INNOVATE/FINANCE

Ofcom consultation
"Protecting people from illegal harms online"
Innovate Finance response

About Innovate Finance

Innovate Finance is the independent industry body that represents and advances the global FinTech community in the UK. Innovate Finance's mission is to accelerate the UK's leading role in the financial services sector by directly supporting the next generation of technology-led innovators.

The UK FinTech sector encompasses businesses from seed-stage start-ups to global financial institutions, illustrating the change that is occurring across the financial services industry. Since its inception in the era following the Global Financial Crisis of 2008, FinTech has been synonymous with delivering transparency, innovation and inclusivity to financial services. As well as creating new businesses and new jobs, it has fundamentally changed the way in which consumers and businesses are able to access finance.

When engaging on policy and regulatory issues we aim to reflect the UK FinTech ecosystem and specifically the needs of start-ups, scale-ups and high growth enterprises.

Summary

Innovate Finance welcomes the opportunity to respond to Ofcom's consultation on *Protecting people from illegal harms online*. We have been working on wider regulatory efforts to combat fraud and we see the introduction of the Online Safety Act 2023 as an important contribution to the holistic response needed to tackle fraud, given the scale and complexity of the challenge. As such, while we recognise the range of harms that Ofcoms is seeking to address, we limit our response to issues related to fraud.

We would summarise our views on Ofcom's proposals as follows.

- ***Ensuring a coherent and complementary regulatory framework:*** In considering a number of the proposals put forward by Ofcom, we have viewed them through the lens of the wider regulatory landscape for tackling fraud, in particular the mandatory reimbursement scheme for authorised push payment (APP) fraud being implemented by the Payment Systems Regulator (PSR). From 7 October 2024, payment services providers (PSPs) who are part of the Faster Payments System will be required to reimburse each victim of APP fraud up to £415,000, split equally between the sending and receiving provider. In this context, it is important that Ofcom takes a proportionate approach when designing measures that online platforms must comply with under the Online Safety Act to reduce fraud.

- Given the regulatory requirements that PSPs will have to comply with under the PSR regime, it is only fair and proportionate that online platforms, like social media platforms where a large proportion of overall fraud originates, face stringent regulatory measures. Longer term, we think more work should be done to assess how the biggest offenders of fraud origination, like social media platforms, are brought into scope of the PSR regime as a separate measure to compliance under the Online Safety Act.

- ***Automated content moderation:*** Ofcom is currently prescribing a particular type of automated content moderation in the form of standard keyword detection to combat a specific sub-offence, namely content promoting articles for use in fraud, rather than the priority offence of fraud as a whole. Limiting the focus to a specific sub-category of fraud (i.e. articles for use in fraud), and prescribing a basic form of automated content moderation (i.e. standard keyword detection) is not an adequate approach. We are specifically suggesting that large firms, who conduct a risk assessment and subsequently identify their products and services to be at a high risk of user-generated content facilitating fraud, should be required to introduce automated content moderation controls for fraud.

- The Codes of Practice should set the right incentives on the large user-to-user firms from the beginning. They should require firms that have a significant risk of fraud revealed in their risk assessments to develop an automated content moderation programme that can detect high risk content relating to that priority offence as a whole, in a way that is reflective of the significant technological and financial resources they have access to.

- ***Online peer-to-peer marketplaces:*** Online peer-to-peer marketplaces like Facebook Marketplace are a particular challenge due to the lack of minimum identity verification for potential sellers. We recommend that Ofcom sets out minimum verification rules for both identity and listings that large user-to-user services must conduct. This will clamp down on anonymity, making it more difficult for fraudsters to list fake goods with impunity, thereby cutting down on purchase scams.

- Online marketplaces currently have no obligation to provide a built-in payment feature on their platforms for users, which means that it is up to buyers and sellers to arrange payments. As a result, many online buyers do not have access to secure payment providers when transacting at marketplaces. Ofcom should therefore make integration with secure payment services compulsory because this will require sellers to verify their identity with a regulated PSP. At the same time, these secure PSPs can prevent any payment from being released to fraudsters immediately through standard delays, or until goods are confirmed to have been received.

- ***Dedicated reporting channels for trusted flaggers:*** The dedicated reporting channel for fraud for trusted flaggers is a welcome step and Ofcom highlights the fragmented ecosystem that has prevented more effective action in preventing fraud by reporting

suspected fraudulent content. That said, we would like to see Ofcom go further in its final proposals to cover a wider range of trusted flaggers.

- We encourage Ofcom to consider expanding this list to include the PSR and Pay.UK, in the wider context of their respective roles in implementing and overseeing the mandatory reimbursement scheme for authorised push payments, due to come into force on 7 October 2024. Our members are disappointed that Ofcom has initially concluded that the trusted flaggers will be limited to a narrow range of stakeholders, rather than regulated financial services providers. Instead, Ofcom should take an approach whereby, at least initially, it expands trusted flaggers to cover regulated financial institutions above a certain value and volume of overall faster payment transactions, data which could be accessed relatively easily.

Question answers

Volume 2: The causes and impacts of online harm

Ofcom's Register of Risks

Question 1: Do you have any comments on Ofcom's assessment of the causes and impacts of online harms? Do you think we have missed anything important in our analysis? Please provide evidence to support your answer.

Innovate Finance broadly agrees with Ofcom's assessment of the causes and impacts of online harms. We agree with the causes of these online harms which Ofcom has identified with regards to the proceeds of criminal offences, fraud and financial services offences.

Causes of proceeds of crime and fraud and financial services offences

Our members welcome Ofcom recognising that services with a large user base, such as social media platforms, are particularly susceptible to becoming the place of fraud origination. We agree with Ofcom's assessment that social media has become a place where impersonation fraud, romance scams, identity theft and proceeds of crime offences fester. Social media is rightly identified as a source of online harm given its large user base and that 60% of all APP fraud originate via Meta according to UK Finance data.[1] It is also right that Ofcom has highlighted social media's shortcomings in tackling fraud. For example, Ofcom notes how social media user profiles have enabled fraudsters to operate with ostensible legitimacy and that its provision of boosted posts (where users pay to amplify their content) has provided an *"opportunity for fraudulent actors to access potential victims by presenting a veneer of legitimacy to the content"*.

We also appreciate Ofcom taking a broader approach in identifying messaging services, online marketplaces and also services with a smaller (or more niche) user base such as romance and

[1] Financial Times, *Meta singled out by UK financial lobby group over digital scams.* See here: https://www.psr.org.uk/publications/policy-statements/ps23-4-app-scams-reimbursement-policy-statement/

dating applications as places of fraud origination. This is in line with analysis that over 77% of all APP fraud cases originate online.[2]

In relation to demographics, we broadly agree with Ofcom's assessment that age, financial resilience, race, mental health and media literacy among other factors impact individuals' susceptibility to fraud. On literacy, we concur with Ofcom's assessment that the "media literacy" level of an individual may influence whether they recognise fraud.

However, Innovate Finance would also note that levels of "financial literacy" is another crucial characteristic that determines one's susceptibility to online fraud. Ofcom notes that "media literacy" relates to the *"critical skills to recognise fake propositions"*. While this is indeed important, "financial literacy" which the European Commission suggests relates to the *"knowledge and skills needed to make important decisions"*, stating that *"everyone should be able to understand the risks involved when borrowing or investing money"*.[3]

Media literacy and financial literacy are broadly similar. However, they differ in that while the former puts an emphasis on detecting fraudulent content, the latter focuses on the ability of individuals to understand basic financial concepts, how to use money and the consequences of financial decisions. Financial literacy is therefore also inextricably linked to media literacy in that without basic understanding of financial concepts, users might be unable to recognise fraud or financially misleading information. For instance, financial literacy would be key in reducing victims of investment scams, particularly when such fraudulent investment advertisements *"seem too good to be true"* and downplay the risks even as every investment decision has an element of unpredictability.[4]

Impacts of proceeds of crime and fraud and financial services offences

Innovate Finance believes that Ofcom has rightly noted the impact of proceeds of crime offences, such as money mules being unaware of the consequences of their actions, ultimately becoming victims as they cannot back out of a situation due to the threat of violence, losing their homes, livelihoods and access to financial services.

Our members are also aware that fraud and financial services offences lead to harrowing consequences. It is not just financial loss that victims suffer, but also mental and physical distress. Victims indeed find it difficult to get on with their day-to-day lives due to a loss of confidence and trust. We are also deeply concerned about how online fraud could lead to digital exclusion as victims become fearful of transacting online.

---

[2] UK Finance, *Criminals steal over half a billion pounds and nearly 80 per cent of APP fraud starts online*. See here: https://www.ukfinance.org.uk/news-and-insight/press-release/criminals-steal-over-half-billion-pounds-and-nearly-80-cent-app

[3] European Commission, *Financial literacy*. See here: https://finance.ec.europa.eu/consumer-finance-and-payments/financial-literacy_en

[4] Which?, *How to spot an investment scam*. See here: https://www.which.co.uk/consumer-rights/advice/how-to-spot-an-investment-scam-a7CeY6d5Luf0

As an example, our members recognise that Authorised Push Payment (APP) fraud presents a significant and growing challenge for the payments industry, and that it is important for consumers to be adequately protected in the face of increasingly sophisticated APP scams.[5] Consumer trust and safety is paramount if innovation and competition is to flourish in the UK payments sector.

Our members therefore support the Payment Systems Regulator's (PSR) intended aim of providing a fair level of protection to consumers who fall victim to APP scams, and welcome the introduction of a consistent approach to consumer protection across the industry. However, there are well-founded and consistently shared fears from industry that the PSR's approach to mandatory reimbursement, which is the first of its kind in the world, will have unintended consequences to the FinTech and financial services sectors that will have repercussions for innovation and competition in the payments market, as well as the international competitiveness of the UK. It also will not prevent fraud from happening in the first place unless it is accompanied by, and synchronised with, an economy-wide approach to stopping online scams. This must include social media firms sharing liability with payment service providers (PSPs) in reimbursing victims of online fraud. We believe over time this is how the PSR's mandatory reimbursement scheme should evolve, alongside the implementation of the Online Safety Act.

Hence, we welcome that Ofcom has correctly identified social media as an online source of harm, particularly in relation to fraud, and is attempting to hold Big Tech firms accountable for keeping users safe online. FinTechs, banks, PSPs and the wider financial services sector should be the last line of defence against fraud and not the only line of defence.

Volume 4: What should services do to mitigate the risk of online harms?

Automated content moderation (User to User)

Question 20: Do you agree with our proposals? Do you have any views on our three proposals, i.e. CSAM hash matching, CSAM URL detection and fraud keyword detection? Please provide the underlying arguments and evidence that support your views.

Innovate Finance recognises that all 15 kinds of illegal harms outlined by Ofcom must be considered and tackled. Given our position as the industry body for the global FinTech community in the UK, we will be responding to this consultation solely from the perspective of fraud and financial services offences. Bearing this in mind, we will not be responding to questions in relation to CSAM hash matching, CSAM URL detection and terrorism content.

Automated content moderation

Automated content moderation for the purposes of reducing the risk of users encountering content amounting to a priority offence will be important for Ofcom to effectively deliver a reduction in illegal harms, across the digital economy.

[5] UK Finance reported that £485 million was lost to APP scams in 2022.

Automated content moderation is similar to automated transaction monitoring that financial services firms already conduct to meet their obligations under the Proceeds of Crime Act 2002 (POCA) and the Fraud Act 2006. It is not seen as credible that large firms serving millions of users are able to manually review activity to detect crime. As such, Ofcom should place appropriate emphasis on large firms to introduce automated content moderation, in order for their Codes of Practice to deliver a significant reduction in illegal harm.

The Financial Conduct Authority (FCA) has developed best practice with regard to how automated transaction monitoring systems should be developed, assessed and implemented. This includes outlining methodologies, the development and implementation of such models, effectiveness assessments and oversight mechanisms.[6]

Expanding the requirement for large firms with a high risk of fraud to develop automated content moderation controls

Ofcom is currently prescribing a particular type of automated content moderation in the form of standard keyword detection to combat a specific sub-offence, namely content promoting articles for use in fraud, rather than the priority offence of fraud as a whole, as described in Schedule 7 of the Online Safety Act 2023. Innovate Finance and its members are grateful that Ofcom has identified fraud as the first offence to trial the use of a specific type of automated content moderation technology. Ofcom is right to focus on fraud, due to the scale of this particular harm caused by user-to-user services.

However, limiting the focus to a specific sub-category of fraud (i.e. articles for use in fraud), and prescribing a basic form of automated content moderation (i.e. standard keyword detection) is neither the right, nor adequate approach.

The Codes of Practice should set the right incentives on the large user-to-user firms from the beginning. They should require firms that have a significant risk of fraud revealed in their risk assessments to develop an automated content moderation programme that can detect high risk content relating to that priority offence as a whole, in a way that is reflective of the significant technological and financial resources they have access to.

We are specifically suggesting that large firms, who conduct a risk assessment and subsequently identify their products and services to be at a high risk of user-generated content facilitating fraud, should be required to introduce automated content moderation controls. The controls in place should reflect the fraud risks associated with the specific platform, rather than blanket measures that do not reflect the harms associated with one service or another.

It is worth noting that automated content moderation can include standardised keyword detection as suggested by Ofcom. However, it should also take into account numerous other data points and the technology that large firms have at hand to design processes to detect and flag high risk content, as well as utilise the intelligence provided by trusted flaggers. Ofcom has noted a concern that content moderation must strike a balance between the need to remove content facilitating illegal harms and the risk of false flags. We recognise these concerns and our position is that high

[6] Financial Conduct Authority, *FCTR 4.1*. See here: https://www.handbook.fca.org.uk/handbook/FCTR/4/?view=chapter

risk content identified through automated content moderation rules could be subject to human review, thereby reducing the risk of adverse outcomes.

We are not against the use of a specific proactive technology, but believe there must be a more general requirement for large firms at a high risk of fraud to develop an automated content moderation approach that is reflective of and commensurate to the risk they are introducing into the system. Without such a requirement, Ofcom risks rubber stamping the use of a fairly blunt tool (standard keyword detection) that does not incentivise firms in any way to introduce innovative tools to detect harm and prevent their platform from being used to facilitate fraud. The correct incentives must be set to achieve the desired outcome which is to reduce illegal harms such as fraud.

In order to successfully reduce the likelihood of users encountering content which amounts to priority offences, Ofcom must require firms to assess their risks, and where required, engage in a programme of automated content moderation to proactively identify and flag high risk content.

Building on this, we outline below:

a) Why the scope of the particular harm, namely articles for use in fraud, is too narrow; and
b) The limitations of standard keyword detection, in reducing fraud-related harms.

Weaknesses of relying solely on fraud keyword detection

We welcome that Ofcom is outlining measures that large user-to-user service providers can take to tackle fraud. We acknowledge that Ofcom believes that fraud keyword detection would be an effective means to proactively identify content likely to amount to an offence concerning articles for use in frauds, whereby such content would be considered by services for removal coherent with respective content moderation policies.

We also recognise that keyword detection was chosen due to it not being a novel or fledgling technology. Instead, it has been *"used for years by many of the larger services"*, which is why Ofcom believes that keyword detection is a proportionate measure to impose on large user-to-user firms to tackle fraud. Moreover, this is a technology currently used as part of a wider range of controls that make up transaction monitoring in financial services.

Hence, our first point of concern is that by relying solely on fraud keyword detection, Ofcom is allowing large user-to-user services to use the technology in isolation, when they have the means to utilise other tools to prevent fraudulent content. This would neither be effective nor adequate, which leads us to our next point about the efficaciousness of the technology in itself.

We are concerned about the efficacy of fraud keyword detection given that its effectiveness hinges on fraudsters using very specific keywords, content of keyword lists, and the manner in which keyword detection is conducted. As Ofcom has conceded, fraudsters may circumvent keyword detection by adopting new keywords and combinations of keywords to conceal their activities.

Keyword detection thus relies on firms modifying their systems and constantly updating their keyword lists according to the language that fraudulent actors use. Our members are concerned that keyword detection may not be equally effective in detecting fraudulent content for removal across all services subjected to this requirement .

Our members are sceptical of the efficacy of fraud keyword detection given that Ofcom decided against introducing fraud keyword detection in tackling illegal financial promotions and investment scams. As Ofcom noted, the terminologies in those instances are very common and can be used in many contexts which can *"negatively impact the degree of accuracy and effectiveness of keyword detection technology used in this context, and have significant financial cost implications [...], and significant freedom of expression implications"*.

Scope of keyword detection needs to be broader

While Ofcom has acknowledged the weaknesses of fraud keyword detection, it believes that to be "relatively low risk" because *"those who seek to supply articles for use in frauds online are incentivised to maximise the discoverability of their content for an audience looking to acquire such articles, and frequent changes in terms, or the use of more common words, would make discoverability and dissemination of this content more difficult".* While that may indeed be the case for articles for use in frauds, focusing solely on articles for use in frauds is a weakness of the proposals.

"Articles for use in frauds" is too narrow as it largely focuses on items designed or intended to facilitate fraudulent activities such as content which offers to supply individuals' stolen personal or financial credentials. From the perspective of FinTech and financial services, this is not the only type of fraud that is perpetuated by criminal actors via large user-to-user services, such as social media. Instead, research by NatWest has identified the following as the most types of common scams:[7]

1. Phishing scams (37%)
2. Trusted organisation scams (21%)
3. Refund scams (13%)
4. Friend or Family scams (12%)
5. Get Rich Quick scams (9%)
6. Purchase scams (9%)
7. Investment scams (8%)
8. Safe Account scams (7%)
9. Lottery cons (7%)
10. Befriending scams (6%)

[7] NatWest Group, *Most common financial scams of 2023 revealed.* See here: https://www.natwestgroup.com/news-and-insights/news-room/press-releases/financial-capability-and-learning/2023/oct/most-common-financial-scams-of-2023-revealed.html

One of our members has also provided data indicating the most common types of scams that their users are victims of. See Table 1.

Table 1: Total based on types of scams in the UK in 2023		
Type of scam	**Value (% of total)**	**Cases (% of total)**
Purchase scams	5.2	50.6
Investment scams	59.5	17.6
Impersonation scams	19.4	11.3
Advance fee scams	10.4	10.1
Tax scams	1.7	2.9
Other	3.7	7.4

While phishing scams are the most common form of scam in the NatWest data, and they may relate to articles for use in frauds given that phishing scams are, according to NatWest, *"fake emails, calls, messages or websites that seem to be from legitimate organisations which ask you to provide personal/financial information"*, it is not the only type of scam confronting consumers.[8] Instead, the most common form of APP fraud (which is the focus of our members given the PSR's decision to introduce a mandatory reimbursement regime from 7 October 2024) includes but are not limited to online shopping scams (e.g. fraudulent listings on Facebook Marketplace), investment scams, romance scams, impersonation scams, invoice redirection scams, advance fee scams and CEO fraud scams.

Based on one of our member's data as tabulated in Table 1, purchase scams and investment scams should be given more attention by Ofcom (as opposed to articles for use in frauds). This is clear as while the value of purchase scams is merely 5.2%, it constitutes a staggering 56% of all fraud cases. Furthermore, while investment scams make up just 17.6% of all fraud cases, their value stands at 59.5% of all scams.

We therefore regret that Ofcom has at this stage chosen not to introduce keyword detection measures to tackle purchase scams and investment scams. This is despite its recognition that social media is riddled with fraudulent content. One of our members' data corroborates the view that online platforms are the biggest source of fraud origination (as argued earlier in our response) in the UK whereby scams originating online constitute 86.5% of all scam cases and are worth 76.2% in terms of value in H2 2023. See Table 2.

[8] NatWest Group, *Most common financial scams of 2023 revealed.* See here: https://www.natwestgroup.com/news-and-insights/news-room/press-releases/financial-capability-and-learning/2023/oct/most-common-financial-scams-of-2023-revealed.html

Table 2: Total source of fraud origination in the UK in H2 2023		
Scam origin	**Value (% of total)**	**Cases (% of total)**
Online	76.2	86.5
Phone	19.0	11.5
Other	4.8	2.1

This member's data also highlights the fact that Meta is the single largest source of fraud origination, given that fraud originating from Meta constitutes 60.5% of all reports of fraud it received, amounting to a value of 33.2% of all scams. See Table 3.

Table 3: Total based on source of fraud origination in the UK in 2023		
Platform	**Value (% of total)**	**Cases (% of total)**
Meta (Facebook, Instagram, WhatsApp)	33.2	60.5
Other social media (Reddit, Snapchat, Telegram, TikTok, X (formerly known as Twitter))	4.5	11.5
Other	62.2	27.9

Given that Meta is the single largest source of fraud origination, this member has also provided data (see Table 4) that looks into specifically the types of scams that originate via Meta's platforms. The data shows that 61.1% of fraud cases originating from Meta relate to purchase scams, while investment scams are worth 61.3% of all scams originating from Meta. This highlights the need to introduce measures to curb purchase scams and investment scams, including fraudulent financial promotions.

Table 4: Total based on types of scams originating from Meta in 2023		
Type of scam	**Value (% of total)**	**Cases (% of total)**
Purchase scams	10.0	61.1
Investment scams	61.3	19.1
Impersonation scams	3.2	2.3
Advance fee scams	21.7	10.1
Relationship and romance scams	1.4	2.7
Other	2.5	4.7

We recognise that the proposals to implement the Online Safety Act are now just in Phase One, dealing with illegal harm duties. Hence, we look forward to Phase Three covering "transparency, user empowerment, and other duties on categorised services".[9] Our members would welcome Ofcom setting out its views on duties to prevent fraudulent advertising which will enable them to engage with proposals. It is imperative that fraudulent advertising is tackled for it is inextricably linked to fraud.

The 'polluter pays' principle must be upheld whereby the polluter, in this case social media, must be held culpable for the failure to prevent fraud. Ofcom needs to also recognise that it must pay more attention to tackling purchase scams and investment scams, rather than focusing solely on articles for use in frauds.

Enhancing keyword detection while considering more sophisticated solutions as alternatives

Given that Ofcom has noted that it does not wish to discourage the use of *"a range of significantly more sophisticated automated tools which services use to detect harmful content"*, we would caution Ofcom against being too prescriptive on the tools that large user-to-user services should use to tackle fraud. We encourage Ofcom to take a tech neutral and bolder approach to tackling fraud. Our members have articulated some proposals for Ofcom to consider.

A keyword detection code of practice

We are concerned that relying on standard keyword detection in any case is outdated and prescriptive. Standard keyword detection should be the bare minimum technology that large firms should employ to tackle fraud at source. Nevertheless, given that Ofcom considers this the most proportionate approach, we propose that a code of practice that compels all in-scope large online user-to-user services to proactively identify and accordingly update their keyword lists with new keywords that are associated with articles for use in frauds online.

This will ensure that changes in the use of language by fraudsters engaging in the illegal sale of stolen financial credentials and personal information does not further contribute to the inefficacy of keyword detection. This code of practice must be mandatory with penalties imposed on firms that do not comply or live up to the expectations of the code.

Minimum verification rules on online peer-to-peer marketplaces

Branching out further to purchase scams, firstly, we note that at the moment, regulatory bodies have not established minimum identity verification rules for online peer-to-peer marketplaces. For example, Facebook Marketplace does not appear to have identity verification requirements for sellers in the UK.[10] Any Facebook user is allowed to make a sales listing, even anonymously. The

[9] Ofcom, *Ofcom's approach to implementing the Online Safety Act.* See here: https://www.ofcom.org.uk/online-safety/information-for-industry/roadmap-to-regulation

[10] Facebook Help Centre, *Selling on Marketplace*. See here: https://en-gb.facebook.com/help/153832041692242

closest way to determine whether a seller is trustworthy is through the presence of "seller badges" (e.g. active local seller, very responsive, highly rated, super seller and top sender[11]) on the seller's profile. While this may be an indication of the trustworthiness of a seller, it still falls short of identity verification that will be deterrence to committing fraud.

Secondly, Facebook Marketplace currently does not verify the products for sale on its platform, apart from requiring sellers to upload a photo(s) or video(s) of the items for sale.[12] This is clearly inadequate in preventing the listing of non-genuine products on the online marketplace.

Hence, we recommend that Ofcom sets out minimum verification rules for both identity and listings that large user-to-user services must conduct. Such measures must be consistent and transparent across all user-to-user services, though in the principle of tech neutrality firms should be free to determine the tools by which they conduct verification checks. This will clamp down on anonymity, making it more difficult for fraudsters to list fake goods with impunity, thereby cutting down on purchase scams. This information will also make it easier for user-to-user services to assist law enforcement in retrieving the lost money and taking action against fraudsters.

Online peer-to-peer marketplaces should integrate with secure payment services

Online marketplaces such as Facebook Marketplace currently have no obligation to provide a built-in payment feature on their platforms for users which means that it is up to buyers and sellers to arrange payments.[13] As a result, many online buyers do not have access to secure payment providers when transacting at marketplaces. However, we note that solutions to this problem already exist in the form of PayPal and Stripe Marketplace which allows buyers and sellers to transact securely on the platform.

The impact of these integrations is clear in one of our member's data. Peer-to-peer marketplaces or e-commerce sites that integrate with secure PSPs drive less fraud. One member shared that in the last six months of 2023, customers were more than five times as likely to report being scammed by a seller on Facebook, than on Vinted, which is a rival peer-to-peer marketplace that offers their users the ability to pay via a secure payment service provider.

Ofcom should therefore make integration with secure payment services compulsory because this will require sellers to verify their identity with a regulated PSP. At the same time, these secure PSPs can prevent any payment from being released to fraudsters immediately through standard delays, or until goods are confirmed to have been received. Our members also consider this to be a solution that will enable buyers to easily dispute transactions and receive refunds as opposed to

[11] Facebook Help Centre, *Get seller badges on Facebook*. See here: https://www.facebook.com/help/1684084458520855

[12] Which?, *What are my rights if I buy and sell on Facebook Marketplace?*. See here: https://www.which.co.uk/consumer-rights/advice/what-are-my-rights-if-i-buy-and-sell-on-facebook-marketplace-aTktS5o6v0FW ;
Facebook Help Centre, *Sell something on Facebook Marketplace*. See here: https://www.facebook.com/help/561376580709359?helpref=faq_content

[13] Which?, *What are my rights if I buy and sell on Facebook Marketplace?*. See here: https://www.which.co.uk/consumer-rights/advice/what-are-my-rights-if-i-buy-and-sell-on-facebook-marketplace-aTktS5o6v0FW

working in cash or via bank transfer. It will also incentivise online peer-to-peer marketplaces to ensure that all listings are genuine to keep the cost of their integrations low.

Question 25: The costs of applying our articles for use in frauds (standard keyword detection) measure, including for smaller services; and

Given that the focus of our response is on large user-to-user services such as Big Tech and social media platforms and that standard keyword detection is only being applied to these large services, our position is that Ofcom should prioritise the potential harms averted over the relative costs involved.

From October onwards, PSPs will be required to mandatorily reimburse victims of APP fraud up to £415,000 per case, divided equally between sending and receiving PSPs,under the PSR's finalised proposals to tackle APP fraud.[14] Considering that over 60% of all APP fraud originate via Meta according to UK Finance data, we consider it fair and proportionate to compel large social media platforms to bear additional costs in order to improve their fraud prevention systems and upskill their staff.[15] In fact, Ofcom's estimated costs for large firms to introduce standard keyword detection pale in comparison to what the PSR is expecting PSPs reimburse each victim of APP fraud, regardless of their size.

We do not have evidence on the costs for applying standard keyword detection for smaller services. However, we also recognise Ofcom's concerns about excluding smaller services from its fraud prevention measures. We would urge Ofcom to consider the merits of extending its proposals to smaller services while noting the proportionality of the potential costs, once it has received further evidence from industry.

User reporting and complaints (U2U and search)

Question 28: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.

We welcome the recognition by Ofcom of the scale of the challenge when it comes to fraud, and the societal cost it has on individuals. As the consultation paper highlights, *"the scale of the threat is immense"*. In the evolving regulatory landscape to tackle fraud across different sectors involving different regulators, we also give our full support in efforts aimed at tackling the source of fraud, namely large social media platforms like Meta.

The dedicated reporting channel for fraud for trusted flaggers is a welcome step and Ofcom highlights the fragmented ecosystem that has prevented more effective proactive action in preventing fraud by reporting suspected fraudulent content. That said, we would like to see Ofcom

[14] Payment Systems Regulator, *PS23/4: APP scams reimbursement policy statement.* See here: https://www.psr.org.uk/publications/policy-statements/ps23-4-app-scams-reimbursement-policy-statement/
[15] Financial Times, *Meta singled out by UK financial lobby group over digital scams.* See here: https://www.psr.org.uk/publications/policy-statements/ps23-4-app-scams-reimbursement-policy-statement/

go further in its final proposals to cover a wider range of trusted flaggers, which we break down into two separate categories: public and regulated private entities.

The proposed list of trusted flaggers covers several bodies related to law enforcement, government departments and regulators. We encourage Ofcom to consider expanding this list to include the PSR and Pay.UK, in the wider context of their respective roles in implementing and overseeing the mandatory reimbursement scheme for authorised push payments, due to come into force on 7 October 2024. In addition to the mandatory reimbursement scheme, the PSR has already begun collecting APP fraud data (known as Measure 1) and has tasked industry with developing greater data and intelligence sharing which Pay.UK is taking forward (Measure 2). Given the direct link between respective work streams to tackle fraud we believe they both warrant inclusion as trusted flaggers.

Our members are disappointed that Ofcom has initially concluded that the trusted flaggers will be limited to a narrow range of stakeholders, rather than regulated financial services providers, citing a concern that *"the measure may be ineffective at reducing harm if it is made available to too many organisations at once"*. This maximalist view that expanding the number of trusted flaggers automatically leads to "too many organisations" is a false choice.

Instead, Ofcom should take an approach whereby, at least initially, it expands trusted flaggers to cover regulated financial institutions above a certain value and volume of overall faster payment transactions, data which could be accessed relatively easily. The rationale for our proposition is simple. There are currently 14 financial institutions captured by the PSR's Measure 1 reporting requirements on APP fraud.[16] These firms make up 95% of faster payments volume alone. Bearing this in mind, our members strongly recommend that Ofcom includes these firms in the list of trusted flaggers. This is because these firms already report auditable fraud volumes and case numbers to the PSR, and these metrics have been published publicly since October 2023.[17] It would therefore be relatively simple to adopt the standard as submitted to the PSR for Ofcom's trusted flagger channel.

Our members are also happy to work with Ofcom to develop guidance on when to use the dedicated reporting channel, if it remains concerned about the volume of users (i.e. "too many organisations") as articulated in the consultation. Volume should not be an issue, considering that one of our members has shared that the absolute maximum number of reports it could generate is roughly 6,000 reports over 6 months. This member is confident that this figure is also attributable to major firms. Hence, we would urge Ofcom to review its position on this matter. Taking this position would both limit the burden on online service providers and help fraud prevention at a meaningful scale. While Ofcom is accurate that the FCA regulates *"many tens of*

[16] Payment Systems Regulator, *PSR will publish data on how well customers are protected from scams*. See here for the list of 14 PSPs: https://www.psr.org.uk/news-and-updates/latest-news/news/psr-will-publish-data-on-how-well-customers-are-protected-from-scams/#:~:text=The%2014%20PSP%20groups%20subject,and%20Virgin%20Money%20UK%20plc

[17] Payment Systems Regulator, *Authorised Push Payment (APP) fraud performance report, October 2023*. See here: https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/

thousands of entities", it is a relatively small number of firms that could provide tangible benefits in reducing fraud given their scale and presence in UK payments.

Furthermore, the consultation also states that Ofcom does not feel it is appropriate to extend the dedicated reporting channel to commercial entities because they are *"not subject to the legal duties relating to fairness and human rights which bind public entities"*. While this point is true, PSPs will have a legal duty to reimburse consumers for APP fraud under the PSR's regulatory regime from October 2024. We feel this puts commercial entities in a position of having sufficient standing in matters relating to proactively reporting and reducing potentially fraudulent content. Otherwise, there is a risk a disproportionate burden falls on PSPs to reimburse consumers without having all the tools to effectively prevent future fraud.

Our members also dispute the argument in the consultation that *"much of the evidence relating to relevant fraud offences will often not be observable by the inscope service where the interaction with the victim originates or begins. In contrast, these elements are more likely to be observed by financial services providers*". On the contrary, the fact that the interaction between the victim and fraudster takes place within the online service necessarily means that evidence relating to the relevant fraud offence is potentially detectable. For example, users connecting with individuals they either have no mutual contacts with, reside in different countries, or a spike in the level of communication over a period of time are all potential flags.

The Future of Payments Review led by Joe Garner, commissioned by HM Treasury, and published in November 2023, highlighted the scale of the challenge financial services firms face by being at the end of the fraud chain, concluding that *"Criminals are adept and ingenious in persuading often vulnerable customers to send them their life savings. Additionally, it is very hard for any amount of technology or 'effective warnings' to stop a determined and lovestruck vulnerable customer sending money to someone that they genuinely believe to be their soulmate in distress."*[18]

Given that Section 10(3)(a) of the Online Safety Act 2023 states the goal is to *"minimise the length of time for which any priority illegal content is present"*, the easiest way to achieve this is to ensure a suitable direct means of flagging suspected fraudulent activity between financial institutions and online service providers. Moreover, this seems reasonable given Ofcom's own view that *"the very significant scale and harm of online fraud is such that for some services, even high costs are proportionate.*"

Finally, on the recommendation that at least every two years the service should seek feedback from the trusted flagger, we suggest this is reduced to one year on the basis that the fraud ecosystem and threats evolves so fast, so as to ensure an up to date approach and way of working.

Enhanced user control (U2U)

[18] HM Treasury (author: Joe Garner), *Future of Payments Review*. See here: https://assets.publishing.service.gov.uk/media/6557a1eb046ed400148b9b50/Future_of_Payments_Review_report.pdf

Question 37: Do you agree with our proposals? Please provide the underlying arguments and evidence that support your views.

We welcome the recognition and initial steps outlined by Ofcom on the harm caused by impersonation fraud. We also agree that the scale of the challenge posted by impersonation to commit fraud means that the costs associated with implementing measures to prevent it are justified. The consultation paper acknowledges the fact that *"impersonation is a factor in a much broader range of harms such as romance fraud, [and] fraud on online marketplaces"*. While we welcome the initial steps outlined we think it is important that wider requirements are considered and brought into scope to account for the breadth of impersonation scams online.

Ofcom notes that some types of services, like online marketplaces, operate forms of verification, but we highlight this is not standard practice, and as a result requires urgent attention. Platforms like Facebook Marketplace where identity verification is not required to make a sale have been well publicised in terms of how poor their controls are, with the potential to fraudulent listings and possible sales.[19]

[ENDS]

[19] This is Money, *We 'made' £3000 on Facebook Marketplace scam in just 24 hours*. See here: https://www.thisismoney.co.uk/money/beatthescammers/article-12509577/We-3-000-Facebook-Marketplace-scam-just-24-hours.html