Revolut

Revolut response to Ofcom's Call for Evidence: *Third phase of online safety regulation*

1. Executive Summary

1.1 Revolut and Online Safety:

Revolut welcomes the opportunity to provide input to the third phase of Ofcom's call for evidence on online safety regulation. It is vital that online services implement strong protections to prevent fraudsters from using online advertising to digitally rob consumers. We recognise the Online Safety Act 2023 as a significant lever to help to tackle fraud, and at Revolut, we are committed to ensuring the safety and security of our users. As such, our focus within the scope of this response is on user identity verification and fraud; this is due to our position in the UK as an Electronic Money Institution with over 9 million retail customers and over 250,000 business customers. Digital transactions and online banking are increasing, and keeping our finances safe is more important than ever. Revolut has been instrumental in reshaping digital; we are always improving our technology to stay ahead of fraud and safeguard our users, and we believe that online service providers need to do the same.

1.2 Revolut and Fraud Prevention

Whilst not the sole focus of our response, we will mainly concentrate on Chapter 7 of the call for evidence - fraudulent advertising. This issue is a priority for Revolut, as we continue to be involved in the wider regulatory efforts to combat fraud. We currently employ over 4000 staff in our financial crime department, which accounts for nearly half of our global workforce. We invest millions each year in technology such as Advanced Machine Learning models and Computer Vision to fight against fraud and in 2023 we stopped over £475 million of funds from being stolen from our customers. We appreciate the fact that fraud has been included within the scope of the Online Safety Act, and acknowledge the limitations that Ofcom faces as it is bound by the parameters set by the Act in relation to fraudulent advertising.

Fraud is one of the greatest challenges facing the UK, accounting for 40% of all crime[1]. The UK financial services sector evidently has considerable financial incentives to reduce fraud rates in the UK, and we are very supportive of Ofcom's objectives. Our proprietary fraud detection system is at the forefront of our security measures. It uses cutting-edge machine learning and AI methods to detect suspicious activity. In addition, our 4000+ strong financial crime team works to prevent our customers from falling victim to scams and fraud. We want to work closely with Ofcom in the delivery of the Online Safety Act to ensure the best

[1] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime#:~:text=Fraud%20is%20the%20most%20commonly,crime%20in%20England%20and%20Wales

possible outcomes for our service users. Putting financial incentives on the enablers of fraud will have a far greater impact on reducing fraud rates than putting the sole burden on PSPs, when the fraud has already been committed and victims are already under the spell of scammers.

Shared liability is the only way in which we will achieve significant fraud reduction targets and prevent millions of innocent victims from facing the financial and emotional effects of this devastating crime. As demonstrated in our previous response to *Ofcom's Consultation: Protecting people from illegal harms online*, Revolut's data clearly highlights where action needs to be targeted and we therefore urge Ofcom to use their powers to ensure that the online platforms who enable the vast majority of fraud are finally financially incentivised to actually prevent fraud. **Banks and Financial Institutions should be the last line of defence against fraud, not the only line of defence.**

2. User Identity Verification

Question 31: What kind of user-to-user services currently deploy identity verification and in what circumstances? Including:

- ***the ways in which these identity verification methods are beneficial, both to the user and to the service***

To help prevent fraud, we at Revolut advocate for the inclusion of stringent authentication requirements in the regulatory framework for online services. Multi-factor authentication (MFA) should be a mandatory standard, ensuring an additional layer of security for online platform users. In addition, the adoption of biometric verification could significantly reduce the risk of identity theft and fraud. 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.

At present, online marketplaces have no responsibility to provide a built-in payment feature on their platforms for users, meaning that it is up to buyers and sellers to arrange payments. As a result, the majority of online buyers do not have access to secure payment providers when transacting at marketplaces. To combat this, Ofcom should make integration with secure payment services compulsory. This will require sellers to verify their identity with a regulated PSP that will have already completed the industry regulated onboarding Know Your Customer (KYC) checks. This will create a safer foundation, whilst also allowing the secure PSPs to block any payment from being released to fraudsters immediately through standard delays, or until goods are confirmed to have been received.

Revolut and other financial institutions must follow regulatory KYC requirements, under which we are expected to confirm the identity of our customers. All accounts need to have

their identity verified, and we believe that online service providers should be subject to the same requirements.

3. Fraudulent Advertising

As a global fintech, Revolut remains committed to documenting the type of fraudulent transactions that are recorded on our systems. We do this so that we can better understand and work to prevent fraud, enabling us to better protect our customers in the future.

Question 36: Please provide evidence of the following:

- ***The most prevalent kinds of fraudulent advertising activity on user-to-user and search services (e.g. illegal financial promotions, misleading statements, malvertising);***
- ***The harms associated with different kinds of fraudulent advertisements, the severity of such harms, and, if relevant, how this varies by user group;***
- ***The key challenges to successfully detecting different types of fraudulent paid-for advertising, and how these challenges can be minimised or resolved;***
- ***The prioritisation of suspected fraudulent advertising within all categories of harmful advertising queues, e.g. account verification, user reports, appeals; and***
- ***The proportion of fraudulent advertisements that are currently estimated to remain undetected by services' systems.***

As highlighted in our previous response, Revolut agrees with Ofcom that online platforms with large user bases - such as social media platforms - are the scammers' destination of choice for fraud origination. In terms of the most prevalent kinds of fraud - purchase scams, impersonation scams, job scams and investment scams are very common on social media platforms. It is also highly likely that the precursors to scams, such as identity theft and phishing, occur primarily on social media platforms. We would note that these platforms are appealing to scammers because of their large user base, but also because of the lack of meaningful action by these platforms to significantly reduce fraud rates. There has been a clear shift in perceptions towards a view that these firms are not doing enough to prevent fraud, and financial incentives are the only way in which they will actually take their fraud problem seriously.

[redacted]

As outlined in our previous response, [redacted]

[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

Similar to last year, the majority of these scams were investment and purchase scams. UK Finance recently released their 2024 Annual Fraud Report, with their data confirming that

76% of APP fraud cases originate online[2]. This figure is consistent with the 78% figure they reported for 2022[3], showing that little to no progress has been made. Considering that online platforms are in scope of Ofcom's powers, there is a significant opportunity here to help reduce fraud rates that start online.

Fraudulent advertising not only leads to financial and emotional distress for victims, but could also lead to the distrust of digital payment options. This will damage the UK's international competitiveness in the FinTech and financial services sector. As a way to protect the sector, we would argue that categorised firms should only allow adverts from FCA-regulated financial entities. This is something that Google implemented in 2021, and this verification is required for all ad formats and extensions. The fact that Google and YouTube account for such little amounts of fraud - despite both being amongst the biggest advertisers globally - is notable. Advertisers must have completed the updated verification process to show financial services ads to UK users on their platform. [redacted]

Prevalent kinds of fraudulent advertising activity on user-to-user and search services

Revolut shares Ofcom's view about the devastating impact of investment scams, and the data we highlighted above corroborates this view. [redacted] If Ofcom wants to use its powers to significantly reduce fraud losses, then tackling investment scams should be seen as a priority.

[redacted]

[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[2] https://www.ukfinance.org.uk/system/files/2024-05/Annual%20_Fraud_report_2024_final%20_spread.pdf

[3] https://www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf

Revolut

It is important to highlight that there are major differences in typology when comparing volumes and values. Purchase scams represent more than half of total scam cases - these are scams where people buy fake items (e.g. football tickets) or items (e.g. bicycle) that never arrive. Often, these scams are facilitated through adverts within online marketplaces - commonly Facebook Marketplace. [redacted]These are scams that are facilitated by sophisticated criminals, targeting vulnerable customers and offering too-good-to-be-true opportunities. Often these scams are enabled by advertising on social media platforms, with Facebook and Instagram being a breeding ground for these scams. In addition, we are increasingly seeing case studies where fraudsters take over genuine accounts and then upload fake claims about fantastic investment opportunities. Victims think that because their friends/family have promoted it, then it must be legitimate; but unfortunately these accounts have been taken over by fraudsters who then impersonate the account holder and target their contacts.

Investment scams via paid-for advertising

[redacted] Anecdotally, it is however apparent from victim testimonies that paid-for ads are used to promote scams and to reach victims at scale. Perhaps most concerningly when considering paid-for ads, these are scams that the platforms themselves are profiting from because the scammers are still paying the platforms to advertise on their platform. It is incomprehensible that these platforms can not only enable fraud, but actually profit from it, and Revolut would urge that Ofcom addresses this as a matter of priority. [redacted]Revolut is keen to work with Ofcom on this topic and in addition to responding to this call for evidence we are happy to provide any further materials which could be useful.

Solutions: Additional steps for online platforms

Question 37: What technological developments aiding the prevention/detection of fraudulent advertisements do you anticipate in the coming years, and how costly and effective do you expect them to be? What are the challenges/barriers to their development?

Fraudsters and scammers are using increasingly sophisticated techniques to target victims online and steal their hard-earned money through fraud. Investment in innovation to develop new and advanced detection and prevention methods, such as biometric authentication and generative AI can play a key role in disrupting fraudulent behaviour and protecting

consumers against scams. Last year Revolut prevented over £475 million in fraud[4] against customers, using new and innovative methods of fraud detection. To counter the ever changing tactics of fraudsters, Revolut is constantly strengthening its set of advanced, AI-based tools and techniques to prevent, detect, and disrupt fraudulent activity.

In February 2024, Revolut launched an advanced scam detection feature to protect our customers against card scams. [redacted] We have chosen to heavily invest in creating innovative products like this to ensure that our customers can continue to spend and send their money safely. We would be happy to host Ofcom at our offices to demonstrate this product if that is of interest.

Question 44: Please provide any evidence you have regarding the processes for advertiser onboarding and verification related to protections against fraudulent advertising. In your response, please indicate whether these processes are currently implemented in respect of services which are in scope of the Act or whether they stem from another sector.
In particular, we are interested in relevant information on the following points:

- ***The criteria which advertisers are verified against, including documentation/evidence used to support verification, and what advertisers are required to declare;***
- ***The role of (a) automated processing and (b) human processing in the verification process, and how they interact;***
- ***The costs associated with advertiser verification and how those costs vary as scale increases;***
- ***The percentage of advertiser accounts that are verified;***
- ***Whether advertisers are permitted to publish advertisements on the service while the verification process is ongoing;***
- ***Whether there are additional/specific verification checks for advertisers placing adverts of certain kinds or targeting certain audiences, such as about specific products or services, or targeting users under the age of 18;***
- ***Whether the verification of an advertiser account expires after a certain amount of time or certain activity, such as when advertisers make changes to their account or profile.***

In addition to technologies being established to tackle adverts, there are a lot more steps that these platforms could implement that would make it more difficult for fraudsters. Working with the online platforms that are used to defraud consumers is the most effective route to tackling these types of scams. As highlighted in our previous response, the introduction of additional friction into the online journey for advertising products would be a step in the right direction. By emulating something similar to KYC for onboarding of FS customers, it will ensure that only verified users can access these online services. The

[4] https://assets.revolut.com/pdf/Revolut_Consumer_Security_Insight_Report_2023.pdf

introduction of mandatory inclusion of relevant Companies House data to enable the creation of a Facebook Business account for example, could also make a meaningful impact in this space.

As previously highlighted, Revolut is also supportive of the requirement for any company advertising financial services to UK consumers on search engines and social media to be authorised by the FCA. We recognise that some platforms do this already, and see a noticeable difference in fraud levels compared to those who do not.