Written evidence submitted by UK Finance

Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation's inquiry into online safety and online harms

UK Finance evidence

September 2021

Introduction

1. UK Finance is the collective voice for the banking and finance industry in the UK. Representing almost 300 firms, we act to enhance competitiveness, support customers and facilitate innovation[1]. This includes helping lead the industry's collective fight against economic crime in the UK, including combatting fraud and cybercrime.

2. We welcome the opportunity to provide evidence to the DCMS Sub-Committee on Online Harms and Disinformation's inquiry into online safety and online harms.

3. As part of this inquiry's examination of key omissions within the draft Online Safety Bill (the Bill), our response focuses on proposals to enhance measures within the Bill aimed at tackling fraudulent online content that leads to economic crime, and why the draft Bill's current approach to tackling some aspects of fraud risks ineffective legislation, leaving criminals with the opportunity to exploit online systems.

4. Following the Government's welcomed inclusion of user-generated fraud within the Bill, we firmly believe that the scope should be expanded to fully include all online-enabled fraudulent and scam-related content when it is formally introduced. In particular, to match the Prime Minister's words that "…one of the key objectives of the Online Safety Bill is to tackle online fraud"[2], we strongly recommend that the necessary mechanisms to tackle all online fraud, including those facilitated via adverts and cloned websites, should be dealt with by this legislation.

Questions

How has the shifting focus between 'online harms' and 'online safety' influenced the development of the new regime and draft Bill?

5. As confirmed alongside the publication of the draft Bill on 12 May 2021, the scope of the Bill has now been expanded to include fraudulent user-generated content[3]. This followed sustained advocacy from a cross-sector coalition of stakeholders across industry, consumer groups and law enforcement[4] on this issue, alongside support from other public bodies, including the Financial Conduct Authority (FCA)[5] and Bank of England[6].

---

[1] We are particularly grateful to our associate member TLT LLP for their invaluable assistance with this response.
[2] https://committees.parliament.uk/oralevidence/2308/default/
[3] https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published

6. This represents a shift in the Government's position, who previously stated in their full response to the Online Harms White Paper in December 2020 "…that the fraud threat will be most effectively tackled by other mechanisms and as such the legislation [the Bill] will not require companies to tackle online fraud…"[7].

7. We are pleased that Government has now recognised that this Bill is the right legislative instrument to effectively tackle the growth in online-enabled fraud. This will mean online companies will, for the first time, have to take responsibility for tackling fraudulent user-generated content, such as posts on social media, on their platforms.

8. However, at present, the draft Bill leaves a large proportion of fraud outside the scope of this legislation. We believe this partial shift in the Government's position has created an arbitrary distinction between user-generated fraud, which will be within scope of the legislation, and fraud facilitated via adverts or cloned websites, which will not presently be protected against by the Bill.

9. The Government's press release accompanying the Bill stated that "…romance scams and fake investment opportunities posted by users on Facebook groups or sent via Snapchat"[8] would be within scope of the Bill. However, as currently drafted, these types of scams will only be caught by the legislation to the extent they are distributed by user-generated content. The Bill will not presently legislate against romance scams and fake investment opportunities if they are promoted by paid-for adverts or cloned websites. This creates a clear lacuna in the law, particularly as an individual user-generated scam may fall out of scope of the legislation if it is promoted via an advert or cloned website.

10. For the benefit of the Sub-Committee, Annex 1 illustrates the different forms of online-enabled fraud and how they come about, in order to highlight how criminals not only rely on user-generated content, but also paid-for adverts and cloned websites to target victims by exploiting vulnerabilities that currently exist on online platforms[9].

11. As we will set out in further detail below, we believe this distinction risks undermining the Government's intention of tackling the growth of online fraud, as it leaves too much room for criminals to exploit the new regulatory framework set out in the draft Bill; inadvertently creating loopholes for fraudsters to capitalise on.

12. Alongside the problems created by this distinction, the text of the draft Bill has no specific mentions of the types of user-generated fraud that will be legislated against by the Bill, and it is not yet clear how the new regulatory framework will capture these types of activity.

13. We would appreciate further clarity from Government on how the new regulatory framework will require companies that fall within its scope to take measures to tackle fraud, such as how the application of illegal and harmful content provisions within the Bill might apply to fraudulent content.

---

[4] https://conversation.which.co.uk/wp-content/uploads/2021/05/Open-Letter-Scams-and-the-Online-Safety-Bill.pdf
[5] https://committees.parliament.uk/committee/158/treasury-committee/publications/oral-evidence/
[6] https://www.ft.com/content/aa0f0763-8692-4211-92e0-c9bcb2655d0e
[7] https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response
[8] https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published
[9] See Annex 1.

What are the key omissions to the draft Bill, such as a general safety duty or powers to deal with urgent security threats, and (how) could they be practically included without compromising rights such as freedom of expression?

14. Given there is no mention of fraud or scams in the draft Bill, it appears that the limited measures to tackle user-generated online fraud will rely on the wider duties in the Bill in relation to tackling illegal content. However, the draft Bill's proposals expressly carve out paid-for advertising from the scope of the legislation, and fraud facilitated via cloned websites is likely to be inadvertently excluded because "infringements of intellectual property rights" is excluded from the definition of a "relevant offence" in the draft Bill.

15. We believe that this approach is fundamentally flawed. Given it is already an illegal offence, if the Bill is to effectively tackle online fraud, it must explicitly define fraudulent content as illegal content and amend the Bill to include a new Schedule that specifies the types of fraud offences that will be captured by the Bill, which includes fraud committed through paid-for advertisements and cloned websites.

16. We also believe that the harmful content provisions should be expanded to include financial impacts on individuals in any assessment of harmful content, alongside psychological and physical impacts on individuals which are already included in the draft Bill's harmful content provisions. Taken together, this will embed the Government's commitment to tackling fraud and ensure it is fully recognised as illegal and harmful content within the legislation.

17. As this Sub-Committee will be aware, fraud poses a major threat to the UK public. According to ONS data, there were 4.3 million incidents of fraud in the year ending June 2020, making fraud the most likely crime that adults can fall victim to in the UK[10]. Action Fraud data shows that there was an increase of 413,000 reports of fraud over the past year, estimated to cost £1.7 billion[11]: equivalent to every person in the UK losing £25 last year. Given cases of fraud often go unreported – with the National Crime Agency estimating that fewer than 20 per cent of incidents of fraud are actually reported[12] – this is likely to substantially underestimate the true scale of fraud that takes place in the UK.

18. Fraudsters are increasingly evading banks' advanced security systems by employing sophisticated methods of social engineering scams via online platforms. Often these methods target victims directly and trick them into giving their money away through online-enabled push payment fraud. Overall losses to Authorised Push Payment (APP) fraud[13] increased by 5 per cent in 2020, totalling £479 million[14].

19. The increase in online-enabled push payment fraud has only been accelerated due to the consequences of the Covid-19 pandemic. With people spending more time online, criminals exploited many individuals heightened financial insecurities, particularly in the context of record low interest rates, to entice victims into fraudulent investment opportunities. In addition, due to lockdown and shielding advice for vulnerable individuals, many who previously avoided internet shopping began to order online, creating a new cohort of

---

[10] Fraud overtook theft against the person as the most commonly experienced crime type in the Crime Survey for England and Wales in 2017. See Office for National Statistics, 'Crime in England and Wales: Year Ending June 2020', https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2020#fraud

[11] https://www.thetimes.co.uk/article/now-for-the-next-uk-pandemic-financial-fraud-vt86pw2lr

[12] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime

[13] In an authorised push payment fraudulent transaction, the genuine customer themselves is duped into making a payment to another account which is controlled by a criminal.

[14] UK Finance, Fraud - The Facts 2021, https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2021

inexperienced internet shoppers for criminals to target. With people unable to meet in person, criminals even exploited the rising use of online dating apps during lockdown, employing clever tactics which convinced people into thinking they've met their perfect partner online, duping victims into sending money to fraudsters[15].

20. UK Finance also saw the emergence of criminals openly advertising fraud and scam services for sale online, including template phishing websites and custom-built scam apps which replicate real banking apps[16].

21. Collectively, this resulted in a significant growth in money mule activity and romance scams, alongside investment and purchase scams in 2020, facilitated by weaknesses in online platforms to combat fraud and scam-related content, such as cloned websites easily promoted on search engines via paid-for adverts, which are increasingly exploited by criminals[17].

22. For example, investment scams, which are often promoted through paid-for adverts on search engines or social media offering higher than average returns, increased by 32 per cent in 2020. The nature of this scam means there are often life-changing sums involved in individual cases, so while investment scams accounted for only six per cent of the total number of APP fraud, they accounted for 28 per cent of the total value of all APP fraud[18].

23. A separate analysis by UK Finance of nearly 7,000 APP scam cases show that 96 per cent of investment scams originate online, and almost 70 per cent of all APP fraud now originate on an online platform[19].

24. The growth in online fraud does not just create significant financial losses, but also has a devastating emotional impact on victims. As online-enabled fraud often involves victims being directly manipulated, or duped into making a fraudulent payment themselves, this can have a more damaging psychological impact than more traditional types of fraud. According to the Money and Mental Health Institute, 40 per cent of victims have felt stressed and three in ten have felt depressed as a result of being scammed[20].

25. Even if the customer is compensated in full by their finance provider, the criminals that perpetrate these frauds retain the illegal proceeds and still profit.

26. For example, money mules are recruited, sometimes unwittingly, by criminals to transfer illegally obtained money between different bank accounts. Money mules, who are typically younger individuals (such as students), receive the stolen funds into their account. They are then asked to withdraw it and wire the proceeds to a different account, often overseas, keeping some of the money for themselves.

27. During the pandemic, money mule recruiters targeted 'generation Covid' – those looking for work or to earn easy money – by posting fake adverts on job websites and social media sites.

28. Recent research from Cifas revealed there were 17,157 cases of suspected money muling activity involving 21-30-year-olds in 2020, a five per cent increase on the previous year.

---

[15] https://www.ukfinance.org.uk/press/press-releases/criminals-exploit-covid-19-pandemic-rise-scams-targeting-victims-online
[16] Annex 2 includes screenshots of this activity, ibid.
[17] ibid
[18] Ibid.
[19] https://www.ukfinance.org.uk/press/press-releases/over-two-thirds-of-all-app-scams-start-online%E2%80%93new-uk-finance-analysis
[20] https://www.moneyandmentalhealth.org/wp-content/uploads/2020/12/Caught-in-the-web-full-report.pdf

This age group accounted for 42 per cent of money mule activity in 2020, up from 38 per cent three years ago[21].

29. Cash laundered by money mules is used by criminals to facilitate serious crimes, such as terrorism, drug trafficking, child exploitation and people smuggling.

30. Often, people are unaware that allowing their bank accounts to be used in this way is a crime with consequences under criminal and civil law. Besides a criminal record, the individual could have their bank account closed and difficulty opening one elsewhere, and trouble obtaining mobile phone contracts or accessing credit in future.

31. Separate research from the Royal United Services Institute (RUSI) highlights that links between fraud, organised crime and terrorism pose a significant and growing threat to our national security[22]. Importantly, Police Foundation research from 2017 found that between 31 per cent and 45 per cent of fraud investigated by local police forces was linked to organised criminal gangs[23].

32. However, the distinction created by the current proposals within the draft Bill would arbitrarily legislate against certain types of user-generated online fraud, whilst leaving a large proportion of online fraud, such as money mule recruitment via job websites or promoted social media posts, outside the scope of the legislation.

33. Money and Mental Health have shown that half of adults reported they had seen a scam advert on social media at least once a month (50 per cent), whilst four in ten (43 per cent) had seen a user-generated scam in the same period[24].

34. Not including fraud resulting from paid-for online advertisements or cloned websites within the scope of the Bill would block any meaningful efforts aimed at properly tackling online fraud, particularly as criminals will adapt their tactics to any opportunity or loophole.

35. To illustrate the problem, we have included two case studies based on real-life scenarios which demonstrate the challenges created by the proposed scope of the Bill.

Case Study 1 – Impersonation Scam (currently <u>in scope</u> of the legislation)

During lockdown a customer aged 25, who was looking for investment opportunities after being furloughed, fell for an impersonation scam via Instagram.

The Instagram account, which had over 7,000 followers, impersonated a legitimate Forex trading opportunity and the customer saw a number of shoutouts and positive reviews on Instagram which enhanced the account's legitimacy. The customer made two payments of £500, two payments of £1500 and £600. A further two payments were made of £1000 and £1200 via mobile banking.

The customer realised it was a scam when he received no return on his investment and he was blocked from the site's Instagram account. The customer lost over £5000.

---

[21] https://www.cifas.org.uk/newsroom/money-mules-target-generation-covid
[22] https://static.rusi.org/the_silent_threat_web_version.pdf
[23] Ruth Crocker et al., 'The Impact of Organised Crime in Local Communities', Police Foundation, June 2017, p. 62
[24] https://www.moneyandmentalhealth.org/wp-content/uploads/2020/12/Caught-in-the-web-full-report.pdf

Case Study 2 – Investment Scam (currently not in scope of the legislation)

A retired NHS employee in his 80s encountered an online advertisement for investments in Bitcoin. He was drawn to the advertisement because it included a purported endorsement from former Manchester United manager Sir Alex Ferguson, which gave him some comfort that this was a legitimate investment. The endorsement was fabricated and there was no connection with Sir Alex.

The fraudsters were using a company name that was very similar to that of a genuine FCA-authorised investment company. Although there were some online reports indicating that this was a scam, the victim spoke to representatives of the company who were very articulate and convinced him that the negative reports were defamatory reviews from their rivals. He was promised substantial returns and began making deposits into a crypto-currency e-wallet set up in his name.

The funds were immediately paid away into the fraudsters' accounts. The victim lost £250,000, which was his life savings. The bank is supporting attempts to recover the

36. The two case studies show that, from the victims' perspective, there is no difference in terms of increased consumer harm as a result of user-generated fraud, versus fraud caused by paid-for advertising. To the victim, the loss of money and harm caused is not lessened simply because the fraud is not user-generated. Furthermore, the outcome is also the same for the criminal: receiving ill-gotten proceeds which can be used to fund damaging activities, such as child exploitation, human trafficking and terrorism-related activity.

37. Given user-to-user generated fraud is already within scope of the new regulatory regime set out by the draft legislation, expanding the Bill to tackle fraud facilitated via paid-for advertising (such as the investment scam in Case Study 2) or cloned websites will therefore not involve any further compromising of rights, such as freedom of expression.

38. Since the publication of the draft Bill, in recent evidence to Parliament[25], the CEO of the FCA and Governor of the Bank of England have remained unchanged in their view that, in order for the Bill to adequately tackle the growth in online fraud, it should be expanded to include paid-for advertising. Alongside a wide coalition of industry groups, consumer champions and law enforcement representatives who previously called for its inclusion prior to the publication of the draft Bill, our united view remains unchanged that the Government's current approach to tackling online fraud is flawed. In order to achieve better outcomes for consumers, we need an Online Safety Bill that takes a more comprehensive approach to tackling online fraud[26].

39. On top of this, almost 90 per cent of people think Government should legislate to ensure search engines and social media sites do not mislead consumers or promote financial scams, and 85 per cent think search engines should be responsible for advertising content on their platforms so that it is not misleading, according to the latest Aviva Fraud Report[27].

---

[25] https://committees.parliament.uk/publications/6956/documents/72760/default/

[26] https://www.moneyandmentalhealth.org/press-release/coalition-consumer-groups-charities-include-scam-ads-online-safety-bill/

[27] https://www.aviva.com/newsroom/news-releases/2021/08/latest-aviva-fraud-report-calls-for-online-safety-bill-to-include-financial-scams/

40. The banking and finance industry fully recognise the importance of tackling fraud, and it is already highly regulated with respect to this. The FCA is responsible for securing an appropriate degree of protection for consumers[28], and requiring firms to ensure communications are fair, clear and not misleading[29]. In 2020 banking systems blocked almost £7 in every £10 of attempted unauthorised fraud[30] – equivalent to £1.6 billion[31].

41. However, we are reaching the limits of what we can do alone, particularly as the nature of online fraud increasingly evades banks' own security systems. Currently, liability for financial fraud falls on banks and payment service providers, with zero liability on online platforms that allow these fraudulent posts and websites to propagate. User-generated content is a very small section of fraud, and whilst the industry welcomes it as an important first step, the Bill should be more ambitious in order to seriously address the issue.

42. We believe that including all online fraudulent and scam-related content within the scope of this legislation is about building a more comprehensive regulatory framework which puts in place stronger incentives for online platforms to work together with other sectors to better tackle fraudulent content that leads to economic crime. Collectively, this would help prevent fraud from happening in the first place.

43. We therefore strongly urge the Government to reconsider measures within the Bill aimed at tackling fraud and include the necessary mechanisms to tackle all online fraud when it is formally introduced, and in particular fraud facilitated via adverts and cloned websites promoted on online platforms.

44. One solution to better legislate against fraud within the Bill would be to amend Section 41 (4) of the draft Bill, and other related references to explicitly include all fraudulent offences as illegal content within the Bill. At present the text of the draft Bill gives no mention of fraud, scams or economic crime. Explicitly defining fraud offences as illegal content will give recognition to the significant prevalence, risk and severity of harm already created by online fraud, as outlined in this evidence, and will help put in place proper protections within the existing framework set out by the draft Bill to tackle all online fraud.

45. We propose that Section 41 (4) of the draft Bill should be amended by inserting the following line:

"41 Meaning of "illegal content" etc

(4) "Relevant offence" means—
- *(a) a terrorism offence (see section 42),*
- *(b) a CSEA offence (see section 43),*
- *(c) a fraud offence (see [new] section 44),*
- *(d) an offence that is specified in, or is of a description specified in, regulations made by the Secretary of State (see section 44), or*
- *(e) an offence, not within paragraph (a), (b) or (c), of which the victim or intended victim is an individual (or individuals)."*

---

[28] Section 1C of the Financial Services and Markets Act 2000 (as amended)
[29] https://www.handbook.fca.org.uk/handbook/COBS/4/2.html
[30] In an unauthorised fraudulent transaction, the account holder themselves does not provide authorisation for the payment to proceed and the transaction is carried out by a third party. Customers are legally protected against losses caused by unauthorised fraud.
[31] UK Finance, Fraud - The Facts 2021, op. cit.

46. Building on this, we propose inserting a new Section 44, which refers to a new Schedule 4 within the Bill which defines the offences that constitute fraudulent offences, including fraud facilitated via paid-for adverts and cloned websites. This will be based on existing domestic legislation, including the Fraud Act 2006, and should not introduce any new offences. As with Section 42 and Section 43 in the draft Bill for terrorism and CSEA activity respectively, the Secretary of State will have powers to amend this new Schedule through subsequent regulations.

47. We propose a new Section 44 as follows:

"[NEW] 44 Offences relating to fraud

(1) In this Part "fraud offence" means an offence specified in [NEW] Schedule 4

(2) Secretary of State may by regulations amend [NEW] Schedule 4"

48. Building on this, we propose a new Schedule 4 as follows:

"SCHEDULE 4

[NEW] Section 44

FRAUD OFFENCES

1. *An offence under any of the following provisions of the Fraud Act 2006 —*
   a. *Section 2 – Fraud by false representation*
   b. *Section 3 – Fraud by failing to disclose information*
   c. *Section 4 – Fraud by abuse of position*
   d. *Section 6 – Possession or control of articles for use in fraud*
   e. *Section 7 – Making or supplying articles for use in fraud*
   f. *Section 9 – Participating in fraudulent business*
   g. *Section 11 – Obtaining services dishonestly*

2. *An offence under section 5(2) of the Criminal Law Act 1977 (conspiracy to defraud).*

3. *A money laundering offence under Part 7 of the Proceeds of Crime Act 2002."*

49. We also propose amending Section 41 (5) of the Bill on the meaning of illegal content by inserting the following technical line that clarifies when the relevant offence is a fraud offence, the content is described as fraudulent content respectively:

"Illegal content—

(a) is "terrorism content" if the relevant offence is a terrorism offence;

(b) is "CSEA content" if the relevant offence is a CSEA offence;

(c) is "fraudulent content" if the relevant offence is a fraud offence;

(c) is "priority illegal content" if the relevant offence is an offence that is specified in, or is of a description specified in, regulations under subsection (4)(c)."

50. From this, we propose a new Section 7 (8) (b) (iii) (and respectively, Section 19 (3) (a) (iii)) of the draft Bill, by inserting the following line to require service providers to identify, assess and understand the risks of fraudulent content on their platforms:

> *"Definitions*
>
> *(8) An "illegal content risk assessment" of a service of a particular kind means an assessment to identify, assess and understand such of the following as appear to be appropriate, taking into account the risk profile that relates to services of that kind –*
>
> *(a) the user base;*
> *(b) the level of risk of individuals who are users of the service encountering the following by means of the service—*
> *(i) terrorism content,*
> *(ii) CSEA content,*
> *(iii) fraudulent content,*
> *(iv) priority illegal content, and*
> *(v) other illegal content,"*

51. We also recommend that the safety duties about illegal content (Section 9 and Section 21) require that providers take further proactive measures to minimise the presence, time and dissemination of fraudulent content. It is not enough for providers to simply undertake a risk assessment for fraudulent content and take down this content when reported.

52. This would be best achieved either through a commitment from Government that fraud offences will be treated as priority illegal content through later regulations referred to under Section 41 and Section 44 as it stands in the draft Bill, or by a specific reference to fraudulent content in Section 9 and Section 21.

53. Additionally, we propose a new Section 29 (3) which recognises that OFCOM prepares codes of practice specifically relating to fraudulent content, as follows:

> *"29 Codes of practice about duties*
>
> *(3) OFCOM must prepare a code of practice for providers of regulated services describing recommended steps for the purposes of compliance with duties set out in section 9 or 21 (safety duties about illegal content) so far as relating to fraudulent content."*

54. Alongside this, we recommend that Section 63 of the Bill should be amended to include fraudulent content to provide the statutory basis for OFCOM's power to require a service provider to use accredited technology to identify and remove fraudulent content on private and public channels.

55. We also believe that the harmful content provisions should be expanded to include financial impacts on individuals in any assessment of harmful content, alongside psychological and physical impacts on individuals which are already included in the draft Bill's harmful content provisions (Section 45 and Section 46).

56. Finally, we would recommend that the Bill adopts the FCA's recommendation[32] of expanding the Duties of Care (Chapter 2 and Chapter 3 of Part 2) to encompass an obligation to prevent the communication of financial promotions which have not been approved for communication by an FCA-authorised firm. To fulfil this duty, online platforms and their senior managers should be required to implement measures including:

    - Appropriate gateway systems and controls to prevent publication.
    - Steps to ensure fraudulent and misleading financial promotions are dealt with rapidly.
    - Processes that allow authorities to share intelligence on non-compliant financial promotions.

Are there any contested inclusions, tensions or contradictions in the draft Bill that need to be more carefully considered before the final Bill is put to Parliament?

57. Whilst there is no specific mention of the types of user-generated fraud in scope within the text of the draft Bill, this Sub-Committee will be aware that paid-for advertising is explicitly out of scope of the draft Bill.

58. For the reasons outlined above, we believe that this exclusion contradicts the Government's ambitions within the Bill in relation to fraud. Only legislating against specific types of user-generated fraud, and not wider online fraud, such as those facilitated by adverts, will be ineffective in practice; leaving a large proportion of online fraud outside the scope of this legislation and inadvertently creating a loophole for criminals to exploit.

59. As highlighted by research from the Money and Mental Health Institute[33], the distinction between paid-for and user-generated content can often be subtle with the only difference to the user being small "ad" labels on promoted social media posts or search engine results. Research for the Advertising Standards Authority found that a third of people were unable to identify that a post on social media was an advert, leaving many individuals uncertain of what is promoted content, and user-generated content[34].

60. At present, it is also unclear whether a scam post generated by a user would fall out of scope of the Bill if the post was promoted by a paid-for advert; thereby almost immediately creating an opportunity for fraudsters to circumvent the proposed legislative measures by promoting user-generated content through paid-for adverts.

61. For example, it is unclear whether the impersonation scam in Case Study 1 above would fall out of scope of the legislation if the criminal paid to promote the Instagram posts which attracted the victim into falling for the fraudulent investment opportunities.

62. This ambiguity would be resolved by a clearer definition of fraudulent online content within the Bill (whether user-generated or paid-for), as proposed in answer to the previous question above.

63. Instead of a more comprehensive response to tackling online fraud within the Bill, the Government's current position is that fraud facilitated via paid-for advertising will be

---

[32] https://committees.parliament.uk/publications/6692/documents/71799/default/

[33] https://www.moneyandmentalhealth.org/wp-content/uploads/2021/06/Safety-first_-Why-the-online-safety-bill-should-tackle-scam-adverts.pdf

[34] Ipsos Mori. Research on the Labelling of Influencer Advertising. On behalf of the Advertising Standards Authority. 2019.

covered through a separate Online Advertising Programme, led by DCMS. This work is yet to commence, with a consultation not due until later this year, and the Government's planned response not until 2022, with no forthcoming legislative timetable following that[35].

64. Even if legislation were forthcoming, we believe that complicating the legislative response to online fraud through the separate Online Advertising Programme, will lead to a more complex, cumbersome and incomplete patchwork approach to regulation, taking longer to implement and creating even further delay in the urgent need to tackle the growth in fraudulent online advertising now. Counterproductively, the Government's proposed patchwork approach is also likely to bring further challenges in the consistent and effective use of such legislation.

65. As stated in a joint letter by the Home Secretary and Secretary of State for Digital, Culture, Media and Sport of 16 June 2021, it is the Government's stated ambition to "…work to reduce fraud and make sure that the UK is the safest place to be online…"[36]. However, this is currently at odds with the muddled approach proposed by these separate initiatives which will only cause delay and create ineffective legislation.

66. By contrast, the Online Safety Bill is a ready-made legislative instrument to fully tackle these issues at pace.

67. We therefore recommend that the Government reconsiders the exclusion of paid-for advertising and cloned websites in relation to their role in facilitating fraud, and instead includes the necessary mechanisms to tackle all online fraud within the Bill when it is formally introduced.

68. To achieve this, we propose that Section 39 (2) (f) of the draft Bill should be altogether removed, which currently excludes paid-for advertisements from the scope of regulated content.

69. There is also a risk that the Bill's exclusion of intellectual property (IP) rights may inadvertently exclude fraud facilitated via cloned websites from the scope of the Bill. The interests of the consumer are best protected not through separate enforcement of the IP holders' rights (which will inevitably take time) but through requiring the online service provider to take down the offending advert or cloned website as soon as it is brought to its attention. Relying on the Advertising Standards Authority or the individual IP rights holder to take remedial action to rectify the position may be less immediately effective than requiring the online service provider (through powers in the Bill) to take down the offending material or to remove or suspend the cloned website as soon as it is pointed out and its bona fides questioned.

70. We therefore recommend that fraud facilitated via cloned websites are fully included within the scope of the Bill by amending Section 41 (6) (a) of the Bill to ensure that this does not unintentionally exclude fraud facilitated by cloned websites.

ENDS

---

[35] https://www.gov.uk/guidance/digital-regulation-overview-of-government-activity
[36] https://pimfa.uk/drive/s/K7Gvz2SIBfEftWYkZLmzrdmrUbTe3g

Annex 1

Understanding the different types of fraud and illustrating the importance of widening the Online Safety Bill's scope

For the benefit of the Sub-Committee, we have included examples below of some of the different types of fraud that commonly take place on online platforms, demonstrating how the partial inclusion of user-generated fraud within the draft Bill will fail to tackle a vast proportion of fraud carried out via paid-for adverts and cloned websites promoted by online platforms.

The below case studies are based on real-life reports that we have received from UK Finance member firms. Unless otherwise referenced, figures in this section are from UK Finance's report Fraud the Facts:2021[37]*.*

Investment Scams

In an investment scam, a criminal convinces their victim to move their money to a fictitious fund or to pay for a fake investment. These scams are often promoted through adverts on social media sites or search engines offering higher than average returns and may lead to cloned/fake websites impersonating real investment firms.

In 2020, more than £135 million (an increase of 42 per cent from 2019) was lost to investment scams affecting nearly 9,000 victims.

During this period, payment services providers returned £49 million of losses to victims.

The nature of the scams means that the sums involved in individual cases can be high, so while investment scams accounted for only six per cent of the total number of APP scam cases, they accounted for 28 per cent of the total value of all APP fraud.

Criminals have been increasingly preying on people's financial insecurities during the pandemic through investment scams promising high returns. Some criminals may initially pay out returns on their victim's investment to convince them to invest more money.

Individuals of all ages are at risk from investment fraud as criminals target them by exploiting online services. Anecdotal intelligence suggests younger individuals may be more vulnerable to malicious social media posts promoted via paid-for adverts offering false investment opportunities, whilst older generations are more likely to fall victim to fake comparison sites or search engines which push victims to cloned investment sites. Indeed, National Fraud Intelligence Bureau statistics based on a rolling 13 months of data from Action Fraud[38] shows that the number of investment fraud victims are broadly evenly split across the 20-79 age ranges.

Investment scam case study *– See Case Study 2 in the main response.*

Romance Scams

---

[37] https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2021
[38] https://colpolice.maps.arcgis.com/apps/opsdashboard/index.html#/60499304565045b0bce05d2ca7e1e56c

In a romance scam, the victim is persuaded to make a payment to a person they have met, often online through social media, dating websites and apps or gaming sites, and with whom they believe they are in a relationship.

A total of £21.2 million was lost to romance scams in 2020 (an increase of 17 per cent from 2019), affecting nearly 9,000 reported victims (32 per cent higher than 2019) - driven by the rise in online dating during the pandemic.

The nature of the scam means that the individual is often convinced to make multiple, generally smaller, payments to the criminal, as indicated by an average of around five payments per case.

Whilst these frauds typically start on dating sites and apps or social media sites, the majority of cases move to instant messaging services such as WhatsApp.

Romance scam case study

In October 2020, a 60-year-old male from London searched for a companion using Google. He was directed to a third-party website promoted on Google where he subscribed and then interacted with a user purporting to be a 40 year-old female from Romania. The profile was fake and was operated by fraudsters who had cloned a genuine account from the platform so that it appeared legitimate.

Over the proceeding months, messages were exchanged which led to a proposed meeting in London. The fraudsters convinced the user to transfer £2,000 for flights for the meeting. Shortly before flights were scheduled, the fraudsters fabricated reasons why the flight had been missed and requested funds to pay for urgent medical care or customs duties.

This happened repeatedly and in total, £75,000 was sent to the fraudsters account.

Purchase Scams

In a purchase scam, the victim pays in advance for goods or services that are never received. These scams usually involve the victim using an online platform such as social media marketplaces, where scams are often promoted via paid-for adverts.

Common scams include a criminal posing as the seller of a car or a technology product, such as a phone or computer, which they advertise at a low price to attract buyers. Criminals also advertise items such as cheap holidays, travel deals and concert tickets. While many online platforms offer secure payment options, the criminal will persuade their victim to pay via a bank transfer instead. When the victim transfers the money, the seller disappears, and no goods or services arrive

Purchase scams were the most common form of APP scam in 2020, with the 78,720 cases accounting for 52 per cent of the total number of APP scam cases.

A total of £57.1 million was lost to purchase scams in 2020, with the vast majority of losses being from personal accounts.

Purchase scams case study

Callum bought a laptop advertised on social media at a heavily discounted price compared to the one he had seen on the official seller's website.

Upon contacting the seller, he was told that the offer was for a limited time only therefore if Callum wanted the laptop, he needed to pay quickly by bank transfer.

Proof of payment was sent to the seller but when Callum asked for a tracking number, he received no response. After numerous attempts to contact the seller, Callum searched their name and came across numerous bad reviews from other people. He never received the laptop.

Impersonation Scams

In this scam, victims are convinced to make a payment to a criminal claiming to be a trusted individual, or from a trusted organisation such as their bank, the police, a utility company, or a Government Department.

In 2020, the number of reported impersonation scams increased by 95 per cent from 2019, with nearly £97 million lost to criminals affecting over 39,364 victims.

Common scams include claims that the victim must settle a fictitious fine, pay overdue tax or return an erroneous refund. Sometimes the criminal requests remote access to the victim's computer as part of the scam, claiming that they need to help 'fix' a problem.

Criminals will often research their targets first, using information gathered from scams, social media and data breaches.

Impersonation scams case study *– see Case Study 1 in the main response.*

Money Muling

Money mules are recruited, sometimes unwittingly, by criminals to transfer illegally obtained money between different bank accounts. Money mules, who are typically younger individuals (such as students), receive the stolen funds into their account. They are then asked to withdraw it and wire the proceeds to a different account, often overseas, keeping some of the money for themselves.

Research from Cifas[39] revealed there were 17,157 cases of suspected money muling activity involving 21-30-year olds in 2020, a five per cent increase on the previous year. This age group accounted for 42 per cent of money mule activity in 2020, up from 38 per cent three years ago.

During the pandemic, money mule recruiters targeted 'generation Covid' – those looking for work or to earn easy money – by posting fake adverts on job websites and social media sites.

Often, people are unaware that allowing their bank accounts to be used in this way is a crime with consequences under criminal and civil law. Besides a criminal record, the individual could have their bank account closed and difficulty opening one elsewhere, and trouble obtaining mobile phone contracts or accessing credit in future.

Money muling case study

A 26-year-old male had a friend on Snapchat that he had known for a couple of years that asked for a favour.

A friend of the friend reached out to the male and asked him to receive money into his account, alongside receiving packages to his house which were then collected in person. Some of the

[39] https://www.cifas.org.uk/newsroom/money-mules-target-generation-covid

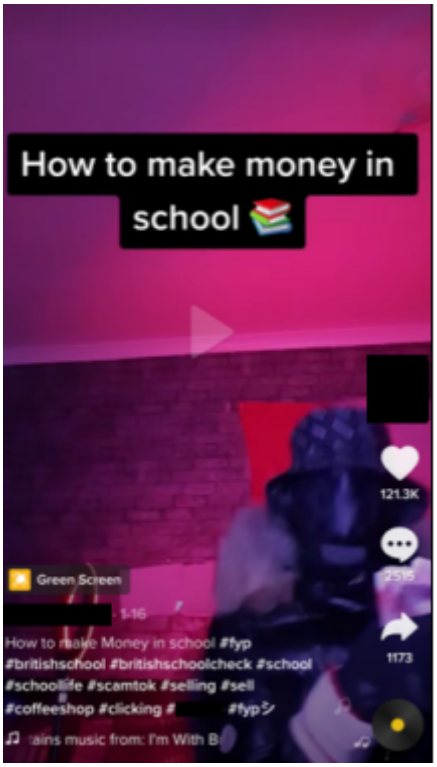
packages contained iPhones, but the individual didn't know what was in all the packages. He was told that he would be paid for this but didn't keep any of the money that was moved through his account.

Money was transferred into other accounts of the customer as well as his account with the bank. The person he was in contact with had an active Snapchat account where he promoted stories of a lavish lifestyle which led the man to believe this activity to be legitimate. After failing to be paid, the male contacted the police, where he informed them and the bank of the activity he had taken part in. We do not know if any action was taken by the police to reprimand the individual, however the bank made the decision to close his account down.

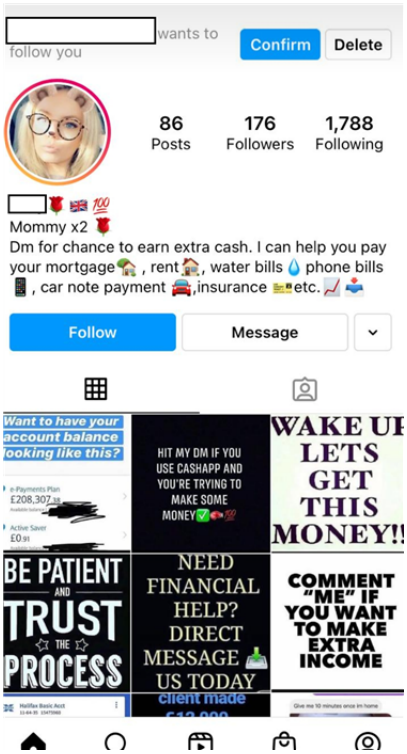
Annex 2

<u>Emergence of criminals openly advertising fraud and scam services for sale online</u>

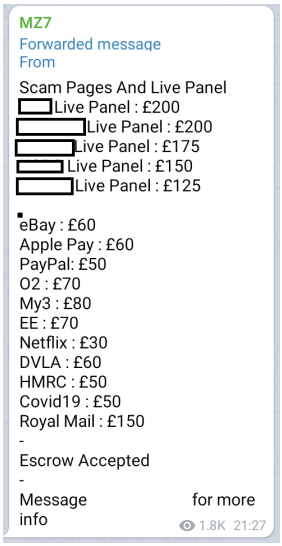
For the benefit of the Sub-Committee, we have included screenshots below illustrating how criminals openly advertise fraud and scam services for sale online, including template phishing websites and custom-built scam apps which replicate real banking apps.

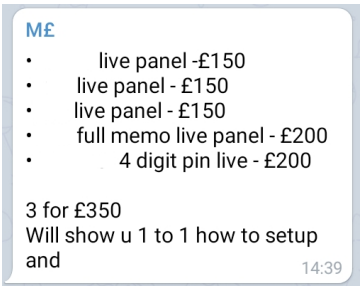


Screenshot 1 – fraudsters have been targeting students into using fraud and scam services online, often through posts such as this screenshot from TikTok using the hashtag *#scamtok*. Whilst initially user-generated, these can also be promoted on users' feeds by paid-for adverts to maximise the number of impressions. Note 121,000 likes on the post above.



Screenshot 2 – fraudsters also target individuals' financial insecurities such as difficulties paying mortgage payments, rent and water bills. These can often lead to scams in themselves or move onto encrypted messaging services like WhatsApp or Telegram where criminals sell scam services (see screenshots below).





Screenshots 3 and 4 – fraudsters then move to encrypted messaging service platforms such as Whatsapp and Telegram to sell fraud and scam services online, including template phishing websites and custom-built scam apps which replicate real banking apps. Note 1,800 members in the Telegram group in Screenshot 3.