# Government Response

## House of Lords Fraud Act 2006 and Digital Fraud Select Committee Report

## *Fighting Fraud: Breaking the Chain*

Fourth Report of Session 2022 – 23

### Introduction

This is the government's response to the Lords Fraud Act 2006 and Digital Fraud Select Committee report *'Fighting Fraud: Breaking the Chain'* (HL87) published 12 November 2022. The report made a total of 65 recommendations, which the government has carefully considered. For ease, these have been numbered in line with the review's summary of conclusions and recommendations (pages 156-166) of the report itself.

### Overview

The government is grateful to the Committee for undertaking its rigorous investigation into the impact of digital fraud, and to all those who provided insight and evidence for the report.

The Committee highlighted several important areas for our attention and this response sets out how we intend to address these. The recommendations proposed cover a range of topics including and not limited to, upskilling the public to spot scams, working with the finance, telecommunications and technology sectors to design out fraud and modernising the UK's legislative framework to combat fraud.

We recognise that the government will be unable to fight fraud alone and that a unified and co-ordinated response from government, law enforcement and the private sector is required. Together we can better protect the public and businesses, reduce the impact of fraud and increase the disruption and prosecution of fraudsters. We welcome the report and thank the Committee for the recommendations they have made, many of which have helped shape the forthcoming government Fraud Strategy.

# The Inbound Route 1.1

**Background**

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)

**Recommendation**

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)

**Government Response**

The government acknowledges the need for improved information on fraud, which will require a collaborative effort from key partners and regulators. Ofcom already carries out significant work to understand the scale of the scam calls and texts, sharing their findings with government, other regulators, law enforcement, and consumer groups.

In February 2022, Ofcom published an overview of their role and approach to tackling scam calls and texts, aiming to better understand the scale of telecoms-enabled fraud. In November 2022 Ofcom published data from their scams survey, which recorded measures used by consumers to screen incoming calls; the incidence of receiving suspicious calls, texts and messages; the incidence of falling foul of such a call, text or message; and whether and to whom these were reported.

Ofcom also established a Strategic Working Group with major telecoms providers in 2015 to work on reducing the impact of nuisance calls. Members of this group submit data to Ofcom, which is collated and shared amongst the members of the group. This internal data, along with consumer complaints data held by Ofcom, helps inform Ofcom's enforcement work.

On the Committee's recommendations regarding publication of enforcement data, it should be noted that information on enforcement cases is already published on Ofcom's website. The upcoming government Fraud Strategy will further detail Ofcom's role in preventing fraud.

# The Inbound Route 1.2

**Recommendation**

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)

**Government Response**

The government agrees that effective parliamentary oversight has an important role to play in scrutinising the evolving remit of various regulators in light of wider digital regulation, and specially Ofcom, ahead of the Online Safety Bill's passage into law. We welcome the contributions that have been made by this Committee, the House of Lords Communications and Digital Committee, the DCMS Select Committee, as well as the Joint Committee on the Online Safety Bill.

# The Inbound Route 1.3

**Recommendation**

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). (Paragraph 96)

**Government Response**

The government agrees with the Committee regarding the importance of ensuring that our regulatory system keeps pace with developments in digital technologies and markets. The creation of the Digital Regulation Cooperation Forum (DRCF) has been an important step forward in delivering our ambition for a coherent digital regulatory landscape. Since then, we have been working closely with Ofcom, the Information Commissioner's Office, the Competition and Markets Authority, and the Financial Conduct Authority, via the DRCF, to support collaboration and promote a joined-up approach to regulating digital technologies and services.

We recognise the strong stakeholder interest in the activities of the DRCF and the ensuing importance of transparency in the way the DRCF operates. The former Secretary of State for Digital, Culture, Media and Sport highlighted this as a crucial issue for consideration in her statement of priorities for the digital regulation landscape to the CEOs of the DRCF in 2022.

The government welcomes the DRCF's subsequent actions, including the publication of the Terms of Reference for the Forum, as well as through the delivery of its programme of work for 2022 to 2023. This has included the strengthening of its ongoing programme of engagement with industry, Parliament, regulatory bodies, and international partners, to ensure stakeholders understand the priorities of the Forum and have the opportunity to input into its latest thinking.

We would welcome any further steps the DRCF takes to engage Parliament, although as an independent body, it will be for the Forum to decide how it intends to do this. Government will continue to work with the DRCF and parliamentarians as the digital regulation landscape evolves, to ensure this is accompanied by the right governance and accountability.

In relation to the recommendation that Ofcom should be part of the NECC, please see the answer to the recommendation at Paragraph 284 (*the Government response to fraud 1.2*).

# The Inbound Route 1.4

**Background**

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)

**Recommendation**

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)

**Government Response**

All companies in scope of the Bill, including dating platforms, will need to assess the risk of fraud occurring through their services and then take proportionate but effective measures to mitigate these risks.

The Bill does not prescribe specific tools companies should take in order to comply with their duties. This will ensure that the legislation is future proofed. Moreover, given the range of services in scope of the Bill, different types of services will need to take different types of measures to comply, to reflect their specific risk profile.

Ofcom will issue codes of practice which set out recommended measures that companies can take to fulfil their duties under the Bill. Ofcom will also consult widely on what the most effective and proportionate measures are in order to tackle fraud to ensure it benefits from external expertise relevant to the duties. This may include user verification in some cases.

# The Inbound Route 1.5

**Recommendation**

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)

**Government Response**

We recognise that online platforms provide fraudsters with the opportunity to collect personal information or commit crimes through impersonation. We believe that working with online platforms, such as social media and dating platforms, to improve standards around identity authentication and practices around checking for duplicative or fraudulent accounts, will make identity-enabled frauds more difficult for fraudsters. The government Fraud Strategy will further detail how we will work with technology companies to design-out fraud.

Proactive technologies can play an important role in helping companies to identify and tackle fraudulent advertising and illegal content on their platforms. We will therefore give Ofcom the power under the Online Safety Bill to recommend or require the use of proactive technologies, if necessary, to help ensure that companies, including in-scope dating platforms, are meeting their duties to protect users from fraudulent advertising and illegal online activity under the Bill.

Ofcom will have discretion on what technologies it recommends or requires, although this will depend on what is necessary and proportionate in the given scenario and factors including the accuracy, effectiveness and lack of bias of the technology in question. The detail of how the Online Safety Bill provisions will apply to regulated firms is being led by Ofcom and will be published soon after the Bill receives Royal Assent.

# The Inbound Route 1.6

**Background**

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)

**Recommendation**

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)

**Government Response**

The government is committed to tackling fraudulent content online and bringing those who profit from it to justice. That is why, as noted in the response to the recommendation in Paragraph 112, the Online Safety Bill will ensure tech companies, including social media services, take proactive action to tackle the use of their platforms to commit fraud. All social media services in scope of the Bill will have a duty to set out clearly in terms of service how users will be protected from illegal content, and must ensure that these terms are consistently applied.

In recognition of the detrimental effect that fraudulent advertising can have, the government has also included the standalone fraudulent advertising duty for the largest social media and search services. This will require these services to prevent the publication of fraudulent adverts on their services.

The Bill gives Ofcom robust enforcement powers, allowing them to impose financial penalties of up to £18 million or 10% of qualifying worldwide revenue, whichever is higher, on services that do not fulfil their duties, including in relation to fraudulent advertising. These enforcement powers will incentivise companies to implement robust systems for tackling fraud.

In addition, the Online Advertising Programme is considering how advertising regulation should be modernised for the digital age. The programme is reviewing the spectrum of harms caused across all forms of online advertising. In relation to fraud, the Online Advertising Programme will build on the fraudulent advertising duty in the Online Safety Bill, and will look at the role of the entire advertising supply chain.

# The Inbound Route 1.7

**Recommendation**

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)

**Government Response**

The government welcomes the actions taken by online platforms, who are taking steps to ensure that only FCA authorised firms can advertise financial services products through their platforms. The Online Safety Bill will strengthen further the responsibilities on online platforms, by ensuring that user-generated content does not breach rules on advertising of FCA regulated financial services and by introducing a standalone duty for the largest social media and search services to ensure that fraudulent advertising, including of financial services, is not hosted on their platforms.

FCA rules already require that financial promotions must be clear, fair and not misleading. This includes making clear where a specific activity or product is not regulated by the FCA. The FCA takes action where financial promotions do not meet its rules, and in 2022 quarter 3, FCA engagement with firms resulted in 4,151 amendments or withdrawals of financial promotions.

To further strengthen the overall quality of financial promotions, the government is also legislating through the Financial Services and Markets Bill to introduce a new regulatory "gateway" for the approval of financial promotions. This measure will require FCA-authorised firms to obtain the FCA's permission before approving the financial promotions of unauthorised firms, allowing only those authorised firms that the FCA assesses as suitable and with sufficient expertise to approve such promotions.

# The Inbound Route 1.8

**Background**

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)

**Recommendation**

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 leafleting and door-stepping, and it must support those who are typically targeted by them. (Paragraph 138)

**Government Response**

The government recognises the vital work that local police forces do, to track down fraudsters and support victims. Despite the growth of online-enabled fraud, analogue forms of fraud still pose a significant risk to UK residents and businesses. The forthcoming Fraud Strategy will make clear the need for a whole systems approach to tackle all manifestations of this crime type, ensuring police forces have the training and resources required to do so. Further, the Fraud Strategy will cover the importance of empowering the public and supporting the most vulnerable in society to spot scams so they can avoid becoming victims in the first place.

# Interaction 1.1

**Background**

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)

**Recommendation**

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)

**Government Response**

The government recognises the importance of consumer trust in telephone numbering identity and the impact number spoofing has. Ofcom has undertaken work to help combat number spoofing and Calling Line Identification (CLI) abuse. In November 2022, following a consultation process on strengthening CLI, Ofcom published a statement announcing new requirements on telecoms operators to identify and block spoofed numbers.

Ofcom has modified one of their rules (General Condition (GC) C6) to require telecoms operators, where technically feasible, to identify and block calls with invalid CLI data. Ofcom has also published updated guidance for telecoms operators on complying with the modified rules on CLI. In order to bring these new protections in place for consumers as soon as possible, Ofcom has given telecoms operators until May 2023 to implement these new CLI requirements.

We are pleased to note that Ofcom are currently exploring the viability of further interventions to require network providers to certify that the numbers used for a call are legitimate when passing it to the network of the call's recipient, referred to as 'CLI authentication'. A similar approach has already been implemented in the US and is due to be implemented in France. Full implementation in the UK will not be possible until voice services have migrated to new Voice over Internet Protocol (VoIP) network technology. Ofcom are starting work now to understand how CLI authentication could work in practice, the potential benefits, and the costs of implementation. The government is supportive of Ofcom's efforts in this workstream.

The Public Switched Telephone Network (PSTN) migration to VoIP technologies is industry led and not being undertaken by the government. The migration to VoIP is a complex process that requires the telecom providers to support vulnerable customers and Critical National Infrastructure sectors using the PSTN. Given the PSTN is an increasingly unreliable and out of date network, industry is implementing this change as quickly as possible with the current target for completion being 2025.

# Interaction 1.2

**Recommendation**

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)

**Government Response**

The government has mandated high standards for the financial sector through application of Strong Customer Authentication. Secure and trusted digital identities will give companies different options for identifying consumers more easily and more securely as they will make it possible for people to prove things about themselves in a secure and trusted way without showing paper documents.

One of potential benefits of secure digital identity use in the UK is to help protect against the harmful effects of identity fraud. We are putting in place a framework so that everyone can know what a 'good' digital identity looks like. It will allow digital identities to be used in line with robust, privacy-centric standards which defend against weaknesses in systems and reduce opportunities for fraudsters.

Organisations seeking to protect their services from identity fraud can choose to adopt trust-marked digital identity services. These services will follow a robust process to verify users' identities. They will be built on trustworthy data sources and will follow fraud management best practices.

We are doing this in a way that maintains people's choice, security and control of their data, and supports growth and innovation across the economy. We have no plans to make digital identities compulsory.

# Interaction 1.3

**Background**

Social engineering is a cruel tactic used by fraudsters to manipulate their victims. It has long standing 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)

**Recommendation**

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)

**Government Response**

The government recognises the importance of protecting the public from frauds and believes that a fundamental part of this work lies in empowering the public to have the right knowledge and tools to enable them to identify and stop frauds. The government will continue to encourage the private sector to continue to develop initiatives to support customers in this way.

# Interaction 1.4

**Background**

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)

**Recommendation**

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)

**Government Response**

Ofcom regulates Internet Service Providers to ensure fair competition and consumer access to the Internet, but its remit does not include protecting ISP users from harm.

Registries and registrars are not (nor can they be) responsible for the content of websites established through the domain names they issue. However, if sites are used for certain malicious activities (such as phishing) then the names can be withdrawn.

The NCSC continues to develop ways to prevent attacks from reaching the public online, including its new Share and Defend capability which was launched in 2022. This capability allows NCSC to share information about malicious websites with industry at scale and in real time. At the time of writing, half of all UK ISPs customers are able to benefit from this service and by the end of 2023, 80% will be covered.

We are examining what more ISPs, domain hosts, and the wider industry can do to provide protections and we will take forward action that we identify that will increase safety and confidence in how the public access the internet.

# Interaction 1.5

**Recommendation**

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

**Government Response**

The government agrees with the Committee's view that a sector charter with the tech sector is an important programme of work, which will be outlined in the upcoming Fraud Strategy. The Home Office is intending to launch a tech and online charter with industry, which will include public and private actions that will drive down fraud in these sectors and improve collaborative working.

The government also agrees that ISPs are an important partner in our approach to tackling fraud. Telecommunications companies, in their capacity as ISPs, are working with the National Cyber Security Centre through its takedown service. Under the Telecommunications Fraud Sector Charter, they are also carrying out an ambitious programme of wider work to prevent fraud carried using their networks. We are examining what more ISPs and the wider industry can do to provide protections to this and we will take forward action that we identify that will increase safety and confidence amongst the public to use technology.

# Cashing Out 1.1

**Background**

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)

**Recommendation**

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).

**Government Response**

Under the current Payment Services Regulations 2017, the principal law governing UK payment services, banks and other payment service providers must ensure payments are credited to the receiving account by the end of the next working day. Under these regulations, payment service providers can already hold payments up to the legal timescales, and refuse to make payments where this is both permitted in their contract with a payment servicer user, and in accordance with existing law.

However, following representations from the payments industry, in particular noting the need for adequate time for firms and the police to engage the Banking Protocol Cross Channel in cases of suspected fraud, the government is investigating amending legislation to enable payment service providers to delay payments beyond the existing legislative timescales in limited, high-risk fraud scenarios, in order for enhanced customer engagement to take place. This could enable firms to take more of a ‘risk-based’ approach to payments processing.

HM Treasury is considering this issue to understand what measures should be taken. It will be essential that risks to legitimate payment flows, including those made by account holders or payment initiation providers acting at their request, are not inadvertently blocked.

# Cashing Out 1.2

**Recommendation**

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).

**Government Response**

The government supports the Payment Systems Regulator's (PSR) existing interventions to widen the coverage of Confirmation of Payee to reduce fraud, including its most recent actions to direct several hundred more payment service providers, which include electronic money institutions, to implement Confirmation of Payee.

The PSR expects this action will increase CoP coverage to 99% of payments made via the Faster Payments system, enabling almost all system users to benefit from the protection that Confirmation of Payee provides, regardless of whether they make a payment via a bank or an electronic money institution.

# Cashing Out 1.3

**Recommendation**

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).

**Government Response**

The government recognises the importance of industry led initiatives such as the Banking Protocol and the important part they play in stopping fraud. We also recognise the good work of scheme members and law enforcement to prevent fraud in progress through the scheme.

The Protocol has prevented £230.1 million in fraud and led to 1,079 arrests since it launched in 2016 and in the first half of 2022 alone, £27.4 million was stopped through the scheme, which trains bank branch staff to spot when someone is about to fall victim to a scam and try to prevent them from withdrawing cash to give to a fraudster. After this the staff can request a police response to the branch to investigate the suspected fraud and catch those responsible.

In 2020, banks announced the intention to extend the scheme to cover phone and online banking transactions of scheme members, and to also allow police to visit the customer’s home if they cannot come to a branch. The government supports this extension.

# Cashing Out 1.4

**Recommendation**

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).

**Government Response**

As part of their responsibility to ensure the integrity of the UK financial markets, all firms authorised by the FCA under the Financial Services and Markets Act 2000 are required to have systems and controls in place to mitigate the risk that they might be used to commit financial crime, this includes money laundering and fraud. Separately the FCA is a supervisor under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. This remit only includes certain financial institutions including banks, e-money institutions and cryptoasset businesses. The FCA is tasked with overseeing how these organisations meet the requirements in Money Laundering Regulations to have appropriate and risk-based policies and procedures to identify their customers and monitor activities to identify unusual or suspicious activity.

The FCA are developing their approach for effectively supervising the anti-fraud systems and controls of the firms they regulate. So far, they have undertaken assessments of firms' anti-fraud systems and controls to understand and evaluate how they are protecting consumers from fraud. They are also looking at the fraud risks in the retail banking sector, including future threats posed by technological advances This work will inform their view of current processes used to prevent, identify and mitigate the ease of fraudsters being able to open new accounts, and provide further learnings that can feed into the wider work of the industry. As a result, while not in the form of thematic review, FCA believe work in this area will meet the substance of the recommendation.

# Cashing Out 1.5

**Recommendation**

The FCA and PSR should work with PSPs to increase transparency and customer understanding about measures in place to prevent fraud, including possibly slowing pace of transactions and KYC checks. This work should feed into the government's centrally led public awareness campaign (see paragraph 418). (Paragraph 233).

**Government Response**

The Financial Conduct Authority (FCA) works closely with the PSR to counter fraud risks, particularly authorised push payment fraud. As part of the FCA's 2022-2025 strategy published in April 2022 there is a commitment to tackle financial crime and consumer understanding of fraud risks will form a key part of this work.

The FCA have run the loan fee fraud partnerships campaign, the ScamSmart campaign to help consumers spot the risks of investment scams, and InvestSmart, which attracted almost 70,000 views across both Instagram and TikTok. The government continues to support the FCA, in their engagement with industry on fraud education.

Firms may implement bespoke systems to prevent fraud and making these systems public can allow criminals to then adapt their tactics. It is expected, however, that firms will communicate with their customers on the information or documentation they need to complete Know Your Customer (KYC) checks and explain, where they can, the necessity of any additional controls, including why payments might be delayed or stopped.

# Cashing Out 1.6

**Background**

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)

**Recommendation**

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)

**Government Response**

As of 10 January 2020, UK cryptoasset exchange providers and custodian wallet providers are now in scope of the UK's Money Laundering and Terrorist Financing Regulations (MLRs). This means a range of UK cryptoasset firms are required to register with the UK's Financial Conduct Authority (FCA), carry out appropriate checks on their customers and report suspicious activity.

All cryptoasset firms operating in the UK are therefore required to meet the obligations set out in the MLRs before they can operate. The FCA ensures this through assessment of firms and its officers. During this process the FCA has at times requested additional information from firms to ensure appropriate checks and controls are applied to customers and transactions. This iterative process has involved direct firm engagement as well as the provision of wider guidance, for example through the FCA's Financial Crime Guide.

In addition, the government passed legislation in 2022 to implement the Financial Action Task Force's (FATF) Travel Rule that will become effective in September 2023. This international standard requires the extension of the information sharing and retention requirements that apply to bank transfers to transfers of cryptoassets, to ensure that the identities of the originator and beneficiary of a transfer of cryptoassets are known. More specifically, the Travel Rule will require cryptoasset businesses to collect, transmit, and store information about the originator and beneficiary of cryptoasset transfers, to enable the detection and prevention of money laundering.

# Cashing Out 1.7

**Recommendation**

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)

**Government Response**

The government is committed to creating a regulatory environment in which firms can innovate, while crucially maintaining financial stability and regulatory standards so that people and businesses can use new technologies both reliably and safely. And, at Fintech Week 2022, the government announced its commitment to consult on a world-leading regime for a broader set of cryptoasset activities.

The government has brought forward an amendment to the Financial Services and Markets Bill to ensure the Treasury can introduce comprehensive regulation of the broader cryptoasset sector in an agile way. The Financial Services and Markets Bill will also bring cryptoassets known as 'stablecoins' within the regulatory perimeter, where they are used as a form of payment. This legislation will ensure that the UK's regulatory framework is equipped to harness benefits of stablecoins, supporting the adoption of cutting-edge technologies, while mitigating the potential risks. The changes will ensure that consumers can use stablecoin services with confidence. For firms, this Bill will create the conditions for stablecoin issuers and service providers to operate and grow in the UK.

Additionally, the government and UK authorities have already taken a range of regulatory measures to mitigate market integrity risks, protect consumers and support innovation in the cryptoasset market. To protect consumers, the FCA has banned the sale of cryptoasset derivatives to retail consumers. Since January 2020, cryptoasset firms operating in the UK have been subject to Money Laundering Regulations. And, on 18 January 2022, the government also set out its intention to legislate to bring certain cryptoassets into financial promotion regulation. This would ensure that relevant cryptoasset promotions are held to the same high standards for fairness, clarity and accuracy that exist in the financial services industry.

# Cashing Out 1.8

**Recommendation**

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)

**Government Response**

Building on the recently enacted Economic Crime (Transparency and Enforcement) Act, the Economic Crime and Corporate Transparency Bill will bear down on kleptocrats, criminals and terrorists who abuse our open economy, strengthening the UK's reputation as a place where legitimate business can thrive while driving dirty money out of the UK.

The Bill was introduced on 22 September 2022. It provides additional powers to law enforcement so they are able to more quickly and easily seize and recover cryptoassets which are the proceeds of crime or associated with illicit activity such as money laundering, fraud and ransomware attack.

We want to modernise our proceeds of crime and counter-terrorism legislation, to introduce new powers to recover cryptoassets in more circumstances than at present. Existing forfeiture powers are currently limited to cash and listed assets. The creation of a cryptoasset specific civil forfeiture power from the Bill will mitigate the risk posed by those that cannot be prosecuted but use their funds to further their criminality or for terrorist purposes.

# Cashing Out 1.9

**Background**

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)

**Recommendation**

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)

**Government Response**

Education and awareness raising is an important part of the government's approach to tackling money mule activity, and a wide variety of age groups and demographics can be at risk from money mule recruiters. In late 2022 the National Crime Agency completed a 6-week social media campaign targeting young people and warning them of the risks of money mule recruiters operating online. The campaign used adverts and popular influencers to reach young people directly, as well as a new resource page with advice for young people, parents and education professionals: *Money Mules - National Crime Agency*.

The campaign was supported by outreach to universities and shared with around 10,000 schools in the country, responsible for 4 million children. This campaign, alongside prevention work by banks, police forces, charities and other partners, will form part of a longer-term awareness raising and education strategy. Further detail will be set out in the forthcoming Fraud Strategy.

# Cashing Out 2.0

**Recommendation**

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)

**Government Response**

The government recognises that innovation and cross-industry collaboration by the financial sector, including banks, payment service providers, and crypto exchanges, is key to tackling the movement of funds through money mule networks.

In September, the Financial Conduct Authority (FCA) and Payment Systems Regulator (PSR) ran a tech sprint with industry participants to develop potential solutions to fraud which considered the role of money mule accounts and how alerts can be used throughout the system. Participants in particular noted the need for further data sharing, an area which the FCA is now more keenly looking at. In addition, the PSR is currently working with industry to improve data sharing between the sending and receiving banks to give a more complete risk assessment of each transaction, including the involvement of a mule account as the receiving account. The government will continue to encourage new solutions in this area.

# The Government response to fraud 1.1

**Recommendation**

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)

**Government Response**

The Economic Crime and Corporate Transparency Bill, currently going through parliament, will reform the role of Companies House and improve transparency over UK companies and other legal entities in order to strengthen our business environment, support our national security and combat economic crime, whilst delivering a more reliable companies register to underpin business activity.

# The Government response to fraud 1.2

**Recommendation**

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)

**Government Response**

The National Economic Crime Centre brings together law enforcement and justice agencies, government departments, regulatory bodies and the private sector with a shared objective of driving down serious economic crime, protecting the public and safeguarding the prosperity of the UK as a financial centre. This includes other regulators involved in fighting financial crime.

Whilst Ofcom is not directly involved in the criminal investigation of fraud, Ofcom is engaging closely with the NECC and other law enforcement organisations as part of its wider regulatory activity. Both Ofcom and the NECC keep their engagement under close review and regularly evaluate opportunities for closer collaboration, including whether Ofcom secondees could further augment the NECC's technical expertise in areas relating to telecommunications and online fraud.

We agree with the Committee on the importance of ensuring there is effective join up across the wider digital regulatory landscape, and government highlighted this as a key priority through the Plan for Digital Regulation as well as in the letter issued to the CEOs of the DRCF in March last year by the former Secretary of State for Digital, Culture, Media and Sport.[1]

We note, however, that the DRCF is a voluntary cooperation forum that facilitates engagement between regulators on digital policy areas of mutual interest. Law enforcement agencies such as the NCA fall outside of the DRCF's membership eligibility criteria, as addressed in the response to Recommendation 90.

[1] H.M. Government, 2022. Letter from DCMS SoS to DRCF.

# The Government response to fraud 1.3

**Recommendation**

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)

**Government Response**

The National Crime Agency (NCA) continues to work closely with regulators (including Ofcom), government and law enforcement partners to combat fraud. The Strategic Priorities for 2022-23, as set by the previous Home Secretary under section 3 of the Crime and Courts Act 2013, provide a high-level steer for the NCA in their role of combatting serious and organised crime, and calls on the NCA to strengthen their response in tackling fraud.

Work is currently underway to review the Strategic Priorities for 2023-2024, which will include consideration of fraud as a vital part of the NCA's work.

# The Government response to fraud 1.4

**Recommendation**

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)

**Government Response**

The government recognises that fighting fraud requires a concerted and coherent public-private sector approach, which is why the Security Minister chairs the Joint Fraud Taskforce, which brings together all relevant government departments, law enforcement partners, charities, regulators and private sector stakeholders. Further details about the Taskforce, including minutes of meetings, can be found online here.

# The Government response to fraud 1.5

**Background**

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)

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

**Recommendation**

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)

**Government Response**

We recognise that there needs to be improvements in the response to fraud, from the reporting process through to investigations. That is why we have been working with partners in law enforcement, the public and private sectors to explore all options available to policing to ensure they keep pace with criminals and encourage innovation within industry.

The government Fraud Strategy will set out a new approach to tackling fraud, building on the existing strengths of the City of London Police (CoLP) as the national lead for fraud and the National Economic Crime Centre (NECC) based in the NCA.

The NECC, supported by CoLP, are the whole system lead responsible for allocating cases to local and regional economic crime teams. CoLP are responsible for national fraud policing strategy and guidance, the national reporting system (Action Fraud) and the National Fraud Intelligence Bureau.

# The Government response to fraud 1.6

**Recommendation**

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)

**Government Response**

We recognise the need to take a wholistic and national view of the recruitment and development of a policing workforce that are capable of combating online crime, including types of fraud. The government Fraud Strategy will outline the further steps we are taking to ensure law enforcement have the skills and training required to tackle fraud.

The government is supportive of College of Policing's (CoP) desire to ensure police professionals have access to high standards of learning and professional development, to equip those who might deal with fraud with the right skills and knowledge. CoP are working with the national policing lead City of London Police to review policing arrangements for fraud.

Currently, there are four key strands of fraud training, including specific learning products available through the City of London Police Economic and Cyber Crime Academy; and from the College of Policing's Digital Intelligence and Investigation suite.

The curriculum for all new starters includes digital investigations training, understanding the digital crime scene and recovery of digital material. This is supported by content which helps new and serving officers, police staff and volunteers to acquire the digital skills they need to undertake investigations effectively.

We acknowledge that there is more to be done to draw on expertise from the academic and private sectors, to ensure Law Enforcement have the training they need to effectively fight fraud. We continue to support CoP, as they bring together forces and experts to share best practice and develop collaborative plans for policing to improve their work to detect, prevent and disrupt fraud.

# The Government response to fraud 1.7

**Recommendation**

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)

**Government Response**

The upcoming Fraud Strategy will detail how the government is funding law enforcement to tackle fraud. £400 million has been allocated, through the Spending Review, to be spent on tackling economic crime including fraud, over the next three years. In parallel, the Home Office continues to commit funding to the NECC in the NCA, and police forces, including over £15m each year to CoLP as the national lead force for fraud.

Given the nature of fraud and the scale of the challenge to tackle it, the government recognises that increasing Law Enforcement resource alone will not be sufficient and that private sector partners will need to play a significant part in combating this crime.

# The Government response to fraud 1.8

**Recommendation**

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)

**Government Response**

The Economic Crime (Anti-Money Laundering) Levy (ECL), charged on businesses subject to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, is part of the government's wider objective to develop a long-term Sustainable Resourcing Model to tackle economic crime.

The government consulted on the extension of the levy to fraud. Respondents did not support this, arguing unlike money laundering, where the risk rests with the regulated sector, responsibility and benefit for countering fraud sits across society so should be funded via general taxation.

# The Government response to fraud 1.9

**Recommendation**

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

**Government Response**

The Strategic Policing Requirement (SPR) sets out what, in the Home Secretary's view, are the national threats at the time the document is issued, and appropriate national policing capabilities to counter those national threats. There is an expectation that Police and Crime Commissioners and Chief Constables have regard to the SPR, this means that they should follow the SPR unless they are satisfied that, in the particular circumstances, there are good reasons not to. Home Office officials have worked with policing partners to shape a revised version of the SPR, which has now been published, giving fraud greater prominence. The government recognises recommendations that have been made in this area, and will set out its updated position in the SPR.

# The Government response to fraud 2.0

**Background**

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)

**Recommendation**

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)

**Government Response**

The government agrees that law enforcement should have the training and tools available to support the development of specialists. The response to recommendation made in paragraph 324 of the Committee's report outlines the work already undertaken by the College of Policing to upskill the police force to better tackle online-enabled crime and fraud.

The CPS have established a new Serious Economic, Organised Crime and International Directorate (SEOCID), which will further the development of specialist personnel training by bringing together experts from a wide range of law enforcement and legal backgrounds.

Separately, the judiciary of England and Wales is independent of Government and to preserve that independence, the Lord Chief Justice, the Senior President of Tribunals, and the Chief Coroner have statutory responsibility for training of the judiciary. Training responsibilities are exercised through the Judicial College, which is committed to identifying and addressing judicial training needs. Judicial training is not overseen by the government.

# The Government response to fraud 2.1

**Recommendation**

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)

**Government Response**

The government agrees with the importance of ensuring that law enforcement and criminal justice partners are well trained to adhere to data protection laws.

As an independent regulator, it is right that the ICO sets its own operational priorities to deliver its statutory duties and it is not for the government to mandate formal working groups. The ICO does, however, have a responsibility to provide the necessary advice and guidance to regulated entities and promote good practice. The Crown Prosecution Service (CPS) and the College of Policing (CoP) already engage with the ICO and its guidance.

The CPS and police engage regularly with the ICO regarding data protection implications of processing information, this includes but is not limited to law enforcement purposes. This engagement supported the publication of joint principles and guidance on redaction alongside joint FAQs which are reviewed at least annually.

The College of Policing launched refreshed Managing Information e-learning at the end of 2022 which covers information handling, security and sharing. This training course is intended for everyone in policing and reflects current legislation and best practice. The refresh was led by subject matter experts and included evidence from the Information Commissioners Office audits.

# The Government response to fraud 2.2

**Recommendation**

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)

**Government Response**

Effective disclosure of unused material remains a crucial part of a fair trial and is essential to avoiding miscarriages of justice. However, for economic crime and fraud cases, the volume of digital material creates challenges for prosecutors and investigators undertaking their disclosure obligations. The government has set a multiagency working group to consider these challenges and the forthcoming Fraud Strategy will detail the further steps we are taking.

The 2018 Attorney General Review of disclosure in the criminal justice system highlighted significant concerns with the culture around disclosure, engagement between relevant parties (prosecutors, investigators, and defence practitioners), and the challenges of modern technology. Following the review, the Guidelines were revised (December 2020).

In May 2022, the Attorney General's Office published the first annual review of the Disclosure Guidelines, which concluded that the current Guidelines are a functional and effective tool but noted that future work may be needed to revisit disclosure in complex crime. Further amendments were made to the Guidelines in order to deliver improvements. These came into force in July 2022.

The Attorney General's Office regularly reviews the Disclosure Guidelines and is in the process of considering their operation in fraud cases. They will also work with the Ministry of Justice to consider how the disclosure regime in the CPIA impacts upon the efficacy and speed of prosecutions.

# The Government response to fraud 2.3

**Recommendation**

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)

**Government Response**

The government recognises that technology can play an important part in supporting Law Enforcement to triage and evaluate disclosure evidence gathered in complex economic crime cases. Given the sheer volume of material obtained in complex cases, it is imperative that processes are identified that maximise efficiencies and minimise the burden on Law Enforcement resource.

This issue was highlighted in the recent review of the Attorney General's Disclosure guidelines, and the AGO will be working with Law Enforcement Agencies to consider the development of guidance on Block Listing and Digital Sifting.

There is more that can be done to streamline this process and the upcoming fraud strategy will outline steps that the government will take to ensure Law Enforcement are best equipped to tackle complex economic crime cases, including fraud, in the digital age.

# The Government response to fraud 2.4

**Background**

There is scope to increase the use of civil remedies to take action against fraudsters and achieve justice for victims. (Paragraph 357)

**Recommendation**

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)

**Government Response**

The government is open to considering any measures that will deter and penalise fraudsters and provide adequate redress for victims of fraud where it has taken place.

Existing legislation does enable criminal and civil justice enforcement action to be taken, and in 2020/21 the National Crime Agency pursued Civil Recovery Orders with a total value of £12.7 million. Any review would need to include an assessment of the degree to which civil remedies are already available and what barriers may be perceived to using them, including legislative, procedural or financial.

To this end we propose to undertake a scoping exercise initially to make a full assessment, and seeking initial views from stakeholders including CPS, professional and industry bodies on the current use of civil remedies in tackling fraud. This initial stage will be completed in the Spring, and we will update the Committee with the conclusion and proposed next steps.

# The Government response to fraud 2.5

**Background**

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)

**Recommendation**

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)

**Government Response**

The Victims Bill and Victims' Code are designed to improve the experiences of victims of all crime types and, should they choose to report the crime, help them stay engaged with the criminal justice system. We agree that victims of economic crime, such as fraud, should benefit from the measures in the Victims Bill and the entitlements in the Code and they are already captured by the Bill and Code's definitions of a victim. Therefore, we do not see any changes as necessary.

Further to this, all victims who make a report to Action Fraud, receive advice on how to protect themselves including how to spot potential frauds and the steps to take to avoid them. The Home Office is working with the City of London Police (CoLP) to expand the Action Fraud National Economic Crime Victim Care Unit (NECVCU) across England and Wales from 2023, for victims whose cases are not investigated by the police.

Alongside this, we are also supporting the National Trading Standards Scams Team in the national rollout of Multi-Agency Approach to Fraud (MAAF) within England and Wales. This will bring together relevant agencies at a local level to improve the quality of support available to fraud victims. The agencies that form the hubs will work together to ensure that the victim is provided with the right level and type of support, delivered by the agency best able to provide that support. The team hopes to deliver full coverage of England and Wales by September 2023.

# The Government response to fraud 2.6

**Background**

The Government must consider the local needs of victims as part of any future review of the policing structure for fraud. (Paragraph 380)

**Recommendation**

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)

**Government Response**

The government is committed to a victim focused service for reporting fraud and the upcoming Fraud Strategy will detail the actions we are taking to support fraud victims We are providing over £30 million to CoLP over the next three years to replace the Action Fraud service and we are considering the merits of giving the new service a different name. Improvements already in place include better training for call handlers, with training being reviewed on a 6-month basis.

The new service will crucially improve: the ease of reporting; quality and validation of data; timeliness of the reports from the public; and provide law enforcement with better intelligence to investigate and disrupt more fraudsters.

Anyone reporting to the new service will be able track the progress of their report and receive far more timely updates. As part of the Victims Code of Practice (VCOP) police forces are mandated to provide regular and meaningful updates on the progression of their case. The government's response to the Committee's recommendation in paragraph 379 further details improved victim support roll-out.

Web reports are also now analysed to detect specific words and information to detect a victim's likely vulnerability and prioritise them for immediate assessment and one-to-one support. This can include bespoke prevention and protect advice, through to referring to their local force to initiate a home visit. When a victim meets the criteria for vulnerability, a referral is made to the victim's home force to enable contact to be made regardless of whether their case is going to be taken forward for investigation. Appropriate support is then provided.

# The Government response to fraud 2.7

**Background**

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).

**Recommendation**

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)

**Government Response**

The government agrees with this recommendation and that APP fraud (estimated by UK Finance to stand at £249 million for the first half of 2022) poses a devastating risk to UK customers, who are currently unprotected for reimbursement, unlike in cases of unauthorised fraud. Recognising the urgency to ensure customers are protected, the government have introduced a measure in the Financial Services and Markets Bill, that will allow the Payment Systems Regulator to direct banks to reimburse victims of authorised fraud on the Faster Payment System.

Short and long-term risks associated with the legislation have been appropriately captured within the Impact Assessment accompanying the Bill. The PSR has also issued a comprehensive consultation on their proposals for the future reimbursement mechanism and will respond shortly.

# The Government response to fraud 2.8

**Recommendation**

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).

**Government Response**

The government recognises that many sectors have a role to play in preventing fraud, as evidenced by the inclusion of the fraudulent advertising duty in the Online Safety Bill. The Bill will ensure that in-scope tech firms more effectively prevent fraud on their platforms. Departments across government will continue to work together to ensure that other sectors play their part.

Payment service providers are responsible for ensuring that their anti-fraud systems are effective, and that they are diligent when providing payment accounts knowing such services could be exploited for criminal gain. Firms will often have much more insight about whether a payment is suspicious than a customer who has been convinced by a highly sophisticated scam. As such, the government considers these firms best placed to reimburse victims.

Beyond reimbursement by the financial sector we continue to work with all industries, including the telecommunications and tech sectors, to ensure that protections are in place to protect the public from losing their hard-earned money and to ensure that every company does what it can to support victims.

# The Government response to fraud 2.9

**Background**

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)

**Recommendation**

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)

**Government Response**

The government recognises the importance of raising public awareness on fraud, which will form a key part of our forthcoming Fraud Strategy. One of best ways to safeguard the public is to ensure people are well-informed about the threat and how to protect themselves.

That is why we have established a new public engagement team at the NECC/NCA to drive work across the public and private sectors to coordinate anti-fraud communications, analyse what is most effective, and create consistent messages for the public.

There are numerous existing campaigns that deliver fraud messages, including National Cyber Security Centre's Cyber Aware, FCA's ScamSmart, the UK Finance run Take 5 To Stop Fraud, and others run by voluntary and private sector organisations. Action Fraud also conduct regular awareness raising campaigns. We continue to support partners to ensure these communications campaigns are well coordinated, clear and empower the public.

However government also recognises that fraudsters constantly adapt their methodologies which limits the ability of communications campaigns to protect against evolving frauds. Our new Fraud Strategy will set out how we are also expecting industry to do more to block frauds in the first place.

# The Government response to fraud 3.0

**Recommendation**

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)

**Government Response**

The government agrees that increased public awareness of counter-fraud efforts through advertising campaigns would be beneficial. We have welcomed the provision of advertising credits, by Google, toward the FCA to amplify their counter-fraud messaging. We also welcome the ongoing provision of credits by the broader tech sector, including several search engines and social media companies, to UK Finance's Take 5 campaign. As outlined in the government's response to the Committee's recommendation in paragraph 418, the government is clear that counter-fraud messaging is a vital tool in our approach to keeping the public safe.

In addition to the Online Safety Bill legislation, the Online Advertising Programme is considering how advertising regulation should be modernised for the digital age, whilst building trust in the online advertising sector. We will consider how additional non-legislative interventions can support increased public awareness, including through regulators' use of public service advertising.

The tech sector and financial sector, along with government and law enforcement, are also closely engaged on the matter, including through the Online Fraud Group (OFG), which brings together these partners. The OFG has been monitoring this work and further promotion of counter-fraud messaging will take place in due course.

# The Government response to fraud 3.1

**Recommendation**

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)

**Government Response**

The government recognises that digital skills are now, more than ever, essential to supporting a successful economy and protecting UK residents from online harm. Therefore, we are investing £1.6bn over the next three years through the National Skills Fund, which will offer Digital skills bootcamps and help adults gain the skills that are sought by employers. There are currently 26 digital apprenticeship standards approved for delivery, and the government is establishing 21 Institutes of Technology across the country, with the aim to help close skills gaps in key STEM areas, including digital skills.

The government also provides full funding for adults with no or low level digital skills to study new Essential Digital Skills qualifications and we are reforming the Functional Skills qualifications (FSQs), with new digital FSQs being introduced from August 2023.

The government also supports adults through community learning which helps learners gain news skills and build confidence, including learning for work, independent living skills, and family learning. Provision also includes English, maths, English for Speakers of Other Languages and essential digital skills.

We are also supporting schools to deliver STEM related careers education through programmes such as STEM Ambassadors. This is alongside other initiatives, including the £84m investment in the National Centre for Computing Education. Ensuring that all children, regardless of their background, have the world-class digital and computing knowledge and skills they need for the future is a key priority of this government.

The government Fraud Strategy will further detail the action we are taking to ensure young people and adults have key anti-fraud and cyber security skills.

# The Government response to fraud 3.2

**Recommendation**

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)

**Government Response**

The government agrees that it is essential that pupils are well prepared to manage their money safely, make sound financial decisions and know where to seek further information.

Financial education forms a compulsory part of the National Curriculum for mathematics and citizenship which, for secondary pupils, includes compulsory content covering the functions and uses of money, financial products and services, and the need to understand financial risk[2]. The National Curriculum also includes content about online safety and appropriate behaviour that is relevant to pupils' lives; how information and data is shared; and the dangers associated with online activity.

The computing curriculum, which covers the principles of e-safety at all Key Stages, also equips pupils to keep personal information private, protect their online identity and have the fundamental knowledge that supports them to make well informed choices about technology..

The Department for Education and The Money and Pensions Service are planning a series of financial education webinars to be delivered during this academic year. In parallel, the Money and Pensions Service has published financial education guidance to enhance schools' financial education and signpost resources aimed at equipping pupils to protect their personal data, critically evaluate online content and identify scams.

The Department for Education has published resources to support teaching about online safety. We acknowledge there is more to be done and therefore the Home Office will work to develop key anti-fraud and cyber security skills, including producing training materials to equip teachers to deliver effective fraud lessons in schools.

[2] The national curriculum sets out the programmes of study and attainment targets for all subjects at all 4 key stages. All local-authority-maintained schools in England must teach these programmes of study

# The Government response to fraud 3.3

**Recommendation**

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)

**Government Response**

Telecommunications

The government agrees with the Committee's comments on the need to educate consumers about the risks of telecoms-enabled fraud. However, as work is already underway by Ofcom, industry and wider stakeholders to help raise awareness of fraud, we currently do not believe there is a need to set formal requirements for the industry.

Ofcom published advice and launched a scams awareness campaign in 2022, on the practical steps people can take if they have received a scam call or text, including reporting them to 7726. Telecoms providers regularly publish advice on their websites on the risks of fraud and how to report it.

Industry signatories to the Home Office led Telecoms Fraud Sector Charter will also be reviewing the effectiveness of existing awareness measures and will consider using more consistent cross-sector messaging for consumers.

Online platforms

We agree that platforms should be more transparent, which is why the government has introduced the Online Safety Bill, which will require all regulated services to have systems and processes in place for users to easily report illegal or harmful content. Companies will also be required to take action in relation to those complaints, such as removing content, sanctioning offending users, or explaining why no action was taken.

Ofcom will set out expectations for these mechanisms in its codes of practice which will be risk-based and proportionate. The government expects the codes to cover areas such as accessibility (including for children), transparency, communication with users, signposting and appeals. If platforms don't comply with their duties, Ofcom, the regulator, will be able to take enforcement action and fine the relevant company up to £18 million or 10% of their global annual revenue.

# The Government response to fraud 3.4

**Recommendation**

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)

**Government Response**

The government acknowledges the vital importance of fraud prevention, and that effective customer engagement by payment service providers in relation to potentially fraudulent payments is key. The government will consider how the legislative framework, for which it is responsible, can promote effective customer engagement in relation to potentially fraudulent payments, including when considering legislative changes to enable a 'risk-based' approach to payments.

On day-to-day interventions and their effectiveness, this is a matter for the relevant supervisory authorities. In relation to its work on authorised push payment reimbursement, the PSR has been working closely with the Lending Standards Board to understand how the existing voluntary code is being applied, including in relation to effective warnings under the Code, in order to inform its approach to APP scam reimbursement.

The public engagement team at the NECC/NCA are also driving work across the public and private sectors to coordinate anti-fraud communications, analyse what is most effective, and create consistent messages for the public.

# The Fraud Act 2006 and the legislative framework 1.1

**Background**

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).

**Recommendation**

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).

**Government Response**

The independent Sentencing Council has responsibility for the creation and amendment of sentencing guidelines, which the courts must follow unless it would be contrary to the interests of justice to do so.

While sentencing is a matter for the independent courts, the fraud guideline is already clear that sentencing should take account of the harm caused to the victim, whether that is financial harm or otherwise. After determining the category of harm based on the financial loss caused or intended, the court must then consider whether there was any additional harm to the victim and increase the sentence accordingly. The more serious the detrimental impact, the higher the harm factor will be. Judges must also take into account vulnerabilities of the victim that might have been taken advantage of during the course of the fraud, for example, age, financial circumstances or mental capacity.

The government recognises that the current law on Corporate Criminal Liability does not adequately hold organisations and their senior persons to account for offences committed by the corporation and their associated persons. In November 2020, the government asked the Law Commission to do a thorough examination of the issue and present options for reform. This review was published in June 2022. We are working in collaboration with colleagues across government to consider the Law Commission's paper and determine a case for strengthening the law on corporate criminal liability. The government has committed to addressing the need for a new failure to prevent offence through the Economic Crime and Corporate Transparency Bill.

# The Fraud Act 2006 and the legislative framework 1.2

**Background**

The review of the Computer Misuse Act is welcome, however it cannot be delayed further. (Paragraph 450)

**Recommendation**

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)

**Government Response**

The government published its response to the Call for Information on the Computer Misuse Act on 7 February. The government is consulting on a number of new powers for law enforcement agencies to enhance their ability to investigate and prevent cybercrime. In addition, further work is needed on the issue of defences, which will be taken forward through engagement with stakeholders.

.

# The Fraud Act 2006 and the legislative framework 1.3

**Recommendation**

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)

**Government Response**

The government recognises how valuable it is that whistleblowers are prepared to expose wrongdoing, and believes that they should be able to do so without fear of recriminations.

The government does not support providing financial incentives to whistleblowers. The Employment Rights Act 1996, amended by the Public Interest Disclosure Act (PIDA), already gives legal protection to those who speak up in the public interest. The legislation is intended to build openness and trust in workplaces by ensuring that workers who hold their employers to account are treated fairly. Workers who believe that they have been dismissed or otherwise detrimentally treated for making a protected disclosure can make a claim to an Employment Tribunal, who can award unlimited compensation.

In relation to the SEC's regime, incentives in the US benefit only the small number whose information leads directly to successful enforcement action resulting in the imposition of fines (from which the incentives are paid). Most whistleblowers are not rewarded. Introducing incentives would require a complex and costly governance structure. The FCA's SYSC 18 rules and guidance sets out the FCA's expectations of firms in relation to their internal whistleblowing systems. Incentivising whistleblowers could impede firms in running and developing their own internal whistleblowing systems, which the FCA is keen to support.

We have continued to make both legislative and non-legislative improvements to the Whistleblowing framework to make it more robust and increase support for whistleblowers. Most recently, we have implemented a new requirement for most prescribed persons to produce an annual report on whistleblowing disclosures made to them by workers. The government has also kept the Prescribed Persons list up to date, including by adding six new bodies and all Members of the Scottish Parliament in December 2022. The government has committed to conduct a review of the Whistleblowing framework and it is our intention to add online safety regulation to the list of matters that whistleblowers are able to disclose to Ofcom in its role as a 'prescribed person.'

The government does not support the proposals in the Protection of the Whistleblower Bill as this would repeal the Public Interest Disclosure Act 1998 and introduce a new legal framework for whistleblowers.

# The Fraud Act 2006 and the legislative framework 1.4

**Background**

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)

**Recommendation**

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).

**Government Response**

We agree that identity theft is vector used by fraudsters to commit fraud, but current legislation provides an effective avenue to prosecute those committing identity frauds. The Fraud Act 2006 captures those selling and using stolen personal information to commit fraud, and legislation around data security captures the act of stealing personal information.

We believe the best response is to deny criminals the opportunity to commit identity theft through introducing measures that make identity theft and the fraud it enables a less attractive option for fraudsters.

We recognise the harm caused by identity theft to victims and are working with partners to create a victim pathway for identity and identifying ways to help victims take the steps needed to repair their identities once their identity has been stolen.

# The Fraud Act 2006 and the legislative framework 1.5

**Background**

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).

**Recommendation**

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)

**Government Response**

The Information Commissioner's Office (ICO) will update its guidance in light of the Data Protection & Digital Information (DPDI) Bill to support compliance with data protection laws. The ICO is operationally independent and will set its own priorities and approach; the new DPDI Bill will set out the ICO's overall objectives and duties that it is required to deliver against. The regulator is ultimately accountable to Parliament.

# The Fraud Act 2006 and the legislative framework 1.6

**Recommendation**

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)

**Government Response**

Fraud is a very serious crime and, as such, actions taken to prevent, investigate or detect it would be regarded as 'recognised legitimate interests' for the purposes of clause 5 and paragraph 5(a) of Annex 1, Schedule 1 to the DPDI Bill. Indeed, paragraph 681 of the explanatory notes to the Bill make this point clear:

*"Paragraph 5 [of Annex 1, Schedule 1] provides a condition for processing where it is necessary for the purposes of detecting, investigating or preventing crime or apprehending or prosecuting offenders. The reference to 'crime' would also cover economic crimes such as fraud, money-laundering, terrorist financing etc."*

These provisions should give data controllers greater confidence to process personal data for crime prevention purposes, but they are intended to capture all types of crime. Singling out fraud and not any other serious offences, might lead to unhelpful inferences being drawn about the applicability of the provisions to the offences omitted.

# The Fraud Act 2006 and the legislative framework 1.7

**Recommendation**

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)

**Government Response**

We are encouraged by the sharing of fraud risk data which is already happening in the financial sector but agree more can be done to remove barriers for effective collaboration with law enforcement. The upcoming Fraud Strategy will detail the steps we are taking to improve data sharing mechanisms.

Persons working in the regulated sector are required under the Proceeds Of Crime Act 2002 (POCA) and Terrorism Act 2000 (TACT) to submit a "Suspicious Activity Report" in respect of information that comes to them in the course of their business if they know, or suspect or have reasonable grounds for knowing or suspecting, that a person is engaged in, or attempting, money laundering or terrorist financing. This includes cases where the predicate offence relates to fraud.

Failure to do so could result in both the employee and the employer being prosecuted for criminal offences and/or facing action from the regulator. The offences of failing to disclose come under sections 330-331 of POCA and sections 19 and 21A of TACT, and the penalties for conviction on indictment are up to five years' imprisonment or a fine, or both.

It is also vitally important that industry share data with each other in order to prevent frauds, and industry have set up a Joint Industry Working group to examine standardised risk data, what information might be useful to share and the best way to share the data. The government is encouraged by this work and regulators attend the group as observers. In their consultation in 2021, the Payments Systems Regulator announced plans to ask the group to develop outcomes and timelines and also to examine the role of Pay.uk in developing rules and standards.

We are also providing £30 million to City of London Police over the next three years to support the upgrade in the Action Fraud service which will introduce substantial improvements to the process for reporting fraud and improve the quality and timeliness with which cases are sent to law enforcement for action. This will provide greater intelligence and insight to policing for investigations on fraud and allow for greater prevention and disruption at scale.

# The Fraud Act 2006 and the legislative framework 1.8

**Background**

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).

**Recommendation**

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)

**Government Response**

Tackling and reducing the impact of telecoms-enabled fraud remains a priority for the government. Telecom companies already undertake significant activity to detect, report and block scam messages and calls using their networks.

In relation to the Committee's recommendation, we do not believe that the Telecommunications (Security) Act 2021, as enacted, could be used in the way the Committee recommends.

The Act amended the Communications Act 2003 and created two powers:

1. Security regulations and codes of practice related to telecoms infrastructure but not how they are used; and
2. National security powers for the DCMS Secretary of State to limit the use of high-risk vendors.

It is not possible to use these powers, in the way the Committee suggests, to deal with matters relating to fraud or how services are used. The government will continue to assess and review options for reducing telecoms-enabled fraud through alternative routes.

# The Fraud Act 2006 and the legislative framework 1.9

**Background**

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).

**Recommendation**

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)

**Government Response**

The government recognises that the current law on Corporate Criminal Liability does not adequately hold organisations and their senior persons to account for offences committed by the corporation and their associated persons.

In November 2020, the government asked the Law Commission to do a thorough examination of the issue and present options for reform. This review was published in June 2022.

We are working in collaboration with colleagues across government to consider the Law Commission's paper and determine a case for strengthening the law on corporate criminal liability. The government has committed to addressing the need for a new failure to prevent offence through the Economic Crime and Corporate Transparency Bill.

Similarly, the Online Safety Bill will, for the first time, create a duty on social media and search engine companies to put into place systems and processes to prevent fraud on their platforms. Ofcom will have extensive powers to enforce this duty, including significant fines and business disruption.

# The Fraud Act 2006 and the legislative framework 2.0

**Recommendation**

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).

**Government Response**

The government agrees that while the sector has taken steps to address fraud taking place on their networks, more can and should be done to coordinate activity and protect customers. However, we do not believe that placing a duty on telecommunications providers to prevent the facilitation of fraud is the best approach.

Operators already undertake significant activity to prevent fraudulent calls and messages on their networks. The sector's willingness to sign up to the Telecoms Sector Fraud Charter highlights their commitment on this issue. The sector also continues to engage with Ofcom and is already working to a formal timetable set by the regulator, for the implementation of measures to combat voice call spoofing.

Government will continue to work closely with Ofcom and the sector to examine all possible steps that can be taken to tackle telecommunications-enabled fraud.

# The Fraud Act 2006 and the legislative framework 2.1

**Background**

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).

**Recommendation**

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).

**Government Response**

Action 5 of the Telecommunications Fraud Sector Charter references data sharing with the aim of developing rapid sharing of information on sources and nature of fraud attacks. We are pleased to be working with the Charter signatories and expect all telecoms companies to do their utmost to stamp out fraud. The Charter is voluntary, however, if we identified a lack of engagement, we would consider alternative options, including a 'duty to report'.

Additionally, Ofcom's recently published industry guidance notes the expectation for providers to maintain a record of any investigations, outcomes and action taken in relation to incidents of suspected misuse, working with other providers and organisations, including law enforcement, as appropriate.

Under the Online Safety Bill, the largest service providers will have to publish annual transparency reports, which will provide insights into how providers are dealing with illegal content, and the processes in place for users to report content. These reports will ensure that users can make informed decisions about the services they use. Ofcom will also publish its own annual report, which will include insights from the company transparency reports.

Clause 85 of the Data Protection and Digital Information Bill amends the Privacy and Electronic Communications Regulations 2003 ("PECR"). PECR provides specific rules in relation to privacy and electronic communications. Clause 85 introduces a duty on communications networks and service providers to report to the Information Commissioner's Office (ICO) when they have reasonable grounds to suspect contravention of PECR's direct marketing rules.

Prior to the enforcement of the duty, the ICO will be required to produce and publish guidance for organisations expected to comply. The guidance will be developed in consultation with the Secretary of State, OFCOM, and providers of public electronic communications networks and/or services. Once the duty is commenced, the ICO will investigate reports of suspected PECR contraventions and share relevant information with its law enforcement partners when criminal activity is uncovered.

# The Fraud Act 2006 and the legislative framework 2.2 & 2.3

**Background**

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).

**Recommendations**

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).

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).

**Government Response**

We agree that companies must take preventative steps to tackle fraudulent advertising. As set out previously, the Online Safety Bill will impose a duty on the largest social media and search engines to take proactive steps to prevent the publication of fraudulent adverts on their services. These companies pose the greatest risk to users regarding fraudulent advertising and we want to ensure they will no longer be able to profit from illegal activity. We have designed the Online Safety framework to be proportionate. Smaller companies pose a smaller risk and have fewer levers over paid-for ads. Ofcom will set out details on how platforms can comply with their duties in codes of practice.

The advertising duties in the Bill will only apply to the largest service providers, who have greater control over the adverts that they host. The Online Advertising Programme will consider whether it is proportionate to expand regulation to smaller services and examine the whole advertising ecosystem. This will ensure UK residents are protected from a broad range of advertising harms, wherever these occur online.

# The Fraud Act 2006 and the legislative framework 2.4

**Recommendation**

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)

**Government Response**

The Online Safety Bill will apply to services that allow users to post content online or to interact with each other (user-to-user services) and search services. This will include a broad range of websites and services, including social media services, peer-to-peer services and online marketplaces. All services in scope of the Bill will need to take action to tackle fraud, where it is facilitated through user-generated content or via search results.

The government consulted publicly on its proposals for the Online Advertising Programme earlier this year. The Online Advertising Programme is considering how advertising regulation should be modernised for the digital age. The programme is reviewing the spectrum of harms caused by online advertising and is looking at the role of all parties in the supply chain, including advertising intermediaries, services and publishers not currently covered by regulation, to provide a holistic review of the regulatory framework. We will be publishing a response to the consultation in due course.

We are continually examining the interdependencies and overlaps between online advertising and other digital regulatory initiatives. We are committed to ensuring that we do not duplicate these efforts, but instead achieve forward-looking and coherent regulatory outcomes.

# The Fraud Act 2006 and the legislative framework 2.5

**Recommendation**

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)

**Government Response**

The government recognises the importance of ensuring that Ofcom is able to work closely with, and disclose information to, other UK based regulatory bodies. We are engaging with the Digital Regulation Cooperation Forum to ensure there is strong coordination in place across the regulatory landscape.

Where appropriate and proportionate, we have included legislative measures in the Online Safety Bill to strengthen cooperation between regulators. This includes amending the Communications Act 2003 to allow OFCOM to disclose information regarding a particular business without the consent of said business for the purposes of facilitating their functions and by ensuring that Ofcom consults with the ICO on codes of practice and when issuing guidance that could have a privacy impact.

# The Fraud Act 2006 and the legislative framework 2.6

**Recommendation**

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)

**Government Response**

Government agrees with the Committee that the Digital Regulation Cooperation Forum (DRCF) plays an important role in the UK's digital regulatory landscape and provides the framework and foundations that will be needed for future coordination (please see further detail in responses made to the Committee's recommendations in paragraphs 96 and 284).

As set out in our responses to the House of Lords Communications and Digital Committee[3] and the Joint Committee on the Online Safety Bill,[4] we recognise that as the digital regulation landscape continues to evolve so will the DRCF need to adapt, but we have significant concerns about establishing the DRCF as a statutory body.

Above all, we are concerned that the creation of a statutory coordination body with powers to direct regulators would confuse issues of regulator independence and accountability, and would inappropriately delegate power to manage trade-offs between regulators and conflicts in remit, that should properly be addressed by the government working with the legislature.

We are, however, committed to continue working with the DRCF to maximise its efficacy. The work of the DRCF demonstrates the rapid progress that can be made through non-statutory forms of coordination. The Joint Statements on the interactions between online safety, data, and competition regimes[5,6,7] have shown the degree of join-up already possible.

The creation of the DRCF marked an important step forward in the effective join up across the digital regulatory landscape but we note that a wider range of regulators including Ofcom, ICO, the CMA and FCA, also play an important role. Therefore, we welcome the DRCF's commitment to revisit its membership on an annual basis, which is open to independent public sector bodies with statutory powers for regulating digital services[8], and its engagement with the Payment Systems Regulator through its quarterly roundtables.

We recognise the need for the DRCF to strike a balance between the breadth of the projects undertaken and the appropriate engagement of other public sector bodies. We note, however, the DRCF is a voluntary cooperation forum that facilitates engagement between regulators on digital policy areas of mutual interest and law enforcement agencies such as the National Crime Agency fall outside of its membership eligibility criteria.

[3] H. M. Government, 2022. Response to the HoL Communications and Digital Select Committee's Report on Digital Regulation.
[4] H. M. Government, 2022. Response to the Report of the Joint Committee on the Draft Online Safety Bill.
[5] Digital Regulation Cooperation Forum, 2021. CMA-ICO joint statement on competition and data protection law.
[6] Digital Regulation Cooperation Forum, 2022. CMA-Ofcom joint statement on online safety and competition.
[7] Digital Regulation Cooperation Forum, 2022. Ofcom-ICO joint statement on online safety and data protection.
[8] Digital Regulation Cooperation Forum, 2022. DRCF Terms of Reference.

# The Fraud Act 2006 and the legislative framework 2.7

**Recommendation**

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)

**Government Response**

Under current plans, any fine income resulting from financial penalties levelled under the Online Safety Bill will go to the Consolidated Fund to ensure the most efficient allocation of those funds.

# The Fraud Act 2006 and the legislative framework 2.9

**Recommendation**

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)

**Government Response**

The government agrees with the urgency to introduce the Digital Markets, Competition and Consumer Bill (DMCC). This is why, at the 2022 autumn statement, the government announced that it will bring forward the DMCC Bill, and introduce the Bill in the third Parliamentary session. The DMCC Bill will establish new tools to drive competition in digital markets, update the existing competition regime, and improve outcomes for consumers.