Written evidence submitted by UK Finance (COR0149)

Online harms

1. UK Finance is the collective voice for the banking and finance industry. Representing more than 250 firms, we act to enhance competitiveness, support customers and facilitate innovation.

2. We welcome the opportunity to provide evidence to the Home Affairs Committee's inquiry into the preparedness of the Home Office for covid-19 on:

   - the nature, prevalence and scale of online harms during the covid-19 period;
   - steps that could be taken to mitigate these concerns; and
   - the adequacy of the UK government's online-harms proposals to address issues arising from the pandemic, as well as issues previously identified.

3. We strongly recommend that economic crime be brought into the scope of the new online-harms regulatory framework in line with our response to the government's white paper[1] and the attached briefing document. To summarise:

   - Economic crime is a significant threat to the security, prosperity and reputation of the UK.
   - The illicit funds gained can enable and fund serious crimes—including terrorism, modern slavery, child sexual exploitation and drug trafficking—that damage our communities, even if the original victim is refunded.
   - The criminals responsible exploit some of the most vulnerable in society to scam them out of their money, with a devastating effect on victims.
   - The private sector is the first line of defence. The banking and finance sector spends billions of pounds each year to tackle economic crime, but we cannot stop economic crime on our own. We have forged strategic partnerships across the public and private sectors that harness our combined capabilities, resources and experience.
   - We are delivering initiatives such at the Banking Protocol,[2] supporting law enforcement with the Dedicated Card and Payment Crime Unit,[3] and helping customers stay safe through the Take Five to Stop Fraud campaign.[4]
   - Now we need the cooperation of other industries to tackle the complexity of the task at hand because fraud, bribery and corruption happen across all sectors.
   - This includes technology firms preventing their platforms from being used by criminals, service providers ensuring customer data are kept safe, and regulated

[1] https://www.ukfinance.org.uk/policy-and-guidance/consultation-responses/UK-Finance-response-to-the-online-harms-white-paper.
[2] https://www.scotland.police.uk/keep-safe/personal-safety/the-banking-protocol.
[3] https://www.financialfraudaction.org.uk/about-ffa/the-dedicated-card-and-payment-crime-unit/.
[4] https://takefive-stopfraud.org.uk/.

industries such as legal services and real estate going further to identify money-laundering in their businesses.

- By doing so, we can make the UK the safest and most transparent place in the world to conduct financial business.

Online-harms regulatory framework: ensuring economic crime is in scope

Executive summary

UK Finance strongly recommends economic crime be brought into the scope of the online-harms regulatory framework.

A holistic approach is most effective at keeping customers safe
Tackling online harms requires a holistic approach by which every sector contributing to the problem of economic crime is held to account. Furthermore, it should be recognised that issues already in scope, such as terrorism, are in part enabled by funds derived from economic crime.

The banking and finance sector invests significantly to protect customers from fraud
In 2019, more than £1.8 billion of unauthorised fraud was stopped by advanced security systems and innovations in which the banking and finance sector invested to protect customers. Despite this, criminals still managed to steal £1.2 billion from customers using fraud and scams.

Social-media platforms are exploited by criminals for the purposes of economic crime
The increasing growth of social media and their use as a vehicle for economic crime underscore the importance of introducing an online-harms regulatory framework that protects consumers to the best extent possible. In 2019, worldwide social-media users grew to almost 3.5 billion, with 288 million new users in the past 12 months. In the UK, there are now 45 million social-media users—two thirds of the population. The fight against economic crime must keep pace with technological change.

Economic crime is not an either/or issue as proceeds fund harmful and illegal activities
Economic crime can have a devastating impact on victims, and even if the customer is compensated in full by their finance provider, the criminals that perpetrate these frauds still profit. The criminal proceeds are reinvested to fund harmful and illegal activity such as terrorism, modern slavery, drug trafficking and human trafficking.

Moral, social and financial responsibility for cross-sector efforts to combat crime
The banking and finance sector is not solely responsible for the fight against economic crime, and there is a moral imperative for social-media firms to do more. When an economic crime is committed, there are social and financial costs for both the victims and society. Given increasing economic crime and rising social-media use, the need for cross-sector efforts to combat crime is growing, otherwise there will need to be a significant uplift in law-enforcement resources—as well as in other sectors—to respond to the growing number of frauds.

The banking and finance sector stands ready to play its part and work with online-platform providers, but bringing economic crime into the scope of the regulatory framework would ensure <u>all</u> sectors undertake efforts to remove vulnerabilities in their systems and organisations, ultimately giving criminals fewer opportunities to target and exploit vulnerable people and the UK economy.

Economic crime and the abuse of social media

The abuse of social-media platforms by organised criminals for the purposes of financial crime has increased significantly, and there is little doubt that this trend will continue to grow. Intelligence from law enforcement and other sources indicates there are thousands of social-media accounts in operation by criminals at any one time, the majority being openly advertised and visible to users. These accounts facilitate advertising for “money mules” (for the purposes of money laundering), selling stolen identity and credit-card data, phishing, bogus investment scams and impersonating legitimate companies such as banks to enable fraud.

- Financial fraud and scams on social media increased fourfold in 2019 to 383,000. 41 per cent of these were identified as fraud-related, 21 per cent money flipping, 18 per cent fundraiser scams and 16 per cent giveaway and coupon scams.[i]

- Over 14,000 phishing links were shared on social-media platforms in 2019.[ii]

- One bank reported that 50 per cent of the scams it saw originated from social media in the previous 12 months.[iii]

- **53 per cent of social-media logins are fraudulent**, and 25 per cent of all new account signups are fake.[iv]

- There has been **a 188 per cent year-on-year increase in the number of removals** of malicious content from social-media posts and imposter accounts.[v]

- **88,000 indications of fraud and scams were identified on various social-media platforms** between May 2018 and May 2019. This are data sourced from just one security-monitoring company.[vi]

- The number of **children acting as money mules has risen by 73 per cent in two years** as criminals target youngsters on social media.[vii] The growing use of social media means there has now been more opportunity for young people to become victims of economic crime. Many are also unaware of the consequences that crime can have for their future opportunities.[viii]

- **There has been a sharp rise in those over the age over 40 acting as money mules**, with a 25 per cent increase in money-muling activity in those aged 41-50 and a 26 per cent rise in those aged 51-60 over the nine months up to September 2019.[ix]

- Investment scams are becoming increasingly sophisticated, with criminals targeting online investors by impersonating private banks and investment firms on social media. **The amount of financial loss because of investment scams in 2019 increased by 90 per cent** compared with 2018, from £50.1 million to £95.4 million.[x]

The potential for real benefits by bringing economic crime in scope

The inclusion of economic crime would ensure all online platforms join cross-industry efforts to tackle fraud and money laundering. The benefits are significant. First, economic crimes are intrinsically linked to crimes already identified as within the scope of the online-harms regulatory framework, so enabling more effective tackling of all illegal and harmful-but-legal activity when such a holistic approach is taken. Second, including economic crime would require all online platforms to play their part in cross-sector efforts to protect consumers. Third, the cost of economic crime to the financial sector is substantial, even when the vulnerability originated in another sector. All efforts that contribute to the reduction of economic crime benefit society and reduce online harms.

Case studies

The UK banking sector, Facebook and Instagram working together to combat crime

These case studies demonstrate the positive outcomes that can be achieved as a result of cross-sector collaboration and how providing holistic consumer protection is the key to combating online harms. However, this approach is currently the exception rather than the norm, something that must be addressed if the fight to combat online harms is to be successful.

Case study 1
Industry-funded police unit the Dedicated Card and Payment Crime Unit (DCPCU) has been working with Facebook and Instagram to tackle economic crime. Since January 2019, more than 1,600 social-media accounts have been successfully taken down. Broken down by type of economic crime, these were:

- 525 “ghost brokers” using stolen credit cards to purchase goods and resell at discount.
- 487 money-mule recruiters and money-laundering offenders.
- 248 stolen payment-credential sellers.
- 405 others (flips, fake notes, insider recruitment etc.).

These accounts had over 645,000 followers, and taking them down prevented £3.8 million of financial loss.

Case study 2
In June 2019, a UK Finance member raised the issue of fraudulent social-media profiles offering half-price goods (known as ghost brokering) to Facebook and Instagram. This notification was based on UK Finance intelligence alerts about ghost brokering.

This public/private engagement between the banking sector and Facebook led to strategic mitigation solutions being developed and is helping to prevent ghost brokering on the social media platform.

Economic crime and other illegal activities: you cannot tackle one without the other

- **Money laundering is a critical enabler of serious and organised crime**, costing the UK an estimated £24 billion a year.[xi]

- **Fraud and cybercrime amount to almost a third of all crimes** and continue to be among the most commonly experienced in the UK. 3.7 million incidents of fraud were recorded in the year ending December 2019.[xii]

- The overall scale of economic crime is estimated to be £7.3 billion per year. **The cost to businesses and the public sector from organised fraud is £5.9 billion per year.**[xiii]

Unquestionably, there is a clear link between economic crime and the funding of illegal activity, with online platforms being increasingly exploited by criminals.

The UK government's Serious Organised Crime Strategy 2018 recognised that the "increasingly pervasive nature of technologies will allow less skilled and resourced criminals to gain access to markets and tools that were previously out of their reach,"[xiv] and the National Crime Agency assessed that "the threat from serious and organised crime is increasing and serious and organised criminals are continually looking for ways to sexually or otherwise exploit new victims and novel methods to make money, particularly online."[xv]

Case study **The UK banking sector and the DCPCU combating organised crime during covid-19**
During April 2020, 10 DCPCU warrants were executed in relation to covid-19. These successfully targeted and disrupted several criminal gangs involved in sending scam texts and emails to unsuspecting members of the public. Three search warrants in Leicestershire, Dorset and southeast London identified several suspects and saw mobile phones and other devices seized. DCPCU officers then searched an address in Leicester on 15 April as part of an investigation into fake HMRC text messages. A number of mobile phones and over 20 SIM cards were seized that were being used to send out texts that included links to bogus HMRC sites offering financial support and refunds to assist recipients during the outbreak. https://www.ukfinance.org.uk/PRESS/PRESS-RELEASES/BANKING-INDUSTRY-FUNDED-POLICE-UNIT-CRACKS-DOWN-ON-COVID-19-TEXT-MESSAGE-SCAMS#NOTES.

Further examples of covid-19 harm

Money-muling. Attackers have begun using covid-19 as a lure. Victims are asked to send money abroad for soldiers affected by the virus or to citizens trapped due to quarantine measures, among other scenarios. Often, victims of money-mule scams are driven to action by a desire to help others. Those who fall for these scams may never realise that what they are doing is illegal and they are assisting in a scam.

Scams. The majority of scam reports are related to online shopping where people have ordered protective face masks, hand sanitiser, covid-19 testing kits and other products that have never arrived.[2] If they have arrived, in many cases they have been substandard. Other frequently reported scams include:

- Victims trying to apply for a government grant to assist their business but being informed their business had already received a grant and is therefore ineligible for any more financial assistance. The victim did not make the initial application and does not recognise the account to which the payment was made.
- Fraudsters advertising a pet online and using the outbreak as a reason the victim cannot come to see the animal. The fraudsters send photos and persuade the victim to make a payment in advance. The fraudsters will often try to get the victim to pay additional unforeseen costs (e.g. for insurance and vaccinations) after the initial payment but never provide the pet.[3]
- Fraudsters incorporating covid-19 into their social-engineering approaches by using the outbreak to convince victims to speak with the suspect on the phone, saying the banks are closed etc.
- Victims being persuaded by fraudsters to make an advanced payment for a rental property or car. The fraudsters use covid-19 as the reason for the victim being unable to view the item, which does not exist.

Phishing/smishing. Such attacks have been prevalent, with fake or cloned websites supporting the spread of misinformation and duping consumers into falling victim to fraudsters. The National Cyber Security Centre has taken down thousands of scam sites.[4]

HMRC phishing emails. Emails are often sent from different Hotmail accounts, but the sender name is spoofed to read “Helping you during this covid from government” or “HMRevenue & Customs(HMRC).” They offer a grant of between £2,500 and £7,500 to taxpayers out of work or working less because of the pandemic, or the message informs the recipient they are eligible for a £698.99 tax refund that they need to claim within 24 hours by clicking on a link. The links have been identified as malicious.

Contact-tracing app. Fraudsters have developed a scam based on the rollout of the government's covid-19 contact-tracing app. Consumers across Britain received scam texts purportedly generated by the app, with a message link leading to a fake website that asked for personal details.[5]

Bitcoin investment. Emails advertising investments in Bitcoin platforms that claim to “take advantage of the financial downturn” and help with recovery from bankruptcy. A link is provided in the email that claims to take recipients to a website that explains how Bitcoin trading platforms work. This link has phishing and malware threats to victims, with the suspect trying to steal credentials and/or get the recipient to download a virus.[6]

TV Licensing. A range of fake TV Licensing emails with minor changes to the messaging and links appeared with covid-19–related lures. The emails claim the recipient’s direct debit failed and they need to pay to avoid prosecution. These emails display the subject header “We couldn't process the latest payment from your Debit Card - COVID19 Personalized Offer: You are be eligible for a 1 x 6 months of free TVLicence.” They include a link to set up a new direct debit on a website controlled by the criminals. At the end of the email, to lure recipients in, the fraudsters also offer six months of free TV licence. Recipients are asked to click on a link to apply for the offer. The link takes them to a sign-in page where they are asked to complete an online application form, providing the criminals with an opportunity to steal email logins, passwords, and personal details.[7]

GOV.UK council-tax reduction. Fake government emails are circulating that claim to help individuals on benefits or a low income to pay their council tax. The subject line of the email reads “*Online application – (COVID-19) – You are getting a Council Tax Reduction (Total amount of benefits: GBP 385.55) Stay at home this weekend.”* The recipients are told they are eligible for a council-tax reduction and are asked to click on a link to claim the benefit, which will be automatically transferred to their debit/credit card. The sender name has been spoofed to read “Council Tax – GOV.UK.”[8]

[1] ZeroFOXInc, Phishing and Fraud in Financial Services, 2020.
[2] https://www.actionfraud.police.uk/a-z-of-fraud/online-shopping-fraud.
[3] https://www.actionfraud.police.uk/news/animal-lovers-looking-for-pets-in-lockdown-defrauded-of-nearly-300000-in-two-months.
[4] https://www.bbc.co.uk/news/technology-52361618.
[5] https://www.bbc.co.uk/news/uk-england-hampshire-52647919.
[6] https://twitter.com/actionfrauduk/status/1262681679161888768.
[7] https://twitter.com/actionfrauduk/status/1260582920865165312.
[8] https://twitter.com/actionfrauduk/status/1261303127585820678.

May 2020

---

[i] ZeroFOX, Phishing and Fraud in Financial Services, 2020.
[ii] ZeroFOX, Phishing and Fraud in Financial Services, 2020.
[iii] UK high-street bank, UK Finance anonymised data, 2018.
[iv] Arkose Labs, Fraud and Abuse report, 3Q2019.
[v] ZeroFOX, Financial Services Digital Threat Report, 2019. Removal figure includes takedowns May 2018–May 2019.
[vi] ZeroFOX, Financial Services Digital Threat Report, 2019.
[vii] CIFAS, annual figures from 2016-18.
[viii] Leicestershire Police, Don't be Fooled campaign: letters sent to parents, 2019.
[ix] CIFAS, Research reveals sharp rise in middle-aged money mules, 2019.
[x] UK Finance, Half-year fraud update, 2019.
[xi] NCA, Money laundering and illicit finance, 2015.
[xii] Office for National Statistics, Crime in England and Wales: year ending June 2018, 2018.
[xiii] Home Office, Understanding organised crime 2015/16, Second Edition, p. 38, February 2019. Figures exclude money laundering and corruption.
[xiv] UK government, Serious Organised Crime Strategy, p.14, November 2018.
[xv] UK government, Serious Organised Crime Strategy, p. 5, November 2018.