Online-harms white paper: UK Finance response

Date: 1 July 2019

Sent to: onlineharmsconsultation@culture.gov.uk

Introduction

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. Our response to the UK government's online-harms white paper addresses aspects of direct interest to the banking and finance industry. Foremost among those is economic crime, and our answers to the questions posed by the white paper relate to that interest. But we also set out other interests in the overview below.

3. If you have any questions relating to this response, please contact Matthew Conway, Director of Government & Regulatory Affairs, at matthew.conway@ukfinance.org.uk.

Overview

The government should include economic crime among the harms companies will be held to account for tackling

4. Fraud poses a major threat to the UK. It is a crime that the banking and finance industry is committed to tackling, but it requires the combined efforts of every sector, both public and private, to overcome. This is strongly echoed by the National Economic Crime Centre (NECC), which has conducted the UK's first public-/private-sector threat assessment of economic crime. This states that combating economic crime can only be achieved by a true public/private partnership. We agree that only by harnessing the capabilities, expertise and powers of both the public and private sectors can we truly create a step change in our approach to economic crime. By working together collaboratively across all sectors, we believe the UK can truly be a world leader in the global fight against economic crime. Our position as a global financial centre means it is incumbent on us to continually strengthen our domestic response and demonstrate real leadership in building up the capability of the international network to combat economic crime. We consider that a strong response to economic crime demonstrates to the world that the UK is a safe, secure and transparent place to do business and promotes the prosperity of society.

5. In 2018, the advanced security systems and innovations in which the banking and finance industry invests to protect customers stopped more than £1.6 billion of unauthorised fraud. Despite this, criminals still successfully stole £1.2 billion through fraud and scams.[1] These crimes can have a devastating impact on victims, and even if the customer is compensated in full by their finance provider, the organised criminal gangs that perpetrate these frauds still profit from the proceeds. Such monies can go on to fund illicit acts—terrorism, drug trafficking and people smuggling—that damage the fabric of our society.

[1] UK Finance, *Fraud the Facts 2019*. https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019.

6. While we therefore welcome and support the aims and objectives set out in the white paper, we strongly encourage the additional inclusion of economic crime (e.g. fraud and money laundering) in the scope of online harm. This would ensure regulation remains relevant to tackling these aspects of online harm.

7. The abuse of social-media platforms by organised criminals for the purposes of financial crime has increased significantly. One bank reports almost half the scams it has seen this year originated from social media, and intelligence from law enforcement and other sources indicates there are thousands of accounts in operation by criminals at any one time and the majority are openly advertised and visible to users. These facilitate advertising for money mules (for the purposes of money laundering), selling stolen identity and credit-card data, phishing, impersonating legitimate companies (e.g. banks) to steal customer banking details and financing terrorism.

8. The white paper refers to other separate government and regulatory measures and initiatives to tackle fraud (e.g. the Home Office Joint Fraud Taskforce), but the scope of these programmes of work only includes some aspects of the problem and excludes certain fraud types and their root causes. Moreover, there is currently little incentive to compel the online platforms and services in scope of the regulatory framework ("online-service providers") to participate and act.

9. In addition, limited overseas jurisdiction and domestic gaps in the powers of law enforcement are hampering economic-crime disruption and prosecution efforts. For example, the Regulation of Investigatory Powers Act 2000 (as amended) does not cover a device data request to social-media companies.

10. The government accepts the current response to fraud is inadequate compared to the scale of the threat seen in the UK and so is working with the banking and finance sector on a national economic-crime plan. As such, online-service providers should have to play their part in tackling harms such as fraud.

11. The Office for National Statistics cited fraud as the most commonly experienced offence in England and Wales in the year ending September 2016.[2] Much of this activity is perpetrated online and enabled in part through online-service providers. Other reported statics show there are 1,000 victims per week of online-purchase scams, equating to a financial loss of £46.4 million and resulting in part from criminals' use of social-media and auction sites. This type of scam is currently forecast to grow to 2,000 victims per week over the next five years. This is just a subset of the fraud losses as social media inadvertently contribute to other scam types and fraud areas.

12. Data breaches should also be within scope due to the indirect harm to the public. Breaches at third parties continue to be a major contributor to fraud losses, with several high-profile incidents in 2018 involving well-known brands where customer data were stolen. Whether at a retailer, a utility company, a transport provider or elsewhere, the theft of personal and financial data can both directly lead to fraud losses and be used by criminals as part of their scams. The data can be used for months—even years—after the breach takes place. These incidents occur outside banks' control, yet it is they and their customers who bear the impact. It is therefore imperative that any organisation that controls customer data does everything in its power to keep them secure.

[2] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016.

13. Although the General Data Protection Regulation and the Network and Information Systems Regulations 2018 require notification to the Information Commissioner's Office (ICO) in the event of a breach that meets certain criteria, the visibility and connection to the advice provided by the National Cyber Security Centre (NCSC) to online-service providers could be more prominent and advertised more widely to enable greater take-up and a more rapid response in the event of a reportable breach. We would welcome more comprehensive guidance, perhaps provided jointly by the NCSC and ICO, on the latest thinking and best practice that organisations should (or should not) consider taking to protect individuals in the immediate aftermath of a breach.

14. Additional measures whose consideration we encourage are annexed to this response. These were drafted by the banking and finance sector, and we feel they strike a good balance between being effective in tackling online harm and not being overly burdensome for companies. They would complement the measures set out in the white paper, making the regulatory framework for online safety more robust.

It is important to maintain the distinction between the proposed regulatory framework for online safety and the existing regulatory framework for financial services

15. The banking and finance sector is already highly regulated, with the Financial Conduct Authority (FCA) charged generally with securing an appropriate degree of protection for consumers[3] and requiring firms to ensure communications are fair, clear and not misleading.[4] Specific online consumer protections include the Payment Services Regulations 2009 (implementing the EU Payment Services Directive[5]) and the recently introduced Contingent Reimbursement Model code for authorised push-payment scams.[6]

16. There is no expressed intent for the proposed regulatory framework for online safety to overlap in any way with the existing regulatory framework for financial services, and we believe it important that the government maintain that separation in the decisions it takes in the light of responses to the white paper. In particular, the government should take forward the duty-of-care proposals in the white paper in light of the specific problems caused by online harms. We do not consider it appropriate or necessary for the regulatory framework for financial services to incorporate such a duty, and the FCA has recently concluded that "consumer harm can be caused by different things, so there is unlikely to be a one-size-fits-all solution to any weaknesses in consumer protection." As such, it does "not consider that this is a sufficient basis for making changes to primary legislation" in respect of a duty of care.[7]

17. Of course, a regulated financial-services firm separately undertaking activities in scope for regulation according the white-paper proposals should be separately regulated in respect of those activities.

The implications of how online activity is monetised

18. The payments industry recognises its role in helping disrupt the collection and distribution of funds that underpin illegal activity by identifying instances of fraud, money laundering etc. As the prevalence and availability of communications and video-streaming channels expands, the wider

---

[3] Section 1C of the Financial Services and Markets Act 2000 (as amended).
[4] https://www.handbook.fca.org.uk/handbook/COBS/4/2.html.
[5] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.
[6] https://www.lendingstandardsboard.org.uk/contingent-reimbursement-model-code/.
[7] https://www.fca.org.uk/publications/feedback-statements/fs19-2-duty-care-and-potential-alternative-approaches.

payments ecosystem needs to better engage with established entities that play a pivotal role in monetising video content (e.g. the use of multichannel networks). Such organisations have the primary commercial relationship with many online-service providers and manage the accounts, clawback of monies and distribution of payments based on the activities and revenues generated through a proprietary video channel owned by a content creator.

19. In terms of specific online harms (e.g. problem gambling), the banking and finance industry is looking at tools that can help protect consumers and support customers to self-exclude (e.g. better signposting customers to third-party organisations that can help address the underlying causes of the harm). While helpful, these tools still require a level of analysis and real customer interaction to determine whether they are likely to be of any practical effect and have a measurable impact so as to be considered "financial aids" able to improve the financial health of an individual who is demonstrating signs of problem gambling.

The government should not rely too heavily on credit products for proof of age

20. The card-payments industry has a strong record of ensuring legal compliance by its merchants with regulatory requirements, but there must be statutory underpinning, clear and unequivocal evidence to act (e.g. terminating contracts) and active regulatory monitoring. Payment firms also cannot make judgments on the suitability of content or age-verification processes on websites. For example, children can make use of parents' or others' credit cards and could be more inclined to do so when no charge will be made against the card, as may well be the case when the purpose is simply age verification. Moreover, although under-18s cannot be held to a credit-card agreement, they can be authorised users on another primacy credit-card holder's account (and while this is not known practice among UK issuers, it might be in other countries). Finally, if consumers become accustomed to the idea that they must use a credit card to demonstrate their age, this will make it easier for criminals to successfully set up fraudulent websites and acquire consumers' credentials, facilitating impersonation and fraud. For all these reasons, age verification must remain the responsibility of online-service providers.

The government should ensure a level regulatory playing field for banking and finance providers

21. Financial-services customers in the UK enjoy a rich set of protections within an established regulatory framework that encourages competition. It is right that these evolve to match the products and services they consume no matter the provider, and the set of measures proposed in the white paper are a positive step in this direction.

Answers to questions

Question 1. This government has committed to annual transparency reporting. Beyond the measures set out in this white paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

22. We support the measures set out in the white paper as a good starting position. To ensure the long-term effectiveness of the regulatory framework, periodic threat-harm reviews should be undertaken to determine if better and/or additional data are needed. The NECC has conducted the UK's first public-/private-sector threat assessment of economic crime, and this is an effective tool in identifying and then helping tackle harms. The NECC's assessment and the learnings from it should be considered the model to replicate here. Also, the threats highlighted in the assessment relate in part to the online harms featured in the white paper (e.g. money mules

recruited via social media) and so can be used to inform the government's periodic assessment of online harms.

23. We strongly support the approach set out in paragraph 3.18. We believe published benchmarking reports will incentivise online-service providers to become best in class and enable the public to make better informed choices.

Question 2. Should designated bodies be able to bring "super complaints" to the regulator in specific and clearly evidenced circumstances?

24. Yes.

Question 2a. If your answer to question 2 is "yes," in what circumstances should this happen?

25. Where there is clear evidence that one or more of the online harms in the scope of the regulatory framework shows no sign of abating and/or is not being effectively addressed by relevant online-service providers.

26. It will also be important to consider new and evolving online harms that clearly demonstrate harm to the public and/or the economy.

Question 3. What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity and/or breaches of the duty of care?

27. We believe the measures set out in the white paper are appropriate.

Question 4. What role should parliament play in scrutinising the work of the regulator, including the development of codes of practice?

28. No response.

Question 5. Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach?

29. Yes, albeit we feel strongly that economic crime (e.g. fraud and money laundering) should be brought into scope as this would help tackle a significant and growing threat to the UK public and economy and ensure regulation remains relevant to tackling these aspects of online harm.

Question 6. In developing a definition for private communications, what criteria should be considered?

30. No response.

Question 7. Which channels or forums that can be considered private should be in scope of the regulatory framework?

31. All social-media channels and public discussion fora that also provide a private or direct-messaging service, including Facebook, Instagram, Snapchat, Twitter and WhatsApp. Intelligence from banks and law-enforcement agencies shows private communication channels pose the same financial-crime risks—advertising for money mules (for the purposes of money laundering), selling stolen identity and credit-card data, phishing and impersonating legitimate companies (e.g. banks) to steal customer banking details—as open/public fora due to the multiple

ways in which they are abused to enable and facilitate financial crime and provide criminals with a greater ability to avoid detection. This exacerbates the challenges law enforcement faces in identifying harmful activity.

Question 7a. What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

32. The use of artificial-intelligence software could be an effective means of identifying harmful activity taking place on private communication channels. This could also have the added benefit of helping alleviate privacy concerns.

Question 8. What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?

33. We support the risk-based approach proposed in the white paper.

34. We believe the regulator should undertake periodic assessments of the online-harm threat landscape, with wider input and support, to remain up to date with the nature and volume of the most harmful activities. This will help target enforcement and so ensure regulation remains proportionate.

35. We also see merit in a self-certification or kite-mark approach to develop a common understanding for the public.

Question 9. What, if any, advice or support could the regulator provide to businesses, particularly start-ups and SMEs, to comply with the regulatory framework?

36. We see merit in:

- easily understood and adoptable best-practice guidance;
- typologies of new threats, language, trends and behaviour;
- encouraging information and intelligence sharing between online-service providers and law enforcement and with other sectors with a vested interest in mitigating online harms;
- kitemark standards to demonstrate online-service providers are complying with the regulatory framework; and
- regular and coordinated education and awareness activities.

Question 10. Should an online harms regulator be (i) a new public body or (ii) an existing public body?

37. We believe Ofcom should take on this role. As a consequence, its consumer-protection remit should be extended to include the prevention of financial crime.

Question 10a. If your answer to question 10 is (ii), which body or bodies should it be?

38. See above.

Question 11. A new or existing regulator is intended to be cost neutral. On what basis should any funding contributions from industry be determined?

39. No response.

Question 12. Should the regulator be empowered to (i) disrupt business activities, (ii) undertake ISP blocking or (iii) implement a regime for senior-management liability? What, if any, further powers should be available to the regulator?

40. We believe the regulator should be empowered in all three respects as each can be applied appropriately to different types of online service and online-service providers will themselves exhibit different characteristics (e.g. domestic vs. offshore).

Question 13. Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

41. Yes, if this contributes to addressing the online harms within the scope of the regulatory framework.

Question 14. In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

42. No response.

Question 14a. If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?

43. N/A.

Question 14b. If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

44. N/A.

Question 15. What are the greatest opportunities and barriers for (i) innovation and (ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

45. We see the following barriers:

- little incentive for online-service providers to combat/reduce harmful behaviour themselves;
- a lack of legal powers and collaboration in information and intelligence sharing;
- difficulties in monitoring and predicting evolving harmful behaviour; and
- difficulties in monitoring and policing online services given the sheer volume of activity.

Question 16. What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

46. Better information and intelligence sharing on existing and evolving online harms and how they are perpetrated (e.g. the techniques and language used and obvious signs/red flags to look out for).

Question 17. Should the government be doing more to help people manage their own and their children's online safety and, if so, what?

47. We believe more should be included in the national curriculum in this respect.

Question 18. What, if any, role should the regulator have in relation to education and awareness activity?

48. We believe education and awareness about economic crime (e.g. the risks of young people and students becoming money mules) should be a key component of the regulatory framework. This should include:

- engaging with the general public and the education sector;
- encouraging users to report online harms and online-service providers to create dedicated teams to investigate such reports;
- promoting better awareness among providers of how their online services can be misused to propagate online harm;
- providing guidance for online-service providers on the level of education and awareness activity expected of them; and
- international and/or extraterritorial cooperation and/or information sharing between regulators to mitigate potential detriment at an early stage.

Annex: additional measures

49. We set out below additional measures whose consideration we encourage. These were drafted by the banking and finance sector, and we feel they strike a good balance between being effective in tackling online harm and not being overly burdensome for companies. They would complement the measures set out in the white paper, making the regulatory framework for online safety more robust.

- A standardised service-level agreement (including timeframe) for online-service providers responding to requests to take down harmful content.
- Expanded community guidelines to address the full range of online harms (e.g. the inclusion of brand infringement and information on the harm it causes).
- An effective mechanism across all online platforms for denoting genuine high-profile/celebrity/influencer accounts (e.g. a kite mark or identifier unique to the person or company). This would help prevent online identities being misused for malicious purposes (e.g. promoting harmful behaviour or illegal services).
- A forum for formal engagement and cooperative working among online-service providers. This would be an ideal place to share insights (e.g. into the evolution of online harms) and coordinate action.
- Work in conjunction with, and alongside, existing fraud bodies and campaigns to raise education and awareness of economic crime.
- Work with the banking and finance industry to encourage online-service providers to increase education and awareness about money mules and promote messaging that prevents young people and students from becoming money mules.
- Sharing common jargon/language used by criminals and making this accessible to online-service providers and law enforcement in order to act appropriately in real time.
- A blacklist of malicious hash tags.
- Splash pages on profile takedown.
- Legislative change to provide law enforcement with the necessary powers and to bring online-service providers within the scope of the Suspicious Activity Reporting regime.
- Intelligence data on the following, which would identify criminals if there were a legal obligation for online-service providers to report suspicious activity:
    - mule recruitment sites;
    - changes in search profile—lone-wolf attack typology;
    - grooming (terrorism, insider recruitment or mules); and
    - personal data (including or excluding card data) for sale on e-commerce sites.