Online Dating Association – Written evidence (FDF0028)

About the Online Dating Association:

The Online Dating Association is the trade association recognised internationally as the voice of the online dating sector, supported by a membership of dating services who believe in trust, safety, honesty, clarity, and privacy; who believe in creating a positive experience for users; and who support a technology ecosystem that encourages innovation in online dating. We build trust and confidence in online dating through a set of industry standards and promote safe online dating education to users of apps and websites

Response:

1. The Online Dating Association is particularly knowledgeable about romance fraud, as our members are dedicated to being fraud-free platforms. Romance fraud is usually carried out through a personal relationship between two individuals fostered on either a dating service, online gaming platform or social media service. This can include both traditional romance fraud, which usually takes the form of asking for money for business or personal expenses, or the form investment fraud initiated through romantic relationships~~.~~.

Fraud Landscape

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

2. During the Coronavirus pandemic, there was a noticeable increase in fraud, as everyone ‘went online’ not only for their necessary daily activities, but also for social and emotional wellbeing. According to the FTC Consumer Sentinel Network, the amount lost in 2021 is over $547million to romance scams.
3. In most romance fraud cases, individuals are particularly vulnerable when they are feeling isolated or lonely, have recently experienced heartbreak, or have not received sufficient education on social engagement in digital spaces. With romance fraud, the greatest risk to the individual is being vulnerable and uneducated. Fraudsters are extremely adept at emotional manipulation and recognising the signs of those who are vulnerable and ‘easy targets’.
4. Fraudsters are increasingly more sophisticated. Although the sector is always looking for new and innovative means of stopping fraud on their platforms and backing this up with investment, it is difficult to keep pace with the ingenuity of fraudsters. The online dating industry is dedicated to creating safe and scam-free environments for users, as this is both good for users and good for the company. Services utilise new technologies to remove fraudsters, from profile and conversation moderation by humans

and AI, to background checks and ID verification, to educational resources for users. However, dating services will continue to be vulnerable to romance and investment fraud, as it is a convenient way for fraudsters to attempt to meet victims. We believe dating services are a safer community with more frameworks for protection than either gaming or social media and take the remit to protect users from fraud very seriously.

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

5. Developments in identity theft and AI photo generation will make it more difficult for dating services to catch fraudsters, as will further encryption for messaging and technological advances in hiding IP addresses or locations. The advance in cryptocurrency also means it may be harder to trace payments, if the victims and the perpetrators are not using traditional banks. In romance fraud, the bank often gets involved with questionable payments and is a key partner in protecting victims.
6. The economic situation will also continue to impact the prevalence of romance and investment fraud. For instance, if the economic situation (like Covid) leaves individuals feeling vulnerable, they will be more at risk of becoming victims. Economic uncertainty, such as the cost-of-living crisis or the war in Ukraine, can also be used as part of a manipulative conversation to get victims to part with their money. For example, a romance fraudster may build a relationship and then share with the victim he/she is in Ukraine and needs money to escape.
7. Technology companies play a really important role combatting fraud. Both online dating services and their ancillary services are at the forefront of creating innovative methods of fraud detection, from image-based AI to voice and video moderation to specialised services. A joined-up approach from the wider tech ecosystem would be beneficial, for instance, the app stores hold financial details of users and could be the first line in fraud detection by looking for inconsistency, verifying identity or stopping anonymity.
8. Technology companies, including the ODA, its Members and its Associates are dedicated to finding new ways to combat fraud, with regular webinars and training sessions to share and collaborate. The ODA and its Members also work closely with wider stakeholders who deal with fraud, such as the police, Action Fraud and NFIB.

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

9. Fraud victims are treated as a priority by dating services that are members of the ODA. There are regular improvements to reporting and

protection systems on dating services. There is a financial incentive for online dating platforms to keep fraudsters away, as fraud also creates a disincentive for users to continue subscriptions.

10. However, there are difficulties for dating services with sharing information with police who are looking to support victims. There is not a framework for direct information sharing with the police when a user has been suspended for fraud; the dating sector would be very open to a well-organised framework for accomplishing this and would support Government engagement in the matter. A case cannot be taken against a fraudster without a victim, so dating services can share information, but not pursue a case.

11. The ODA advocates for more support for cross-sector working between Government, law enforcement, public and private sector, including support in both time and money to create better frameworks for data sharing, with appropriate data protection policies.

12. Victim support with the police themselves should also be a priority, and we would support any move towards more capacity for the police to increase their victim support work.

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

13. In romance fraud, there is a prevalence for fraudsters from certain African countries. At the ODA we are not experts in this, but our Members work on this through blocking IP addresses from specific countries, as well as more advanced technological processes.

14. The ODA sees the barriers to tackling borderless fraud as the ability to prosecute criminals abroad. As illustrated by the well-known television programme 'The Tinder Swindler' and the case of Simon Leviev, it was very difficult for disparate police forces to come together to gather evidence and make any convictions. This means there is very little deterrent to criminals.

15. The different laws and police enforcement practices in different jurisdictions make it difficult.

Action to Tackle Fraud

5. How effective is the current structure for policing fraud? How successful are the City of London Police, including Action Fraud and the National Fraud Intelligence Bureau, at executing their role as the lead police force for fraud?

16. The ODA works closely with the City of London Police, Action Fraud and the NFIB to discuss ways of combating romance fraud. We note there is a need for increased capacity and support to do important research on romance fraud as well as to support the police in delivering prosecutions and convictions.

17. We also work with the above organisations to do public outreach, and while these campaigns have an impact we feel more could be done to educate the public. The industry is keen to support public outreach, and regularly shares evidence of the challenging areas for education on safe online behaviour.

6. Are sufficient resources available to Government organisations (such as the Serious Fraud Office and Crown Prosecution Service) and wider police forces to tackle fraud and support victims, and how should this be addressed if not? Answers need not be limited to financial resources.

18. As we outlined, we support larger capacity for the Government organisations and police forces who deal with fraud, and better frameworks for data sharing and collaborative working across sectors that deal with fraud. Dealing with romance fraud victims is a sensitive and complicated matter, and requires a deep understanding to tackle these issues.

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

19. The online dating sector takes their role in protecting the public from romance fraud very seriously. ODA members are spending significant amounts of money increasing trust and safety departments and utilising technology services to protect users including significant moderation tactics with both human and AI processes. Please reference the ODA Standards for the industry to understand further how seriously we take dealing with fraud, and other online harms. These include how to let potential victims know they have been engaging with a removed user.

20. We believe it is essential the private sector supports education on online harms, and specifically romance fraud. Many of our campaigns are focused on educating users how to date safely online, and we have an entire section on our website dedicated to public resources. However, as a small organisation with limited funding we would support a bigger push for digital education.

21. The most important part of tackling fraud is to have outcomes based frameworks in regulation. Rather than legislating or regulating which processes or technologies to use to tackle fraud online, all regulation should focus on the outcomes of limiting the ability for fraudsters to operate and decreasing the amount of fraud happening and the financial losses of victims. We also advocate that outcomes should be proportionate to the risk and size of the companies involved.

22. It is essential that user to user platforms which host content are not made liable for the actions of users on their platforms. The loss of the concept of the ‘safe harbour’ for those hosting content would heavily hinder innovation and the intention of the UK to continue to be a tech hub. A prohibition of any ‘general monitoring’ clause for platforms hosting

content would be welcome, and a focus on outcomes-based risk assessment and mitigation would be the best way for both decreasing fraud and supporting innovation to exist simultaneously.

23. There may be some siloed working practices, but the ODA and others strive to come together to discuss updates on romance (and other) fraud. However, this could be strengthened by capacity and financial support for the possibilities discussed in meetings of cross-sector working groups. In some instances, competitive practices between app store gate-keepers, platforms and those who hold personal data (ie banks) may hinder cooperative working.

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

24. GDPR and any future data protection regime can be an impediment to data sharing. Law enforcement and the fraud related organisations often want data shared on those who have been suspected of fraud, and especially those that have been removed from dating apps due to suspected fraud. The online dating sector has concerns about GDPR in relation to how this data could be used, as they have very specific Terms and Conditions for data processing. In order to share data, there would need to be a clear framework for sharing and use of data.

25. For instance, many anti-fraud organisations advocate for the sharing of information with potential victims i.e. if a user has been removed for potentially fraudulent activities on a dating service, all 'matches' with the removed user should be notified. This would combat potential fraud, but also creates considerable concern in the sector in relation to privacy, data protection and libel.

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

26. The ODA advocates for better education for the public on romance fraud, and all fraud. Consumers are not as well informed as we would like, and we are committed to campaigns to educate the public. We have a set of safe online dating resources, and we would like to see these across different channels of public engagement - from television, to newspapers to schools. Ideally, there would be a dedicated, well resourced body educating the public on fraud in all its forms. It is too much for the current capacity of bodies like the ODA, the City of London police, NFIB and Action Fraud to truly deliver what is needed. Members themselves educate the public through their apps and websites, as well as social media campaigns, but are limited to those who engage through those platforms.

27. Educating the public must include 'thinking outside the box', such as social media, gaming, schools and engaging with elderly support groups.

Romance fraud is most successful on those that are lonely or isolated and looking for connection, so combining fraud education with social engagement would bring significant benefit.

Legislative Remedies

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

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

28. The ODA would advocate for legislation that is both proportionate and outcomes based in tackling fraud, and legislation that delivers the appropriate resources to the appropriate organisations to truly create a chain of delivery from stopping fraud to supporting victims and catching perpetrators.

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

13. Are sanctions and penalties for criminals who commit fraud an effective deterrent against future criminal activity, and if not, what might be more successful?

29. The ODA would suggest that because it is difficult to prosecute and convict those who make money from romance fraud, it is not a sufficient deterrent. As mentioned, an improved data sharing arrangement, with consistent and regulated frameworks, would help in creating better deterrents.

Best Practice

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

30. Our key policy recommendation is to speak directly with those who are combating fraud every day, and create policy which can be regularly updated and future-proofed when technologies change. Legislation may be out of date as soon as it is created. Policy should be outcomes based and provide the capacity to deliver on the intended outcomes.

21 April 2022