Deloitte.
Together makes progress

Navigating the digital minefield:
Tackling online fraud and scams

2026

Executive summary

Fraud costs the UK economy a staggering **£14.4 billion every year**[1] — and the digital landscape is at the heart of the problem. Four in five scams are now digitally enabled,[2] with online fraud accounting for **50 per cent of all online crime.**[3] Nearly nine in ten (87 per cent) UK adult internet users report encountering suspected scams,[4] exposing individuals to severe financial and emotional harm while critically eroding the user trust upon which digital businesses depend. The UK Government has responded with over **£250 million in committed investment** between 2026 and 2029,[5] underscoring the severity of the threat.

The imperative: responding to an evolving threat

In this paper, we dissect the evolving landscape of online fraud, from sophisticated marketplace and social media scams to malicious apps and AI-accelerated methods. The unprecedented growth in the scale, diversity and complexity of online fraud now requires platforms to build strong, resilient systems that can respond to the rapid rise in new and emerging threat types.

The regulatory hammer is falling

This paper highlights the imperative for platforms to act in response to stringent new regulations in both the UK and EU. The UK Online Safety Act (OSA) 2023 introduces a legal duty for online services to implement proportionate measures to protect users from illegal content, including fraudulent advertisements, with penalties of up to **£18 million** or **10 per cent** of qualifying worldwide revenue, whichever is higher. Meanwhile, the UK Digital Markets, Competition and Consumers Act (DMCCA) 2024 further strengthens consumer protection, targeting fake reviews and deceptive practices with substantial fining powers.

In the EU, the Digital Services Act (DSA) 2022 mandates that platforms conduct risk assessments and mitigate systemic risks associated with illegal content, including fraudulent activity, backed by sanctions of comparable severity to the OSA. Emerging regulations such as the forthcoming EU Payment Services Directive 3 (PSD3) signal a future where platforms may also face direct financial liability for victim reimbursement, extending beyond traditional fines. The growing financial cost of noncompliance demands a coordinated response from companies to proactively identify, assess and mitigate risks of fraudulent content on their platforms.

Beyond compliance and the avoidance of significant financial penalties, a robust approach to fraud risk management can serve as a powerful differentiator to attract and retain users. As central conduits for online interaction and commerce, platforms are increasingly being called upon to protect users and maintain trust in the digital ecosystem. Proactivity around the online fraud threat signals a platform's meaningful commitment to social responsibility, which may support long term value creation through improved customer retention and reduced churn.

Deloitte's solution: your partner in building trust and resilience

Finally, we explain how Deloitte partners with services to meet escalating regulatory demands and build operations that are robust, compliant, and resilient to online financial crime. Our expertise in Financial Crime Regulation and Digital Regulatory Compliance, including deep specialisation in the OSA and DSA, enables us to design and implement fraud risk management frameworks tailored to the unique needs of individual services. We empower compliance teams to protect users, prevent reputational damage, and ensure the long-term integrity of platforms in an increasingly complex digital age.

1. The online fraud problem: Understanding the rapidly evolving threat landscape

Getting to grips with the online fraud problem

Online fraud represents a significant and growing threat to individuals, businesses, and the broader economy. The sheer scale of the fraud problem underscores the urgent need for comprehensive preventative and responsive measures.

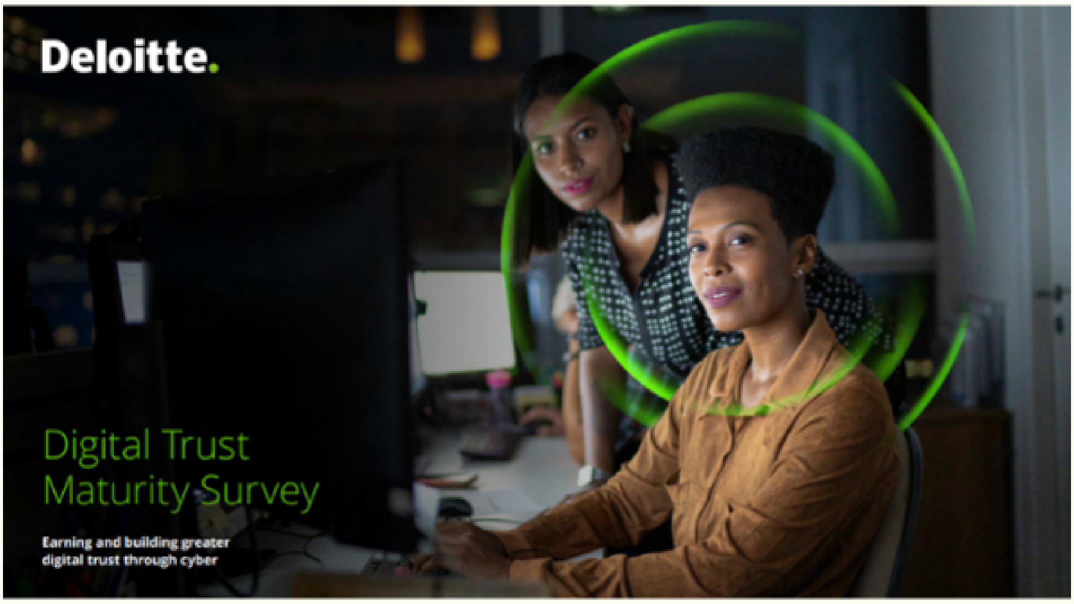
As more financial activity shifts online, digital platform users are increasingly susceptible to online forms of fraud; an estimated **60 per cent of incidents** are cyber-related, with recent reported increases being driven by crimes involving online banking, online shopping and social media scams.[6] In 2025, UK Finance reported that fraud now accounts for 50 per cent of all online crime in the UK,[7] with **£629.3 million stolen through fraud** in the first half of 2025 alone.[8] While the widespread availability of social media has accelerated communication, it has also provided powerful tools for malicious actors to exploit.

The impacts on individual platform users are far-reaching. Ofcom's research indicates that nearly nine in ten UK adult internet users (87 per cent) report encountering material they believe to be fraudulent or part of a scam online,[9] demonstrating the public's widespread exposure to risks of financial harm. The UK's Fraud Strategy 2026 to 2029: Disrupting crime, supporting economic resilience and delivering justice (the 'Fraud Strategy') was presented to Parliament in March 2026 and sets out how the UK government will combat fraud against individuals and businesses over the period 2026 to 2029.[10] It highlights the severely damaging effects of these crimes beyond financial loss: **92 per cent of fraud victims experienced emotional or mental health symptoms**, **57 per cent experienced physical health symptoms**, and **63 per cent reported behavioural changes** as a result of their victimisation.[11]

These harms signal a growing imperative for businesses to build safer and more trustworthy online experiences. As outlined in our 2026 Trust & Safety report,[12] trust is the crucial currency companies must use to earn the attention, business and loyalty of their customers.

Our Digital Trust Maturity Survey[13] findings show:

- Trustworthy companies can outperform non-trustworthy companies by 2.5 times.
- Improving digital trust encourages repeat business – **88 per cent of customers who highly trust a brand will buy again from that brand.**
- For high digital trust maturity companies, **71 per cent of companies reported improved confidence in tech integrity**, which is 50 percentage points higher than their low digital trust maturity counterparts.



The threat extends beyond individual consumers – according to the Fraud Strategy,[14] one in four UK businesses with more than one employee experienced fraud, amounting to approximately **389,000 businesses and 6.04 million instances of fraud**. Notably, 8 per cent of affected businesses reported being discouraged from carrying out intended future business activities as a result, demonstrating the damaging effect of fraud on economic growth and enterprise.

The online element of many frauds brings additional complexity by spanning multiple jurisdictions, posing a challenge to launching successful interventions against offending. As the online fraud threat is global in nature, there is a growing need for authorities to coordinate effective responses across borders. Our 'Tackling Fraud in a Borderless World' report sets out our thinking on what a genuinely global fraud response architecture could look like.

To effectively address the pervasive nature of the online fraud problem, it is crucial to understand some of the most prevalent tactics currently being used by malicious actors. While the full extent of fraud threat methodologies is continuously evolving, some of the more notable manifestations include the forms listed below:[15,16]

Impersonation and identity fraud:

Fraudsters impersonate individuals or legitimate organisations (e.g., financial institutions, professional services, public bodies etc.) to steal personal and financial information from victims (e.g. counterfeit websites, impersonation, identity fraud).

Investment and financial opportunity scams:

Malicious actors lure victims using fake investment opportunities, often offering high levels of return that appear 'too good to be true' (e.g. pension schemes, loan fee fraud, and cryptocurrency investment opportunities).

Online marketplace and consumer fraud:

Fraudsters exploit online trading platforms to perpetrate a variety of fraudulent offences against buyers and sellers (e.g. non-delivery of goods, sale of counterfeit items, fake reviews, and fraudulent rental fee schemes).

Social media scams:

Criminals take advantage of the ability to access audiences and develop personal connections with victims on social media platforms, often by building false relationships or promoting fraudulent offers (e.g. romance/dating scams, fraudulent advertising, and impersonation of public figures).

Malicious software & ransomware scams:

Offenders use software to infiltrate victims' devices, disable system protections and perform actions including theft of data and financial assets (e.g. deployment of malware and ransomware).

Direct online payment fraud:

Fraudulent activities directly targeting online financial transactions, such as Authorised Push Payment ("APP") scams where victims are tricked into sending money, or credit/debit card fraud.

AI-enhanced deception and automation:

Advanced technologies such as AI are used to create highly convincing fraudulent content at scale (e.g., deepfakes, voice cloning) – this is a cross-cutting enabler that amplifies the impact of the other categories.

New technologies are rapidly accelerating risks

The threat landscape is being reshaped by rapid technological advancement. Emerging technologies are equipping threat actors with powerful new capabilities, enabling fraud at unprecedented scale and sophistication. The Government's National Security Strategy 2025 identifies fraud as a technology-enabled hybrid threat, posing a significant challenge to national security and economic growth.[17]

As reported in the Fraud Strategy,[18] the UK's reliance on online platforms for banking, shopping and communication has increased the vulnerability of users to unknown threat actors who are now able to perpetrate fraud at scale, often without the knowledge of their victims. The UK Government further identifies data breaches and phishing scams as critical accelerants of online fraud.

Amongst several bodies responding to the rapid evolution of fraud threat methodologies, the National Crime Agency's National Economic Crime Centre (NECC) reports[19] that advancements in AI are enabling massive-scale fraud in several ways:

Deepfakes:

AI-generated scripts, audio and videos are being exploited to manipulate potential victims, including by targeting them with increasingly personalised communications; AI can be used to create 'spoof' telephone numbers, websites and applications that can be used in offending. In response, the Government has launched a Deepfake Detection Challenge 2026[20], hosted in partnership with Microsoft, and is working with the Department for Science, Innovation and Technology (DSIT) and the Alan Turing Institute to develop a framework for detecting deepfake media.

AI-driven automation:

AI increases the scale of attempted frauds, enabling perpetrators to target a higher volume of victims in less time; UK Finance similarly notes that agentic AI will supercharge offender behaviours, enabling them to scale, simplify and cut costs of execution.[21]

AI-enabled scam designs:

Cyber criminals can leverage AI to gather information on how to commit offences, improving their knowledge of scamming methodologies.

2. The challenge for platforms: responding to the impacts of online fraud

Services under the spotlight of increasing regulatory scrutiny

As the scale of the online fraud problem grows, so too do challenges for digital platform companies. Policymakers expect providers to play an increasingly proactive role in identifying and mitigating the risks of fraud on their platforms.

To illustrate the regulatory impact, we examine below three key pieces of legislation that significantly affect platforms operating in the UK and EU.

UK Online Safety Act (OSA) 2023

The OSA introduces a legal duty for online services to implement proportionate safety measures to protect users from illegal content, including fraudulent advertising. The regulator is empowered to enforce compliance through significant fines ("£18 million or 10 percent of qualifying worldwide revenue, whichever is higher) or service blocking. This Act marks a significant shift, placing direct and legally binding responsibility on platforms to protect users from online financial harm.

EU Digital Services Act (DSA) 2022

The DSA seeks to create a safer and more accountable online environment by mandating that online platforms conduct risk assessments to identify and mitigate systemic risks associated with the dissemination of illegal content and consumer protection, including fraudulent content. The largest platforms and search engines are subject to annual audits of their approach to systemic risk management, posing a risk of sanctions including fines or even enforced suspension of services.

UK Digital Markets, Competition and Consumers Act (DMCCA) 2024

Strengthens consumer protection by explicitly prohibiting fake reviews and binding platforms to actively prevent them, while also introducing new rules for clearer subscription contracts and empowering the CMA with substantial fining powers for breaches.

Anticipated regulatory developments

In the UK, further developments will enhance the current regulatory framework surrounding online fraud. In Summer 2026, Ofcom is expected to publish its register of 'categorised' services, which will be subject to additional duties to address online fraud.[22] Ofcom intends to consult on the detail of its recommended fraudulent advertising measures, with duties expected to come into force in 2027.[23]

Following the closure of Ofcom's Additional Safety Measures consultation in October 2025, the regulator is expected to publish its final statement later this year, including details of its recommended 'proactive technology' measures (including content identification, user profiling or behaviour identification technology) for identification and removal of 'relevant' illegal content, including fraudulent content.[24]

Authorities partnering to tackle online fraud

The multi-dimensional nature of online fraud has prompted a collaborative regulatory response, with the Financial Conduct Authority (FCA) joining alongside Ofcom's efforts to tackle this widespread problem. Under the banner of the Digital Regulation Cooperation Forum (DRCF), the regulators have initiated an Illegal Online Financial Promotions workstream[25] to identify the overlap between online safety and financial services regulations and improve clarity for online services.

Under Ofcom's Online Safety regime, the FCA is listed as one of several recommended 'trusted flaggers', for which relevant services at risk of fraud are responsible for establishing a dedicated reporting channel to receive reports of suspected fraudulent content.

Beyond its role as a 'trusted flagger', the FCA is actively enhancing its capabilities for proactive disruption of online scams. This includes leveraging advanced intelligence gathering to identify emerging scam trends and the networks behind them, enabling faster takedowns of fraudulent websites and social media posts in collaboration with platforms.[26] In its own capacity, the FCA also plays a critical role in scanning c. 100,000 websites daily to identify potential online scams, including the rising volume of 'finfluencer' user-generated content.[27] In response to direct engagement from the FCA, several large platforms have now adjusted their policies to only permit paid-for ads for financial services that have been authorised by the regulator, significantly reducing the volume of paid-for scam ads.[28]

The Fraud Strategy[29] recognises progress made by the technology sector to improve collaboration with law enforcement following publication of the Online Fraud Charter, noting that data-sharing and collaboration between platforms and other sectors has increased since the Charter was signed in 2023. However, it also acknowledges that broader progress remains uneven and significant weaknesses persist on some services and platforms. The Government plans to build upon this foundation by launching a new Online Advertising Taskforce between the Home Office, Department for Culture, Media and Sport (DCMS), and the Internet Advertising Bureau UK (IAB UK).[30] Significantly, the Government has stated that if industry partnership and market incentives alone remain insufficient to drive improvements, it will take legislative action within this Parliament.[31]

Mobilisation of the broader anti-fraud ecosystem

The broader ecosystem of organisations focusing on the fraud problem, including law enforcement and justice agencies, government departments and the private sector, are also placing increasing pressure on digital platforms to act.

The NECC, for example, has highlighted the role that social media providers should play in preventing fraud in its written evidence submissions to UK Parliament. It cites that the UK has a significantly higher proportion (27 per cent) of its retail economy online compared with other EU countries (15 per cent average) or the US (19 per cent), posing significant risks.[32] In furtherance of the fight against online fraud, the NECC works closely with industry partners, including social media companies, through its Public Private Partnerships initiatives.

Industry collaboration is increasingly recognised as an effective mechanism for driving down online fraud. The Fraud Intelligence Reciprocal Exchange (FIRE) established by Meta and members of Stop Scams UK, for example, facilitated the sharing of threat intelligence on prominent platform scams, resulting in the removal of approximately 20,000 fraudulent accounts during its six-month pilot.[33]

Comparatively, in the financial services sector, initiatives such as the Banking Protocol and Confirmation of Payee have materially reduced fraud losses, while the Retail Banking Fraud Charter continues to drive improvements in fraud prevention and victim support. These examples illustrate the value of meaningful cross-industry collaboration, and the Government has made clear its expectation that all sectors – including digital platforms – must contribute substantively to the collective fraud response.

The Fraud Strategy announced the establishment of the new Online Crime Centre (OCC), backed by £31 million in Government funding.[34] The OCC represents a cross-agency partnership uniting UK policing, the UK Intelligence Community (including GCHQ, the National Cyber Security Centre and the National Cyber Force), and private sector partners. The OCC will initially prioritise three core functions: data-sharing and analysis to improve the intelligence picture on online fraud; reducing harm by designing technical solutions and supporting platform-level interventions; and protecting users by advising industry partners on emerging trends, crime prevention and safeguarding measures.

The Government is also investing in improved fraud reporting infrastructure. The existing Action Fraud service is being replaced by a new Report Fraud service, operational from 2026, incorporating upgraded technology and improved victim support.[35] Additionally, a new Fraud Victims Charter is planned for 2027, setting national standards for victim care.[36] These developments will reshape how fraud is reported, and intelligence is shared, with implications for how platforms engage with law enforcement and support affected users.

3. How digital platforms can respond effectively:

Building robust online fraud risk management frameworks

In response to the growing challenge of online fraud, platforms can begin prioritising several core activities to develop the systems and processes needed to effectively identify, assess and mitigate associated risks. These actions are key building blocks of a comprehensive approach to managing risks of fraudulent content online.

Developing a strategy

- **Understand your risk landscape:** Identify and assess the risks of online fraud to your business and users, recognising the potential impacts to reputation, customer trust, and financial stability. Recognise distinct customer vulnerabilities and platform capabilities across your services and prioritise risk mitigation efforts accordingly.
- **Strategic partnerships:** An effective fraud reduction strategy should not be devised in isolation; through meaningful partnership engagement with third-party stakeholders including 'trusted flagger' organisations, platforms can develop a more-informed understanding of their fraud threats, harms and risks.
- **Governance and accountability:** Define clear lines of leadership and accountability for your fraud reduction strategy to provide clear strategic direction, ensure effective implementation and monitoring of operational performance.

Training your people

- **Staff training and internal comms:** Continuous internal communication and training is critical to shaping an ethical culture, raising awareness of fraud risks, ensuring everyone understands their role in the prevention and detection of online fraud.

Refining your operating model

- **'No regret' actions:** Prioritise immediate actions such as enhancing user authentication, improving content moderation, implementing Know Your Business Customer (KYBC) checks for sellers, and streamlining reporting mechanisms for users.
- **Devise a comprehensive governance and risk management framework:** Align Governance, Risk and Compliance (GRC) activities across relevant risk domains including financial, privacy and online safety compliance. Develop robust internal controls, policies, and procedures for fraud detection, prevention, and response, integrating these into existing risk frameworks and ensuring they are regularly reviewed.
- **Reporting and takedowns:** Develop clear pathways for users to report fraudulent material and implement effective systems for removal of fraudulent content.
- **Intelligence operations:** systematise approaches for gathering the latest insights and intelligence on the evolving online fraud threat. Share information with key stakeholders such as law enforcement agencies, government and regulatory bodies.

Embedding tech-enablement

- **Invest in technology:** Leverage AI and machine learning for automated content moderation, enabling real-time fraud detection for scams and unauthorised financial promotions, anomaly identification, and content analysis; safe and secure digital identification can also provide an additional safeguard against online fraud.
- **Implement technical safeguards:** Devise robust controls on technology implementation, promoting ethical and quality outcomes for users; remain cognisant of the risks of false positives, privacy impacts and negative user experiences. Promote transparency and accountability as core principles underpinning use of technical tools.

How Deloitte can help

We are uniquely positioned to help digital platforms navigate the complex and evolving landscape of online fraud and regulation. Our expertise in Financial Crime Regulation is complemented by our experience supporting global online services with Digital Regulatory Compliance challenges, including emerging online safety regulations such as the OSA and DSA. Our insight across domains enables us to deliver comprehensive compliance solutions suited to the complexities of this growing risk area.

?

Digital Regulation	Financial Crime
• OSA/DSA Compliance • DSA Systemic Risk Assessments • OSA Illegal Content Risk Assessments • DSA Independent Audit and Audit Preparation Services • Regulatory Horizon Scanning • Compliance Strategy & Operating Model Services • Compliance Issue Remediation	• Support the development and implementation of fraud governance including a fraud risk strategy, fraud risk management and fraud policy assurance. • Fraud risk and threat identification to allow the setting of risk appetite. • Evaluation of fraud control environment • Fraud control gap assessment including a remediation and enhancement plan. • Development and implementation of fraud operating procedures and fraud prevention technologies (e.g. onboarding, authentication, behaviour and payment monitoring). • Develop and implement employee fraud training. • Review fraud detection capabilities • Design, assessment and embedding of whistleblowing process or fraud/financial crime incident reporting • Forensic Investigation Services

We support services to develop comprehensive risk management strategies built around their existing governance, risk and compliance structures. An effective online fraud reduction strategy should be multifaceted, involving effective management of people, processes and technology to reduce the risk of harm suffered by users.

Illustrative case study: Enhancing platform integrity for a global e-commerce giant

To demonstrate how Deloitte can help services with strategic and operational fraud risk management challenges, we have developed an illustrative case study below. This case study draws together typical challenges we support clients with, showcasing the breadth of our capabilities for providing a comprehensive and coordinated response to online fraud.

Company overview:

'Safespend' is a leading e-commerce platform hosting sales of second-hand goods and services, with a significant presence established in both the UK and EU. The company has been on an impressive growth journey, developing from a budding start-up to a global platform with customers in over 30 regions. The company is projected to continue with its impressive year-on-year growth thanks to its consistent development of innovative new features, including an enhanced customer review module enabling users to freely share information on the quality and trustworthiness of sellers on the platform. Trust is a key aspect of Safespend's value proposition, offering users a reliable and relatively frictionless trading experience.

Client challenge:

Safespend faces escalating risks of online marketplace fraud, with recently recorded spikes in sales of counterfeit goods, non-delivery scams, account takeovers and fake reviews. AI has accelerated the spread of disinformation on the platform, resulting in several high-profile scams attracting media coverage across prominent news outlets. The platform's international compliance team is aware of pressing new obligations under the UK Online Safety Act and EU Digital Services Act but has limited regional resources to dedicate to addressing the requirements of both regimes.

Our approach:

To assist Safespend with developing a comprehensive approach to managing its growing fraud risks, we would provide the following services:

- **EU/UK regulatory readiness:** Conduct a detailed analysis of OSA, DSA, and DMCCA regulatory requirements to identify Safespend's obligations for identifying, assessing and mitigating risks of fraudulent content.
- **Compliance strategy:** Engage senior business leaders across Product, Compliance and Legal departments to align on requirements to deploy dedicated compliance programmes targeting Safespend's online fraud risks.
- **Online safety risk assessments:** Develop Safespend's risk management architecture, enabling completion of detailed online safety risk assessments. These would uncover the extent of Safespend's online fraud risks and identify mitigations recommended by the regulator to address these challenges.
- **Regulatory engagement:** Engage Deloitte's regulatory SMEs to support Safespend with preparing responses to EU and UK regulators, assisting with briefings and developing responses to requests for information.
- **Fraud control design:** Engage Financial Risk and Digital Regulation colleagues to codesign a set of recommended control measures to address Safespend's risks, including more robust seller vetting frameworks, user reporting functionality, identity verification tools, and establishment of a reporting channel for 'trusted flagger' organisations to report fraud.
- **AI-assisted threat detection:** Implement automated threat detection capabilities enabling Safespend's Trust & Safety team to collect real-time intelligence on emerging online fraud risks, including through anomaly detection and behavioural analytics techniques. This equips the business to identify fake listings, fake reviews, and patterns indicative of non-delivery scams.
- **Incident response & training:** Update Safespend's fraud crisis management protocols, conducting tabletop exercises, and delivering comprehensive training to compliance and Trust & Safety team leaders to enable coordinated responses to emerging risks.

Typical outcomes:

By performing the services above, we typically see the below outcomes for our clients:

- **Reduced fraud incidents:** A significant reduction in reported instances of online fraud, including counterfeit goods, non-delivery scams, and account takeovers.
- **Enhanced compliance:** Full readiness for evidencing compliance with OSA and DSA obligations, with a deeper relationship with EU and UK regulators.
- **Improved customer trust:** Positive feedback from customers regarding increased security and integrity, leading to improved brand reputation.
- **Brand reputation gains:** Reduced negative media coverage and the ability to share 'good news' stories externally, demonstrating best practice approaches to mitigating online fraud.
- **Operational efficiency:** Streamlined fraud investigation processes and reduced manual effort through automation and advanced analytics.

This case study exemplifies how Deloitte partners with organisations to not only address immediate fraud challenges but also to build sustainable, compliant, and resilient digital operations in the face of evolving threats.

Key Contacts

Amber Andrade
Partner,
Forensic & Financial Crime

Lauren Taylor
Partner,
Ethics & Regulatory Compliance

Nick Seeber
Partner,
Digital Regulation

Garikai Mparutsa
Director,
Forensic & Financial Crime

Authors

Lead Authors

Jeevan Sahota
Manager,
Digital Regulation

Amber Andrade
Partner,
Forensic & Financial Crime

Supporting

James Smith
Assistant Director,
Head of Trust & Safety

Nick Evans
Senior Manager,
European Centre for Regulatory Strategy

Joana Varga
Manager,
Digital Regulation

Sabrina Law
Senior Manager,
Forensic & Financial Crime

Sam Peel
Senior Manager,
Forensic & Financial Crime

Endnotes

1. UK Government, 'Economic and social cost of fraud', 2023-2024
2. Cifas, 'Fraudscape', 2026
3. UK Finance, 'Annual Fraud report', 2025
4. Ofcom, 'Online Information Advisory Committee Report: Understanding Online Financial Harm, Fraud, Scams and Disinformation', 2025
5. UK Government, 'Fraud Strategy', 2026-2029
6. Ofcom, 'Understanding Online Financial Harm Literature Review', 2025
7. UK Finance, 'Annual Fraud report', 2025
8. UK Finance, 'Half Year Fraud Report', 2025
9. Ofcom, 'Online scams and fraud research summary report', 2023
10. CP 1523 – Fraud Strategy 2026-2029 Disrupting crime, supporting economic resilience and delivering justice.
11. UK Government, 'Fraud Strategy', 2026-2029
12. Deloitte, 'Trust & Safety Report', 2026
13. Deloitte, 'Digital Trust Maturity Survey', 2023
14. UK Government, 'Fraud Strategy', 2026-2029
15. Ofcom, 'Online scams and fraud research summary report', 2023
16. Ofcom, 'Understanding Online Financial Harm Literature Review', 2025
17. UK Government, 'National Security Strategy', 2025
18. UK Government, 'Fraud Strategy', 2026-2029
19. National Crime Agency, 'Summary of written evidence submitted by the National Crime Agency to Parliament', 2023
20. UK Government, 'Government leads global fight against deepfake threats', 2026
21. UK Finance, 'Annual Fraud report', 2025
22. Ofcom, 'Ofcom's approach to implementing the Online Safety Act', 2025
23. UK Government, 'Fraud Strategy', 2026-2029
24. Ofcom, 'Ofcom's approach to implementing the Online Safety Act', 2025
25. DRCF, 'Tackling Online Fraud and Scams', 2024
26. FCA, 'Business Plan', 2025
27. FCA, 'FCA tackling scams faster as part of data strategy', 2025
28. FCA, 'targeted and outcomes-based approach to tackling financial crime', 2025
29. UK Government, 'Fraud Strategy', 2026-2029
30. UK Government, 'Online Advertising Taskforce - progress report', 2025
31. UK Government, 'Fraud Strategy', 2026-2029
32. National Crime Agency, 'Summary of written evidence submitted by the National Crime Agency to Parliament', 2023
33. Stop Scams UK, 'Meta and Stop Scams members announce FIRE expansion', 2024
34. UK Government, 'Fraud Strategy', 2026-2029
35. City of London Police, 'Report Fraud service goes live with full public launch in January 2026', 2025
36. UK Government, 'Fraud Strategy', 2026-2029

Deloitte.

Together makes progress

Designed by CoRe Creative Services RITM2504615