Online Fraud Charter

Signatories agree to adopt the following measures within **6 months:**

Blocking	Deploy measures to detect and block fraudulent material
Reporting	Have a simple and quick route to report fraudulent material
Takedowns	Take action against fraudulent content and users straight away
Advertising	Deploy measures to protect people from fraudulent adverts
Law Enforcement	Have dedicated liaisons who will respond to law enforcement requests
Intelligence Sharing	Engage with initiatives to quickly share information about frauds
Transparency	Provide information about fraud risks and what is being done to address them
Comms	Deliver simple messaging to support the public to recognise and avoid online fraud
Horizon Scanning	Contribute to horizon scanning exercises to stay ahead of the threat

Signatories

amazon
ebay
facebook
Google
Instagram
LinkedIn
Match Group
Microsoft
Snap Inc.
TikTok
YouTube
techUK
FOR WHAT COMES NEXT
HM Government

Signatories of this Charter are not limited to those outlined here. We urge others to agree to the actions enclosed to better protect their customers and the wider public.

Opening Statement

The tech sector facilitates many positive changes to the way we live and the way we do business. Online platforms and services are now integral to the everyday lives of UK citizens and companies, and this Government wants them to be the best they can be.

However, online platforms and services are increasingly being exploited by criminals for the purposes of fraud and money laundering. Fraud accounts for around 40% of all crime in England and Wales,[1] with an estimated 80% of that cyber-enabled including through online platforms and services.[2] In turn, these companies are well placed to help prevent online fraud and to keep their users and the public safe from this crime.

Tackling fraud is a priority for the Prime Minister and this Government. In May 2023, the Government launched its Fraud Strategy. Building on the successes of previous voluntary charters with the retail banking, telecoms and accountancy sectors, the strategy set out plans to deliver a voluntary Online Fraud Charter. Through this charter, firms show that they recognise the risk of fraud and financial exploitation to the UK public on their platforms and commit to tackling it.

The Online Safety Act (OSA) will also go far to improve the response to online fraud in the long-term. Against the backdrop of an ever-evolving problem, this charter demonstrates the ambition and willingness of signatories to work collaboratively with Government, ahead of regulation fully coming into force, in a targeted manner reflecting each company's unique business model.

Commitments

Each firm will implement the actions that apply to them, based on their unique business models. The commitments and actions in this Charter are voluntary and are intended to be applied on a proportionate basis and not all will apply to every company or in every circumstance. See ***Categories of firms*** in the ***Definitions*** section.

This Government expects actions to be **completed within 6 months** of the Charter being published, and ongoing where relevant. To avoid duplication or divergence from regulatory requirements, reviews will be held after 6 months from publication and once Ofcom's OSA Codes of Practice for illegal harms are in force. See ***Reviewing and future iterations of the Charter*** section.

Online fraud also has many of the same enablers and impacts as other cyber-facilitated crimes. The commitments in this charter will therefore be hugely beneficial to preventing and mitigating the impacts of other harmful crimes such as theft, extortion, sexually motivated crimes, abuse and more.

For the purpose of this document, references to fraud and counter-fraud activity include money mule recruitment.

[1] Crime in England and Wales - Office for National Statistics (ons.gov.uk)
[2] 2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf (actionfraud.police.uk)

Blocking

1. Deploy measures to detect and block fraudulent material. These actions are intended to complement with Ofcom's forthcoming consultation on the Online Safety Act's illegal harms code of conduct where relevant. We intend to review this section once Ofcom's relevant codes of practice, and therefore the illegal content safety duties, come into force to avoid any duplication.	
All firms	a. Ensure fraud, money muling and associated behaviours are addressed in community standards, guidelines or terms of service as non-compliant activity. b. Have, or adopt, and maintain effective processes to identify, flag and remove content and accounts that meet internal thresholds of suspicion. c. Have, or adopt, and maintain effective processes to block users from creating new accounts when they have previously been removed for fraud, excluding those who have had their accounts taken over. d. Offer appropriate login authentication methods in line with the National Cyber Security Centre's (NCSC) password protection and encourage users to adopt two-step verification guidance.
Standalone online dating service providers	e. Give users the choice to verify their identity on platforms to allow other users to know they are genuine, allowing users to opt to interact with verified people only.
Social media/ networks with peer-to-peer marketplaces	f. Provide guidance to users for how to stay safe when buying and selling items directly with other users on listings for high-risk and high-value goods.
eCommerce marketplaces and social media/ networks with peer-to-peer marketplaces	g. Offer a mechanism for and/ or provide information on secure payment services that can be used for purchases originating on relevant signatories' platforms and marketplaces. h. Deploy verification measures of sellers using relevant signatories' platforms, services or marketplaces.

Reporting

2. Have a simple and quick route to report fraudulent material.	
All firms	a. Have, or adopt, and maintain a simple mechanism to report fraudulent content generated by users, which can be accessed within two clicks of a button. b. Action user reports as swiftly as possible. c. Run and maintain a simple and direct process for law enforcement and trusted partners to quickly, and easily, report suspected fraudulent activity occurring on the company's platform or services. d. Provide information to users on how to report incidents of fraud to law enforcement and their bank, and where to seek support, preferably at the point of reporting or in easily accessible help-centre resources.
Social media networks	e. Provide or develop appropriate warnings where users are contacted by unknown accounts or individuals, through direct messages, who may present a risk of fraud.
Standalone online dating service providers	f. Alert and provide education resources to users that have engaged in two-way communications (and have been confirmed to have sent or received contact information), with another user who the platform has positively identified as likely to be involved in financial crimes.

Takedowns

3. Take action against fraudulent content and users straight away.	
All firms	a. Remove fraudulent content immediately, once found to be contravening terms of service by the firm, unless in exceptional circumstances. b. Take appropriate and timely enforcement action against users suspected of posting, sending or sharing fraudulent content, once found to be contravening terms of service by the firm. c. Have a clear process in place to reinstate victims' accounts following an account takeover or fraud, with consideration for when linked recovery accounts have also been hacked.

Advertising

4. Deploy measures to protect people from fraudulent adverts.	
All firms	a. Engage with the Online Advertising Programme's Taskforce as required.
Firms with paid advertising services	b. Deploy verification measures for new advertisers. c. Confirm UK regulated financial services companies are authorised by the Financial Conduct Authority prior to serving their adverts. d. Screen adverts for suspicious content and scan embedded URLs to monitor if they change during the lifecycle of the advert. e. Identify and assess the legitimacy of an advert when it has adopted URL cloaking to hide a destination website's URL by redirecting it to another web page. f. Commit to and/ or move towards developing a simple fraud reporting mechanism on advertising services and open display advertising so users can access the reporting function for fraud within two clicks of a button.

Law Enforcement

5. Have dedicated liaisons who will respond to law enforcement requests. The Government and law enforcement will streamline and prioritise requests to industry.	
All firms	a. Prioritise and respond to law enforcement requests detailing criminal users or content as soon as possible. b. Respond to law enforcement requests to provide information, by due process, on persistent and prolific serious and organised crime actors targeting the UK public, to support investigative and intelligence operations. c. Engage in public private partnership initiatives with law enforcement and industry to develop and share best practice. d. Consider other ways to contribute resources for crime prevention, including the provision of technical training and/ or secondees to work within law enforcement units tackling online fraud.

Intelligence Sharing

6. Engage with initiatives to quickly share information about frauds. The Government will assist this work by scoping how regulation and guidance can facilitate greater information sharing, and where needed processes and infrastructure.	
All firms	Work with the Government, NCSC, the Information Commissioner's Office (ICO) regulator, law enforcement and other industry partners to: a. Contribute to a sector-wide 'gap analysis', to identify blockers for Government to act on. b. Explore what data, both internal and external, could facilitate the identification and prevention of fraud. c. Help stakeholders identify mechanisms and legal frameworks to share data, including mapping any current or potential industry-standard third-party databases. d. Discuss and agree typologies and taxonomies useful for clarifying data sharing. e. Share best practice and identify opportunities to work toward sharing data with other sector partners and other industries.

Transparency

7. Provide information about fraud risks on platforms, and what is being done to address them.	
All firms	Provide help centre articles and/ or transparency reports on how platforms are working to keep users safe, and how users can keep themselves safe from fraud.

Comms

8. Deliver simple messaging to support the public to recognise and avoid online fraud. The Government and law enforcement will provide toolkits and necessary resources whilst involving industry in its upcoming fraud campaign(s).	
All firms	a. Work with the Government on its upcoming comms campaign to help the public spot and avoid fraud. b. Amplify this messaging during the campaign, through ad credits and boosted content or through content made specifically for the platform, on top of the firm's protective messaging and alerts already communicated to users. c. Continue engaging users with messaging regarding the risk they can face from fraud and scams, outside of the Government campaign.

Horizon Scanning

9. Contribute to horizon scanning exercises to stay ahead of the threat.	
All firms	a. Analyse established and emerging methods and typologies of fraud on signatories' platforms and services. b. Undertake horizon scanning exercises to assess signatories' platforms and services for the risks that future technologies pose, focusing on intervention points and opportunities to tackle fraudsters. c. Share findings of both 9a. and 9b. with appropriate groups and organisations, where appropriate and permitted by law.

Reviewing and future iterations of the Charter

After 6 months from publication and following the consultation period for Ofcom's Codes of Practice, a review will be conducted to ensure Charter commitments are not duplicative or divergent from regulatory requirements.

A further review will be held once the OSA is in full effect to ensure the Charter continues to focus action on the most serious fraud trends and is best aligned with current regulations.

Governance

The Joint Fraud Taskforce (JFT), chaired by the UK Home Office Minister for Security, will hold companies to account for delivering the actions.

The Online Safety Act and the Online Fraud Charter

The OSA will require companies in-scope of regulation to tackle online fraud and take proportionate steps to mitigate the risks posed by online fraud and scams. A subset of these services will also have additional duties to take proportionate steps to prevent users from encountering paid-for fraudulent adverts.

Ofcom, as the independent regulator, will consult on and then publish the Codes of Practice which will set out the recommended steps online services may follow to comply with these duties.

In contrast to the OSA, the Online Fraud Charter is specifically configured to drive voluntary and more targeted action amongst a smaller, targeted subset of online platforms and services.

In this context, it is important to highlight that fulfilment of this charter's commitments will not automatically equate to compliance with fraud-related duties under the Online Safety Act, and the associated recommended steps set out in Ofcom's Codes of Practice, as the codes are separate and distinct from the Charter. For the avoidance of doubt, where there is direct conflict, regulatory requirements will take precedence.

Definitions

Categories of firms

- **All firms:** All signatories of this charter.
- **eCommerce marketplaces:** Companies providing a platform that enables consumer-to-consumer and/ or business-to-consumer sales.
- **Firms with paid advertising services:** Companies running or offering AdTech intermediary services to deliver paid-for marketing/ advertising content. There is no expectation for signatories to take on responsibility for the activities of organisations outside of their control so for the purpose of this charter this excludes firms acting as publishers using third party AdTech intermediary services or eCommerce marketplaces.
- **Social media/ networks:** Companies offering services to create and share content and/ or platforms enabling user-to-user communication. For the purpose of this charter this includes entertainment platforms offering some or all of these services.
- **Social media/ networks with peer-to-peer marketplaces:** As above with the addition of offering a platform that connects people who own a product or offer a service with people who want to buy, rent or otherwise own it.
- **Standalone online dating service providers:** Companies whose main business operation is to promote and provide mechanisms to facilitate online dating.

What is fraud and money muling?

- **Fraud**[3] involves an act or intention of dishonesty, normally through deception or breach of trust, with the intent to either make a gain or cause a loss of money or other property.
- **Money mules**[4] are individuals recruited by fraudsters and serious organised crime groups to move criminal funds on their behalf – through their banking or cryptocurrency accounts, or through cash. Children and vulnerable adults can be coerced, groomed, or deceived into laundering funds this way and in these cases are the victims of financial exploitation, and should be recognised as such.
- **Cyber-crimes**[5] (defined as Computer Misuse Act offences) occur when there is unauthorised access to computers, networks, data and other digital devices. This can allow cyber criminals to commit further malicious cyber activities such as ransomware attacks, unauthorised account access, intellectual property theft, denial of service attacks, or the stealing of large personal data sets. Unauthorised computer access can enable and facilitate a wide range of frauds, theft, sextortion and more.

[3] Fraudulent dishonesty and engaging in fraudulent behaviour defined in England, Wales and Northern Ireland by the Fraud Act 2006 and in Scotland under Common Law. Broader financial fraud in the UK is defined through Financial Services Act 2012 S89-90, Financial Services and Markets Act 2000 S23-25.
[4] Money laundering through the use of money mule networks defined in UK law under the Proceeds of Crime Act 2002 S327-329.
[5] National Cyber Strategy 2022, published 15 December 2021, GOV.UK website, National Cyber Strategy (publishing.service.gov.uk)

Online fraud risks

Fraudsters are adaptable and the ways in which they commit their crimes are numerous. Below are some common typologies both in terms of volume and harm. Industry has a unique insight into fraud typologies, so signatories will continue to identify and define the risks they see on their platforms and services.

- **Purchase fraud** – Criminals rely on the anonymity of the internet to sell non-existent products or products that never arrive. Data from banks suggests these are overwhelmingly committed on social media platforms and online marketplaces, with one major UK bank finding over 80% of all purchase scams reported to them happened on online platforms.
- **Romance fraud** – Criminals go to great lengths to exploit online platforms to target often vulnerable individuals, using social media and dating apps to find and contact victims. They will manipulate people into trusting them and believing they are in a genuine relationship. These victims will then be pressured into sending money to the fraudster through highly manipulative and emotive requests. These criminals often move onto other online platforms and messaging services to further engage with victims over a longer period to elicit further money.
- **Investment fraud** – Criminals offer lucrative and often convincing investment opportunities. Once a victim engages, they will be contacted by the fraudster who will pressure them into investing, typically increasing amounts, into a fictitious fund or service. These frequently occur on search functions through adverts and search results, social media through adverts and user-generated content, and publishing websites through display adverts.
- **Impersonation fraud** – Criminals pretend to be a trusted figure, ranging from a celebrity or legitimate organisation such as a bank, to deceive victims into sending money for ultimately bogus reasons. Criminals use fake social media accounts and posts, take out online adverts and appear in search results to lure in victims.
- **Phishing** – Criminals communicate with people to encourage them to take an action that may lead to them being defrauded, such as clicking a bad link that will download malware or direct them to a fraudulent website that will harvest their details. This can happen through almost all online communication channels including email, online messaging, social media and through links in search results and online advertising.
- **Money mules** – Money mules are individuals who move the proceeds of crime on behalf of criminals, sometimes in exchange for payment or other benefit. This can include via physical cash and financial products such as bank and cryptocurrency accounts. Children and adults at risk can be coerced, controlled, manipulated or deceived into facilitating the movement of funds and in such cases, these people are victims of money-laundering linked financial exploitation.