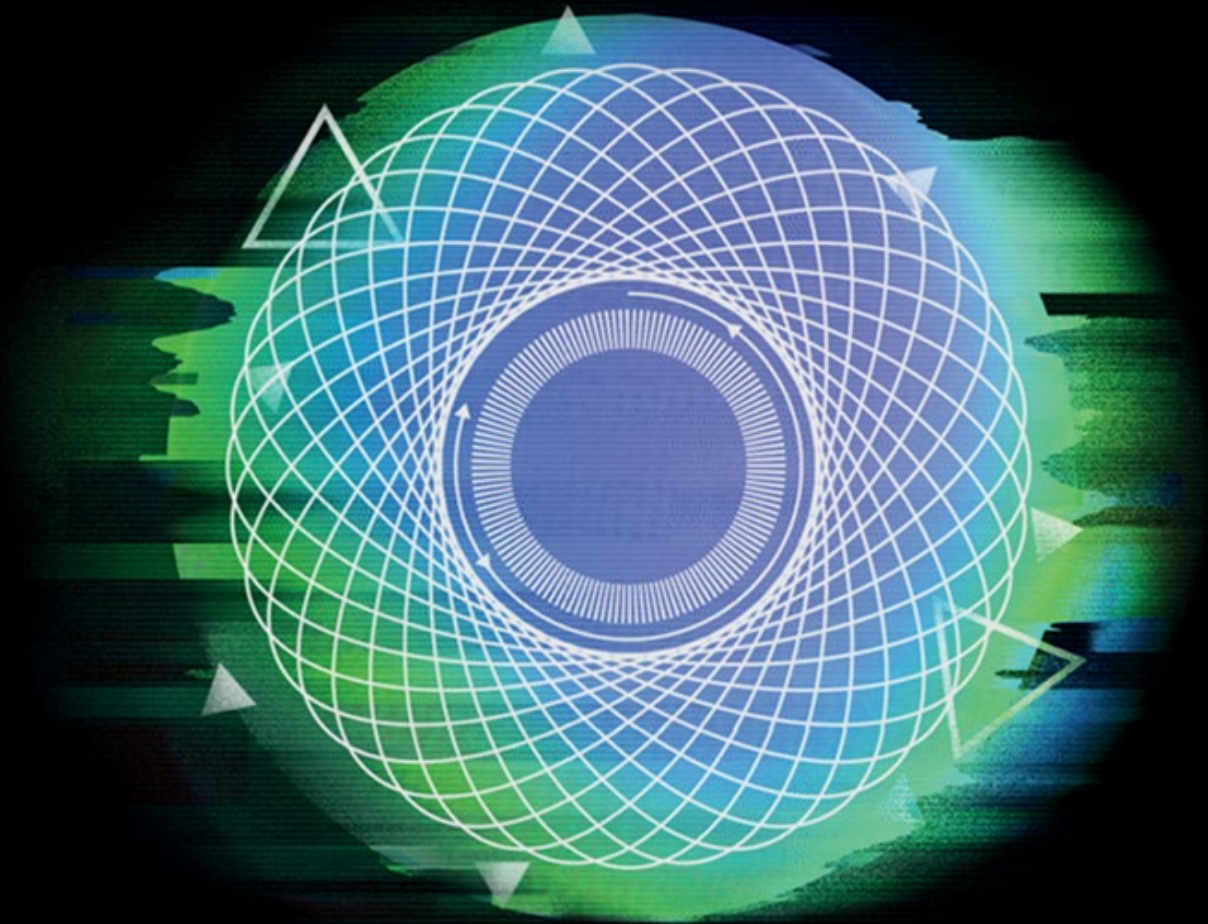




A Matter of Trust:
Tackling the Fraud
Epidemic in the UK

Guidance for digital platform companies



The National Fraud Bureau states that around 80% of reported fraud is cyber-enabled¹, including payment diversion fraud, investment fraud and romance fraud, amongst others. Additionally, according to research commissioned by Ofcom, around nine in ten online adults in the UK have seen content online which they suspected to be a scam or fraud.² On the flipside of consumer fraud is corporate fraud, and last year employees and management were involved in nearly half of all UK fraud cases over £100k to the combined value of £221m.

Why is fraud such an acute problem in the UK?

Between April 2022 and March 2023, 3.5 million incidents of fraud were reported by people aged 16 and over in the UK⁴, demonstrating that the UK encapsulates a number of market factors that make it a particularly attractive locus for fraudulent activity.

So why is this the case? The UK has the twelfth largest population in the world³ and in economic value terms, the UK's Gross Domestic Product per capita ranks at 20th globally. The UK is also the third largest eCommerce marketplace⁵ (trailing only China and the US) and the third largest advertising market globally⁶ (where 78% of UK ad spend is online⁷). When you add to this the universality of the English language and the UK's fast and frictionless payment system, it is not difficult to see why it represents a large and lucrative target for fraudsters here in the UK and around the world.

How is the UK government trying to tackle fraud?

Over the last 10 years, the Home Office has attempted to ratchet fraud higher up the political agenda: agreeing a succession of fraud charters with industry; publishing a 10-year fraud strategy⁸; and supporting new legislative vehicles to hold key fraud ecosystem actors to account.

These legislative vehicles include the Economic Crime and Corporate Transparency Act ("ECCTA") (which includes the new Failure to Prevent

¹ <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime#:~:text=It%20accounts%20for%20over%2040,adults%20aged%2016%20and%20over.>

² Scale and impact of online fraud revealed - Ofcom

³ <https://data.oecd.org/pop/population.htm>

⁴ <https://socialcatfish.com/scamfish/state-of-internet-scams-2023/>

⁵ <https://www.mobiloud.com/blog/e-commerce-market-size-by-country#:~:text=China%20is%20the%20%231%20eCommerce,online%20sales%20around%20the%20world.>

⁶ Annual Review 2023: UK Advertising's Success on the World Stage - Advertising Association (adassoc.org.uk).

⁷ UK Advertising Reports £36.6BN Spend in 2023 - Advertising Association (adassoc.org.uk)

⁸ https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf

Fraud Offence) and the UK Online Safety Act (“OSA”), both of which received Royal Assent in October 2023.

The introduction of new legislation covering both consumer and corporate fraud provides a clear signal from the government that the era of self-regulation is over. As they are subject to both sets of legislation, the impact on digital platform companies (“DPCs”) from this renewed focus on fraud is likely to be pronounced. This article seeks to explain what is required from DPCs, both in terms of corporate governance and the management of fraud risks to end users, as well as outlining how they can stay compliant while continuing to operate successfully in the UK.

What is the new legislation designed to do and how will it help tackle fraud?

The Failure to Prevent Fraud Offence

The new failure to prevent fraud offence, introduced by the ECCTA, represents a significant shift in responsibility, with the onus being placed on organisations to ensure they have reasonable procedures in place to prevent fraud. The purpose of this legislation is to discourage organisations from turning a blind eye to fraud

by employees or associated persons which may benefit the organisation, and to encourage organisations to implement and improve their prevention procedures. The hope is that it will drive a major shift in corporate culture to reduce corporate fraud.

Under the offence, an organisation will be held liable where a specified fraud offence is committed by an **employee** or **agent** of the organisation, for the **benefit of the organisation** and where the organisation did not have **reasonable fraud prevention** procedures in place.

Only large organisations fall in scope, defined as organisations meeting two of the three following criteria: (i) more than 250 employees; (ii) more than £36m in turnover; and (iii) more than £18m in total assets.

The reasonable procedures which organisations need to have in place, need to be proactive, meaning that measures must be in place to prevent fraud not just to react to it after it has happened.

The guidance on what procedures need to be in place has not yet been published (currently expected in Q3 or Q4, 2024), however we can expect that it will be based around the following principles:

- 1. Governance (including top-level commitment):** is there appropriate governance of fraud risk in place, has a clear tone from the top and middle of the organisation been set and has a senior leader been nominated?
- 2. Risk Assessment:** has there been a review of existing fraud risk assessment activities and, where necessary, a new assessment undertaken which includes a focus on fraud risk areas that may be committed by the organisation?
- 3. Proportionate procedures and controls including due diligence:** are controls aligned to the risk assessment and have any gaps identified been remediated. Are processes and controls clearly documented, easy to understand, easy to find and regularly referred to?
- 4. Communication and training:** are policies, procedures and controls embedded and understood? Have employees and third parties received initial and ongoing training on the new offence, their responsibilities and the wider threats posed by fraud?
- 5. Monitoring, review and assurance:** are processes in place to review the design implementation and operating effectiveness of the anti-fraud controls.





The UK Online Safety Act

The OSA is a comprehensive piece of legislation aimed at making the internet a safer place for everyone. While its primary focus is on protecting children from harmful content, it also includes provisions to tackle the scourge of online fraud and scams, including fraudulent advertising.

Key OSA provisions for tackling fraud include:

- 1. Duty to Prevent Fraud:** a new duty of care on the largest and most popular online platforms, requiring them to take proactive steps to prevent paid-for fraudulent adverts from appearing on their services. This includes ads related to investment scams and romance fraud.
- 2. Risk Assessments:** all companies will be required to conduct thorough risk assessments to identify and understand the specific fraud risks their users face. This will help them implement fraud prevention measures accordingly.
- 3. Proactive measures:** larger platforms must implement proportionate systems and processes to tackle fraudulent advertising. This includes measures to detect and remove fraudulent ads, verify the identity of advertisers, and educate users about the risks of scams.
- 4. Cooperation with the regulator:** the OSA requires DPCs to cooperate with Ofcom, the UK's communications regulator, in responding to information requests, and investigating and addressing fraudulent activity.
- 5. Enforcement and penalties:** Ofcom will have the power to impose significant fines of up to £18 million or 10 per cent of a company's global annual turnover (whichever is higher) for non-compliance with the OSA.

So what does this all mean for DPCs?

With these two new pieces of legislation there is now increasing pressure for DPCs to take **a holistic and comprehensive view to tackling fraud**, considering both the threat from within, and the threat posed by, and to, users of their services. As a result, DPCs have an increased responsibility to **invest in robust fraud prevention technologies, systems and processes**, coupled with a requirement to be **more transparent** about the risks that their users face and the fraud prevention measures they have in place.

Where should DPCs start?

Whilst the two pieces of legislation look at fraud from different angles, there is clear overlap in how companies are expected to respond to fraud challenges, and therefore there are synergies to be gained by DPCs who consider the impact of both simultaneously. For example, both sets

of legislation recommend a **strong tone from the top, a fraud risk assessment and proportionate procedures** as pillars of the fraud response. This should form the bedrock for how DPCs address both Failure to Prevent Fraud and the anti-fraud provisions within the OSA.

Further, identifying where your risks lie is the starting point so that you can implement effective controls to protect against the risks faced. This applies to both fraud committed within the organisation and fraud committed by users of a company's services. With that in mind, a **fraud risk assessments can be designed by following the seven key steps below:**

1. Bringing the right people in to drive the risk assessment process.
2. Ensuring all areas of the business are captured and the scope of fraud defined;
3. Initial information gathering from identified data sources;
4. Identifying fraud risks and suitable controls;
5. Analysis and control mapping;
6. Documentation of the risk assessment and implications; and
7. Remedial measures and recommendations.

Conclusion

There is no getting away from the fact that new fraud legislation does place an increased compliance burden on DPCs, who are trying to balance fraud prevention measures and monitoring activity with freedom of expression and maintaining the user experience. The combined legislation is likely to lead to increased scrutiny of DPCs' practices, as well as the potential for current regulations to serve as a floor, not a ceiling - pushing for higher industry standards in online safety and fraud prevention overall. Therefore, it is vital that companies have the right tools and policies in place and ensure staff have the awareness required so that, as and when new legislation or guidance comes into force, they are ready to quickly adapt to any required changes.

There is also hope that the new legislation will have a positive impact on society to assist in reducing the prevalence of online fraud, benefiting both DPCs and their users. If the legislation is implemented and enforced effectively, both by companies and enforcers, the result should be an increase in online safety for users leading to increased trust between the public and DPCs.

To learn more about Deloitte's recommended approach to developing a fraud risk assessment, take a look at our more [detailed guide](#).



Contact us

If you would like to discuss any of the issues raised in this paper in more detail, please do get in touch with one of our team.



Amber Andrade

Director, Forensic
amandrade@deloitte.co.uk
+44 20 7007 3169



Brij Sharma

Associate Director, Risk Advisory
bmsharma@deloitte.co.uk
+44 20 8071 3988



Sophie Wogan

Manager, Forensic
swogan@deloitte.co.uk
+44 118 322 2782

Deloitte.

This document is confidential and it is not to be copied or made available to any other party. Deloitte LLP does not accept any liability for use of or reliance on the contents of this document by any person save by the intended recipient(s) to the extent agreed in a Deloitte LLP engagement contract.

If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please [click here](#) to learn more about our global network of member firms.