate reform including the introduction of a statutory defence to protect cyber security researchers from prosecution.***

452. ***The FCA should review the SEC's regime for rewarding whistleblowers where their information leads to a conviction or retrieval of money obtained through fraud. In particular, it should bring forward legislation to protect those who come forward in breach of a non-disclosure agreement to share information with a regulator. The Government should also give serious consideration to The Protection for Whistleblowing Bill.***

Identity theft

453. Identity theft is often a predicate action to the criminal offence of fraud, as well as other offences including organised crime and terrorism, but it is not a criminal offence.[674] Cifas data shows that cases of identity fraud increased by 22% in 2021, accounting for 63% of all cases recorded to Cifas' National Fraud Database. 91% of cases occurred via an online channel.[675]

454. Fraudsters harvest personal data through various avenues, for example via data breaches. They trade this personal information on the criminal sites for exchanging information, such as the dark web.[676]

455. Identity scams often bypass the need for interaction with a real victim as fraudsters can use stolen personal data to impersonate customers. Mike Haley said that after the information is stolen "the criminal enterprise then either impersonates a genuine person or creates what we call a synthetic identity to make applications for bank accounts, credit cards, loans or mobile phones at scale."[677]

456. We have heard evidence that identity theft should be made a criminal offence. Michael Skidmore told us that identity theft is "instrumental" to some of the most serious types of fraud, adding that "there is some merit in trying to get upstream of a crime such as identity theft through an identity theft Act."[678]

457. In February 2022, the Government confirmed that there were no plans to introduce a new criminal offence of identity theft as "existing legislation is in place to protect people's personal data and prosecute those that commit crimes enabled by identity theft", including the Fraud Act 2006 and the Computer Misuse Act 1990.[679]

458. **Identity theft is a fundamental component of fraud and is routinely used by fraudsters to steal money from legitimate individuals and organisations yet it remains out of scope of criminal offences.**

---

674 Written evidence from Cifas (FDF0015)
675 Cifas, *Fraudscape 2022* (July 2022): https://www.fraudscape.co.uk/ [accessed 1 November 2022]
676 Q 14 (Mike Haley)
677 *Ibid.*
678 Q 90 (Michael Skidmore)
679 Written answer UIN 127498, Session 2021–22

459. ***The Government should consult on the introduction of legislation to create a specific criminal offence of identity theft. Alternatively, the Sentencing Council should consider including identity theft as a serious aggravating factor in cases of fraud.***

The Data Protection Act 2018 and GDPR

460. The importance of data sharing, both within and between the public—including law enforcement—and private sector, was a common theme in evidence. We heard that limitations on the extent to which stakeholders can share information with other relevant stakeholders is inhibiting efforts to fight fraud and allowing fraudsters to slip through the net.

461. There are several ways that organisations can share high-level information with each other. This includes public-private forums like the Joint Fraud Taskforce as well as private sector stakeholder groups such as Stop Scams UK. These groups meet to share best practice and updates on the fraud landscape. However, we have heard that current legislation may indirectly prevent organisations from sharing detailed data on fraud risk signals due to their risk appetite or perceptions of data protection legislation.

462. This may prevent the sharing of information that could combat fraud. One victim of fraud told us that she made several bank transfers totalling tens of thousands of pounds that should have raised 'red flags' with her banks due to their abnormality with her normal banking activity, however the banks in question did not alert one another and are not required to do so even if they think their customer has been a victim of fraud.

463. Data protection is currently governed by GDPR and the Data Protection Act 2018. The Act controls how personal information is used by organisations, business or the government. Those responsible for using personal data have to follow data protection principles.[680]

> *"Santander believed that I was a victim of fraud but still allowed me to transfer three payments of over £52,000 to HSBC which went straight into other accounts. Why didn't my banks talk to each other about the warning signs?" - Rachel*

464. The Committee heard that GDPR is viewed by some as an impediment to effective data sharing between and within public and private sector companies and law enforcement in the pursuit of fraud prevention. Graham Pullan told us that he believes that GDPR inhibits sharing the details of suspected romance scammers with other platforms, which could prevent repeat or new attacks across those other platforms.[681] While in support of the need to share information, the Online Dating Association cautioned that such restrictions lead to "considerable concern in the sector in relation to privacy, data protection and libel".[682] Firms also consider themselves at risk of fines for sharing information. Elizabeth Kanter told us that the company fears being fined for GDPR breaches should they share information with law

680 HM Government, 'Data protection': https://www.gov.uk/data-protection [accessed 1 November 2022]
681 Q 140 (Graham Pullan)
682 Written evidence from the Online Dating Association (FDF0028)

enforcement about one of their users, jeopardising their privacy or their data protection rights.[683] The Fraud Advisory Panel told us:

> "Both law enforcement and the private sector are concerned that they may fall foul of the GDPR when considering whether or not they can share data on specific fraudsters, and even on fraud risks. The GDPR legislation is complex and confusing, and as such the easiest position for law enforcement or the private sector is simply not to take the risk of breaching the law, and not to share any data."[684]

465. Others argued that the GDPR is merely being used as an excuse by organisations due to the fear of investigation and possible sanctions not to share data that might help to prevent fraud. JobsAware, a non-profit organisation supporting job seekers, told us that "companies would rather not share data than face investigation by the ICO".[685] Richard Emery, an Independent Bank Fraud Investigator, argued that there should be a regulatory requirement for banks actively to cooperate with police investigations, rather than "hiding behind GDPR".[686]

466. The ICO has oversight of UK GDPR. It told us that it has produced a "wealth of guidance" to help organisation to understand and comply with data protection law.[687] For example, under UK GDPR, Article 6(1) allows for the processing of personal data where necessary for the purposes of "legitimate interests".[688] There is no definition of "legitimate interests", however, ICO guidance sets out that fraud prevention either constitutes or should be regarded as a legitimate interest.[689]

467. Despite this, misconceptions about the GDPR and information sharing restrictions are widespread. Cifas highlighted a lack of awareness of section 68 of the Serious Crime Act 2007, which allows for a public authority to disclose information as a member of an anti-fraud organisation for the purposes of preventing fraud.[690]

468. To encourage greater proactivity, Elizabeth Kanter called for a 'good Samaritan' clause to be inserted into data protection regulations to encourage private sector companies to share information that might prevent fraud. Kanter said this would allow private companies to share information that might be useful to law enforcement and ensure that they will be protected and not face a fine if they do.[691]

469. However, exemptions already exist within Schedule 1, para 10 and Schedule 2, para 2 of the Data Protection Act 2018 that are relevant to the prevention and detection of crime. Any 'good Samaritan' who fell within these provisions, determined by the ICO, would be exempt from sanctions.[692] Brian Dilley

683 Q 140 (Elizabeth Kanter)
684 Written evidence from the Fraud Advisory Panel (FDF0048)
685 Written evidence from JobsAware (FDF0043)
686 Written evidence from Richard Emery (FDF0040)
687 Written evidence from the ICO (FDF0017)
688 Regulation (EU) 2016/679 of the European Parliament and of the Council, Article 6(1)
689 ICO, 'When can we rely on legitimate interests?': https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/when-can-we-rely-on-legitimate-interests/ [accessed 1 November 2022]
690 Written evidence from Cifas (FDF0015)
691 Q 140 (Elizabeth Kanter)
692 Data Protection Act 2018, Schedule 1, para 10 and Schedule 2, para 2

told us that even though the exemption for fraud is common knowledge, there is still confusion about the extent to which it can be applied:

> "GDPR and the data protection legislation have an exemption for fraud, but it is still fairly limited and not every bank has the same view of what it can share, or the same risk appetite for some of the civil liability that might come from sharing information on their customers".[693]

470. Julia Lopez MP, Minister of State at DCMS, told us explicitly that "data protection law does not prevent sharing data between law enforcement authorities and other organisations in order to discharge their statutory law enforcement functions". She said that the Government does "encourage" organisations to share data to stop scams.[694]

471. RUSI argued that the barriers to information sharing appear to be "cultural rather than a result of any legislative or regulatory impediment". It called for further proactive communications from regulators.[695] Ghela Boskovich went further, making the case for a legislative framework to compel PSPs to share data for the purposes of preventing fraud.[696]

472. Earlier this year, the Government announced plans to overhaul GDPR regulation via the Data Protection and Digital Information Bill. One of the broad aims of the Bill is to enable public bodies to share data to improve the delivery of services.[697] It proposes a limited, exhaustive 'safe list' of legitimate interests for which organisations could use personal data without applying the balancing test. In this test, data controllers must weigh up whether their interests including preventing crime in processing personal data outweigh the rights of data subjects.[698] The Bill states that "detecting, investigating or preventing crime" is a recognised legitimate interest and the Bill's explanatory notes make clear that this provision includes preventing economic crimes such as fraud.[699] The Data Protection and Digital Information Bill is currently on pause, with the Culture Secretary, Michelle Donelan, promising to replace GDPR with a new system.[700] Julia Lopez told us:

> " … the Bill will provide organisations with greater clarity and confidence in the legal bases for sharing data for law enforcement purposes and to safeguard national security."[701]

---

693 Q 37 (Brian Dilley)
694 Letter from Julia Lopez MP to Chair (27 October 2022): https://committees.parliament.uk/publications/30543/documents/176142/default/
695 Written evidence from RUSI (FDF0036)
696 Q 79 (Ghela Boskovich)
697 HM Government, *The Queen's Speech 2022* (10 May 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1074113/Lobby_Pack_10_May_2022.pdf [accessed 1 November 2022]
698 DCMS, 'Data: a new direction: government response to consultation' (23 June 2022): https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation [accessed 1 November 2022] and letter from Julia Lopez MP to Chair (27 October 2022): https://committees.parliament.uk/publications/30543/documents/176142/default/
699 Data Protection and Digital Information Bill, 5(a) and Explanatory Notes to the Data Protection and Digital Information Bill, [Bill 143 (2022–23)-EN]
700 Reuters, 'Britain to replace GDPR data privacy regime with own system' (3 October 2022): https://www.reuters.com/legal/litigation/britain-replace-gdpr-data-privacy-regime-with-own-system-2022–10-03/ [accessed 1 November 2022]
701 Letter from Julia Lopez MP to Chair (27 October 2022): https://committees.parliament.uk/publications/30543/documents/176142/default/

473. In addition, the Economic Crime and Corporate Transparency Bill has provisions for improving data-sharing:

- Clause 148 will enable businesses to share information more easily to prevent, investigate or detect economic crime by disapplying civil liability for confidentiality breaches where firms share information to prevent such crime. For example, this could happen when a bank has noticed an irregular transaction and wants to request more information from the other party. Subsection (4) sets out a warning condition to facilitate sharing in cases in cases where a bank wants to warn another about a customer if they have taken safeguarding action or would have done so in the case of a previous customer.[702]

- Clause 149 will enable information sharing via a third party intermediary akin to the Cifas National Fraud Database.[703] For example, a bank could do this when it has information about a customer whose account has been closed due to fraud concerns and wants to warn other banks of the risk of onboarding that person as a customer. [704]

- Clauses 145 and 146 will enable law enforcement to gather data more proactively by strengthening the powers of the NCA's Financial Intelligence Unit to obtain information from businesses relating to money laundering.[705]

474. We welcome these provisions in their ambition however, more needs to happen in order to enhance the benefits data sharing could bring. As they stand, we do not believe that the provisions go far enough to incentivise organisations to share information proactively. This is due to some of the other barriers previously set out around perceptions of GDPR. In addition, we recognise the challenges of data quality within institutions (which is not in scope of this Bill) and note a lack of regulatory incentive or obligation for data sharing.

475. We recognise the work of the regulators to do more on this front. The PSR's latest consultation sets out under Measure 2 plans to improve data sharing between PSPs. The PSR is working with UK Finance and Pay.UK to roll out rules and standards to allow PSPs to share real-time data by 2023.[706]

476. We also recognise the ICO's efforts to do more to encourage information sharing practices. The regulator is working on a programme in collaboration with the Home Office, UK Finance and nine banks to explore how information about customers that pose the highest financial crime risk can

---

702 Explanatory Notes to the Economic Crime and Corporate Transparency Bill [Bill 154 (2022–23)-EN]

703 HM Government, 'Fact sheet: Economic Crime and Corporate Transparency Bill overarching' (22 September 2022): https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/fact-sheet-economic-crime-and-corporate-transparency-bill-overarching [accessed 1 November 2022] and Home Office, 'Factsheet: Economic Crime and Corporate Transparency (ECCT) Bill' (22 September 2022): https://homeofficemedia.blog.gov.uk/2022/09/22/factsheet-economic-crime-and-corporate-transparency-ecct-bill/ [accessed 1 November 2022]

704 Explanatory Notes to the Economic Crime and Corporate Transparency Bill [Bill 154(2022–23)-EN]

705 House of Commons Library, *Economic Crime and Corporate Transparency Bill 2022–23*, Research Briefing CBP 9625, 7 October 2022

706 PSR, *Authorised Push Payment (APP) scams: Requiring reimbursement* (September 2022): https://www.psr.org.uk/media/kzlncenx/psr-cp22-4-app-scams-reimbursement-september-2022-v6.pdf [accessed 1 November 2022]

be shared more effectively so that other banks can review it.[707] However, we are concerned that the ICO is not using its enforcement powers to the best effect. Digital fraud often relies on the malignant abuse of personal data, for example through phishing, which is central to the ICO's purview. It must use its powers more frequently in order to hold data controllers to account.

477. Given the transnational nature of fraud, members of the Midlands Fraud Forum warned that until data and information is shared on a global basis, fraudsters will continue to get away with their crimes. Some participants suggested a global equivalent of Cifas should be created to allow for more international data sharing. There are mechanisms for sharing data with overseas law enforcement agencies. For example, the UK-US Data Access Agreement allows law enforcement directly to request data held by telecommunications providers in the other party's jurisdiction for the exclusive purpose of preventing, detecting, investigating and prosecuting serious crimes including terrorism and child sexual abuse and exploitation.[708]

478. The on-hold Data Protection and Digital Information Bill proposes new international alerting data sharing agreements and will set parameters for sharing of data between UK law enforcement and a third country.[709] While it is expected to "enable swift implementation of new international alerting data sharing agreements", we recognise that potential EU resistance to the measures, primarily based on concerns about adequacy of EU legislation, may hinder these ambitions.[710]

479. **While data protection regulations are not in themselves an inhibitor of information sharing in the pursuit of prevention and detection of fraud, they are perceived by some to be so. This perception has the effect of stifling or delaying the sharing of information that could support the fight against fraud. Information sharing is a critical component of the counter-fraud effort and must proactively be encouraged by regulators and legislation.**

480. ***The ICO must issue updated statutory guidance alongside an action plan to raise awareness of the provisions under the Data Protection Act 2018 and the new Data Protection and Digital Information Bill. The ICO must encourage a permissive attitude or 'safe harbour' about the sharing of data by the private sector for the purpose of preventing fraud.***

481. ***In the interests of greater transparency, The Data Protection and Digital Information Bill should be amended to include 'fraud' as a named crime under section 5(a).***

482. ***The Government should establish a regulatory obligation for regulated private sector organisations to share fraud risk data more regularly with law enforcement for the purposes of preventing fraud.***

---

707 ICO, 'Current projects': https://ico.org.uk/for-organisations/regulatory-sandbox/current-projects#financial-institutions [accessed 1 November 2022]

708 Home Office, 'Policy factsheet on the UK-US Data Access Agreement' (21 July 2022): https://www.gov.uk/government/publications/uk-us-data-access-agreement-factsheet/policy-factsheet-on-the-uk-us-data-access-agreement [accessed 1 November 2022]

709 Explanatory Notes to the Data Protection and Digital Information Bill [Bill 143 (2022–23)-EN]

710 *Ibid.*, and Pinsent Masons, 'UK Data Protection and Digital Information Bill: in detail' (20 July 2022): https://www.pinsentmasons.com/out-law/analysis/uk-data-protection-digital-information-bill [accessed 1 November 2022]

The Telecommunications (Security) Act 2021

483. The Telecommunications (Security) Act 2021 introduced a general duty for public electronic communications network and service providers to identify and reduce the risk of security compromises and prepare for their occurrence, as well as a duty on them to prevent, remedy or mitigate any adverse effects.[711] While we did not hear a great deal of evidence on the Act, we have considered how the Act due to its broad scope might be used as a vehicle for counter-fraud measures to be implemented.

484. The Act is directed primarily to cyber-security. Adrian Gorham told us that the Act was intended to address how networks are designed, built and operated so that they are more resilient and less prone to security incidents.[712] Hamish MacLeod emphasised the work being done by industry to make sure that the networks are "completely secure" from hacking and cyberattacks.[713]

485. Under the Act, providers of electronic communications networks or services must take appropriate and proportionate measures for the purposes of identifying and reducing the risks, and preparing for the occurrence, of security compromises. 'Security compromises' are defined broadly and include "any unauthorised access to, interference with or exploitation of the network or service or anything that enables such access, interference or exploitation".[714] This could be considered broad in scope to include fraud conducted by telephony, for example smishing.

486. The Minister for Tech and the Digital Economy told us that this option was "worth looking into".[715]

487. **The telecoms sector has for too long been allowed to stand by while fraud is facilitated via its services (see Chapters 2 and 3). While we have explored how the provisions and principles in the Online Safety Bill might apply to the telecoms sector, the Committee propose that any new legislation specifically targeted at the telecoms sector to tackle fraud could be introduced under the Telecommunications (Security) Act.**

488. ***The Government should consider how the Telecommunications (Security) Act 2021 might be used as means of introducing new measures to require the telecoms sector to clamp down on fraud taking place via its networks and services.***

Corporate criminal liability

489. While we recognise the work of coalitions of the willing such as Stop Scams UK, the Committee heard much evidence on the extent to which the private sector is not incentivised to act on fraud. We heard that for too many companies, fraud is seen as a 'cost of doing business'. Mark Fenhalls KC told us:

> "It is important when thinking about what fraud means to the public, the scale of it and where it is. In a sense, society as a whole has, over the past decade or more, tried to turn a lot of this into a cost of business. There

711 Telecommunications (Security) Act 2021
712 Q 237 (Adrian Gorham)
713 Q 50 (Hamish MacLeod)
714 Telecommunications (Security) Act 2021, section 1
715 Q 257 (Damian Collins MP)

> is a real issue for us as a society as to who we make the gatekeepers in relation to all these issues. Are we making them the companies, banks, building societies, tech companies? Where do we create liability for being the gatekeepers?"[716]

490. Some sectors are financially incentivised to act against fraud. As has been noted, the banking sector is responsible for reimbursing victims of fraud via the voluntary CRM Code. The industry finances the Dedicated Card and Payment Crime Unit, a specialist police unit, and several banks are also members of industry working groups including Stop Scams UK, which includes some telecoms and technology firms. TSB concludes that the financial services sector "has the right commercial and regulatory incentives to drive this kind of voluntary action."[717]

491. The FCA's New Consumer Duty has set clearer and higher expectations for firms' standards of care for consumers.[718] The duty includes rules that firms must avoid causing "foreseeable harm" to customers, including scams, and they will be required to communicate with customers so that they can make informed decisions about financial products.[719] TSB told us that a principles-based approach with "strong oversight and robust enforcement and penalties" in this area is a highly effective approach and should be extended to other fraud-enabling sectors.[720] However, the Transparency Task Force cautioned that the new Duty does not amount to a 'duty of care'.[721]

492. However, there are a wide range of sectors involved in the fraud chain, which begins further upstream than the point of payment. Telecoms services are one such sector. Their role in phishing, smishing and number spoofing has been discussed earlier in this report. While the Online Safety Bill is not the right vehicle to tackle fraud enabled via telecoms services, it is clear that the telecoms sector in particular present a lacuna in digital fraud prevention. Under the Bill, Ofcom will issue codes of practice recommending measures providers can take to comply with the Online Safety Bill and will be granted the power to fines online platforms or to block services that do not comply. Under new and separate legislation, similar principles could be extended to telecoms companies so that they are subject to the same duties to prevent fraud as online platforms.

493. The CCSG disagreed that more incentives needed to be levelled against telcos, arguing that "views that communications providers are incentivized commercially to deliver bulk inbound voice and messaging scams are, frankly, not correct." It noted that the profitability of telecoms companies depends on customer satisfaction, which in turn relies on providing services that are not polluted by scams.[722]

494. Yet, the Fraud Advisory Panel told us that more needs to be done to encourage businesses to do more to stamp out fraud at design stage:

---

716 Q 204 (Mark Fenhalls KC)
717 Written evidence from TSB (FDF0066)
718 FCA, 'CP21/13: A new Consumer Duty' (updated 27 July 2022): https://www.fca.org.uk/publications/consultation-papers/cp21-13-new-consumer-duty [accessed 1 November 2022]
719 FCA, *Finalised Guidance: FG22/5: Final non-Handbook Guidance for firms on the Consumer Duty* (July 2022): https://www.fca.org.uk/publication/finalised-guidance/fg22-5.pdf [accessed 1 November 2022]
720 Written evidence from TSB (FDF0066)
721 Written evidence from the Transparency Taskforce (FDF0092)
722 Written evidence from the CCSG (FDF0063)

> "We need to encourage businesses to do the right thing and design fraud out from their products and services before they bring them to market or face the risk of regulatory and enforcement action. Voluntary codes are not enough and do not work in a consistent or effective manner."[723]

495. Encouragement does not go far enough. We believe that real action will only be prompted if liability is imposed or increased on fraud enabling sectors, that are not taking sufficient steps to prevent fraud or tackle its consequences. There are two ways of achieving this: criminal offences and regulatory measures.

Failure to prevent offences

496. The Committee has taken evidence suggesting that the criminal law should be reformed to hold businesses to account more effectively rather than relying on regulatory punishments alone. Regulatory punishments may not be enough to act as a deterrent for the most egregious types of corporate wrongdoing.

497. The Law Commission recently consulted on the law relating to corporate criminal liability in instances where an employee or agent has committed fraud for the benefit of the company. In June 2022, the Commission suggested a range of options, which the Government is now considering.[724]

498. One of the options put forward includes extending failure to prevent offences to fraud as a strict liability offence covering a situation in which the company has failed to put in place measures to prevent employees or agents committing fraud for the benefit of the company. Corporates could defend themselves by proving that they had sufficient prevention procedures in place as was reasonable in the circumstances, or that it was reasonable not to have any procedures in place.[725] This approach has proven effective in other legislation, for example the Health and Safety at Work Act 1974.

Box 18: The Health and Safety at Work Act 1974

Health and safety legislation demonstrates the ways that strict liability duties can be used to best effect. The Health and Safety at Work Act (HSWA) 1974 is the main legislation governing health and safety in the workplace. It sets out employer and employee responsibilities as well as responsibilities for some self-employed people. Section 2(1) of the Act sets out that it is the general duty of employers to "ensure, so far as is reasonably practicable, the health, safety and welfare at work of all his employees". The main requirement on employers being to write and maintain a written policy for maintaining the health and safety of their employees is to have a risk assessment caried out of potential hazards that may cause harm (Section 2(3)).

723 Written evidence by the Fraud Advisory Panel (FDF0048)

724 Law Commission, *Corporate criminal liability: an options paper* (10 June 2022): https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/06/Corporate-Criminal-Liability-Options-Paper_LC.pdf [accessed 1 November 2022]

725 *Ibid.*

The Act imposes a strict liability on employers to do this. This means that if an employer does not carry out this duty of care, they are liable. If a company commits an offence under the Act, its directors can be prosecuted if that offence was due to their consent or connivance, or can be attributed to their neglect. They could face disqualification under the Company Directors Disqualification Act 1986.

This legislation, in particularly the statutory duty of care was used as a model during early consideration of the draft Online Safety Bill. William Perrin and Professor Lorna Woods of Carnegie UK, a trust focussing on improving wellbeing and tackling harms to collective wellbeing, developed an approach to harm reduction in social media based on a duty of care, in which they set out:

> "Duties of care set out in law 40 years ago or more still work well–for instance the duty of care from employers to employees in the Health and Safety at Work Act 1974 still performs well, despite today's workplaces being profoundly different from 1974's." [726]

Such an approach could clearly work in the case of digital fraud perpetrated by online platforms.

Source: Health and Safety at Work Act 1974, section 2

499. The extension of failure to prevent offences to fraud has precedent in other existing law, which provides for such offences for bribery and tax evasion:

- Under Section 7 of the Bribery Act 2010, if a person such as an employee associated with a commercial organisation commits an offence under the Bribery Act, the company will be liable and will only have a defence if it can show that it had adequate procedures in place to prevent bribery.[727]

- Under Part 3 of the Criminal Finances Act 2017, corporates can be prosecuted for failure to prevent the facilitation of tax evasion under two corporate criminal offences (domestic and overseas). Similar to the Bribery Act, organisations can defend themselves by proving that they had reasonable procedures in place to prevent the facilitation of tax evasion.[728]

The impact of failure to prevent on corporate behaviours

500. We heard support for an extension of the 'failure to prevent' model to fraud, including from key law enforcement agencies such as the NECC.[729] In written evidence, the CPS argued that such offences are a useful tool for prosecutors and ultimately help to drive better corporate behaviours.[730] Dr Susan Hawley said that "a failure to prevent offence would absolutely

726 Carnegie UK, 'Reducing harm in social media through a duty of care' (8 May 2018): https://www.carnegieuktrust.org.uk/blog-posts/reducing-harm-in-social-media-through-a-duty-of-care/ [accessed 1 November 2022]

727 Thomson Reuters Practical Law, 'Bribery Act 2010: corporate criminal liability: available at https://uk.practicallaw.thomsonreuters.com/5-505-3552 [accessed 1 November 2022] and Bribery Act 2010, section 7

728 Thomson Reuters Practical Law, 'Failure to prevent the facilitation of tax evasion: prevention procedures and policies': available at https://uk.practicallaw.thomsonreuters.com/w-010-3551 [accessed 1 November 2022] and Criminal Finances Act 2017, Part 3

729 Written evidence from the NECC (FDF0044)

730 Written evidence from the CPS (FDF0004)

transform this landscape", noting the impact of the Bribery Act on corporate behaviours.[731]. Mike Haley agreed, adding:

> "If there was a general duty on that organisation to do everything in its power to prevent fraud and economic crime, and to have a due diligence defence as there is under anti-bribery legislation, there would be some downside to enabling fraud. If I had one wish, it would be for that to drive the behaviours in the right way, as it has under anti-bribery and corruption."[732]

501. Mark Shelford suggested that this approach would have a positive impact on corporate behaviours within the tech sector. Asked for a single policy he would like to see taken forward, he said:

> "It would be a carrot and stick approach to the platforms. The carrot is working well right now, but the stick approach would be to consider revising current corporate criminal liability to include a new failure to prevent offences of economic crime, including money laundering and fraud."[733]

502. We also heard arguments against such an approach. For example, Karl Laird warned that big businesses would likely transfer the cost of compliance to customers.[734] He cautioned that expanding the model may result in the burden being felt most acutely by SMEs, which may not have the means to put in place sophisticated anti-fraud policies, and which may be considered 'low-hanging fruit' for prosecutors.[735] While we recognise these concerns and suggest that fines are proportionate to turnover, the evidence we have heard points to the beneficial use of failure to prevent offences in bringing about behaviour change, particularly within large companies.

503. Mark Fenhalls KC warned that we do not know how much the offence has impacted levels of bribery and cautioned against "legislating just for the sake of it".[736] RUSI's Kathryn Westmore's research shows that that the lack of prosecutions to date under the Criminal Finances Act calls into question the effectiveness of such offences, arguing that the corporate criminal offences legislation has ultimately been seen as a "damp squib". However, she recognises that such offences may be aimed more at changing corporate behaviours than securing convictions.[737]

504. Indeed, the Security Minister told us that behaviour change is often the primary aim of such offences and that they incentivise upstream changes rather than driving up prosecutions after an offence is committed. He said:

> "The Bribery Act, the Health and Safety at Work etc. Act and various other Acts have seen behaviour changes but not large numbers of prosecutions. We do not want a large number of prosecutions; we want the end of the behaviour that puts people at risk. "[738]

731 Q 89 (Dr Susan Hawley); written evidence from Spotlight on Corruption (FDF0053)
732 Q 16 (Mike Haley)
733 Q 221 (Mark Shelford)
734 Q 205 (Karl Laird)
735 *Ibid.*
736 QQ 206-7 (Mark Fenhalls KC)
737 RUSI, *Corporate Criminal Liability: Lessons from the introduction of failure to prevent offences* (30 September 2022): https://static.rusi.org/340_EI_Corporate Criminal Liability_Westmore_web_final.pdf [accessed 1 November 2022]
738 Q 265 (Tom Tugendhat MP)

Director liability

505. Some groups have gone further than seeking to encourage behaviour change by suggesting that senior directors should be held liable. The APPG on Anti-Corruption and Responsible Tax and the APPG on Fair Business Banking recommended a failure to prevent offence in their Economic Crime Manifesto.[739] The Chairs of the two APPGs reportedly are due to propose an amendment to the Economic Crime and Corporate Transparency Bill that would include corporate and director liability for failure to prevent fraud, similar to those that exist for bribery and tax evasion.[740]

506. Provision already exists in the Company Directors Disqualification Act (CDDA) 1986 to disqualify a director. A court can make a Directors Disqualification Order (DDO) where the defendant has been convicted of certain indictable offences in connection with the company. A DDO may follow a range of offences, not just fraudulent trading, including theft, insider dealing or deception. The offence does not need to have taken place within the company, it need not concern misconduct of the company's affairs or dishonesty, the defendant does not have to have been a director at the time of offending or at the sentencing hearing, nor does the defendant have to be a shadow director.[741]

507. Further, under Section 8 of the CDDA, the Secretary of State has the power to make an application to the Court for a disqualification order if it appears expedient in the public interest. The test for the Court is whether the director's conduct in relation to the company makes them unfit to be concerned in the management of a company. This civil route is separate to a DDO following a criminal conviction; however, a court will be reluctant to impose a director disqualification if an alternative court has refused to do so.[742]

508. The Minister for Tech and the Digital Economy told us that the Online Safety Bill includes the ability to take criminal sanctions against senior individuals for failure to comply with Ofcom's requests, for example for refusing to do a risk assessment, which are part of companies' obligations under the Act.[743]

Considerations for applicability of failure to prevent offences to fraud

509. While existing 'failure to prevent' offences present a useful model in designing an offence to prevent the facilitation of fraud, there are some core issues that need to be considered when considering digital fraud.

510. Under the Bribery Act, it must be proven to the criminal standard that bribery has occurred (i.e. an individual who has committed an offence must be identified, although a conviction is not required) before the offence becomes enforceable against a company. In the context of digital fraud, it may be difficult to identify an individual who has committed a fraud before pursuing a company. While it would be straightforward to prove loss to a customer

739 APPG on Anti-Corruption & Responsible Tax and the APPG on Fair Business Banking, *Economic Crime Manifesto* (May 2022): https://www.appgbanking.org.uk/wp-content/uploads/2022/05/Economic-Crime-Manifesto-1.pdf [accessed 1 November 2022]

740 'Directors face jail for fraud failings' *The Times* (17 October 2022) https://www.thetimes.co.uk/article/db11dfde-4d77-11ed-af60-3f894fe60060 [accessed 19 October 2022]

741 The test requires that the indictable offence must have some relevant factual connection with the management of the company (see *R v Creggy* [2008] EWCA Crim 394)

742 See *Secretary of State for Business, Innovation and Skills v Weston and another* [2014] EWHC 2933 (Ch))

743 Q 258 (Damian Collins MP)

or consumer, identifying a specific person responsible for that loss could be difficult. Further, proving that this specific unidentified individual was dishonest (the requisite *mens rea* for fraud) at the time of their actions could be more difficult again. For example, a technician sending bulk messages on behalf of his employer may unknowingly be assisting in perpetrating a fraud.

511. The Law Commission's proposal for corporate criminal liability has some merit but would only apply to fraud that benefits the company, rather than fraud facilitated by the company not for its own benefit. While this is akin to the approach taken in the Bribery Act, it differs from the approach taken in the Criminal Finances Act, which does not require the underlying tax evasion to have taken place for the benefit of the company. It is the Committee's view that any offence should be drafted broadly in line with the approach taken in the Criminal Finances Act. However, the Committee appreciates that regulatory options might provide an alternative way of achieving corporate criminal liability.

512. Therefore, the Committee have considered how an expanded offence, beyond that associated with an identified employee or agent committing a fraud, could concentrate on loss by the individual and/or harm to the consumer, rather than any specific fraud offence, to precipitate action against a company, without it being for the benefit of the company. This would encourage a company to proactively improve its practices so as to prevent the facilitation of fraud through the company, whether perpetrated by an employee or another.

A criminal 'failure to prevent the facilitation of fraud' offence

513. The Committee has considered how an expanded offence that covers the facilitation of fraud could be introduced. In October 2022, the Justice Committee recommended that a failure to prevent fraud offence should be introduced to encourage better corporate behaviours. However, it appeared to suggest that the offence should be expanded to failure to prevent the facilitation of fraud. It concluded:

> "A similar offence for failure to prevent fraud being perpetrated using a company's platforms would not only aid prosecution for these failures but focus private sector effort on designing fraud out of companies' systems."[744]

514. We recognise and endorse the need for the operators of platforms that facilitate fraud to be brought under legislation in order to prevent fraud, however we are mindful that additional regulation or legislation, such as that being introduced under the Online Safety Bill, may duplicate such an approach or create a risk of separate yet overlapping standards for companies in scope of both potential offences.

515. The former Minister for Tech and the Digital Economy Damian Collins told us that the Online Safety Bill would give the regulator the chance to analyse whether companies are putting in place the measures that they say they are, and how effective these measures are.[745] He told us that this translates to a failure to prevent the facilitation of fraud offence by proxy:

744 Justice Committee, *Fraud and the Justice System* (Fourth Report, Session 2022–23, HC 12)
745 Q 258 (Damian Collins MP)

> "If you look at the principles of the way the Online Safety Bill works, [failure to prevent] does apply. Companies will set out their policies. They have to try to get agreement with Ofcom that they have robust policies to do what they have all been asked to do. If they fail to fulfil those policies, either because they have not resourced them correctly or because they do not work as promised, there is a degree of liability for the failure to prevent something that was anticipated and known about, and the intervention could come. A company could be fined because it failed to put in a robust enough system and failed to do what it said it would do, and therefore is in breach of its obligations under the terms of the Bill as it currently stands."[746]

516. The regulatory approach may prove more effective. Due to the ability of regulators to move more swiftly than the criminal justice process, regulatory options can sometimes prove a more fruitful avenue to incentivise companies to act. Mark Steward told us that regulatory measures are often more effective than "white elephant offences that look good and sound good but cannot be prosecuted." He also said:

> "Practically speaking, it is the regulatory environment that is really able to react far more ably and nimbly. The regulatory environment can also change the rules far more easily as well. A statutory offence needs Parliament to change it if it does not work. That can be a long process."[747]

517. We recognise that there are multiple instances of potentially criminal action being caught by different criminal offences, for example fraudsters can be prosecuted under the Fraud Act 2006 and the Computer Misuse Act 1990. We also recognise that individuals and companies can be covered by more than one regulator, such as the FCA and the CMA. Many regulators have both criminal and regulatory powers. For example, Ofcom has powers under the Communications Act 2003 to require information from providers under Sections 135 and 136. Under Section 138, Ofcom can issue a notice if there is reasonable grounds to believe that these requirements have not been complied with, and a penalty can be issued under 139 for failing to comply with a notice. In addition, under Section 144, Ofcom can issue a fine or imprisonment for false information given under Section 135 and 136.[748] This is an example of the regulatory and criminal power of regulators working in tandem. In this instance, we feel that the powers in the Online Safety Bill are sufficient to effectively encourage companies in scope to introduce measures to prevent the facilitation of fraud.

518. However, due to the lacuna for telecoms companies and ISPs under the Online Safety Bill, the Committee also considered whether a regulatory duty to prevent the facilitation of fraud, applied more widely, could be effective. We considered the extension of existing regulatory regimes such as bolstering Ofcom's General Conditions to deliver more scrutiny of telecoms companies measures to prevent fraud. However, this relies on rigorous enforcement. We also considered whether the Online Safety Bill could be extended to cover telecoms companies, however we felt this option would overcomplicate already extensive legislation. Finally, we considered introducing the duty via new legislation such as the Digital Markets, Competition and Consumer Bill, which could clarify the CMA and/or Digital Markets Unit's regulatory

746 Q 265 (Damian Collins MP)
747 Q 155 (Mark Steward)
748 Communications Act 2003, sections 135–144

perimeter to explain that platforms have a consumer duty to prevent economically harmful material from appearing on their sites, and will be fined if they do not.[749]

519. We have weighed the evidence carefully and consider that introducing additional regulatory requirements at a time when the Online Safety Bill's sweeping reforms are being introduced may result in not only confusion for companies seeking to comply with multiple forms of overlapping regulation but also may result in a 'race to the bottom'. Therefore, we believe that a criminal offence of 'failure to prevent fraud', combined with the powers introduced via the Online Safety Bill, is the best option to engender effective change swiftly.

520. **Many private sector companies consider fraud as a cost of doing business and are not doing enough to stop fraud from being facilitated by their services. Some sectors have less liability for fraud than others and are not held to account effectively for their role in facilitating this crime. We recognise that the role of failure to prevent offences is primarily to inspire behaviour change rather than criminal prosecutions. Corporate irresponsibility will not change until businesses feel the financial impact of liability coupled with reputational damage. It is time for less carrot and more stick. However, we are conscious to avoid regulatory overlap and it is clear that the Online Safety Bill will go some way to meeting some of these ambitions for tech platforms. We remain concerned that there is a lacuna for telecoms companies and ISPs who do not and will not face the same penalties. Equivalent measures should be introduced for these fraud enablers.**

521. ***To inspire behaviour change, we agree with the Justice Committee and others who are calling for the Government to introduce a new corporate criminal offence of 'failure to prevent fraud', accompanied by significant financial penalties, to hold corporates across all sectors to account and to inspire behaviour change. The Government must make it clear that a range of other measures, such as director disqualification, are ready to be enforced if culture change is not forthcoming.***

522. ***To make telecoms companies more accountable for the fraud facilitated via their services, the Government should introduce a systems-led regulatory strategy equivalent to the Online Safety Bill that is directly applicable to telecoms platforms and services. This would comprise an equivalent regulatory duty to prevent the facilitation of fraud. Amending the Telecoms (Security) Act may be an avenue through which to achieve this.***

749 BEIS, 'New rules to protect consumers' hard-earned cash' (20 April 2022): https://www.gov.uk/government/news/new-rules-to-protect-consumers-hard-earned-cash [accessed 1 November 2022] and HM Government, *The Queen's Speech 2022* (10 May 2022): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1074113/Lobby_Pack_10_May_2022.pdf [accessed 1 November 2022]

Regulatory options

A duty to report fraud

523. The Committee has considered the extent to which the introduction of a duty on corporations to report fraud might support efforts to tackle it. Since 2013, Ofcom and the ICO have voluntarily reported the number of complaints that they receive relating to nuisance, spam or scam calls alongside a joint action plan. While welcome activity, we do not consider that this goes far enough towards imposing a general 'duty to report' on all fraud-enabling sectors.

524. Forthcoming legislation will require telecoms providers to report suspicious traffic on their networks. Under Clause 85 of the Data Protection and Digital Information Bill, providers of public electronic communications services must report suspicious traffic to the Commissioner within 28 days. This relies in large part on the contravention of direct marketing regulations. ICO guidance on Direct Marketing references statutory provisions including the Consumer Protection from Unfair Trading Regulations 2008, which prohibits unfair, misleading or aggressive marketing practices.[750] This would encompass "false representations" sufficient to fall within the definition contained within sections 1 and 2 of the Fraud Act 2006.[751] Whether this duty is considered equivalent to a duty to report fraud may rely on the interpretation of the ICO. It does not go far enough to incentivise action to tackle the actor carrying out such activity in addition to notifying the Commissioner. The ICO should issue guidance on the requirement and highlight subsequent action to be taken in order to increase the efficacy of this measure.

525. While efforts are ongoing to increase the extent to which telecoms providers are responsible for reporting suspicious activity, we recognise a greater need for all organisations that play a role within the fraud chain, including online platforms and ISPs, to report the volume and type of scams reported to and identified on their platforms. This would support efforts to analyse trends and enable a swifter response.

526. **It is clear to this Committee that there is a need for greater onus to be placed on private companies in fraud enabling sectors to report publicly and to the authorities the fraud that they detect on their platforms in order to increase transparency about which platforms are failing to stamp out fraud on their services.**

527. ***All fraud-enabling sectors, including tech, telecoms and ISPs, must be subject to a 'duty to report' requiring them to share details of fraud reports with law enforcement and regulators, as well as to display publicly these figures alongside rates of reimbursement as soon as possible. The Government should explore the use of league tables to encourage competition and consumer choice. The ICO must issue clear guidance for businesses on how to comply with Clause 85 of the Data Protection and Digital Information Bill to enable the reporting of suspected fraudulent communications.***

750 ICO, *Direct marketing*: https://ico.org.uk/media/1555/direct-marketing-guidance.pdf [accessed 1 October 2022]

751 Fraud Act 2006, sections 1 and 2

The Online Safety Bill

528. At the time of writing, the Online Safety Bill's passage through Parliament has been delayed as it is being revised by the Government. We understand that this process largely will be about reconsidering the provisions relating to 'legal but harmful' content, and will not affect the measures in Chapter 5 of the Bill about paid-for online advertising.[752] The Committee has considered the Online Safety Bill in its current form.[753] The former Minister for Tech and the Digital Economy Damian Collins told us that the Bill would be reintroduced to Parliament "soon".[754]

529. Our conclusions on the Online Safety Bill's capacity to introduce a regulatory failure to prevent duty on in-scope companies has been explored at paragraph 496. While we consider that the Bill will introduce a range of effective measures to hold tech platforms to account for their record on fraud, we believe that there are parts of the Bill that could be tightened in order to protect the public from fraud.

Fraudulent advertising

530. In Chapter 2, we discussed the threat of fraudulent advertising, including the measures being proposed in the Online Safety Bill to tackle this activity. Initially, search engines were only required to 'minimise' the risk of fraudulent advertising appearing, and we are pleased that the Government listened to arguments from industry that platforms such as Google should face the same demands as social media platforms to prevent fraudulent material.[755]

531. It is unclear how quickly online services could remove fraudulent adverts in satisfaction of the demands of the Online Safety Bill. Under clause 34 (1), Category 1 firms must put in place proportionate systems and processes to "swiftly remove" fraudulent advertising once they are made aware of it.[756] Philip Milton told us that it takes between 24 to 48 hours to review possibly harmful content after it has been flagged to the company. He recognised that due to the deceptive nature of fraudulent advertising, Meta's systems do not always recognise that advertising is fraudulent and therefore, take down rates would be variable.[757]

532. In addition, the Transparency Task Force argued that measures to prevent fraudulent advertising should also apply to advertising that is not paid-for. This might include 'organic' content posted by influencers who are not being paid directly for promoting the product.[758] Joe Lycett told us that "unfortunately a lot of influencers get caught up in promoting products that do not work or sometimes do not even exist."[759] We recognise that this area is

752 See Insurance Times, 'Changed government should not impact counter fraud elements of Online Safety Bill' (13 September 2022): https://www.insurancetimes.co.uk/news/changed-government-should-not-impact-counter-fraud-elements-of-online-safety-bill-ofcom/1442322.article [accessed 1 October 2022].

753 DCMS, 'Online Safety Bill: Factsheet' (updated 19 April 2022): https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet [accessed 1 October 2022] and House of Commons Library, *Analysis of the Online Safety Bill*, Research Briefing CBP 9506, 8 April 2022

754 Q 259 (Damian Collins MP)

755 Written evidence from UK Finance (FDF0058) and Carnegie UK (FDF0060)

756 House of Commons Library, *Analysis of the Online Safety Bill*, Research Briefing CBP 9506, 8 April 2022

757 Q 136 (Philip Milton)

758 Written evidence from Transparency Task Force (FDF0092)

759 Q 92 (Joe Lycett)

complex to regulate. Elizabeth Kanter told us that TikTok operates a varied approach to monitoring crypto-related ads:

> "It would depend on whether it was branded content and they had been paid by a crypto company; that would not be allowed. On the organic side, a user can talk about crypto. We prevent content that tries to inflate or promote a get-rich-quick scheme or an inflated lifestyle, but it is a very nuanced area …"[760]

533. This is a complex area and one that the Online Advertising Programme may address (see paragraph 125).

Platform categorisation

534. Under Schedule 7 of the Online Safety Bill, fraud is priority illegal content. Under Clause 9(3), all user-to-user services must prevent users from coming across such content, minimise the length of time it appears where present, and remove it when it is alerted to it or becomes aware of it. All services must also do risk assessments for illegal content under Clause 8.[761]

535. Clauses 34 to 36 include separate duties on fraudulent advertising for large (Category 1) platforms and search engines (Category 2A). These services have to take steps to prevent paid-for fraudulent adverts appearing on their services, minimise the time that it is present, and swiftly remove it once they are made aware of it.[762]

536. Damian Collins told us that the onus on all platforms to remove fraud is clear in the Online Safety Bill:

> " … this is priority illegal activity, so all the companies in scope are expected to demonstrate to Ofcom the systems they have in place to readily identify frauds and scams as they exist on their own platforms but also through advertising in order to prevent the purchasing of advertising on their platforms as well. These are proactive obligations, so as part of their response to the risk assessments that Ofcom will create, the companies have to demonstrate through the codes of practice what their policies will be."[763]

537. However, we have heard several concerns about the approach to categorisation in the Online Safety Bill regarding fraudulent advertising. We have heard that the size of platforms should not be the only factor in the Bill's application given the importance of platform characteristics and their exposure to different types of risk. Scam ads are prominent across a range of online platforms and services and have the potential to expand further as technologies develop.

538. Carnegie UK argued that the category model is unjustified given the "significance of the harm felt by a fraud victim regardless of platform".[764] The list of qualifying companies in each category is yet to be developed under secondary legislation. Carnegie UK called for all companies to operate systems to mitigate fraudulent advertising. It wrote:

---

760 Q 136 (Elizabeth Kanter)
761 Online Safety Bill, Schedule 7; clause 9(3); clause 8
762 Online Safety Bill, clauses 34–36 and House of Commons Library, *Analysis of the Online Safety Bill*, Research Briefing CBP 9506, 8 April 2022
763 Q 258 (Damian Collins MP)
764 Written evidence from Carnegie UK (FDF0060)

> "Rules will only apply to services defined by the government as 'Category 1' or 'Category 2A'—which currently excludes the smaller, 'user-to-user' websites that host adverts … There is a risk that scammers will target consumers through paid-for content on these sites. The new fraudulent advertising powers should apply evenly to all regulated user-to-user companies and be just as strong and systemic as those for illegal content."[765]

539. Furthermore, the Committee are persuaded by the evidence that the Online Safety Bill may lead to fraudsters diverting their tactics to other platforms not covered by the Bill.[766] UK Finance warned that smaller websites and platforms may be targeted as a result of the measures.[767] Markko Künnapu told us that the impact of the EU's Digital Services Act, which has broadly similar aims to the Online Safety Bill, could result in criminals shifting towards smaller, out-of-scope platforms. Künnapu said:

> "The situation could change and criminals could move from larger to smaller platforms. This forum shopping is not new. There is a serious concern that smaller platforms could be exploited by criminals in the future."[768]

540. Damian Collins defended the categorisation in evidence to this Committee. He said:

> " … the highest level of risk is probably found on the biggest platforms with the greatest number of users, so that is where the greatest amount of harm can occur. Nevertheless, for the worst kind of activity, the most risky activity, those legal responsibilities still apply to everyone else, so that balance is probably the correct one."[769]

541. The Online Safety Bill must go further to tackle fraudulent ads wherever they appear online by adopting a risk-based approach, ensuring all platforms regardless of size or function take steps to prevent fraudulent advertising. It should include a duty for tech platforms of all sizes to assess the risk of users encountering fraudulent advertising on their sites.

Intermediary platforms

542. Intermediary platforms are platforms, businesses or services that connect buyers and sellers. They often leverage data to provide buyers with targeted options for online advertising.[770] Examples might include home rental platforms like Airbnb or job websites. The status of intermediary platforms like Airbnb and job sites under the Online Safety Bill remains unclear.

543. Andrea Garcia Rodríguez, lead digital policy analyst at the European Policy Centre, identified a pan-European increase in intermediary platform usage. She said: "Europe has seen more and more users using online platforms as

765 *Ibid.*
766 Q 176 (Markko Künnapu), written evidence from UK Finance (FDF0058) and Carnegie UK (FDF0060)
767 Written evidence from UK Finance (FDF0058)
768 Q 176 (Markko Künnapu)
769 Q 259 (Damian Collins MP)
770 DCMS, 'Online Advertising Programme consultation' (6 June 2022): https://www.gov.uk/government/consultations/online-advertising-programme-consultation/online-advertising-programme-consultation [accessed 1 November 2022]

intermediaries for their everyday lives… We should do something to prevent illegal activity happening in these platforms … "[771]

544. We have heard that these sites often shirk responsibility for facilitating fraud.[772] Joe Lycett told us that intermediary platforms often try to abdicate their responsibility for facilitating fraudulent material. He said:

> "By that I mean your social media platforms and businesses like Airbnb, but there are lots of businesses like that which are offering an intermediary to a service. They have definitely improved, but a lot of the time they go, 'It's nothing to do with us. We've just offered the platform on which you meet and find these businesses, and if you get scammed it's nothing to do with us'."[773]

545. We understand that the Government intends to address this through the Online Advertising Programme and urge it to take decisive action to tackle fraudulent material that appears on these sites (see paragraph 125).

The role of the regulators

546. If the Online Safety Bill is passed, Ofcom will be responsible for issuing codes of practice to help services to meet their new obligations. Once passed into law, fraudulent advertising regulation will be shared between the ASA and Ofcom and the terms of this relationship, as well as that with other regulators, must be clearly explained to avoid regulatory gaps.

547. It is clear that regulators such as Ofcom will play a key part in the Online Safety Bill, however given the complexity of the internet ecosystem, other regulators such as the FCA, the ASA and the CMA may also play a role (see Table 3). This may lead to regulatory under- or overlap that can be exploited by fraudsters. Mark Steward told us:

> "From a regulatory perspective, everybody has to fit within their statutory remits. Those remits do not always align. There are gaps and there is no overarching regulatory architecture, which we all belong to. That has particular resonance when we consider the issue of fraud, because we know fraudsters are great innovators; they look for these gaps to exploit them."[774]

Table 3: Key regulators involved in the fraud chain

Regulator	Remit
Financial Conduct Authority	Regulates the financial services industry. Its remit doesn't cover sectors further up the fraud chain such as telecoms firms. It applies regulations via rules and can enforce via warning notices and fines.
Payment Systems Regulator	Regulates payment systems including bank transfers and contactless payments.

771 Q 172 (Andrea Garcia Rodríguez)
772 Q 96 (Joe Lycett) and written evidence from Cifas (FDF0015)
773 Q 96 (Joe Lycett)
774 Q 146 (Mark Steward)

Regulator	Remit
Ofcom	Regulates the communications industry and applies regulations via rules, codes and fines. It operates by General Conditions.
Competition and Markets Authority	The CMA is the competition watchdog. It has powers to fine companies for anti-competitive practices and has a role to protect consumers.
Information Commissioner's Office	The ICO regulates data controllers. It applies regulations via principles and gives out declarations, advice and fines.

548. For example, the FCA recently set out its support for the measures in the Online Safety Bill to tackle fraudulent online advertising. Richard Lloyd, interim Chair of the FCA said in October 2022 that "it simply can't be right for massive global online platforms to have no responsibility in law to stop criminals paying for adverts on their sites to defraud innocent people".[775]

549. Given the complexities of the regulatory landscape, it is necessary for regulators to work together to prevent gaps from being exploited. The Digital Regulation Cooperation Forum (DRCF) was established in July 2020 by the CMA, ICO, Ofcom and the FCA. The House of Lords Communications and Digital Select Committee recommended in 2021 that the forum should be placed on a statutory footing and membership should be increased to other regulators and agencies with interests and expertise in the sector.[776] While the Forum works with other regulators such as the Prudential Regulation Authority (PRA) and the PSR, Elizabeth Kanter suggested that its scope might be broadened to include law enforcement agencies such as the NECC and NCA.[777]

550. The Committee has heard positive evidence on the role of the Forum. Mark Steward told us that the forum is making progress on tackling illegal financial promotions and added that "there is an enormous amount of goodwill to try to get things done together".[778]

551. Carnegie UK have recommended that the Online Safety Bill is amended to include a requirement on Ofcom to define the terms of its relationships with other regulators and, in order to encourage joined-up working, Professor Lorna Woods recommended that the Bill should include powers to enable them to work together more effectively.[779] Prof Woods cautioned that forums for cooperation must lead to tangible outcomes:

> "When we are talking about co-operation, are we talking about just a general talking shop, future scanning, and trying to understand the

775 FCA, 'Richard Lloyd: APM opening remarks 2022' (12 October 2022): https://www.fca.org.uk/news/speeches/richard-lloyd-apm-opening-remarks-2022 [accessed 1 November 2022]
776 Communications and Digital Committee, *Digital regulation: joined-up and accountable* (Third Report, Session 2021–22, HL 126)
777 See CMA, Digital Regulation Cooperation Forum: Plan of work for 2021 to 2022 (10 March 2021): https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-202122/digital-regulation-cooperation-forum-plan-of-work-for-2021-to-2022 [accessed 1 November 2022] and Q 145 (Elizabeth Kanter)
778 Q 146 (Mark Steward)
779 Q 56 (Prof Lorna Woods) and written evidence from Carnegie UK (FDF0060)

issues at a general level, or are we looking at a much more granular level of co-operation, even file sharing."[780]

552. Such a move would have precedent given the Digital Markets Unit will have a statutory duty to consult with other regulators under legislation expected to be brought forward in the Draft Digital Markets, Competition and Consumer Bill, which will be published when parliamentary time allows.[781]

553. In addition, there is a need for regulators to work with overseas agencies to tackle international threats. The US Federal Trade Commission (FTC), an independent law enforcement agency and primary consumer protection agency for the US, told us that it cooperates with regulators regularly. It entered into a memorandum of understanding with the ICO in 2014, and a further MOU was signed with the CMA in 2019 to strengthen cooperation on consumer protection matters, including fraud. International agencies also work together through groups such as the International Consumer Protection Enforcement Network.[782] We hope Ofcom will give due consideration to international cooperation with other regulators in light of the global challenge of online fraud.

Identity verification

554. Under the Online Safety Bill, Category 1 companies have to ensure that adult users are given the option to verify their identity. While we do not advocate for all platforms of all sizes to mandate that users of the internet should verify their identity, it is clear that some platforms, such as dating apps, are more susceptible to identity fraud and therefore users must be protected by putting such measures in place.

555. Issues about romance fraud and identity verification on dating platforms have been explored at greater length in paragraph 103.

Use of fines

556. Under the Online Safety Bill, Ofcom will be granted the power to block services that do not comply or issue fines of up to £18 million (or 10% of global annual turnover).[783]

557. We know that law enforcement to tackle fraud is significantly under-resourced and the Economic Crime Levy will not be used to tackle fraud. Given this, the Government should consider reinvesting fines levelled as a result of action taken under the forthcoming Bill to support law enforcement activity.

558. **The Committee welcomes the ambition of the Online Safety Bill with respect to its systems-led approach to tackling fraud as priority illegal content. The Government must urgently reintroduce the Online Safety Bill to Parliament. However, to maximise its potential**

780 Q 56 (Prof Lorna Woods)

781 BEIS and DCMS, 'A new pro-competition regime for digital markets: government response to consultation' (6 May 2022): https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets/outcome/a-new-pro-competition-regime-for-digital-markets-government-response-to-consultation [accessed 1 November 2022] and Commons written answer. UIN 59784, Session 2022–23

782 Written evidence from the US Federal Trade Commission (FDF0093)

783 House of Commons Library, *Analysis of the Online Safety Bill*, Research Briefing CBP 9506, 8 April 2022

to reduce levels of online fraud, we consider that several amendments to the Online Safety Bill must be made.

559. ***The Online Safety Bill must make it explicit that all platforms regardless of size or function should be required to take measures to prevent fraudulent advertising from appearing on their sites to ensure a risk-based rather than size-based approach.***

560. ***This should include a duty of care for all platforms to stop fraudulent advertisements or content appearing on their platforms and to take steps to build in counter-fraud measures at design stage.***

561. ***Given that the Online Safety Bill does not effectively tackle intermediary platforms, the Online Advertising Programme must be expedited to avoid a surge in fraud on these platforms and include a plan to comprehensively tackle fraud.***

562. ***The Online Safety Bill should include a requirement on Ofcom to define the terms of its relationships with other regulators and include powers to enable them to work effectively together, including through information sharing.***

563. ***To ensure regulatory cooperation, we are in agreement with the Joint Committee on the Online Safety Bill and the House of Lords Communications and Digital Committee that the Government should place the Digital Regulation Cooperation Forum on a statutory footing with a remit to engage in forward-looking horizon scanning, to hold the various regulators to account and to compel regulators to work effectively together. Its membership should be broadened to include the PSR, and law enforcement representation such as the NCA.***

564. ***The Government should consider reinvesting fines levelled as a result of action taken under the Online Safety Bill to support law enforcement activity.***

565. ***As an additional element of digital regulation, the Government must urgently bring forward the Draft Digital Markets, Competition and Consumer Bill to bolster protection for consumers.***

SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

The inbound route

1. Phishing and smishing techniques are among the most prolific business models operated by fraudsters. Sending scam emails and texts is a simple and effective tactic, conductible speedily and in volume. While steps have been taken by telecoms companies to prevent such tactics, fraudsters continually evade these efforts and exploit new avenues to reach victims. The Committee believes much swifter and firmer action by telecoms companies needs to be taken to reduce the quantity of fraudulent communications slipping through the net. Ofcom has a broad remit and increasing powers. The level of accountability for Ofcom's regulation of telecoms companies must therefore increase accordingly. (Paragraph 93)

2. *Ofcom must carry out a comprehensive assessment of telephony fraud in order to tackle the worrying information deficit on the scale of the problem. It must bolster its use of, and report on how often it uses, its enforcement powers to hold telecoms and tech companies to account for telephony-based scams. For example, it should report the frequency with which it has used its General Conditions to request that numbers are blocked due to fraudulent activity being detected. It should publish this information as part of an annual fraud report presented to Parliament.* (Paragraph 94)

3. *The ever-increasing role and powers of Ofcom and wider digital regulation should be subject to enhanced parliamentary scrutiny. We add our voice to that of the Communications and Digital Committee in supporting the recommendation of the Joint Committee on the Online Safety Bill that digital regulation requires dedicated parliamentary oversight and therefore a Joint Committee of both Houses should be established to perform this role.* (Paragraph 95)

4. *In addition, we suggest that Ofcom should face further oversight as part of wider scrutiny of the DRCF (see paragraph 563) and that Ofcom should be part of the NECC (see paragrpaph 284).* (Paragraph 96)

5. Online dating is now a common means by which many seek to meet new people. Easy access to potentially vulnerable, isolated or lonely people makes these platforms prime targets for exploitation by fraudsters. Furthermore, as continued technological developments proliferate, fraudsters will find new ways to perpetuate false identities online. We are aware of the wider privacy issues surrounding debate on identity verification, particularly in light of the Data Protection and Digital Information Bill, and consider that further exploration of this issue is needed; therefore, we will not make a recommendation on this issue more widely. However, in the context of online dating it is clear that identity verification is a crucial first step in stamping out romance fraudsters. (Paragraph 110)

6. *The Online Safety Bill must be amended to ensure that dating platforms are subject to mandatory identity verification processes in order to establish that their users are genuine.* (Paragraph 111)

7. *As part of platforms' efforts to design-out fraud (see paragraph 131), online dating platforms must be required to implement checks such as proactively deploying reverse image search, rather than placing the onus on users to do so.* (Paragraph 112)

8. Online advertising is a favoured tool in the fraudsters' toolkit. Scam ads are prominent across a range of online platforms and services and have

the potential to expand further as technologies develop. We welcome new legislation to try to tackle this issue via the Online Safety Bill and Online Advertising Programme, but regulations must go further to ensure that the full suite of tools are used to tackle fraudulent ads wherever they appear online. Recommendations relating to the Online Safety Bill are contained in Chapter 6. (Paragraph 130)

9. *The Government should ensure that the terms and conditions of all social media platforms expressly prohibit fraudulent user-generated content and advertising and that platforms should be held accountable for all fraudulent material that appears thereafter. We urge Meta and other large social media companies to take action more quickly and ensure that safety is considered at design level in all future product developments.* (Paragraph 131)

10. *By Autumn 2023, all online platforms including Meta should be mandated to only allow online adverts for financial services from companies authorised by the FCA. Financial promotions should not carry the words 'FCA authorised' unless they are authorised for the specific activity or product advertised. The FCA should strive towards enforcing this principle of specificity more widely in future.* (Paragraph 132)

11. While digital fraud is increasing, 'analogue' approaches continue to be used by some fraudsters to target victims, particularly those who are digitally excluded. The local policing model has some value in supporting these vulnerable individuals and should be kept in these cases. (Paragraph 137)

12. *The Government's forthcoming Fraud Strategy should not ignore the threat of 'analogue' fraud as well as focussing on the increasing risk of digital fraud. Counter-fraud strategies should be varied to tackle analogue tactics including leafletting and door-stepping, and it must support those who are typically targeted by them.* (Paragraph 138)

Interaction

13. Number spoofing is fundamental to convincing victims that they are being contacted by a genuine, trusted authority. We endorse the valuable work being undertaken by Ofcom and the industry to tackle number spoofing, however efforts to address CLI spoofing must not be watered down or delayed. (Paragraph 158)

14. *Ofcom must expedite its work on number spoofing. It must ensure that technologies that prevent CLI abuse are rolled out as soon as possible, and take all available steps to require the mandatory use of these technologies immediately when possible. Updates to the core network should be made urgently to stamp out fraud, ideally prior to 2025. Where such reasonable steps are not taken, companies must face penalties.* (Paragraph 159)

15. *Companies should phase out the process of identifying consumers via telephone by confirming personal information with them. A more effective solution to this requirement must be sought.* (Paragraph 160)

16. Social engineering is a cruel tactic used by fraudsters to manipulate their victims. It has longstanding impacts on victims, who may find it difficult to trust organisations in future because of the tactics used by fraudsters to manoeuvre them into the 'hot state' in which they make a payment. (Paragraph 170)

17. *Financial institutions, whether banks or building societies, must be encouraged to participate in the 159 initiative, and should be mandated to provide information on the service to their customers if the initiative is extended beyond pilot stage.* (Paragraph 171)

18. Fraudulent websites have become a common means by which fraudsters can convince their victims that they are interacting with a genuine organisation or authority. At present, it is too easy to set up a spoof website. Domain hosts and ISPs have been left out of the debate on how to tackle fraud. This oversight has left them without due scrutiny. These services must be subject to the same stringent counter-fraud controls that should apply across the board. (Paragraph 187)

19. *The Government must clarify within whose regulatory perimeter domain hosts and other ISPs sit and explore whether bringing this issue within Ofcom's regulatory remit would materially benefit its counter-fraud function. The responsible regulator should consult on new regulations requiring domain name providers to enforce greater KYC checks on those registering domain names, and on codes of practice to establish protocols that prohibit domains from being used if it is believed that the intention is to deceive users.* (Paragraph 188)

20. *The Government must expedite the forthcoming Tech Sector Charter and include ISPs within its scope.* (Paragraph 189)

Cashing out

21. The speed with which payments are able to be executed, while beneficial for legitimate customers, is helping fraudsters to get their hands on stolen money at pace. Current provisions in place to help to prevent fraud are welcome but must be strengthened to stop payments reaching fraudsters before they are able to cash out stolen money. (Paragraph 228)

22. *To stop fraudulent payments slipping through the net, the speed with which certain payments can be made should be subject to a delay lasting no more than several hours. This might include high-value payments made by personal customers to new payees, with an option to extend this to existing payees in the case of high-value payments. The PSR should consult with industry on the introduction of such a measure and the value threshold to be set. Implementation of this measure must not impact the application of other measures such as AI-assisted transaction monitoring.* (Paragraph 229)

23. *Approval of a banking and/or e-money licence in the UK must be made conditional upon signing up to Confirmation of Payee.* (Paragraph 230)

24. *The Banking Protocol should be made mandatory and expanded to telephone and online banking. Banks should be required to provide more training to ensure compliance and to help staff to spot 'red flags'.* (Paragraph 231)

25. *The FCA should conduct a thematic review of retail banks to understand how easy it is for fraudsters to open accounts and consult with industry on the possible solutions, including potential reforms to AML procedures. It should encourage the regular stress-testing of KYC procedures in order to address emerging threats such as deepfake technology.* (Paragraph 232)

26. *The FCA and PSR should work with PSPs to increase transparency and customer understanding about measures in place to prevent fraud, including possibly slowing the*

pace of transactions and KYC checks. This work should feed into the Government's centrally led public awareness campaign (see paragraph 418). (Paragraph 233)

27. Alongside the threat of cryptoasset investment scams, cryptoassets are increasingly being used by fraudsters to syphon off their stolen funds, allowing them to disappear without trace. Regulators must focus more tightly on the 'on and off-ramps' that facilitate the transfer of funds from traditional banks into and out of crypto-based wallets. Regulators must use their existing powers to tackle this challenge and support the work of the global regulatory community as it continues to create an aligned approach to cryptoasset regulation. (Paragraph 248)

28. *The Government should work with the private sector to integrate better KYC checks into the cryptoasset account set-up process. This should include designing systems that ensure cryptoassets and crypto-wallets can be traced to an identified individual.* (Paragraph 249)

29. *HM Treasury should urgently bring forward the measures in the Financial Services and Markets Bill to enable the FCA to regulate cryptoassets, as well as its forthcoming consultation on other types of cryptoassets.* (Paragraph 250)

30. *The Home Office should urgently bring forward measures in the Economic Crime and Corporate Transparency Bill to allow the seizure of cryptoassets using civil recovery powers as well as the existing criminal powers.* (Paragraph 251)

31. Money muling is a serious form of money laundering, yet not enough people are alert to the dangers and risks that can follow from allowing their bank account to be used to launder the proceeds of crime. The Committee is concerned that cost of living pressures could force more people from a range of demographic groups towards money muling. (Paragraph 262)

32. *Building on the work of Cifas and UK Finance, the Government should roll out a national campaign in partnership with schools and universities focussed on raising awareness of the dangers of money muling. It should also consider awareness campaigns for demographic groups that are not typically targeted by mule herders.* (Paragraph 263)

33. *In partnership with industry, the Government must explore the functionality of a mechanism akin to Confirmation of Payee that alerts a payee about the dangers of money muling and requests authorisation when they receive a payment from an unknown bank account.* (Paragraph 264)

The Government response to fraud

34. We welcome the re-launch of the Joint Fraud Taskforce and other public-private forums for discussion and cross-sector information sharing. However, we remain concerned that these bodies remain voluntary 'talking shops' and do not maximise their potential for effective leadership in the counter-fraud landscape. While we recognise the merits of appointing a sole point of accountability, this is challenging given that fraud sits across departmental boundaries. We do not wish to add more acronyms to the alphabet soup of stakeholders responsible for economic crime, however it is clear the current approach is not working. Fraud is a national risk and must be treated as a national priority. (Paragraph 282)

35. *The Government should bring forward the Economic Crime and Corporate Transparency Bill to ensure that Companies House becomes a more active and*

transparent gatekeeper of company information to protect consumers. Companies House must be provided with appropriate resources to achieve the ambitions set out in the Economic Crime and Corporate Transparency Bill. (Paragraph 283)

36. *Membership of the NECC should be broadened to include Ofcom given its remit for digital communications and the rapid increase in fraud by exploitation of digital communications. In addition, we recommend that the NCA join the DRCF (see recommendation 86).* (Paragraph 284)

37. *The NCA must treat fraud as a crucial part of its responsibility to address serious crime under the Crime and Courts act 2013. The Secretary of State should explore whether they could encourage more co-operation between the NCA and Ofcom to combat fraud by determining this as a strategic priority under Section 3 of the Crime and Courts Act 2013. Consultation with Ofcom and a direction that the NCA and Ofcom work more closely together should underline and strengthen more proactive enforcement activity by Ofcom.* (Paragraph 285)

38. *A cabinet sub-committee with a clear mandate to tackle fraud should be established, chaired by and accountable to the Security Minister. The sub-committee should bring together more effectively all departments with a portfolio that spans fraud. To ensure transparency, its membership and terms of reference should be made public.* (Paragraph 286)

39. Fraud is the most commonly experienced crime in England and Wales today and represents a substantial national threat. If this were any other type of crime, this would be a matter of national importance. The woeful under-prioritisation from the NCA to local police forces is in part due to public misconceptions about the impact of fraud on victims—it doesn't "bang, bleed or shout"—and competing pressures on already-stretched law enforcement resources, compounded by a fundamental lack of capacity and skills amongst law enforcement staff. More funding is clearly needed, however we recognise the difficulty of securing this from the public purse. (Paragraph 321)

40. Furthermore, the structure of the model for policing in England and Wales is complex and results in siloed thinking that does not effectively serve victims of fraud. However, a wholesale reconfiguration of this approach would not be in the best interests of victims. Therefore, we suggest an approach of evolution rather than revolution. (Paragraph 322)

41. *To address the siloed approach to policing in England and Wales, we recommend an expanded and empowered central command unit to coordinate and steer efforts to tackle fraud with a focus on improving intelligence. Local police forces should retain their responsibility to support victims and tackle 'analogue' fraud.* (Paragraph 323)

42. *To support recruitment and upskilling efforts, the Government should develop a national policing workforce strategy. It must work with law enforcement and the private sector to support the secondment of specialist private sector civilian staff to complement and bolster law enforcement's skills pool through contracting specialist private sector services. It should explore the establishment of a Teach First-style model for recruiting law enforcement officers with specialisms in cyber and digital investigation. Further, we endorse the recommendations made by Policy Exchange to develop greater cyber capabilities specifically focussing on online crime within the police force.* (Paragraph 324)

43. *To support the forthcoming fraud strategy with adequate resources, the Government must commit to a long-term funding strategy with an increased offer for law*

enforcement agencies, focussed primarily on recycling revenue collected by law enforcement agencies back into law enforcement activity. (Paragraph 325)

44. *The Government should broaden the scope of the Economic Crime Levy to cover fraud and it must widen the remit for companies in scope in order to share the load with those in the tech and telecoms sectors.* (Paragraph 326)

45. *To tackle under-prioritisation, we agree with the Justice Committee that fraud should be written into the Strategic Policing Requirement.* (Paragraph 327)

46. Various issues including resourcing and the disclosure regime hinder how effectively the Crown Prosecution Service can bring fraudsters to justice under the Fraud Act 2006. Over time, these developments have resulted in a declining rate of prosecutions for fraud, in stark contrast to the rising number of cases. (Paragraph 348)

47. *The Government should work with the CPS on specialist training for personnel within the criminal justice system, including police officers, prosecutors and judges to expedite cases of complex fraud.* (Paragraph 349)

48. *As part of the Government's reconsideration of the UK Data Protection and Digital Information Bill, the Government should:*

    - *Endeavour to establish a formal working group between the CPS and the ICO on the issue of GDPR (or its replacement) and its use in criminal prosecutions, and to publish guidance and protocols on redaction for police and prosecutors, subject to regular review.*

    - *Require the ICO to work with the College of Policing to support police staff with resources and training to improve their understanding of data protection legislation and use their enforcement powers where needed to support this.* (Paragraph 350)

49. *We agree with the Justice Committee that the AGO should review the disclosure guidelines and consider new guidelines on disclosure in digital fraud cases. More widely, the Government should review the CPIA and in particular how the disclosure regime impacts the efficacy and speed with which fraudsters can be prosecuted.* (Paragraph 351)

50. *The Government should endorse the use of AI and technology-assisted review of material gathered in criminal investigations to shorten the length of investigations, with a mechanism for judicial approval of use pre-charge in individual cases.* (Paragraph 352)

51. There is scope to increase the use of civil remedies to take action against fraudsters and achieve justice for victims. (Paragraph 357)

52. *The Government should launch a review into the use of civil remedies to tackle fraud, including an examination of obstacles, for example, fees to commence civil proceedings, to the use of civil remedies such as asset recovery and injunctions.* (Paragraph 358)

53. While efforts are being made to protect and support victims of fraud, support pathways remain unclear and there are gaps in provision. This is leading to a loss of trust between victims and the systems in place. It remains unclear how the Victims Bill will support victims of fraud and the recent resignation of the Victims' Commissioner has highlighted the lack of due

attention provided to victims across the board. We trust a replacement will be appointed soon. (Paragraph 378)

54. *The Government must specifically include victims of fraud and economic crime in the Victims Bill and consider the recommendations of the former Victims' Commissioner that support for victims of fraud is tailored to the three high-vulnerability groups identified.* (Paragraph 379)

55. The Government must consider the local needs of victims as part of any future review of the policing structure for fraud. (Paragraph 380)

56. *As part of the process of replacing Action Fraud, and to provide clarity for victims, Action Fraud should be renamed to reflect more accurately its role as a reporting service. We agree with the Justice Committee that the new system should be victim-focussed to improve the flow of information about the progress of fraud cases to victims. The new system must be coupled with increased training for fraud call handlers to ensure that vulnerable victims are identified and treated appropriately, and to ensure that cases that are solvable are passed to the NFIB for investigation.* (Paragraph 381)

57. Reimbursing victims cannot be the seen as the primary focus of counter-fraud policy, yet it is a fundamental part of securing justice for victims. While we recognise the case for mandatory reimbursement of victims of APP fraud, we are concerned that a blanket reimbursement policy may lead to increased levels of moral hazard and fraud, and the perception that it is a 'victimless crime'. In some cases, it may even lead directly to new avenues for APP-reimbursement frauds. We also recognise how much banks have done to reimburse their customers. However, banks are the last link in the fraud chain and cannot be expected to foot the fraud bill alone. Furthermore, the inconsistency in the application of the CRM code across the sector demonstrates the need for uniformity. (Paragraph 399)

58. *The Government must revise its proposals to legislate to allow the PSR to mandate blanket reimbursement of APP fraud conducted via Faster Payments. The Committee suggests that further exploration on the long and short-term risks of this approach is required and recommends that the Government seek a solution that achieves a level playing field for all customers.* (Paragraph 400)

59. *To incentivise companies to act on fraud and more accurately reflect the balance of responsibility for fraud, the Government must establish a mechanism by which fraud-enabling sectors—in addition to the outgoing and recipient PSP—are required to contribute to the costs of reimbursement in cases where their platforms and services helped to facilitate the fraud. In making these changes, the Government must ensure that these reforms do not complicate the victims' experience of reimbursement; they should retain a single point of contact.* (Paragraph 401)

60. Public awareness campaigns are a crucial part of the fight against fraud. The Committee recognises that, while personal responsibility and awareness have a role, this should not be an excuse for fraud-enabling sectors to shirk their responsibilities to do more to tackle fraud via systems design. (Paragraph 417)

61. *The Government should oversee the introduction of a single, centrally funded consumer awareness campaign in partnership with industry. This should align with the priorities established in the forthcoming Fraud Strategy and should provide clear guidance on how fraud can be reported.* (Paragraph 418)

62. *The Government must work with the tech sector to establish free advertising credits for the FCA and law enforcement to promote counter-fraud messaging as public service advertising.* (Paragraph 419)

63. *The Government urgently must bring forward the measures outlined in the UK Digital Strategy to strengthen the digital education and digital skills pipeline and ensure that these measures extend to lifelong learning for adults without essential digital skills.* (Paragraph 420)

64. *The Government must support the meaningful inclusion of financial education in the National Curriculum as part of teaching about online safety within primary and secondary schools.* (Paragraph 421)

65. *Ofcom should introduce a measure under part C of its General Conditions of Entitlement that providers of telecommunications services should do more to educate consumers about the risks of fraud, and how to report it via 7726. Ofcom must apply pressure to online messenger platforms to ensure that they make their equivalent scam reporting services more transparent to encourage user reporting. Online messenger platforms must be encouraged to begin piloting their proposed approach under the Online Safety Bill by conducting transparent risk assessments of their services and reporting mechanisms.* (Paragraph 422)

66. *The Government should commission a review of how users respond to warning messages linked to potentially fraudulent payments as part of the customer journey, and whether such messages change their behaviour.* (Paragraph 423)

The Fraud Act 2006 and the legislative framework

67. The Fraud Act 2006 is a sound piece of legislation that is not in need of substantial reform. However, its efficacy is hindered by wider issues relating to its use in the prosecution of fraud cases and shortfalls in the prevention and detection of fraud, and enforcement of the legislation. Reform of corporate criminal liability will be essential in order to maximise the impact of the Fraud Act and other legal tools going forward. (Paragraph 438)

68. *We agree with the Justice Committee that sentencing guidelines should be amended to reflect fully the financial, emotional and psychological harms caused by fraud. The Government should review the sentencing powers for fraud offences to bring sentences for fraud offences in line with money laundering offences. This should be followed by a review of the Sentencing Council's guidelines.* (Paragraph 439)

69. The review of the Computer Misuse Act is welcome, however it cannot be delayed further. (Paragraph 450)

70. *The Government must publish its review of the Computer Misuse Act 1990 with urgency, and consider immediate reform including the introduction of a statutory defence to protect cyber security researchers from prosecution.* (Paragraph 451)

71. *The FCA should review the SEC's regime for rewarding whistleblowers where their information leads to a conviction or retrieval of money obtained through fraud. In particular, it should bring forward legislation to protect those who come forward in breach of a non-disclosure agreement to share information with a regulator. The Government should also give serious consideration to The Protection for Whistleblowing Bill.* (Paragraph 452)

72. Identity theft is a fundamental component of fraud and is routinely used by fraudsters to steal money from legitimate individuals and organisations yet it remains out of scope of criminal offences. (Paragraph 458)

73. *The Government should consult on the introduction of legislation to create a specific criminal offence of identity theft. Alternatively, the Sentencing Council should consider including identity theft as a serious aggravating factor in cases of fraud.* (Paragraph 459)

74. While data protection regulations are not in themselves an inhibitor of information sharing in the pursuit of prevention and detection of fraud, they are perceived by some to be so. This perception has the effect of stifling or delaying the sharing of information that could support the fight against fraud. Information sharing is a critical component of the counter-fraud effort and must proactively be encouraged by regulators and legislation. (Paragraph 479)

75. *The ICO must issue updated statutory guidance alongside an action plan to raise awareness of the provisions under the Data Protection Act 2018 and the new Data Protection and Digital Information Bill. The ICO must encourage a permissive attitude or 'safe harbour' about the sharing of data by the private sector for the purpose of preventing fraud.* (Paragraph 480)

76. *In the interests of greater transparency, The Data Protection and Digital Information Bill should be amended to include 'fraud' as a named crime under section 5(a).* (Paragraph 481)

77. *The Government should establish a regulatory obligation for regulated private sector organisations to share fraud risk data more regularly with law enforcement for the purposes of preventing fraud.* (Paragraph 482)

78. The telecoms sector has for too long been allowed to stand by while fraud is facilitated via its services (see Chapters 2 and 3). While we have explored how the provisions and principles in the Online Safety Bill might apply to the telecoms sector, the Committee propose that any new legislation specifically targeted at the telecoms sector to tackle fraud could be introduced under the Telecommunications (Security) Act. (Paragraph 487)

79. *The Government should consider how the Telecommunications (Security) Act 2021 might be used as means of introducing new measures to require the telecoms sector to clamp down on fraud taking place via its networks and services.* (Paragraph 488)

80. Many private sector companies consider fraud as a cost of doing business and are not doing enough to stop fraud from being facilitated by their services. Some sectors have less liability for fraud than others and are not held to account effectively for their role in facilitating this crime. We recognise that the role of failure to prevent offences is primarily to inspire behaviour change rather than criminal prosecutions. Corporate irresponsibility will not change until businesses feel the financial impact of liability coupled with reputational damage. It is time for less carrot and more stick. However, we are conscious to avoid regulatory overlap and it is clear that the Online Safety Bill will go some way to meeting some of these ambitions for tech platforms. We remain concerned that there is a lacuna for telecoms companies and ISPs who do not and will not face the same penalties. Equivalent measures should be introduced for these fraud enablers. (Paragraph 520)

81. *To inspire behaviour change, we agree with the Justice Committee and others who are calling for the Government to introduce a new corporate criminal offence of 'failure to prevent fraud', accompanied by significant financial penalties, to hold corporates across all sectors to account and to inspire behaviour change. The Government must make it clear that a range of other measures, such as director disqualification, are ready to be enforced if culture change is not forthcoming.* (Paragraph 521)

82. *To make telecoms companies more accountable for the fraud facilitated via their services, the Government should introduce a systems-led regulatory strategy equivalent to the Online Safety Bill that is directly applicable to telecoms platforms and services. This would comprise an equivalent regulatory duty to prevent the facilitation of fraud. Amending the Telecoms (Security) Act may be an avenue through which to achieve this.* (Paragraph 522)

83. It is clear to this Committee that there is a need for greater onus to be placed on private companies in fraud enabling sectors to report publicly and to the authorities the fraud that they detect on their platforms in order to increase transparency about which platforms are failing to stamp out fraud on their services. (Paragraph 526)

84. *All fraud-enabling sectors, including tech, telecoms and ISPs, must be subject to a 'duty to report' requiring them to share details of fraud reports with law enforcement and regulators, as well as to display publicly these figures alongside rates of reimbursement as soon as possible. The Government should explore the use of league tables to encourage competition and consumer choice. The ICO must issue clear guidance for businesses on how to comply with Clause 85 of the Data Protection and Digital Information Bill to enable the reporting of suspected fraudulent communications.* (Paragraph 527)

85. The Committee welcomes the ambition of the Online Safety Bill with respect to its systems-led approach to tackling fraud as priority illegal content. The Government must urgently reintroduce the Online Safety Bill to Parliament. However, to maximise its potential to reduce levels of online fraud, we consider that several amendments to the Online Safety Bill must be made. (Paragraph 558)

86. *The Online Safety Bill must make it explicit that all platforms regardless of size or function should be required to take measures to prevent fraudulent advertising from appearing on their sites to ensure a risk-based rather than size-based approach.* (Paragraph 559)

87. *This should include a duty of care for all platforms to stop fraudulent advertisements or content appearing on their platforms and to take steps to build in counter-fraud measures at design stage.* (Paragraph 560)

88. *Given that the Online Safety Bill does not effectively tackle intermediary platforms, the Online Advertising Programme must be expedited to avoid a surge in fraud on these platforms and include a plan to comprehensively tackle fraud.* (Paragraph 561)

89. *The Online Safety Bill should include a requirement on Ofcom to define the terms of its relationships with other regulators and include powers to enable them to work effectively together, including through information sharing.* (Paragraph 562)

90. *To ensure regulatory cooperation, we are in agreement with the Joint Committee on the Online Safety Bill and the House of Lords Communications and Digital Committee that the Government should place the Digital Regulation Cooperation Forum on a statutory footing with a remit to engage in forward-looking horizon*

scanning, to hold the various regulators to account and to compel regulators to work effectively together. Its membership should be broadened to include the PSR, and law enforcement representation such as the NCA. (Paragraph 563)

91. *The Government should consider reinvesting fines levelled as a result of action taken under the Online Safety Bill to support law enforcement activity.* (Paragraph 564)

92. *As an additional element of digital regulation, the Government must urgently bring forward the Draft Digital Markets, Competition and Consumer Bill to bolster protection for consumers.* (Paragraph 565)

APPENDIX 1: LIST OF MEMBERS AND DECLARATIONS OF INTEREST

Members

Lord Allan of Hallam
Baroness Bowles of Berkhamsted
Lord Browne of Ladyton
Viscount Colville of Culross
Lord Gilbert of Panteg
Baroness Henig CBE
Baroness Kingsmill
Baroness Morgan of Cotes (Chair)
Lord Sandhurst KC
Baroness Taylor of Bolton (to 22 June 2022)
Lord Triesman (from 22 June 2022)
Lord Vaux of Harrowden
Lord Young of Cookham

Declarations of interest

Lord Allan of Hallam
Non-executive Director, Public Data Practice CIC
Baroness Bowles of Berkhamsted
Non-executive Director, London Stock Exchange Plc
Non-executive Director, Valloop Holdings Ltd
Director, Hampden Buildings Ltd
Lord Browne of Ladyton
No relevant interests
Viscount Colville of Culross
No relevant interests
Lord Gilbert of Panteg
No relevant interests
Baroness Henig CBE
Chair, Chartered Security Professionals Registration Authority
President, The Security Institute
Non-executive Chair, Securigroup Ltd
Baroness Kingsmill
No relevant interests
Baroness Morgan of Cotes (Chair)
Non-executive Director, Santander UK
Chair, Association of British Insurers
Non-executive Director, Financial Services Compensation Scheme
Member, UK Advisory Board, Grayling
Lord Sandhurst KC
No relevant interests
Baroness Taylor of Bolton
No relevant interests
Lord Triesman
Group Executive Director, Salamanca Merchant Bank

Lord Vaux of Harrowden

Non-practising Chartered Accountant and member, Institute of Chartered Accountants of England and Wales

Category 4 shareholding in Fidelity National Information Services Inc (owner of Worldpay)

Lord Young of Cookham CH

No relevant interests

A full list of members' interests can be found in the Register of Lords' Interests:

https://www.parliament.uk/mps-lords-and-offices/standards-and-interests/register-of-lords-interests/

Specialist advisers

Kathryn Westmore

Employee, Royal United Services Institute (RUSI)

Member, Institute of Chartered Accountants of England and Wales (ICAEW)

Member, Association of Certified Fraud Examiners (ACFE)

Sam Thomas

Barrister, 2 Bedford Row

Member, IT Panel, Bar Council

Vice-Chair of the Association of Regulatory and Disciplinary Lawyers

APPENDIX 2: LIST OF WITNESSES

Evidence is published online at: https://committees.parliament.uk/committee/582/fraud-act-2006-and-digital-fraud-committee/publications/ and available for inspection at the Parliamentary Archives (020 7219 3074).

Evidence received by the Committee is listed below in chronological order of oral evidence session and in alphabetical order. Those marked with ** gave both oral and written evidence. Those marked with * gave oral evidence and did not submit any written evidence. All other witnesses submitted written evidence only.

Oral evidence in chronological order

*	Alice Adamson, Director for Victims and Vulnerability Policy, Ministry of Justice	QQ 1–12
*	Euan Neill, Head of Fraud Pursue and Law Enforcement, Home Office	QQ 1–12
*	Duncan Tessier, Director, Economic Crime, Home Office	QQ 1–12
**	Arun Chauhan, Trustee Director, Fraud Advisory Panel	QQ 13–22
**	Katy Worobec, Managing Director, Economic Crime, UK Finance	QQ 13–22
**	Mike Haley, CEO, Cifas	QQ 13–22
*	Lord Agnew of Oulton	QQ 23–33
*	Brian Dilley, Group Director of Economic Crime Prevention, Lloyds Banking Group	QQ 34–43
*	Geraldine Lawlor, Global Head of Financial Crime, KPMG LLP	QQ 34–43
*	Nicholas Taylor, Head of Policy and Public Affairs, Revolut UK	QQ 34–43
**	Alex Towers, Director of Policy and Public Affairs, BT Group	QQ 44–51
*	Hamish McLeod, Chief Executive, Mobile UK	QQ 44–51
*	Professor Victoria Nash, Director, Oxford Internet Institute	QQ 52–60
*	Professor Lorna Woods OBE, Professor of Internet Law, University of Essex	QQ 52–60
**	Lulu Freemont, Head of Digital Regulation, techUK	QQ 52–60
**	Kathryn Westmore, Research Fellow, RUSI	QQ 61–69
*	Dr Alice Hutchings, Director of the Cambridge Cybercrime Centre, University of Cambridge	QQ 61–69
*	Dr Konstantinos Mersinas, Senior Lecturer, Royal Holloway	QQ 61–69

*	Ghela Boskovich, Regional Director, Financial Data and Technology Association	QQ 70–79
**	David Pitt, CEO, Pay.UK	QQ 70–79
*	Kate Martin, Markets Editor, Financial Times	QQ 70–79
**	Dr Susan Hawley, Executive Director, Spotlight on Corruption	QQ 80–91
**	Richard Hyde, Senior Researcher, Social Market Foundation	QQ 80–91
*	Michael Skidmore, Senior Researcher, Police Foundation	QQ 80–91
*	Joe Lycett, Comedian and Television Presenter	QQ 92–106
*	Michelle Cox, Producer, Rumpus Media	QQ 92–106
*	Dame Vera Baird, Victims' Commissioner	QQ 107–118
*	Neil Postins, Delivery Manager, National Economic Crime Victim Care Unit	QQ 107–118
*	Pauline Smith, Director, Action Fraud	QQ 107–118
**	Didi Denham, Government Affairs and Public Policy lead on Advertising, Google	QQ 119–134
*	Will Semple, Senior Director, eBay	QQ 119–134
**	Elizabeth Kanter, Director of Government Affairs Public Policy Manager, TikTok	QQ 135–145
*	Graham Pullan, CEO, Fluttr	QQ 135–145
**	Philip Milton, Public Policy Manager, Meta	QQ 135–145
*	Chris Hemsley, Managing Director, Payment Systems Regulator	QQ 146–159
*	Huw Saunders, Director of Network Infrastructure and Resilience, Ofcom	QQ 146–159
**	Mark Steward, Executive Director of Enforcement and Market Oversight, Financial Conduct Authority	QQ 146–159
**	Tom Mutton, Central Bank Digital Currency, Bank of England	QQ 160–170
**	Christina Segal-Knowles, Executive Director for Financial Markets Infrastructure, Bank of England	QQ 160–170
*	Markko Künnapu, Legal Adviser, Estonian Ministry of Justice	QQ 171–178
*	Andrea Garcia Rodríguez, Lead Digital Policy Analyst, European Policy Centre	QQ 171–178
*	Melissa Hodgman, Associate Director, Division of Enforcement, Securities and Exchange Commission, United States	QQ 179–187
*	Superintendent Gerard Pollock, Chair, ScamwiseNI Partnership, Police Service of Northern Ireland	QQ 188–196

*	DCI Stevie Trim, Economic Crime and Financial Investigation Unit, Police Scotland	QQ 188–196
**	Mark Fenhalls KC, Chair, Bar Council	QQ 197–211
*	Karl Laird, Senior Lecturer, Oxford University	QQ 197–211
**	Detective Superintendent Pete O'Doherty, Assistant Commissioner, City of London Police	QQ 212–221
*	Rob Jones, Director General NECC/Threat Leadership, National Crime Agency	QQ 212–221
*	Mark Shelford, Police and Crime Commissioner for Avon and Somerset	QQ 212–221
*	Andy Cooke, Chief Inspector of the Constabulary for the London and National Regions	QQ 222–230
**	Adrian Gorham, Chair, Communications Crime Strategy Group	QQ 231–240
**	Professor Feng Hao, Professor of Security Engineering, University of Warwick	QQ 231–240
**	Max Hill KC, Director of Public Prosecutions, Crown Prosecution Service	QQ 241–249
*	Damian Collins MP, former Minister for Technology and the Digital Economy, DCMS	QQ 250–272
*	Tom Tugendhat MP, Minister for Security, Home Office	QQ 250–272
*	Sarah Connolly, Director for Security and Online Harms, DCMS	QQ 250–272
*	Duncan Tessier, Director, Economic Crime, Home Office	QQ 250–272

Alphabetical list of witnesses

	Advertising Standards Authority	FDF0022
*	Lord Agnew of Oulton (QQ 23–33)	
	Amazon	FDF0073
	Anonymous submission	FDF0010
	Anonymous submission	FDF0081
	Anonymous submission	FDF0102
	Association of British Insurers	FDF0051
	Association of Chief Trading Standards Officers	FDF0018
	Association of Consumer Support Organisations	FDF0033
	Association of Police and Crime Commissioners	FDF0064 FDF0077
*	Dame Vera Baird, Victims' Commissioner (QQ 107–118)	

	Peter Barron	FDF0090
*	Ghela Boskovich, Regional Director, Financial Data and Technology Association (QQ 70–79)	
	Steve Buck	FDF0084
	Building Societies Association	FDF0023
	Professor Mark Button	FDF0032
	Callsign Ltd	FDF0038
	Carnegie UK	FDF0060
	Chartered Trading Standards Institute	FDF0041
	Paul	FDF0103
**	Arun Chauhan, Trustee Director, Fraud Advisory Panel (QQ 13–22)	FDF0048 FDF0100
*	Damian Collins MP, Minister for Technology and the Digital Economy, DCMS (QQ 250–272)	
	Dr Jennifer Collins	FDF0078
*	Sarah Connolly, Director for Security and Online Harms, DCMS (QQ 250–272)	
*	Andy Cooke, Chief Inspector of the Constabulary for the London and National Regions (QQ 222–230)	
*	Michelle Cox, Producer, Rumpus Media (QQ 92–106)	
	Criminal Law Reform Now Network	FDF0083
	CyberUp Campaign	FDF0005 FDF0074
	Naomi Davis	FDF0085
**	Kathryn Westmore, Research Fellow, RUSI (QQ 61–69)	FDF0036
**	Didi Denham, Government Affairs and Public Policy Lead on Advertising, Google (QQ 119–134)	FDF0072
	Devon and Cornwall Police	FDF0009
*	Brian Dilley, Group Director of Economic Crime Prevention, Lloyds Banking Group (QQ 34–43)	
	East of England Trading Standards Authorities	FDF0024
	Liz Eden	FDF0089
	Richard Emery	FDF0040
	Equifax Ltd	FDF0019
**	Mark Fenhalls KC, Chair, Bar Council (QQ 197–211)	FDF0054
	Fighting Fraud and Corruption Locally	FDF0030
	US Federal Trade Commission	FDF0093

**	Lulu Freemont, Head of Digital Regulation, techUK (QQ 52–60)	FDF0059
	John Galvin	FDF0029
	Good Things Foundation	FDF0045
**	Adrian Gorham, Chair, Communications Crime Strategy Group (QQ 231–240)	FDF0063 FDF0088
**	Mike Haley, CEO, Cifas (QQ 13–22)	FDF0015
**	Professor Feng Hao, Professor of Security Engineering, University of Warwick (QQ 231–240)	FDF0079
	Tim Harvey	FDF0097
**	Dr Susan Hawley, Executive Director, Spotlight on Corruption (QQ 80–91)	FDF0053
*	Chris Hemsley, Managing Director, Payment Systems Regulator (QQ 146–159)	
**	Max Hill KC, Director of Public Prosecutions, Crown Prosecution Service (QQ 241–249)	FDF0004
*	Melissa Hodgman, Associate Director, Division of Enforcement, Securities and Exchange Commission, United States (QQ 179–187)	
	HSBC	FDF0106
*	Dr Alice Hutchings, Director of the Cambridge Cybercrime Centre, University of Cambridge (QQ 61–69)	
**	Richard Hyde, Senior Researcher, Social Market Foundation (QQ 80–91)	FDF0026
	Information Commissioner's Office	FDF0017
	Steven Jackson	FDF0011
	JobsAware	FDF0043
	Louise Jones	FDF0086
*	Rob Jones, Director General NECC/Threat Leadership, National Crime Agency (QQ 212–221)	
	Just Group	FDF0062
**	Elizabeth Kanter, Director of Government Affairs Public Policy Manager, TikTok (QQ 135–145)	FDF0071
	Klarna Bank AB	FDF0049
*	Markko Künnapu, Legal Adviser, Estonian Ministry of Justice (QQ 171–178)	
*	Karl Laird, Senior Lecturer, Oxford University (QQ 197–211)	
*	Geraldine Lawlor, Global Head of Financial Crime, KPMG LLP (QQ 34–43)	

	Lending Standards Board	FDF0050
	Les Stirling Plastering Contractors Ltd	FDF0021
	Professor Michael Levi	FDF0042
*	Joe Lycett, Comedian and Television Presenter (QQ 92–106)	
	Kuldeep Maan	FDF0016
	Raimondas Marciulevicius	FDF0003
*	Kate Martin, Markets Editor, Financial Times (QQ 70–79)	
	Michael Mason	FDF0047
*	Dr Konstantinos Mersinas, Senior Lecturer, Royal Holloway (QQ 61–69)	
**	Philip Milton, Public Policy Manager, Meta (QQ 135–145)	FDF0052 FDF0082 FDF0099
*	Hamish McLeod, Chief Executive, Mobile UK (QQ 44–51)	
	Motion Picture Association	FDF0068
*	Tom Mutton, Central Bank Digital Currency, Bank of England (QQ 160–170)	
*	Professor Victoria Nash, Director, Oxford Internet Institute (QQ 52–60)	
	National Anti-Fraud Network	FDF0055
	National Economic Crime Centre	FDF0044 FDF0080
	Nottingham Building Society	FDF0025
**	Detective Superintendent Pete O'Doherty, Assistant Commissioner, City of London Police (QQ 212–221)	FDF0031
	Onbord	FDF0013
	On Demand Payment Technologies	FDF0046
	Onfido	FDF0039
	Online Dating Association	FDF0028
	Tricia	FDF0105
	Dale	FDF0104
**	David Pitt, CEO, Pay.UK (QQ 70–79)	FDF0014
*	Superintendent Gerard Pollock, Chair, ScamwiseNI Partnership, Police Service of Northern Ireland (QQ 188–196)	
*	Neil Postins, Delivery Manager, National Economic Crime Victim Care Unit (QQ 107–118)	

	Premier FX Liquidation Committee	FDF0037
*	Graham Pullan, CEO, Fluttr (QQ 135–145)	
*	Andrea Garcia Rodríguez, Lead Digital Policy Analyst, European Policy Centre (QQ 171–1788)	
	Andrew Rowson	FDF0034
	Santander UK	FDF0094
*	Huw Saunders, Director of Network Infrastructure and Resilience, Ofcom (QQ 146–159)	
	Alvin Scott	FDF0002
**	Christina Segal-Knowles, Executive Director for Financial Markets Infrastructure, Bank of England	FDF0075
*	Will Semple, Senior Director, eBay (QQ 119–134)	
*	Mark Shelford, Police and Crime Commissioner for Avon and Somerset (QQ 212–221)	
	N Sizer	FDF0027
*	Michael Skidmore, Senior Researcher, Police Foundation (QQ 80–91)	
*	Pauline Smith, Director, Action Fraud (QQ 107–118)	
	SnapDragon	FDF0020
**	Mark Steward, Executive Director of Enforcement and Market Oversight, Financial Conduct Authority (QQ 146–159)	FDF0069 FDF0091
	Stop Scams UK	FDF0057
	Mark Taber	FDF0056
*	Nicholas Taylor, Head of Policy and Public Affairs, Revolut UK (QQ 34–43)	
*	Duncan Tessier, Director, Economic Crime, Home Office (QQ 250–272)	
**	Alex Towers, Director of Policy and Public Affairs, BT Group (QQ 44–51)	FDF0067 FDF0098
	Transpact	FDF0061
*	DCI Stevie Trim, Economic Crime and Financial Investigation Unit, Police Scotland (QQ 188–196)	
	Transparency Task Force	FDF0092
	trueCall Ltd	FDF0012
	TSB	FDF0066
*	Tom Tugendhat MP, Minister for Security, Home Office (QQ 250–272)	
	West Midlands Police and Crime Commissioner	FDF0035
	Bob Winsor	FDF0006

*	Professor Lorna Woods OBE, Professor of Internet Law, University of Essex (QQ 52–60)	
**	Katy Worobec, Managing Director, Economic Crime, UK Finance (QQ 13–22)	FDF0058

APPENDIX 3: CALL FOR EVIDENCE

The House of Lords Committee on the Fraud Act 2006 and Digital Fraud was appointed on 19 January 2022. It is chaired by Baroness Morgan of Cotes and intends to report by 30 November 2022.

Fraud is the act of gaining a dishonest advantage, often financial, over another person. Under the Fraud Act 2006, a person can commit fraud by false representation, by failing to disclose information, or by abuse of position. Today, fraud is the most commonly experienced crime in England and Wales, accounting for approximately 42% of all crime against individuals, causing losses of billions per year. The pandemic fuelled growth in the use of online services such as banking. This dependency on digital technology has left more and more people vulnerable to increasingly sophisticated fraudsters. The impact of fraud on victims can be significant both financially and emotionally.

This Inquiry will consider what measures should be taken to tackle the increase in cases of fraud. It will consider how the provisions laid out in the Fraud Act 2006 are used in practice for the detection, prevention and prosecution of fraud, and explore whether the Act is in need of reform. We will pay particular attention to how the Act is being applied to tackle fraud committed online or through digital means.

This is a public call for written evidence to be submitted to the Committee. The deadline is 12:00pm on 22 April 2022.

The Committee would like to hear from a diverse a range of individuals and organisations and is particularly keen to receive submissions from victims of fraud. If you have been a victim of fraud and would like to write to the Committee, you need not feel constrained by the questions listed below. We are keen to learn about your experiences whatever they may be.

If you are an organisation that works with victims, we would be grateful if you are able to share this inquiry with them. To ensure the voice of victims is central to our inquiry, the Committee is also planning to engage with victims willing to share their views in either a private or public setting. Please indicate within your written evidence whether you would be willing to share your experience with the Committee.

Questions

The Committee is happy to receive submissions on any issues related to the subject of the inquiry but would particularly welcome submissions on the questions listed below. You do not need to address every question and you may interpret the questions broadly, providing as much information as possible. Instructions on how to submit evidence are found at the end of this document.

Fraud Landscape

(1) What fraud risks are UK a) individuals, b) the Government and c) businesses particularly vulnerable to today, and what are the reasons for this?

(2) What future economic and technological developments are likely to impact how fraudsters seek to commit crime over the next five to ten years, and how might these be prepared for and mitigated? What role

can technology and tech companies play in combatting fraud across this timescale?

(3) Is fraud and its victims treated as a priority? If not, what are the reasons for this. *The Committee is particularly interested in responses that can explain any barriers preventing effective counter-fraud cooperation within Government, law enforcement, the public sector and the private sector.*

(4) What is the role of international actors in the UK's fraud landscape? What are the barriers to tackling borderless fraud?

Action to Tackle Fraud

(5) How effective is the current structure for policing fraud? How successful are the City of London Police, including Action Fraud and the National Fraud Intelligence Bureau, at executing their role as the lead police force for fraud?

(6) Are sufficient resources available to Government organisations (such as the Serious Fraud Office and Crown Prosecution Service) and wider police forces to tackle fraud and support victims, and how should this be addressed if not? *Answers need not be limited to financial resources.*

(7) What are the responsibilities of the private sector in protecting the public against digital fraud? How can a balance be achieved between the need to tackle digital fraud whilst supporting the growth of these sectors? To what extent is work done to combat fraud across the private sectors undermined by siloed or independent working practices?

(8) What are the legislative or regulatory impediments to sharing fraud risk data across and between the private and public sectors? For example, to what extent does General Data Protection Regulation (GDPR) limit data sharing?

(9) What is the role of the individual in relation to fraud? Are consumers well informed about the risks of fraud and how to prevent them? If not, which bodies or organisations should do more to ensure this? What are the most effective methods of educating the public about fraud crime and prevention?

Legislative Remedies

(10) What is your assessment of the Fraud Act 2006? What has been the impact of the Act and is it having any unintended consequences; if so, what are these?

(11) Is existing legislation effective in tackling the increase in modern forms of fraud? If not, is there a legislative remedy, or should fraud be addressed primarily through implementation of existing provisions? *Answers may refer to existing mechanisms such as increasing the scope and powers of regulators. You may refer to any legislation and are not limited to the Fraud Act 2006*

(12) Is the current system in place for prosecuting fraud cases working effectively? If not, what are the key barriers to prosecution?

(13) Are sanctions and penalties for criminals who commit fraud an effective deterrent against future criminal activity, and if not, what might be more successful? *Respondents may choose to refer to penalties imposed by the judicial system or by specific sectors.*

Best Practice

(14) What lessons can be learned from effective policy interventions and schemes both in the UK and overseas?

(15) Can you suggest one policy recommendation that the Committee should make to the Government?

APPENDIX 4: TELECOMMUNICATIONS FRAUD SECTOR CHARTER

Actions to tackle fraud risks directly affecting telecommunications customers

Action (1)—Work to identify and prevent scam calls

Objective: Reduce the impact of scam calls on customers.

Action: Telecommunications providers will work to identify and implement techniques to block scam calls. This action will be supported by Ofcom through the Strategic Industry Working Group. Data on sources of scam calls will be shared within the industry. Data sharing to combat fraud and scams, will be supported by specific case studies which will be provided to the Information Commissioner's Office (ICO) for potential inclusion in its data sharing hub. Providers will extend data sharing to law enforcement and banking.

Outcome: Enhance call blocking solutions to protect customers and reduce fraud.

Agree approach 3-6 months. Implement 1-2 years.

Actions to tackle fraud risks directly affecting telecommunications customers continued

Action (2)—A co-ordinated approach to tackle smishing

Objective: A coordinated attack on smishing from telecommunications, law enforcement, NCSC and banking.

Action: Telecommunications providers will work to identify and implement additional techniques to block smishing.

This action will be supported by Ofcom and Mobile UK through the Mobile Scams Group. A co-ordinated effort to review the use of the 7726 spam reporting service will be initiated, involving telecommunications providers, law enforcement and banking to explore how the 7726 database can be used more effectively against smishing.

Providers will consider messaging provided to customers using 7726 to encourage adoption.

Providers will share reported URLs and phone numbers suspected to be linked with smishing with the National Cyber Security Centre (NCSC) and National Fraud Intelligence Bureau (NFIB). Providers will seek to restrict access to URLs confirmed by the NCSC as used for smishing in accordance with legal and regulatory obligations.

Outcome: Improve knowledge, and reduce volume and impact, of smishing.

Agree approach 3-6 months. Implement 1-2 years.

Actions to tackle fraud risks resulting in wider customer financial fraud

Action (3)—Use of Dynamic Direct Debit to tackle identity theft affecting customers and subscription fraud affecting providers

Objective: Introduce a banking authorisation step into the Direct Debit initiation for new telecommunications contracts.

Action: The telecommunications industry will be supported by the banking industry in developing a pilot Dynamic Direct Debit system to facilitate three-way authentication and authorisation at the point of sale between a customer, their bank and the telecommunications provider.

The pilot will consider usage by different customer demographics. The telecommunications industry will consider Open Banking to achieve this.

Outcome: Reduce risk of identity theft/subscription fraud.

Pilot approach 3-6 months. Implement 1-2 years.

Action (4)—Use of real-time checking to tackle SIM swap and Mobile Number Porting fraud

Objective: Enable fraud to be reduced by a co-ordinated telecommunications / banking industry effort.

Action: The telecommunications industry will continue to support the banking industry by supplying a consistent real time check of whether or not a mobile phone has recently been subject to a SIM-swap or MNP using GSMA's Mobile Connect Account Takeover Protection standard supported by all providers.

Telecommunications providers will work with UK Finance to ensure the banking sector is fully aware of the SIM-Swap/MNP data available and to explore other information/services which providers may be able to supply to further reduce this fraud.

Outcome: Reduce risk of SIM-swap and MNP fraud.

Implement 3 months—1 year.

Action (5)—Sector information sharing

Objective: Improve industry cohesion in detecting and responding to fraud.

Action: Telecommunications providers will share information within the industry to detect and reduce fraud against customers and providers.

This action will be supported by a specific case study which will be provided to the ICO for potential inclusion in its data sharing hub.

Providers will extend data sharing to law enforcement and banking.

Outcome: Rapid & regular sharing of information on sources and nature of fraud attacks.

Agree approach 6 months. Implement 6-18 months.

Action (6)—Systematic sector analysis of shared fraud information and other intelligence

Objective: Analysis of information to identify participants in significant/ repeated fraud against customers and providers.

Action: Telecommunications providers will analyse shared information (and information from other sources) to identify sources and participants in significant/ repeated fraud against customers and providers to an agreed threshold.

This action will be supported by a specific case study which will be provided to the ICO for potential inclusion in its data sharing hub.

Information will be developed into actionable evidence to be shared with law enforcement.

Outcome: Identification of participants in significant/ repeated fraud against customers and providers made available to law enforcement.

Agree approach 3 months. Implement 3 months—1 year.

Actions to tackle fraud risks resulting in wider customer financial fraud continued

Action (7)—Engagement by law enforcement to investigate significant / repeated fraud against customers and providers

Objective: Create a more effective reporting route for significant / repeated telecommunications fraud.

Action: Telecommunications fraud reports will be submitted to Action Fraud by industry for recording on the national crime database.

City of London Police (CoLP), National Economic Crime Centre (NECC), and NCSC will each appoint a telecommunications fraud point of contact for the providers to discuss significant/repeated telecommunication fraud.

Providers will join the NECC Threat Group, through which they will share information where significant/repeated fraud has been identified that is impacting customers or companies. Where information is presented at the NECC Threat Group, the NECC will consider the optimum approach which may include creation of a pop-up fusion cell to tackle the issue, subject to internal prioritisation.

Outcome: Enhance collaboration to enable a more agile approach to tackling fraud.

Enable action in cases of significant/ repeated fraud.

Agree approach 3 months. Implement 3 months—1 year.

Action to support victims of telecommunications fraud

Action (8)—Improve support given to victims of telecommunications fraud

Objective: Improve fraud victim experience.

Action: Telecommunications providers will work with groups providing support to fraud victims to understand current concerns with telecommunications fraud victim handling and to identify best practice that could be adopted by industry.

Telecommunications providers will work with these groups to respond to reports of poor victim handling.

These groups will support providers with consistent signposting to victims on the support available should they require it.

Outcome: Improve treatment of fraud victims by industry.

Improve current processes for support of victims.

Increase customer awareness of courses of action following fraud.

Initial meeting with victim support groups within 3 months. Agree approach 6 months.

Implement 6-18 months.

Action to increase awareness of telecommunications fraud

Action (9)—Increase fraud awareness

Objective: Implement fraud awareness measures to reduce customer vulnerability.

Action: Telecommunications providers will support law enforcement and government by delivering communications sector fraud awareness messages.

Providers will participate in a public and private sector strategic communication steering group, which will review the effectiveness of existing awareness measures and consider using more consistent cross-sector messaging to the public.

Outcome: Increased fraud awareness; changed customer behaviour and reduced fraud risk.

Agree approach 6 months. Implement 6-18 months.

APPENDIX 5: GLOSSARY AND ABBREVIATIONS

Common abbreviations

Acronym	Definition
ACCC	Australian Competition and Consumer Commission
ACTSO	Association of Chief Trading Standards Officers
AGO	Attorney General's Office
AML	Anti-Money Laundering
APP	Authorised Push Payment
ASA	Advertising Standards Authority
BEIS	Department for Business, Energy, and Industrial Strategy
CCSG	Communications Crime Strategy Group
CDCPCU	Card and Dedicated Cheque and Plastic Crime Unit
CHAPS	Clearing House Automated Payment System
CMA	Competition and Markets Authority
CPIA	Criminal Procedure and Investigations Act 1996
CPS	Crown Prosecution Service
CPSPOC	CPS Proceeds of Crime team
CRM	Contingent Reimbursement Model
DCMS	Department for Digital, Culture, Media and Sport
DWP	Department for Work and Pensions
ECB	European Central Bank
ECSB	Economic Crime Strategic Board
FCA	Financial Conduct Authority
FCDO	Foreign, Commonwealth and Development Office
FSMA	Financial Services and Markets Act 2000
GDPR	General Data Protection Regulation
HMRC	His Majesty's Revenue and Customs
HMT	His Majesty's Treasury
ICO	Information Commissioners Office
ICT	Information and communications technology
JFT	Joint Fraud Taskforce
LSB	Lending Standards Board
MICA Directive	Markets in Crypto Asset Directive
MITS	Mule Insights Tactical Solution
NAFN	National Anti-Fraud Network

Acronym	Definition
NAO	National Audit Office
NCA	National Crime Agency
NECC	National Economic Crime Centre
NCSC	National Cyber Security Centre
NFIB	National Fraud Intelligence Bureau
OAP	Online Advertising Programme
OFSG	Online Fraud Steering Group
ONS	Office for National Statistics
PECR	Privacy and Electronic Communications Regulations
POCA	Proceeds of Crime Act 2002
PRA	Prudential Regulation Authority
PSHE	Personal, social, health and economic education
PSPs	Payment Service Providers
PSTN	Public Switched Telephone Network
PSR	Payment Systems Regulator
ROCUs	Regional Organised Crime Units
SARs	Suspicious Activity Reports
SEOCID	CPS' Serious Economic Organised Crime and International Directorate
SFO	Serious Fraud Office
SMEs	Small- and Medium-sized Enterprises
TCSEW	ONS' Telephone Crime Survey for England and Wales
UKFIU	UK Fraud Intelligence Unit

Common fraud terminology

Term	Definition
Artificial Intelligence (AI)	Technology in which a computing system is coded to 'think for itself', adapting and operating autonomously[784]
Authorised Push Payment (APP) scam	When a person or business is tricked into sending money to a fraudster posing as a genuine payee[785]
Biometrics	Automatic recognition of people from physical attributes like their face, voice, iris or fingerprint[786]

784 Cabinet Office, 'National Cyber Strategy 2022' (7 February 2022): https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#the-national-cyber-security-centre [accessed 1 November 2022]

785 PSR, 'APP scams' (November 2021): https://www.psr.org.uk/our-work/app-scams/ [accessed 1 November 2022]

786 Government Office for Science, *Biometrics: a guide* (5 June 2018): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715925/biometrics_final.pdf [accessed 1 November 2022]

Term	Definition
Blockchain	A way of storing data, a blockchain is an example of a distributed ledger–a type of append-only, tamper-proof storage technology.[787]
Calling Line Identification (CLI)	This tells the network what 'presentation number' a user is calling from on both mobile and landline phones. [788]
Cryptocurrency	A digital currency and payment system e.g. Bitcoin. The Bank of England refers to them as cryptoassets[789]
Cyber-enabled crime	Can be committed without ICT devices but is significantly changed by the use of ICT in terms of scale and reach[790]
Cyber-dependent crime	Can only be committed through the use of ICT devices, where the devices are the target and the tool for committing the crime[791]
Dark web	Part of the internet used for illegal activities only accessible by anonymising software[792]
Deepfake	A process that uses deep learning, a sub-field of artificial intelligence, to make fake pictures or voices.[793]
Digital fraud	Fraud that is facilitated on or by digital services.[794]
Digital identity	A digital representation of a person acting as an individual or as a representative of an organisation[795]
Encrypted messaging	Encryption is the process of encoding data or a message so that it cannot be understood by anyone other than its intended recipient.[796]

787 Cabinet Office, 'National Cyber Strategy 2022' (7 February 2022): https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#the-national-cyber-security-centre [accessed 1 November 2022]

788 ICO, 'Line identification (CLI)': https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/line-identification-cli/ [accessed 1 November 2022]

789 Cabinet Office, 'National Cyber Strategy 2022' (7 February 2022): https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022#the-national-cyber-security-centre [accessed 1 November 2022]

790 *Ibid.*

791 *Ibid.*

792 BBC News, 'Technology explained: What is the dark web?' (11 August 2016): https://www.bbc.co.uk/news/av/technology-37046475 [accessed 1 November 2022]

793 'What are deepfakes: and how can you spot them?' *The Guardian* (13 January 2020): https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them [accessed 1 November 2022]

794 Action Fraud, 'A-Z fraud': https://www.actionfraud.police.uk/a-z-of-fraud-category/other [accessed 1 November 2022]

795 DCMS, 'UK digital identity and attributes trust framework: beta version' (13 June 2022): https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version#what-are-digital-identities [accessed 1 November 2022]

796 BBC Bitesize, 'Encryption': https://www.bbc.co.uk/bitesize/guides/znxxh39/revision/1 [accessed 1 November 2022]

Term	Definition
Encryption	A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it[797]
Fraud	The act of gaining a dishonest advantage, often financial, over another person.[798]
Fraud chain	The series of events that tracks the development of a fraud from initial approach to the response by enforcement bodies.[799]
Identity theft	Identity theft happens when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to commit identity fraud.[800]
Intermediary platforms	Organisations that provide link points between goods or services to their customer base.[801]
Internet service providers (ISPs)	A company that provides access to the internet by a subscription service.[802]
IP address	A unique numerical label that identifies each computer using the internet.[803]
Kill chain	Also called the fraud chain, the steps taken by a fraudster in a scam to 'cashing out'
Know your customer (KYC)	Policies and procedures put in place by businesses to manage risk and verify the identities of customers, clients and suppliers[804]
Know your business customer (KYBC)	As above
Machine Learning	A method by which computers learn and adapt through algorithms and analysis rather than following explicit coded instructions.
Malicious Payee APP fraud	The victim is tricked into purchasing goods which don't exist or are never received.[805]

797 NCSC, 'NCSC glossary': https://www.ncsc.gov.uk/information/ncsc-glossary [accessed 1 November 2022]
798 Fraud Act 2006
799 Q 14 (Katy Worobec)
800 Action Fraud, 'A-Z fraud': https://www.actionfraud.police.uk/a-z-of-fraud-category/other [accessed 1 November 2022]
801 OECD, The Economic and Social Role of Internet Intermediaries (April 2010): https://www.oecd.org/digital/ieconomy/44949023.pdf [accessed 1 November 2022]
802 Thomson Reuters Practical Law, 'Internet service provider (ISP): https://uk.practicallaw.thomsonreuters.com/3-107-6733 [accessed 1 November 2022]
803 Pinsent Masons, 'IP Addresses and the Data Protection Act': https://www.pinsentmasons.com/out-law/guides/ip-addresses-and-the-data-protection-act [accessed 1 November 2022]
804 LexisNexis, 'What is Know Your Customer (KYC)?': https://bis.lexisnexis.co.uk/due-diligence-and-compliance/glossary/kyc [accessed 1 November 2022]
805 Payment Systems Regulator, 'APP Scams': https://www.psr.org.uk/our-work/app-scams/ [accessed 1 November 2022]

Term	Definition
Malicious Redirection APP fraud	Fraudsters use social engineering techniques to convince someone to transfer funds out of their account into that of the fraudster.[806]
Malware	Malicious software, often a virus, that tricks a user into giving up private information or taking control of their computer.[807]
Metaverse	A virtual reality space where users can interact in a computer-generated platform.[808]
Money mule	A form of money-laundering whereby a person who receives money from a third party and transfers it to another[809]
Phishing	Untargeted, mass emails asking for sensitive information (such as bank details) or encouraging a victim to visit a fake website[810]
Ransomware	A form of malware designed to block access to a computer until a sum of money is paid.[811]
Romance fraud	A form of fraud where a romantic relationship is formed with the purpose of deceiving the other into sending money.[812]
SIM farm	Technology that can send thousands of texts an hour by being connected to large numbers of pay-as-you-go sim cards.[813]
Smishing	Phishing via bulk SMS texts[814]
Social engineering	Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker[815]
Spoofing	Changing the appearance of a message, call or website to make it appear as if it is coming from a genuine organisation.[816]
SS7 protocol	Telephone identification protocol used in 2G, 3G and 4G networks.

806 Payment Systems Regulator, 'APP Scams': https://www.psr.org.uk/our-work/app-scams/ [accessed 1 November 2022]
807 CPS, 'Computer Misuse Act': https://www.cps.gov.uk/legal-guidance/computer-misuse-act [accessed 1 November 2022]
808 BBC News, 'Apparently, it's the next big thing. What is the metaverse?' (18 October 2021): https://www.bbc.co.uk/news/technology-58749529 [accessed 1 November 2022]
809 UK Finance, Cifas, 'Don't be fooled': https://www.moneymules.co.uk/ [accessed 1 November 2022]
810 NCSC, 'NCSC glossary': https://www.ncsc.gov.uk/information/ncsc-glossary (accessed 1 November 2022]
811 *Ibid.*
812 Action Fraud, 'Romance Fraud': https://www.actionfraud.police.uk/a-z-of-fraud/dating-fraud [accessed 1 November 2022]
813 BBC News, 'Covid fraud: £34.5m stolen in pandemic scams' (24 March 2021): https://www.bbc.co.uk/news/technology-56499886 [accessed 1 November 2022]
814 NCSC, 'NCSC glossary': https://www.ncsc.gov.uk/information/ncsc-glossary (accessed 1 November 2022]
815 *Ibid.*
816 See Home Office, 'Fraud sector charter: telecommunications' (26 October 2021): https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter/fraud-sector-charter-telecommunications-accessible-version [accessed 1 November 2022].

Term	Definition
Synthetic identity	A form of identity fraud in which a fraudster combines both real and fake information to create a new identity.[817]
TLD squatting	A fraudster registers an identical brand-owned domain name with a different Top Level Domain e.g. Facebook.co instead of Facebook.com[818]
Typosquatting/ URL hijacking	A fraudster registers a site close to an entity's brand or copyright e.g. facebo0k-login.com[819]
Voice Over Internet Protocol (VOIP)	Service that allows calls to be placed via the internet from anywhere in the world be transferred onto traditional telecommunications networks.[820]
Virtual Private Network (VPN)	An encrypted network often created to allow secure connections for remote users, for example in an organisation with offices in multiple locations.[821]

817 LexisNexis, 'Synthetic Identity Fraud is a Complex and Growing Challenge': https://risk.lexisnexis.com/insights-resources/article/synthetic-identity-fraud [accessed 1 November 2022]

818 Techradar, 'Why criminals spoof your domain name' (7 November 2019): https://www.techradar.com/news/why-criminals-spoof-your-domain-name [accessed 1 November 2022]

819 *Ibid.*

820 Thomson Reuters Practical Law, 'Voice-over-internet protocol (VoIP): https://uk.practicallaw.thomsonreuters.com/5-379-0582 [accessed 1 November 2022]

821 NCSC, 'NCSC glossary': https://www.ncsc.gov.uk/information/ncsc-glossary [accessed 1 November 2022]