Written evidence submitted by the Office of the City Remembrancer, City of London Corporation (OSB0148)

Introduction

1. The City of London Police lead for the National Police Chiefs' Council on economic and cyber crime and are the National Lead Force for Fraud. The City of London Police operates Action Fraud and the National Fraud Intelligence Bureau, funded by the Home Office, which is the national reporting and recording centre for fraud and financially motivated cyber-crime. James Thomson, Chair of the City of London Police Authority Board, is also Deputy Lead for Economic and Cyber Crime and the only politically independent Board member at the Association of Police and Crime Commissioners[1]. Angela McLaren joined the City of London Police in November 2020 as Assistant Commissioner and is responsible for the NPCC Economic and Cyber Crime Portfolio. AC McLaren will shortly be taking on the role of Commissioner in the force and will continue to lead on much of the work on Economic and Cyber Crime.

2. As National Lead Force for Fraud, the City of London Police investigates serious, complex and cross-border fraud. It provides training and continuous professional development for the police and private sector workforce through its Economic Crime Academy.

3. Compared to 2019 average reporting levels, there has been a significant increase in frauds facilitated through online channels. This includes:

    - **Online shopping and auction fraud** (43% increase)
    - **Romance fraud** (15% increase)
    - **Investment fraud** (16%increase)

4. There has been a notable increase in the number of investment fraud victims who have been contacted via social media. Social media companies and internet service providers often remove websites and accounts promoting investment frauds too late to prevent the public investing.

5. Online shopping and auction fraud are often promoted through social networking sites and accounts for around a quarter of all fraud reported to Action Fraud. Romance fraud continues to increase year on year, the majority of which is perpetrated online.

6. While the City of London Police is working hard with partners to coordinate pursing individuals responsible and providing protect advice to the public, the scale and reach of this threat requires a whole system approach to tackle it effectively. This must include an obligation on the private sector to continue to play its part. This Bill

[1] The City of London Corporation's Court of Common Council is the Police Authority for the Square Mile as set out in the City of London Police Act 1839. The Court delegates this duty (except for the appointment of the Police Commissioner) to the Police Authority Board and its Committees"

presents such an opportunity and one which must be maximised in order to have the most effective impact possible.

7. The below response seeks to identify areas of concern and potential improvement in the Draft Bill through the lens of the City Police's fraud responsibilities.

8. There are two key areas of concern with the Draft Bill's current provisions. Firstly, fraud must be defined as a priority harm. Across government there is a growing realisation of the spread and depth of the harm caused by fraud (now accounting for a third of all crime, as reported by the latest Crime Survey for England and Wales - 4.6 million fraud offences in the year ending March 2021). During 2020/21, 16% of crime reports to Action Fraud featured at least one social media and communication platform with attributed losses in excess of £165 million. This compared to 12% in the previous year.

9. The degree of harm for individuals can be significant. Last year Action Fraud call handlers supported around 200 individuals expressing intent of suicide or other self-harm requiring an immediate police response. Far from being a victimless crime, fraud is extremely harmful and the impact on victims can be long lasting, often with an unwarranted sense of complicity with the criminals as they may have given them access to their life savings.

10. Inclusion of fraud as a priority harm would provide much needed encouragement for online service providers to take proactive steps to identify and stop malicious content linked to fraud and protect users of their services.

11. The second area of concern is the scope of regulation does not cover paid-for advertising. Use of online advertisements helps propagate a wide range of frauds including online shopping, holiday fraud and investment fraud, which often has life-changing consequences for victims. The platforms to which this legislation relates can make considerable returns on illegitimate adverts being placed on their sites, essentially profiting from criminal activity. Allowing these adverts to be placed can also give them an undue credibility with the public who may be under the impression that if the products were a scam, then they would not be allowed to be advertised on such well-known sites/platforms.

12. This Bill presents an opportunity to address a wider range of online enablers to protect the public, reducing the accessibility that criminals currently freely exploit to spread significant harm online.

13. It is understood that DCMS is currently considering its approach to online advertising regulation and it is strongly urged that this work is brought forward (through this Bill or otherwise).

Will the proposed legislation effectively deliver the policy aim of making the UK the safest place to be online?

14. The Draft Bill takes an important step forward in making the UK a safer place to be online. The inclusion of user-generated fraud within the scope of the Bill will make a real difference in tackling scams such as fake investment opportunities and romance fraud. Not only will this benefit law enforcement agencies in their struggle against these scams, but the Bill will have a huge benefit on the thousands of victims of these emotionally impacting crimes. However, it is unlikely that this Bill will achieve the aim of making the UK the safest place to be online on its own. While many of the measures within this Bill are to be welcomed, the threat to individuals online is extremely broad and extends beyond the scope of this Bill. Within the area of online fraud, this Bill does nothing to tackle fraud via advertising, emails or cloned websites. Furthermore, in assessing the Bill against this policy aim, it is also important to understand how safety online will be measured (in the UK and internationally), to allow for meaningful comparisons between jurisdictions.

15. Effectiveness of this legislation also relies on enforcement and ensuring regulators and law enforcement agencies have sufficient capability, capacity and powers to tackle those falling foul of these regulations.

Will the proposed legislation help to deliver the policy aim of using digital technologies and services to support the UK's economic growth? Will it support a more inclusive, competitive, and innovative future digital economy?

16. If the provisions are implemented effectively, they should certainly contribute to this objective, although it is not the sole means by which this will be achieved. Service providers should be encouraged to be more proactive in protecting their consumers beyond the strict confines of these regulations. It is also worth noting that people will likely feel more comfortable and secure operating online if it can be demonstrated to be safer. This is then likely to increase use across both individuals and businesses, which will contribute to economic growth. However, there may be a competing point from those subject to the statutory duty that they will have to deploy more resource towards meeting this duty which may have a negative impact on their own growth, as well as their ability to meet the demands of their users.

Does the draft Bill make adequate provisions for people who are more likely to experience harm online or who may be more vulnerable to exploitation?

17. The breadth of vulnerability online is extremely broad and all users can find themselves in a heightened vulnerable state at different times in their life. This can include individuals at moments of loneliness or financial vulnerability, both of which increased in prevalence during the pandemic. Furthermore, people engage with the online environment through a variety of touchpoints at work, socially and to manage their personal affairs, creating a matrix of different vulnerabilities and circumstances where they can be exploited by online fraud. All individuals can find themselves at moments of vulnerability based on their personal circumstances or situations where they find themselves online, and can be susceptible to scams from any source, including both user generated fraud and paid advertising. It is therefore disappointing that the Bill seeks only to focus on user generated fraud, when the

potential for harm to vulnerable people remains the same. It is also extremely important that severity of harm is not simply correlated to an absolute figure of financial loss. A pensioner losing £5,000 savings could be life-changing, whereas a multinational business or bank losing £500,000 can be much less impactful. While the sums that individuals may lose to fraud can vary, the impact is far-reaching. 74% of fraud victims were emotionally impacted in the year ending March 2020[2]. This includes depression, anxiety and panic attacks. Victims also experience of loss of trust and confidence in using online services.

Is the "duty of care" approach in the draft Bill effective?

18. If applied and regulated effectively, the Duty of Care approach should be effective. It is a model that has been well embedded in other sectors, such as health and safety, and it describes well the level of expectation on industry to ensure the safety of their users, rather than simply tick-boxing a set of requirements. Indeed, the Health and Safety legislation has made the UK one of the safest construction industries in the world, however this was achieved with a holistic approach, not targeting specific hazards. The onus should be on industry to identify threats to individuals and business users and proactively protect them from them. This is where an obligation to issue prevent advice to consumers.

Does the Bill deliver the intention to focus on systems and processes rather than content, and is this an effective approach for moderating content? What role do you see for e.g. safety by design, algorithmic recommendations, minimum standards, default settings?

19. Robust systems and processes are essential to the successful implementation of the Bill's provisions and companies should be availing themselves of the wide range of tools and skills available to achieve the aims of this bill. Encouraging companies to adopt innovative approaches to protect users by design is absolutely the right approach. The focus should be on having clear outcomes with the onus on companies to demonstrate how they are achieving them. Safety by design under the broader duty of care sets a more positive tone, with a better focus on the individual user and their needs.

20. The risk with minimum standards is that many companies may do the minimum to meet them. However, their use in some areas could be a good starting point, such as minimum standards around how quickly malicious content is taken down once identified. This should include steps to notify users who may have been exposed to malicious content that has been identified.

21. Above and beyond moderating content, companies should be obliged to report suspicious activity in a similar way that banks are obliged to do. However, the

[2] Nature of Crime: Fraud & computer misuse (ONS), available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse

threshold needs to be set at a sufficiently high level that reports can be adequately reviewed, and action taken in a timely manner if needed.

The draft Bill specifically *includes* CSEA and terrorism content and activity as priority illegal content. Are there other types of illegal content that could or should be prioritised in the Bill?

22. Fraud should be prioritised in the Bill. Fraud is a growing threat and accounts for a third of all crime (Crime Survey of England & Wales). Around 80% of fraud reported to Action Fraud is digitally-enabled. In 2020/21, 16% of crime reports featured at least one social media and communication platform with attributed losses in excess of £165 million. This compares to 12% in the previous year. Omitting fraud as a priority harm risks sending the message that it is not considered a serious threat, when all the evidence points to the contrary.

Are there any types of content omitted from the scope of the Bill that you consider significant e.g. commercial pornography or the promotion of financial scams? How should they be covered if so?

23. The propagation of financial scams should certainly be included in the scope of the Bill. The legitimacy afforded to things like investment scams through their inclusion on well-known sites and platforms can disarm individuals who may believe that if it was illegitimate, then it would not be allowed to be advertised. It is precisely to address this point that adverts should be included in the scope of the Bill. However, other threats exist, such as ghost broking, which is becoming more widespread and not only defrauding victims out of money, but also leaving them uninsured on the road and inadvertently breaking the law.

24. This Bill presents an opportunity to address this omission and ensure that the public is better protected sooner rather than later (rather than wait for later legislative opportunities), reducing the accessibility that criminals currently freely exploit to spread significant harm online.

The draft Bill applies to providers of user-to-user services and search services. Will this achieve the Government's policy aims? Should other types of services be included in the scope of the Bill?

25. Paid-for advertising is the obvious current omission (as this is how many scams and fraudulent schemes are propagated). However, the Bill should also encompass other online approaches such as regulation on website domain names, fake websites and typo-squatting. The Bill needs to encompass these approaches in the round. By only focusing narrowly, there is a risk of displacement as criminals simply shift their activity to areas not covered by the regulations. The Bill needs to be as proactive and foresighted as service providers are being obliged to be.

Does the draft Bill give sufficient consideration to the role of user agency in promoting online safety?

26. While individuals will always have a duty of care unto themselves, the legitimacy afforded to things like romance fraud and online shopping scams through their inclusion on well-known sites and platforms can disarm individuals who may believe that if it was illegitimate, then it would not be allowed to be advertised. It is precisely to address this point that the scope of the Bill should sufficiently wide to encompass this.

27. There is a responsibility on both parties – users and service providers to take steps to prevent fraud. However, all companies should have a duty of care to their users to protect them from financial harm.

Are Ofcom's powers under the Bill proportionate, whilst remaining sufficient to allow it to carry out its regulatory role? Does Ofcom have sufficient resources to support these powers?

28. This response does have an insight to Ofcom's current and planned resourcing, however this new role will undoubtedly put a significant extra burden on them. The provisions will only be effective if they are properly enforced.

How will Ofcom interact with the police in relation to illegal content, and do the police have the necessary resources (including knowledge and skills) for enforcement online?

29. Compliance with this legislation is the responsibility of Ofcom and ensuring it has the appropriate powers to enforce the Bill's measures should be an important consideration.

30. It is feasible that despite best efforts by industry to identify and prevent illegal content, policing will continue to identify instances of such content through crime reporting (Action Fraud) and investigative work. Where this is the case service providers will be notified and asked to remove the content (in line with current processes). At the moment the level and speed of response to takedown requests is variable. It is hoped this Bill will result in a faster and more consistent approach to removing content identified by the police across the sector. An industry standard for actioning these requests and an opportunity to escalate to Ofcom where the standard is not being met would be welcome.

31. There should be timely sharing of information between all parties to ensure the most complete and up-to-date intelligence picture can be compiled. This should be used to inform continuous improvement of processes for early identification and disruption of financial harm by Ofcom and service providers, and operational activity by policing.

32. Policing has the knowledge and skills to investigate online criminality although resources are constrained across all crime types. It is important to note, however, that the international nature of online criminality means where offenders are based overseas an enforcement outcome may not always be achievable (or the most effective use of resources). This is why stopping criminals from reaching UK service users in the first instance through this type of legislation is so essential.

27 September 2021