Financial Conduct Authority – Written evidence (FDF0069)

1. **What fraud risks are UK a) individuals, b) the Government and c) businesses particularly vulnerable to today, and what are the reasons for this?**

   The fraud landscape has evolved since 2006 and continues to present new risks for all individuals and businesses operating in the UK. As technology develops, there has been a corresponding increase in online and technology-enabled scams within the UK and overseas targeting UK consumers. The increase in online activity and reliance on online financial services during the Covid-19 pandemic and current cost of living pressure has been exploited by fraudsters, exposing consumers to further vulnerability and risk. The number of fraud offences against individuals continues to rise annually, with a 14% increase in 2021 from 2019.[1] Between April and September 2021, the FCA received 16,400 enquiries about possible scams, up nearly a third from the same period in 2020. Not all of these will be investment scams or within our remit as scams and frauds of all kinds are reported to us. They are all individually assessed to determine whether we have power or remit or whether they need to be referred to another agency or law enforcement body. The type of scam most frequently reported to the FCA are crypto-asset scams, many of which we do not have power to tackle, new types of boiler room scams and recovery scams.

   These reported harms, in aggregate, are important because they affect confidence which, in turn, impacts UK economic and financial security. Fraud not only threatens the financial well-being of consumers, but also imposes a significant cost on businesses who are also threatened by fraudsters.

   Fraud must be tackled directly by Government, not only with strategic planning, but with adequate funding. While the FCA has a clear role to play, especially in ensuring confidence in UK's financial markets, law enforcement agencies need to be adequately funded to tackle economic crime and to ensure it is not de-prioritised.

2. **What future economic and technological developments are likely to impact how fraudsters seek to commit crime over the next five to ten years, and how might these be prepared for and mitigated? What role can technology and tech companies play in combatting fraud across this timescale.**

   Historically, investment scams were driven by 'boiler rooms' where fraudsters set up physical call centres from which they cold-called investors offering worthless, overpriced, or non-existent investments.

   An online fraudster can set up an online scam much more easily without a physical address. These scams operate virtual call centres and can target consumers in the same way legitimate online advertisers target their customers, therefore making it difficult for consumers to differentiate

[1] Crime Survey of England & Wales: 5.2m fraud offences against individuals in YE Dec 21, a 41% increase on levels in YE Dec 19

genuine marketing from fraudulent. In most cases, online scammers use fictitious identities and addresses, giving them anonymity. Identities are further disguised through complex layering across multiple jurisdictions to launder the proceeds of crime.

We welcome the Online Safety Bill (OSB) and Government's focus on ensuring platforms have systems to prevent the publication and hosting of fraudulent advertising. We also welcome the recommendations of the Joint Committee Report on the OSB on the inclusion of paid-for advertising in the Bill's scope, and the Government's response to that recommendation. The establishment of Codes of Practice will set out what platforms will need to do to fulfil their new duties, including verifying the identity of anyone wishing to publish adverts and ensuring that only financial promotions by FCA/PRA-authorised firms (or approved by them) are issues. We look forward to working closely with Ofcom on the Codes' detail.

Following our engagement, Google and Bing changed their policies to only permit FCA-authorised firms to market financial services, including investments. This has proven to be a significant step in ensuring searches for paid-for advertising exclude the most obviously suspect sites. However, scammers will innovate in response, which is why the OSB's measures providing for regulatory innovation and agility via the Codes, is so important.

We understand from engagement with Twitter that they check our Register to verify whether a firm or individual associated with content on its platform is authorised by the FCA. We are continuing to seek further commitments from Twitter. We are speaking to Meta and others to secure similar commitments and action.

There are other new threats on the horizon. Emerging metaverse technology may be susceptible to exploitation in the next few years. Several companies are developing their own metaverse, each likely to have its own set of networks and protocols. It is not yet clear whether identity checks (KYC) required in the "real world" to guard against financial crime will be conducted in these global virtual spaces. The jurisdictional issues regarding 'where' misconduct in the metaverse occurs, and how regulators and law enforcement can engage effectively, must be tackled now rather than when harm occurs.

Those investigating fraudulent representations made in a virtual metaverse environment will find it challenging to locate perpetrators. Even if the jurisdiction of the metaverse server is known, retrieval of evidence from online servers is likely to be challenging and time-consuming without international arrangements for evidence access.

There are steps that can be taken now to tackle this.

We welcome the Crime (Overseas Production Orders) Act 2019, which provides for overseas production orders to require a person based overseas to produce stored electronic data or give access to electronic data. The UK-US Treaty was signed in October 2019, but the provisions are not yet in force. We await the finalisation of terms between the UK and US. This is now an urgent matter.

Fraudsters' ability to misuse technology to "scale-up" automated frauds online to target large audiences is deeply concerning. Knowing that online providers overseas will have to provide information will deter organised criminals and help law enforcement agencies to track them down. This is especially important given online fraud is a global phenomenon operating without boundaries and borders, by contrast to law enforcement agencies and regulators operating within jurisdictional and legislative limits.

Currently, there is no centralised metaverse environment, or clarity on who is responsible for the oversight, regulation and enforcement of these virtual spaces. International co-ordinated regulation may be difficult; for example, jurisdictions do not regulate cryptoassets in the same manner. How to mitigate this emerging threat is a difficult question - the existing counter-fraud framework was not designed to address the unknowns of virtual commerce.

3. **Are fraud and its victims treated as a priority? If not, what are the reasons for this? The Committee is particularly interested in responses that can explain any barriers preventing effective counter-fraud co-operation within Government, law enforcement, the public sector and the private sector.**

Protecting consumers is an operational objective for the FCA. Reducing and preventing serious harm, including reducing and preventing financial crime is a priority commitment outlined in our three-year Strategy supported by our Business Plan 2022/23.

The FCA draws on all tools at its disposal – including scrutinising firms undergoing authorisation, assertive supervision, and sharing intelligence with other agencies - to detect and prevent financial crime, disrupt and pursue individuals, and remove FCA-regulated fraudsters from the financial system. We run media campaigns, monitor social media for suspicious adverts, and operate warning lists to inform consumers (see Q9). We proactively monitor and reduce the prevalence of online investment scams and work with online platforms to remove fraudulent websites.

In many of these cases we prioritise consumer redress and in cases involving regulated firms, have secured very large compensation payments. These are often made voluntarily by firms, incentivised by our commitment to take this into account when imposing penalties and sanctions and, where appropriate, reduce their severity. Compensation is also payable by the Financial Services Compensation Scheme (FSCS). Recently the FSCS paid approximately £50 million in compensation related to action we took against five individuals involved in schemes that led to over 2,000 consumers transferring pension pots into inappropriate high-risk investments.

In cases concerning scams by firms not authorised by us, the chance of obtaining redress (and its extent if obtained) is inevitably much lower. During financial year 2020/21, we pursued approximately 50 cases against unauthorised business with approximately £21.7m compensated to victims for unauthorised investment businesses and nearly £7m being frozen on investors' behalf. The amount of loss to victims in these cases

was much higher, but the rate of return reflects the challenge of recovering money in fraud cases where the fraud involved unauthorised regulated activity.

In our work we see the devastating effects that fraud can have on victims and their families. Beyond the immediate impact of often life-changing financial loss, the mental and physical well-being of victims, their families, and communities is invariably impacted as well. Fraud destroys lives. Financial redress, even if available, cannot fully restore victims to the position they were in beforehand.

Alongside traditional enforcement, preventative campaigns to empower consumers, investor education, and scam disruption are crucial. Our Scamsmart campaigns, based on work with marketing specialists with expertise in developing behaviour change campaigns, use various media including our website to educate consumers on how to identify scams. They emphasise the importance of consumers dealing with FCA-authorised firms. This month we launched our most recent campaign warning consumers about screen-sharing software.

We work with partners including Action Fraud, banks, pension providers, the Pensions Regulator, Money and Pensions Service, and consumer groups, to maximise the reach of our messaging to reach those most at risk.

Over the last 6 years, we have invested in nine multimedia advertising campaigns, targeting specific audiences with evidence-based, creative communications guided by behavioural science designed to build awareness of the risks of investment scams, loan fee fraud and pension fraud.

Data show strong recognition of and engagement with ScamSmart among 'at risk' audiences:

- Over 2 million visitors to the ScamSmart website
- Nearly 250,000 people have interacted with the FCA's Warning List
- Almost 35,000 users of this tool have been warned about an unauthorised firm

Another campaign, InvestSmart is designed to inform newer, often younger, investors tempted to buy complex, higher-risk products that are very unlikely to be suitable for them and do not reflect their risk tolerance. While not specifically for fraud prevention, the campaign aims to help consumers make better-informed investment decisions suited to their financial circumstances and risk tolerance. We reflected our target audience in the media channels we used to disseminate InvestSmart's message - platforms like TikTok, and partnerships and influencers. Early results show TikTok as a successful driver of visitors to our website, where consumers can find further information.

The FCA proactively monitors and conducts surveillance to detect and address suspicious advertising daily. We published over 1,410 consumer warnings in 2021 (over 1,200 were issued in 2020, 573 in 2019) on our

Warning List, which is updated daily, in relation to UK-based or overseas sites and firms suspected of carrying out unauthorised business. We often issue consumer warnings within 24 hours of detecting a suspect site. The List is public so can be used by consumers, and financial services firms to protect themselves and customers.

In March 2021 the FCA launched the Unregistered Crypto Currency Businesses List, which identifies crypto-asset firms that appear to be carrying on business in the UK but are neither FCA-registered nor seeking registration. The aims are to: warn firms that they must abide by the rules and regulations; to provide some consumer safeguard; and to assist FCA-authorised firms in scrutiny of transactions and transfers of funds. There are over 230 firms on the List.

While we have increased funding for Scamsmart, and it has inspired initiatives by other bodies, it is limited to investment fraud. There is no single Government-sponsored site or campaign dedicated to helping the public avoid scams and frauds. There is a risk that individual initiatives by different organisations fragment or dilute the preventative message. Funding for individual campaigns is limited. The cost of a publicly-funded permanent centralised campaign would be justified by the savings to consumers and would ramp up prevention efforts substantially.

4. What is the role of international actors in the UK's fraud landscape? What are the barriers to tackling borderless fraud?

We continually explore greater intelligence sharing across borders, which is restricted by technological and legislative limits, as well as improved collaboration between law enforcement agencies in different jurisdictions, particularly around proactive disclosures.

We benefit from excellent relationships with many of our foreign equivalents, who regularly provide us with assistance when we are investigating persons based in their jurisdictions. However, responses under the various Treaties and Memoranda of Understanding can be slow and, at times, differing regulatory systems present a barrier to the degree and type of assistance that can be offered (e.g., some foreign securities regulators may not currently be able to respond to all requests relating to certain cryptoasset activities).

We know that international cooperation is key to tackling serious harm. There is no global regulatory standard setter overseeing the internet, such as there is for securities regulators (IOSCO). For example, IOSCO was able to drive an agreement by members after the 9/11 attacks in New York which created a multi-lateral MOU (MMoU) for information sharing and enforcement cooperation. It now has over 100 members. The MMoU is very helpful in cases involving financial services or securities. However, scams and frauds are more limited to regulators' domestic jurisdictional limitations, some of whose are narrower than the FCA's.

A global consensus in relation to the internet, at least covering commercial activity on the internet, is needed now given the current jurisdictional arbitrage and the scale of harm affecting everyone.

While arrangements for mutual assistance in criminal cases exist between jurisdictions, they operate slowly and only in support of criminal prosecutions, as opposed to broader law enforcement purposes, including prevention, civil recovery, or setting and enforcing global standards. The absence of such a global consensus is a problem given all jurisdictions are equally prey to these scams, and scams often involve multiple jurisdictions.

Action to Tackle Fraud

5. **What are the responsibilities of the private sector in protecting the public against digital fraud? How can a balance be achieved between the need to tackle digital fraud whilst supporting the growth of these sectors? To what extent is work done to combat fraud across the private sectors undermined by siloed or independent working practices.**

   FCA-authorised firms are required to assess and mitigate the risks that their business may be used for fraud. Our rules also require firms to have systems and controls to ensure they are not used to facilitate any financial crime including fraud.

   Firms are required to monitor transactions and customer behaviours to identify fraudulent transactions and have obligations to report suspicion activity reports (SARs) to the UK Financial Intelligence Unit (FIU), housed in the National Crime Agency.

   We have issued guidance on fair value for vulnerable customers which includes requiring firms to embed practices to protect customers who may be vulnerable to scams. We have published guidance for firms on how they can counter financial crime with examples of good and bad practices in preventing fraud. Firms must also handle consumer complaints about fraud in line with our requirements; in 2018 we extended this to cover the receiving payment service provider (PSP) as well as the sending PSP.

   We recently introduced Strong Customer Authentication requirements for e-commerce, requiring banks to obtain identification for customers accessing online banking through two different categories.

   The FCA is committed to working alongside our public-private counterparts and we support the Government's work in this area, including the Joint Fraud Task Force and three new fraud charters, across the retail banking, telecommunications and accountancy sectors introduced in October 2021 to commit industry leaders to work with Government to deliver new products with the aims of reducing the growing threat, and public protection. The FCA is an influential member of the newly-established UK Digital Regulation Cooperation Forum, established to ensure greater cooperation on online regulatory matters like fraud.

   In 2022 Q3, the FCA, with the Payment Systems Regulator, will be running a TechSprint on Authorised Push Payment fraud which will focus on identifying suspicious social media advertising and scam promotions.

6. What are the legislative or regulatory impediments to sharing fraud risk data across and between the private and public sectors? For example, to what extent does General Data Protection Regulation (GDPR) limit data sharing?

We share data through the NECC and work closely with other law enforcement, regulatory, and industry partners to lawfully share data and intelligence where we identify criminal misconduct. We and other law enforcement agencies use SARs to form a broad intelligence picture to help identify misconduct. SARs can also be used by law enforcement where appropriate to restrain monies to prevent dissipation.

There are also multiple industry-based schemes for sharing data related to fraud[2]. As these rely on firms identifying misconduct prior to submitting reports to mitigate consumer detriment risk, they may not capture all intelligence shared through SARs.

We are aware of a data-sharing pilot between several banks, including sharing data be a recipient to the sending bank in the context of transactions to highlight potential fraud/criminal activity red flags which may cause a payment to be stopped, thereby preventing more consumer losses crystallising. There needs to be further work on understanding what inhibitions affect banks sharing more information with each other, law enforcement agencies, and regulators. While banks owe customers duties of confidentiality, there have been suggestions that there needs to be clearer and broader gateways to exempt banks from compliance with this duty where a clear law enforcement purpose – including preventing financial crime - exists.

Other data-sharing pilots are being run between public and private sectors to test how data-sharing can tackle fraud and better understand data-sharing challenges. Increased and confident use of this type of forum could enable data regarding fraud concerns to be shared more easily, to enable more preventative action.

We note a new Economic Crime and Corporate Transparency Bill was announced in the 2022 Queen's Speech proposing to enable businesses in the financial sector to more effective information-sharing to prevent or detect economic crime.

7. What is the role of the individual in relation to fraud? Are consumers well informed about the risks of fraud and how to avoid them? If not, which bodies or organisations should do more to ensure this? What are the most effective methods of educating the public about fraud crime and prevention?

Consumers need good information to make good decisions. This does not always happen, and consumers are often targeted with adverts that are illegal, unclear, unfair or misleading. Digital services mean that people are spending less time between seeing and buying financial services, often without advice, making it all the more vital to provide consumers with tools to enable them to protect themselves.

[2] e.g. FISS, Hunter, CIFAS

We continue to invest heavily in getting the right information to consumers. Our consumer campaigns are the cornerstone of our response to fraud (Q3).

8. **What is your assessment of the Fraud Act 2006? What has been the impact of the Act and is it having any unintended consequences: if so, what are these?**

   The FCA prosecutes offences under the Fraud Act 2006 where appropriate, alongside investigating misconduct under the Financial Services and Markets Act 2000 (FSMA). The Fraud Act contains clear concepts which enable juries to understand the elements of offences. We do, however have some concerns regarding the challenges of investigating and prosecuting fraud in the new digital climate, which we outline in Q12.

   We cannot use our investigation powers, which come from FSMA, to compel banks and other persons to produce information to us, or compel answers to interview questions, to investigate offences under the Fraud Act. However, where we come across evidence of fraud in carrying out investigations under FSMA, we can prosecute under the Fraud Act. These prosecutions are not carried out under our statutory remit but as private prosecutions (which any person, either a corporate or a natural person, is entitled to carry out, unless prevented by the Attorney-General). This legal distinction can create the misapprehension that because the FCA prosecutes under the Fraud Act, our investigation powers can be deployed in aid of fraud investigations under the Fraud Act.

9. **Is existing legislation effective in tackling the increase in modern forms of fraud? If not, is there a legislative remedy, or should fraud be addressed primarily through implementation of existing provisions? Answers may refer to existing mechanisms such as increasing the scope and powers of regulators. You may refer to any legislation and are not limited to the Fraud Act 2006. How effective is the current structure for policing fraud? How successful are the City of London?**

   We have previously highlighted the need for platform providers to be given clear legal obligations to protect consumers from fraudulent investments promoted online. We welcome the OSB and the Government's focus on ensuring platforms have systems to prevent the publication and hosting of fraudulent advertising appearing on their services.

   We also note the Government's consultation on the Online Advertising Programme, which is exploring how online advertising more broadly is regulated in the UK.

10. **Is the current system in place for prosecuting fraud cases working effectively? If not, what are the key barriers to prosecution?**

    The challenges in investigating and prosecuting fraud are not new. Fraud, especially investment fraud, is often discovered well after it has been

committed, when investors realise their money will not be repaid or recovered. By this time, the trail can be cold, important evidence can be hard to locate or missing, memories are stretched and imprecise, and witnesses are often unwilling to give evidence. The delays in investigation caused by these issues are hard to explain and often underappreciated, understandably so because of the devastating impact of fraud on victims.

However, there are some newer challenges.

First, the online scam phenomenon has increased the volume of frauds (Q2). While the ability to identify suspicious online scams in real time makes prevention more viable than before, and we can issue alerts on our Warning List, the sheer volume means the overall threat to consumers is greater now.

Perpetrators of these scams can too easily hide their identity and location. The OSB and commencement of the Crime (Overseas Production Orders) Act 2019 are vitally important in addressing this, which A global standard setter for the internet (Q4) could support.

The increase in digital data means the prosecution of a small fraud today involves greater resources and more effort than major fraud in a pre-digital world.

The volume of digital data handled by the FCA has grown significantly recently. In 2010 – 2017, during the course of investigations we gathered a total of 230 terabytes (tb). From 2017 to end 2021, we gathered 790 tb. We estimate that one terabyte of data, if printed out, would equate to between 100 – 140 million pages. Whilst not a barrier, the volume of data adds complexity, time and risk to an investigation, the disclosure process and any prosecution. Prosecutors globally face the same challenge – it affects the capacity of law enforcement to deal effectively with such crimes, but also the fairness and integrity of the criminal process.

Regarding disclosure, the identification and review of most relevant unused material i.e., material that is gathered during the investigation but is not used by the prosecution, takes place before a charging decision. Data analytics reduces the pool of potentially relevant material (e.g., through smart searches) but technology-assisted review could be more efficient.

Prosecutors are unlikely to deploy technology-assisted review unless they know that the parties and judiciary have confidence in it. In criminal matters, unlike civil litigation, there is no mechanism for judicial approval of the use of such technology before charge. This should change. As we recently set out in evidence to the Justice Committee, the use of artificial intelligence (AI) to identify relevant material should be given official approval by criminal courts.

While pre-charge engagement by defendants is encouraged in the Attorney General's Guidelines, in our experience, defence assistance to identify relevant material is rarely forthcoming. Disclosure should not be a trap and trials should not be delayed or impeded by a failure by parties to have sensible disclosure arrangements, especially given the outsized volumes. Resource disparity can be addressed if AI searches can be agreed at an early stage, with the product shared by all sides. If the

defence were clear about what the matters are in issue, the prosecution could identify relevant material more efficiently. This would help avoid trials failing because of disclosure problems and create greater efficiency and focus on material relevant to the key issues in the trial.

Disclosure is an essential component of a fair trial and we do not suggest that an obligation on the defence to co-operate should absolve the prosecution of its responsibilities, but delays can be caused by refusing to provide passcodes, or a failure to agree realistic search terms for legally privileged material or for digital devices. In practice, the current regime obliges the prosecution to schedule material that has no relevance to the actual issues in the case. Mandating the early identification of the issues would reduce this unnecessary burden. A corollary of the late crystallisation of issues in the case is that late defence applications for disclosure can be made. At best these are difficult to manage in terms of time and resource; at worst they can have a detrimental effect on the trial.

Allocating a trial Judge with sufficient time and expertise in the challenges of digital data and technology to effectively manage disclosure could lead to efficiencies and avoid disputes causing additional delays.

11. What lessons can be learned from effective policy interventions and schemes both in the UK and overseas?

The FCA works closely with domestic and international counterparts to share knowledge around effective policy interventions to tackle investment fraud.

One recent area of focus for the FCA has been fraud involving crypto-assets. The evolving nature of this risk, and the fact that the harm is often cross-border, has emphasised the importance of international cooperation and knowledge sharing. Developing a legal framework for crypto-assets has been a key challenge for many jurisdictions. We have observed jurisdictions taking two approaches:

1. Amending existing regulations to capture crypto-assets, such as classing crypto-assets as securities. In the UK, HM Treasury has made clear its intention to legislate so that certain currently unregulated crypto-assets, like utility tokens and exchange tokens, will be added to the scope of the existing financial promotions regime.
2. Implementing bespoke regimes. Some jurisdictions have developed a regime whereby firms can "opt in" for ICOs to be regulated and thereby appearing on a "white list" for consumers.

The FCA has industrialised its use of webscraping by using AI to identify websites as being connected to the same actors. We have shared lessons learned in developing our approach internationally, particularly around technologies used.

The FCA and international counterparts have sought to develop relationships with tech firms, to facilitate the identification and removal of

fake adverts and scams themselves. Domestically, the FCA is involved in initiatives like the UK Digital Regulation Cooperation Forum, which are intended to ensure greater cooperation and coordination. Certain jurisdictions have developed powers regarding internet providers blocking websites promoting fraudulent schemes. This is a powerful tool to optimise website takedown rates.

However, takedown requests do not prevent new websites cropping up, and one key takeaway from these initiatives is the importance of, and difficulty in, identifying the bad actors that sit behind these online scams. This remains a key challenge, and one which requires close international cooperation and improved information sharing.

12. Can you suggest one policy recommendation that the Committee should make to the Government?

We consider the following policy areas, directly relevant to our work, to be of particular importance:

1. We ask that the Committee supports the enactment of the OSB, as soon as possible, which is an important step in the right direction.
2. Alongside FCA consumer information and education campaigns (Q9), the police, financial services firms, consumer groups and other public bodies take steps to raise awareness, and inform consumers of, the risks of fraud. Assigning responsibility for this type of fraud prevention work to a central body with allocated funding could be even more effective and better value for money. A fully-funded central campaign strategy, able to reach all consumers with a regular message across all forms of media, using behavioural science, designed to reach the whole population but also capable of targeting specific demographics, would ensure consumer messaging on fraud is not diluted or fragmented and would enhance the gravitas that messaging from any one LEA is able to deliver. It would also reinforce the message to fraudsters that the Government is committed to fraud prevention and public protection.
3. Increased funding for NECC and police to combat fraudsters would enhance this centralised focus and send a deterrent message to would-be fraudsters.
4. We recommend that Government adopt a behavioural science approach focused on confidence-building in financial services and payments, working with MAPs and other partners who lead on financial education. The FCA would be happy to share learnings from the ScamSmart and InvestSmart campaigns.
5. A clear policy endorsing the use of AI and technology-assisted review of material gathered in criminal investigations could shorten investigation length, and the time needed to review and schedule unused material prior to charge. The application of the policy in individual cases could be assured by the introduction of a mechanism for judicial approval of its use pre-charge.

13 May 2022