Written evidence submitted by UK Finance

1. Executive Summary

1.1 UK Finance is the collective voice for the banking and finance industry. Representing more than 300 firms, we act to enhance competitiveness, support customers, and facilitate innovation.

1.2 We welcome the opportunity to respond to the Home Affairs Committee Inquiry into Fraud. As the Committee has noted, fraud is now the most experienced crime in England and Wales, accounting for 41% of all crimes in the year to June 2022.[1]

1.3 A total of **over £1.2billion was stolen through fraud in 2022 alone**, a reduction of eight per cent compared to 2021, with this equating to around £2,300 stolen every minute of last year.[2]

1.4 According to the National Crime Agency however, a significant proportion of fraud instances are estimated to go unreported, this may be due to a variety of reasons but often it is due to a feeling of embarrassment or shame at having fallen victim to the fraud.[3] The numbers quoted here may then be representative of just a small fraction of the fraud threat facing the UK economy.

1.5 Fraud has **devastating consequences for businesses and families** across the UK. At an individual level, this creates financial loss and significant emotional trauma, with lasting consequences. At a national level, fraud on this scale undermines consumer confidence, increases the costs of conducting business and impairs the competitiveness of the UK.

1.6 The **links between fraud, organised crime and terrorism** are under-reported within the public domain but pose a significant and growing threat to the UK's national security. The banking and finance sector is at the forefront of efforts to tackle this problem. But what our industry cannot do alone, is stop fraud at source.

1.7 A common factor underpinning all frauds and scams is the criminals' use of online platforms, mobile phone networks and social media to target their victims and trick them into making payments. This includes fraudulent advertising on search engines, fake websites, and posts on social media. UK Finance has begun collecting and collating data on the origination of APP fraud which shows that 77 per cent of all Authorised Push Payment (APP) frauds during 2022 originated on an online platform. Demonstrating the scale of frauds which are initiated outside of the banking industries control.

1.8 Although these frauds originate elsewhere, in the private sector it is primarily the banking and finance industry who are investing billions in fraud prevention, paying for consumer reimbursement and funding police departments like the Dedicated Card and Payment Crime Unit (DCPCU).

1.9 UK Finance and our members will continue to advocate for increased collaboration with different sectors as the best means to truly impact the UK fraud threat.

1.10 In parallel we remain supportive of the Payment Systems Regulator's (PSR) proposal to introduce an industry wide authorised push payment reimbursement requirement. We stand ready to work with the PSR to make the new reimbursement model a success in the interests of the millions of customers served by the UK payment industry.

1.11 UK Finance and our members believe that consumers are better protected when they are equipped with the knowledge required to enable them to identify potential risks. We therefore need to ensure effective public education of all ages from key stage two through the national curriculum, covering early years, primary, secondary as well as Further Education and Higher Education is essential as are

---

[1] Crime in England and Wales – Office for National Statistics

[2] UK Finance Annual Fraud Report 2023

[3] National Strategic Assessment (NCA) Campaign 2023 – Fraud – National Crime Agency

warnings in the payment journey to ensure all members of the public are skilled and able to identify and prevent fraud.

1.12 Led by UK Finance, Take Five to Stop Fraud is a national behaviour-change campaign that offers straight-forward and impartial advice to help everyone protect themselves from financial fraud. The campaign is delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector organisations.

1.13 Recognition of the Take Five campaign continues to rise, with the latest independent evaluation finding nearly 7 in 10 respondents recognise some element of the campaign activity or messaging when prompted. Those who recognise the campaign are significantly more likely to have enacted all the campaign's Stop, Challenge and Protect behaviours than those who have not.

1.14 Don't Be Fooled aims to inform students and young people about the dangers of giving out their bank details and deter them from becoming money mules. The campaign is a partnership between UK Finance and CIFAS. It educates young people about what a money mule is, how criminals operate, why they are targeted and the serious implications of being a money mule.

1.15 Don't Be Fooled has recently worked with education specialists iChild to create a free education resource pack for primary and secondary school pupils to educate and deter them from becoming a money mule. The resources are available to schools across the country to support teachers in educating their pupils about the dangers and consequences of becoming a money mule. The pilot stage had a target of 200 schools. This was surpassed with 307 schools and an additional 10 colleges signing up.

1.16 Despite good progress on tackling fraud and the introduction of the Government's Fraud Strategy, this is an **evolving and complex threat that continues to do damage to businesses and people across the UK**. If we are to see a real difference, we need all sectors to join up with government in the fight against fraud.

2. The Prevalence of Fraud

How offenders are committing fraud and the impact of this fraud on victims.

2.1 In today's world of fraud and scams criminals mainly focus on social engineering their victims to commit their crimes. These tactics include scam phone calls, text messages and emails, as well as fake websites and social media posts. Their aim is to trick people into handing over personal details and passwords. This information is then used by the fraudster to enable them to undertake a payment transaction or to convince victims to either authenticate the payments or make them themselves.

2.2 Typically, criminals first focus their attempts on socially engineering personal information from their victims with a view to committing APP fraud in which the victim makes the payment themselves. If this is not successful, the criminal often has enough personal information to enable them to impersonate their victims, with a view to either taking control of their existing accounts or applying for credit in their name. To support this, the fraud types that have seen an increase in losses in recent years are those that require the theft of significant amounts of personal information. Fraud has varying levels of impact on victims. In many cases this can be considerable and leave a deep psychological impact. At a financial level, a recent report suggested that "nearly a third (31%) of the frauds most recently experienced by victims had a "major" economic impact."[4] The same report notes that while three in ten victims experienced no discernible negative impacts, seven in ten suffer additional harms – varying from impacts on self-confidence (35%) to detrimental mental health consequences (25%), as well as going into debt and relationship problems.[5] Tragically, there are also cases of suicide, with fraud being mentioned in the suicide note.[6]

---

[4] https://www.smf.co.uk/wp-content/uploads/2023/07/Fraudemic-July-2023-2.pdf , Page 1

[5] https://www.smf.co.uk/wp-content/uploads/2023/07/Fraudemic-July-2023-2.pdf, page 17

2.3 The nature of impact can be influenced by a range of factors which include:

- The means by which the fraud occurred.
    - Victims of unauthorised fraud may have had an element of social engineering, but this is less personal in approach and victims are reimbursed within a defined period. An authorised fraud in comparison relies on manipulation of the victim (akin to grooming in most cases). A criminal will trick their victim into sending money directly from their account to an account which the criminal controls resulting in monetary loss. At present, there is no guarantee of reimbursement and claim handling times can vary. The response for victims of authorised fraud is set to improve with a more consistent approach to be implemented via the introduction of the Payment Systems Regulators APP reimbursement requirement, due to be implemented in 2024.
    - Similarly, for card fraud, consumers are impacted differently depending on whether the loss occurred on their debit or credit card. Consumers often perceive debit card losses as 'their own money' and are therefore more impactful, while for credit cards the perception is the money belongs to the card issuer.
- The impact of monetary loss may be proportionate to the customer's financial circumstances. With the ongoing cost-of-living crisis, fraud of any value, whether a low value purchase scam or a high-value investment fraud may be more impactful than in times of economic stability.
- Existing customer vulnerability. – for examples, victims of a romance scam, who are potentially already in a vulnerable position, can feel even more exposed and vulnerable post-scam, potentially resulting in long-term harm, such as social isolation and long-term trust issues. Fraudsters adapt quickly to take advantage of societal issues to increase their chance of success. The Covid pandemic was a perfect storm for criminals, with more than 6,000 cases, totalling £34.5m, of Covid-related fraud and cyber-crime recorded by the UK's police forces during the pandemic.[7] More recently we have seen criminals "masquerading as victims of the war in Ukraine" to steal money from the generosity of the British public,[8] or exploiting challenges people are facing due to the cost-of-living crisis.[9]

2.4 Individuals who act as money mules, allow their account to be used for the purpose of moving fraudulent funds away from the account of fraud victims are rarely seen as victims. However, in recent years we have seen a growing percentage of money mules who are themselves victims of crime. For example, vulnerable victims of romance scams who are manipulated into moving funds for their 'partner', but which are in fact the proceeds of another crime, or at the extreme end of the scale, young individuals who willingly allow their account to be used to launder funds, but which leads onto more harmful exploitation such as their involvement in county line activity or sexual exploitation.

2.5 The impact of fraud on victims is considerable, and in some cases can be devasting and irreversible. We welcome the Fraud Strategy's focus on pursuing fraudsters and supporting victims, but we must also remain focused on the delivery of a whole system approach to drive forward prevention, education, and awareness to stop the fraud from occurring in the first place.

How the emergence of new types of technology, such as artificial intelligence, is being used to commit fraud.

2.6 Artificial intelligence (AI) is being used by criminals to generate infrastructure and create malware interfaces and websites more quickly. AI is now commonly being used to create fake celebrity

---

[6] Gwynedd man killed himself after paying romance scammers - BBC News; Mother and daughter killed themselves after being targeted in elaborate scam | Crime | The Guardian; Fighting Fraud: Breaking the Chain (parliament.uk)

[7] https://www.bbc.co.uk/news/technology-56499886

[8] Ukraine war: Fraudsters exploit crisis to steal money - BBC News

[9] Criminals are using the cost of living crisis to scam the public – don't become a victim | Action Fraud

endorsements for investments, which provides an element of credibility to the scam. These risks accelerate the potential rate of harm to victims.

2.7 From a sending payment service provider (PSP) perspective, AI is not a significantly emerging trend observed by the financial sector. Whilst there is speculation that voice biometrics could be spoofed, the banking sector is developing risk mitigating solutions to minimise their impact. The greater risk is being observed in the mules account space where we are seeing an emergence of deepfake software being used during customer onboarding. Deepfake software is used to create a digital version of someone. This maps a person's face and mouth movements so that it can then copy them. Amateur deepfakes can usually be spotted by showing unusual flickering or blurring around someone's face. However, with technology in this space advancing, more realistic deepfakes are appearing which can be used to mimic the image displayed on a genuine driving licence, or other form of photographic ID, during on-line and in app account applications. PSPs are actively sharing intelligence and emerging trends to support mitigation of this risk.

The role of internet providers and social media providers in enabling or preventing fraud and actions they could take

2.8 In a continuation of a longer-term trend, the cost-of-living crisis, combined with amended shopping behaviours post Covid, means more consumers are looking to online marketplaces for convenient and cost-effective shopping.

2.9 When internet providers and social media firms are alerted to fraudulent domain names and scam pages, adverts, and profiles, the financial sector believe they are too slow to act. This leaves the fraudulent websites and social media pages active, and the risk of continued consumer interaction remains present.

2.10 There is minimal friction in place to prevent new scam accounts being opened or to warn the general public of the prevalence of fraudulent adverts on social media. UK Finance members would welcome activity to mitigate this within the anticipated Tech Charter and Online Safety Bill codes of practice from Ofcom.

2.11 The issues are well known by the financial sector, law enforcement and HMG and there are multiple programmes of work, initiatives and strategies running in parallel designed to increase collaboration between the payments industry and big tech companies to mitigate risk. However, we believe these could be improved by clearer timelines and closer cross-sector/public-private leadership to minimise duplication of efforts. There remain gaps in the coverage of the following initiatives, and whilst there are mechanisms coming into place, it is challenging to assess the future gaps which criminals will exploit:

- **Online Advertising Programme** – Following the Online Advertising Programme consultation, published in March 2022, the government set out its next steps for the online advertising programme. The programme will look specifically at paid-for online advertising to ensure holistic coverage across the online content that can create harm for consumers and businesses alike. To deliver the activity set out in the programme the government has formed a ministerial Task Force. The Task Force does not have attendance from the financial services sector to inform the harms, track the impact nor contribute lessons learned. This is a missed opportunity as financial services intelligence could aid focus of the work-plan. This is a multi-year programme of work, with widening responsibilities. It is critical that through campaigns and requirements placed on those firms who host fraudulent advertising it is made clear to the public the risks they face. It is our industry's belief that true cross-system collaboration, from all sectors involved in the process of fraud, is required if we are to make a material difference to the threat posed.

- **Cyber Duty to Protect** – the Home Office believes there is a need to consider new proposals to reduce this threat, by reducing the burden on the public for cyber security. The working title for these potential measures is the 'Cyber Duty to Protect'. This will create new responsibilities on sectors that could prevent criminals from leveraging their services as a mechanism for targeting victims.

- **Government Fraud Strategy**
  The banking and finance industry has, in recent years, established good relationships with telecommunication companies, internet and social media providers. We look forward to strengthening this engagement further through the delivery of coordinated cross-sector prevention activity. The Government has a clear role to play in fostering and supporting collaboration and would be an ideal convener of formal cross-sector alliances.

The cross-cutting nature of fraud, e.g., how it may start as one type of fraud and progress into another.

2.12 To commit unauthorised fraud, criminals typically employ a range of social engineering techniques to trick victims into giving away their personal and financial information, such as their internet banking one-time passcodes and log in details. This includes using impersonation scam calls, emails or text messages typically exploiting current affairs (energy bill discounts, cost-of-living support, etc.) by impersonating trusted organisations such as HMRC, internet service providers (ISPs) and e-commerce companies. The stolen details are then used to access a customer's online account and to make an unauthorised transaction. Criminals also abuse remote access software applications to gain control of their victim's online banking facilities. The criminals will typically claim to be providing support from an IT service or ISP and convince the customer to download and install remote access applications to their laptop or PC.

2.13 As outlined earlier in this response, for authorised fraud, the use of social engineering tactics to defraud people remains a key driver behind the losses. Typically, these deception and impersonation scams involve the criminal posing as a genuine individual or organisation and contacting the victim using a range of methods including via telephone, email, and text message. Criminals also use social media to approach victims, using adverts for goods and investments which never materialise once the payment has been made. APP fraud losses continue to be driven by the abuse of online platforms used by criminals to scam their victims. These include investment scams advertised on search engines and social media, romance scams committed via online dating platforms, and purchase scams promoted through auction websites.

2.14 The payments industry holds a wealth of actionable intelligence, which we believe could be used by online platform providers to support prevention of fraud at source. A mechanism is however, yet to be identified which will support the ingest of relevant data from all regulated sectors within a set service level agreement.

2.15 At present, financial fraud is often captured within wider policy infractions. There is a need for greater, standardised fraud classifiers within other sectors. Without this it is difficult to focus in on specific areas of criminal activity. Internet infrastructure providers and social media firms must have fraud as a priority category for tracking.

2.16 We see a wide range of frauds that evolve into other frauds or crime types, some examples are provided below:

Recovery scams
Fraudsters of this scam type prey on victims of fraud by posing as agencies who can help them to recover funds lost as part of a previous fraud. The victim is convinced that by paying a small amount, often described as an admin fee or tax, the money they lost, often to an investment fraud can be recovered. Victims of larger value frauds are often more susceptible to this type of criminal approach, as they may be more willing to part with a proportionally small sum of funds to regain the previously lost funds.

Romance scam to an investment scam
A consumer on a dating website looking for a connection is befriended, and an online relationship is formed. Over time rather than the victim being asked to pay money for fictious legal or medical bills they are encouraged to make investments, opening e-wallets with crypto exchanges, of which they give the fraudster access. The victim is then continually encouraged to pay in until such a time as they recognise that they are being scammed or until someone intervenes to stop further payments.

Romance scam to money mule
Very similar to the above, however instead of the victim being asked for money, they are asked to receive money and send it on to other accounts controlled by the fraudster. These funds would have originated from another fraud and this victim, in allowing their account to be used for the transfer of funds, is themselves involved in the facilitation of the crime.

Romance scam to sextortion (including the use of AI to create fake images) – these cases start as online relationships, with the fraudster making requests for payment. However, the relationship evolves when the victim is blackmailed by their 'partner', usually under the proviso that they have images (legitimate or AI-generated) that they will send to friends or family members unless a payment is made.

2.17 In addition, we see hybrid cases where victims are encouraged to use various methods of payment as part of a single scam. An example is where current account funds and savings are exhausted to fund an APP fraud, and victims, to continue to meet the requests of the criminal will then use credit cards (Authorised Card Scam) or take out loans.

2.18 Social engineering underpins all of these frauds, with varying levels of emotional damage suffered by the victims. Whilst financial compensation may cover some of the damage done with regards to financial loss, this will not remedy the emotional harm caused and the loss of confidence or trust.

3. Reporting, investigating and prosecuting fraud

The effectiveness of the current system for reporting investigating and prosecuting fraud, including work with international partners in tackling fraud

3.1 It has been reported that only 2% of police funding is dedicated to combating fraud despite its accounting for 41% of reported crime. We welcome the Fraud Strategy's consideration of fraud as a strategic policing requirement and the creation of a new fraud focused intelligence team.

3.2 Action Fraud estimate that only a small percentage of victims, approximately 10 percent, report frauds through their platform, whilst the National Crime Agency believe that 86% of frauds go unreported.[10] The mechanisms for consumers to report fraud must be improved. We should be moving towards a position where consumers are only required to report once.

3.3 Current systems are not interoperable. They should be reviewed to identify the development required to enable a consumer to report once, through their preferred route, i.e., the Action Fraud on-line portal, direct to their payment provider or via social media or telecommunication platforms and for this information to then be communicated to all relevant stakeholders. Simplifying reporting options for consumers will encourage increased reporting and enabling this data to be shared across stakeholders will provide both industry and law enforcement with a better understanding of the full impact of fraud and early identification of evolving trends.

3.4 In the design of any change to consumer reporting, banks and payment providers should be informed as early as possible, given their ability to prevent the onward movement of money, reducing criminal gain and enabling funds to be returned to victims or the reimbursing PSP.

3.5 An increased volume of timely reporting will provide law enforcement with the relevant intelligence to take enforcement action where possible. However, we must recognise the scale of the problem we face and the limited resources available across law enforcement to investigate. As such, law enforcement must prioritise activity which may prevent frauds from occurring. **UK Finance and our members are then disappointed by the increasing number of regional forces who are considering downgrading the Banking Protocol response**. The Banking Protocol is a UK-wide initiative which enables branch staff in financial institutions to call 999 and receive an emergency

[10] National Strategic Assessment (NSA) Campaign 2023 - Fraud - National Crime Agency

response where somebody is in branch, withdrawing cash, or making a transfer which the financial institution believe may be part of a scam. The Banking Protocol has been hugely successful preventing over £282.3 million in fraud and enabling 1,298 arrests since it launched in 2016. On average the initiative now prevents between 5 and 6 million pounds per month. With the volume of authorised frauds remaining high, it is concerning that law enforcement would consider downgrading their response at this time.

International dimensions

3.6 Fraud is an international concern, with criminals acting globally, however there is only limited international investigation of these crimes with most UK law enforcement resources focused on regional activity.

3.7 UK Finance members sympathise that a global response strategy to fraud is a hugely challenging task, but this should not negate the necessity of working towards a coordinated global response. We see pockets of international partnerships, such as the European Money Mule Action (EMMA) initiative which takes place yearly and delivers tangible results. EMMA is a period of intensification coordinated by Europol, from which we could derive best practice, however it is unlikely this international way of working will ever become business as usual activity until a long-term international fraud strategy is developed.

3.8 One of the significant barriers to increased international collaboration is the existence of differing legislation internationally. We have seen recent cases of holding accounts, located within the UK, which are used to credit funds into wallets held within a different jurisdiction. Where PSPs have the mechanism in place to engage with the receiving PSP and fraudulent funds are frozen, it is not always possible to repatriate due to conflicting legislation. We regularly see legislation which acts as a barrier to international data sharing and funds repatriation. We must act now to deliver a legislative landscape which supports international collaboration through data sharing and law enforcement investigation. Through the presence of the Prime Minister's Anti-Fraud Champion, the hosting of an international summit in 2024 and the focus on fraud provided by the Fraud Strategy and inquiries like this, we believe the UK is ideally placed to put fraud on the multilateral agenda.

The response of the criminal justice system to rising fraud, including in sentences and other outcomes

3.9 UK Finance believes others will be able to provide the Committee a detailed view on this, however we would draw the committees attention to the House of Lords report 'Fighting Fraud – Breaking the Chain'[11], published in June 2022 which provides a comprehensive view of the status, gaps, and recommendations for improvement in the criminal justice systems response to rising fraud.

Given that it is estimated 70% of fraud either originates aboard or has an international element, what is being done to prevent fraud arising through those international channels?

3.10 UK Finance believes others will be able to provide the Committee a detailed view on this. it sympathises with the challenges Government faces to cause change and improvement from overseas jurisdictions vulnerable to criminal activity in the fraud landscape. However, given the scale of the problem and the direct effect this has on the UK, it is paramount that significant action is taken.

What other countries are achieving in terms of detection, prevention, and prosecution of fraud.

[11] https://lordslibrary.parliament.uk/tackling-fraud-lords-committee-report/

3.11 UK Finance would call out the below examples of positive international examples:

Australia: The Australian Payments Network are mirroring activity already underway across the UK, such as twice-yearly fraud trend reporting to raise consumer awareness of fraud and the coordination of prevention activities such as Do Not Originate and MEF sender ID replications and SMS firewalls.

Brazil: In October 2020, the Central Bank of Brazil introduced PIX, a real-time payments system offering speed and ease of use. PIX was introduced to bring interoperable QR codes to digital wallets 24/7/365, meaning that person-to-person (P2P) payments can be made conveniently and instantly, and that merchants can accept payments without incurring extra acquiring charges. There are conflicting views regarding the success of PIX in countering fraud, but what is clear is that the scheme has been built with a high ability to evolve in line with the changing fraud landscape.

Netherlands: Five Dutch banks have joined forces under the name Transaction Monitoring Netherlands (TMNL) to tackle financial crime by collaboratively monitoring the banks' payment transactions for signs that could potentially indicate money laundering and the financing of terrorism.

Singapore: The Anti-Scam Centre (ASC) was set up by the Singapore Police Force (SPF) under the Commercial Affairs Department on 18 June 2019 to serve as the Police's nerve centre for investigating scam-related crimes. The ASC aims to disrupt and prevent scam operations to mitigate victims' monetary losses through the swift recovery of proceeds of crime, amongst other initiatives. To combat scams, the ASC adopts six Is in its approach – Information processing, Intervention, Investigations, Initiatives, Inculcation, and International Co-operation

The Global Anti-Scam Alliance (GASA): This is a non-profit organization primarily developed to tackle on-line scams globally. The alliance aims to raise awareness, organize research, enable prevention tools, support legal best practices, and train consumers on how to avoid scams online.

3.12 One question we believe should be explored further is whether there would be merits in a fraud equivalent of FATF. The Financial Action Task Force (FATF) leads global action to tackle money laundering, terrorist, and proliferation financing. The 39-member body sets international standards to ensure national authorities can effectively go after illicit funds linked to drugs trafficking, the illicit arms trade, cyber fraud, and other serious crimes.

How better to collect and use data on the scale, cost, and nature of fraud.

3.13 UK Finance and our members believe that there should be a single 'tell us once' fraud reporting system, enabling consumers impacted by fraud to report to their platform of choice and for the platform to disseminate the information to the impacted PSP's, law enforcement, social media, etc.

3.14 In the absence of a 'tell us once' fraud reporting system, it is essential that consumers are incentivised to report all fraud events. This is the first step to the payment industry and law enforcement having access to adequate data. We are disappointed that in the recent PSR consultation into the APP reimbursement requirement, consumer standard of caution, the regulator stepped back from the inclusion of a requirement for all victims of authorised fraud to report to law enforcement prior to reimbursement. This is in direct contrast to the position of the EU Commission, who in the drafting of PSD3 introduced a requirement of consumers to file a police report and notification to their PSP without undue delay prior to financial reimbursement.

3.15 We also believe that there is a need to distinguish enablers, delivery mechanisms and precursor events consistently for all reported fraud cases. Currently the most prevalent delivery channels

exploited by criminals to engage with consumers are telecommunication and social media. An end-to-end measurement of attribution and identification of intervention opportunities is required.

3.16 There is no common standard across stakeholders for the recording of enabler data. Therefore, the enabler may be listed differently dependent on where or how a fraud is reported. This makes management information recorded by different sectors incomparable. For example, the WhatsApp scam often starts on SMS before moving onto the WhatsApp platform and finally into the payments sector. A consumer may report the scam to any one of the impacted providers and in the current climate it may be recorded differently.

3.17 An exercise should be conducted to attribute an average cost to all impacted parties, i.e., consumers, banks, law enforcement, telcos etc. broken down per fraud type and subcategory. These values can then be used to calculate the cost of fraud to the United Kingdom enabling trend analysis.

4. Government's response to fraud

The Home Office's progress to date on tackling fraud

4.1 Ensuring that fraud is not considered in isolation but is examined in the context of economic crime is critical. The links between fraud, organised crime and terrorism pose a significant threat to the UK's national security as both the Economic Crime Plan and Government Fraud Strategy recognise.

4.2 We welcome the Committee's approach to consider the Government's new Fraud Strategy launched in May 2023. The strategy sets out a plan to stop fraud at source and pursue those responsible wherever they are in the world, reducing fraud by 10%, based on 2019 levels, by December 2024. We remain concerned that not enough responsibility is being placed upon what the House of Lords calls "fraud enablers" in big tech and telecoms.[12] The burden of liability cannot solely sit with banks. The rationale being that the divergence between 'voluntary' and 'proportionate' versus 'must reimburse' is too great creating limited incentives for others involved to put right victims through financial reimbursement.

4.3 Whilst the strategy seeks to take a holistic approach to tackling fraud, the asymmetry of responsibilities and lack of clear road map remains of concern. There have been several consultations released focusing on this subject, which is positive, but the delivery timeframes of the components remain unclear.

4.4 Fraud undermines consumer confidence, increases the costs of conducting business, therefore worsening the cost-of-living crisis, and in the case of public sector fraud, compromises the government's ability to deliver services and achieve intended outcomes.

4.5 We welcome the Online Safety Bill, Online Advertising Task Force and Cyber Duty to Protect in demonstrating the government's commitment to regulate origination and publication of fraudulent content which we believe will compel action on the part of online platforms.

- **Online Safety Bill** – The Online Safety Bill is a proposed new law to protect children and adults online. It will make social media companies more responsible for their users' safety on their platforms. The Online Safety Bill will also introduce a standalone measure for in-scope services to tackle the urgent issue of fraudulent advertising. There are dependencies on secondary legislation for the advertising element, which means there is timeline delay for fraudulent advertising being mitigated.

- Given the importance of the role of Ofcom as the online safety regulator, it is important Ofcom is adequately resourced, funded, and prepared (including skill and expertise) for the enormous task that lays ahead of them.

[12] Fighting Fraud: Breaking the Chain (parliament.uk)

- As Ofcom's ***information gathering powers*** do not come into place until royal assent of the OSB, the regulator will need to produce codes of practice for consultation without having had the benefit and insight that these powers can provide. As a result, there is a risk there will be an iterative approach with the codes of practice, and this will create extended lead times for effective implementation. We believe that the information gathering powers will need to be leveraged during the earliest stages of the consultation cycle to ensure the most robust codes of practice can be created in the first instance.
- The precision of Ofcom's ***codes of conduct*** and ***risk assessment guidance*** will determine the efficacy of the online safety regulation and implementation by the platforms. As such, these codes and risk assessments should have a focus on ***impact and incidents as a core consideration***, rather than the relative volume or victims as the impact faced could be significant. Proportionate controls based on legitimate and illegitimate activity could overshadowed the harms faced by victims given the size of the online platforms.
- There is an urgent need for ***supporting mechanisms to ensure delivery*** against the 'duty to operate a service using proportionate systems and processes designed to— (a) minimise the length of time for which any priority illegal content is present; (b) ***where the provider is alerted by a person to the presence of any illegal content, or becomes aware of it in any other way, swiftly take down such content.'***
  - The platforms typically provide either consumer or law enforcement reporting options which either dilutes or sets the bar too high for the regulated sector intelligence. This significantly limits the rich intelligence available from the regulated sectors impacted by online harms, as the Financial Services sector often has actionable intelligence, that can often be explicitly linked to criminality. However, currently many platforms have 'conduct rules' and therefore will not remove content that is not explicitly illegal unless it breaches these conduct rules. Definition and alignment of the key requirements for removal of harmful content should be defined before data sharing to ensure consistency and efficiency of action off the back of data sharing between platforms and financial services.
  - There is also currently no mechanism available to feed this information into online platforms from regulated sectors nor any SLAs for treatment of the issues identified.
- It is unclear what the targets for prevention will be and what non-compliance to the duties to prevent fraudulent advertising will look like. Ofcom must be suitably empowered and supported to take serious action against offending parties, in the way regulators such as the FCA are.

4.6 Industry data indicates that approximately 77 percent of scams originate via on-line platforms, as well as 3rd party fraud being facilitated on platforms. The proposed cap of £18million may then seem disproportionate to the scale of harm enabled.

4.7 Economic Crime Plan 2 (2023-26)[13] includes commitments to help prevent and reduce fraud against the public sector. Though outside the scope of our specific remit, we recognise the significance of public sector fraud in the UK and the need to act. We remain committed to supporting Government in its actions.

4.8 Increased education, particularly of those consumers with greatest vulnerability, is needed to further empower the public to be better able to detect, respond and report potential fraud. **The financial sector has acted to include warnings, advertisements, and significant friction in the payment process to educate and help customers.** At 41% of all crime, we believe it is paramount that **other sectors in the fraud process are mandated to do the same.**

4.9 Greater understanding of economic crime through the roll out of basic training is needed across the UK Police and law enforcement community to ensure that the policing response to fraud in the UK is effective. Economic Crime investigation and prevention needs to be considered as a career path within law enforcement. Officers are generally seen as a resource to be deployed where needed, but economic crime is a complex subject taking time to fully understand. However experienced officers are frequently moved off to other teams, taking their knowledge with them.

---

[13] Economic Crime Plan 2 2023-26 (publishing.service.gov.uk)

4.10 There is no shared view of threats and coordination of activity across the public sector. This results in ever increasing and conflicting demands on the regulated sector and a lack of alignment towards allocation of resource to higher priority threats/areas of focus.

4.11 There is an absence of legal gateways to permit regulated firms to share information with each other prior to suspicion without liability for breach of confidence. We urge the Home Office to ensure these gateways are delivered.

Whether its recently published Fraud Strategy does enough to combat fraud

4.12 We believe that the Fraud Strategy is a good start but needs to go further. It includes many positive steps around mass-text aggregators, cold calling, SIM farms, the Online Safety Bill, Online Advertising Guidance, re-platforming of Action Fraud and the inclusion of fraud education in the curriculum.

4.13 The scale of attack against the UK is vast and shows no sign of abating. The recent iSpoof case is a clear representation of the scale of the challenge we face. Millions of calls were made to UK citizens in a brief period. It should be noted that whilst the Fraud Strategy applies to England and Wales, fraud is a UK-wide problem. It must also be acknowledged that fraud is not limited to consumers; many businesses and corporate entities are being targeted.

4.14 Whilst the Government Fraud Strategy aims to provide a holistic response, there remains a range of initiatives being progressed, for example Public Private Sector Partnerships via cells run by the NECC and initiatives being delivered by the Joint Fraud Task Force. We recognise there is an ambition to tie this all together through the development of an economic crime data strategy, as set out in the Economic crime plan, but there is a risk that if all of these activities are not brought together the overall impact will be diluted.

4.15 In addition, we note that the Strategy does not impose controls on other sectors, focusing exclusively on the activities of the financial industry, e.g., there is no mention of monetary contributions to the reimbursement of victims of fraud, or the funding of prevention activity by enabling sectors. We have long called for a fairer share of funding across the ecosystem and welcome the Financial Conduct Authority's recent recognition that "Online platforms are a significant source of fraudulent activity. While several of the largest technology and social media firms have taken steps to tackle problematic promotions and advertising on their platforms, far more needs to be done. The banking industry has also called for a more balanced distribution of costs associated with compensation of fraud to customers, including an appropriate contribution from technology and social media platforms."[14]

4.16 We are supportive of an ambitious Tech Sector Charter which we hope will be accompanied by a credible list of proposals. We are committed to working closely with the ecosystem to reduce the harm caused by fraud.

Whether the current machinery of Government is sufficient in tackling fraud

4.17 There are multiple initiatives being launched in this space, but there is no holistic view and no clear steer as to who is leading each. We believe that the Economic Crime Plan and Fraud Strategy need to lead delivery of the outlined actions rather than general monitoring of the landscape.

4.18 Tackling fraud is, and should remain, a cross-party objective. The well documented scale of the challenge, its continuing evolution and the national security risks posed by fraud means that the Fraud Strategy should be the start of a concerted, joined up approach to tackling it rather than an end in itself.

---

[14] https://www.fca.org.uk/publication/correspondence/fca-chancellor-provision-banking-services.pdf

FRA0048

October 2023