Future of fraud

A UK view from the 2030s

August 2024

pwc

STOP SCAMS UK

Contents

Foreword by Stop Scams UK

The Scams Emergency remains a blight on society. For many, the experience of being scammed can be devastating, often tearing people's lives apart.

Scams do not discriminate. They affect us all, doing untold damage, eroding trust and shattering confidence throughout society.

When consumers hesitate to conduct online transactions for fear of deception, legitimate businesses lose revenue and the economy splutters. This fear can also discourage investment and innovation, hindering growth. A healthy economy relies on trust and confidence, with criminals determined to undermine that very foundation.

That's why we believe our work in this arena, particularly our Scam Intelligence project, is increasingly vital. Scammers are agile, constantly adapting their methods and techniques. We must build robust societal defences that are not only capable of addressing today's challenges but can also adapt to the threats of tomorrow and beyond.

The constantly accelerating pace of technological change further underscores this need. As we enter the next decade, our defences against fraud – individual, organisational, and societal – must remain agile and flexible to accommodate the evolving landscape.

This includes new payment methods, the constant development of communication networks, and the emergence of technologies like AI that can be harnessed both for good and nefarious purposes. We must also consider how best to safeguard future generations as they navigate an increasingly digital world.

Though change may not happen overnight, collective action is essential to set ourselves on the right path. This is a pivotal moment, with a new government shaping its agenda. Such a scenario presents a crucial opportunity to reinvigorate our collective fight against scams and place us on the path toward long-term success.

This report represents a significant step in that direction. Born out of a collaboration between Stop Scams UK and PwC, it builds upon the valuable insights gained from the House of Lords report "Fighting Fraud: Breaking the Chain", published by The Fraud Act 2006 and Digital Fraud Committee. We are grateful to Baroness Morgan of Cotes, who chaired that committee, for the insight, enthusiasm and expertise that she shared during her keynote speech at an event arranged by Stop Scams UK and PwC in June.

The discussion allowed us to leverage the expertise of Stop Scams UK members from across the banking, technology and telecoms space, as well as other industry and civil society specialists, to explore the potential scam landscape of the future and the key challenges we might face collectively. Importantly, the report from PwC proposes ambitious yet practical strategies to protect society from the harm caused by criminals who continue to exploit people through scams.

In this ever-evolving environment, cross-sector collaboration is paramount. By working together, sharing knowledge, and developing innovative solutions, we can create a more secure future for all and take strides towards stopping scams at source and instigating growth in the UK economy.

Ruth Evans,
Chair Stop Scams UK

STOP SCAMS UK

Introduction

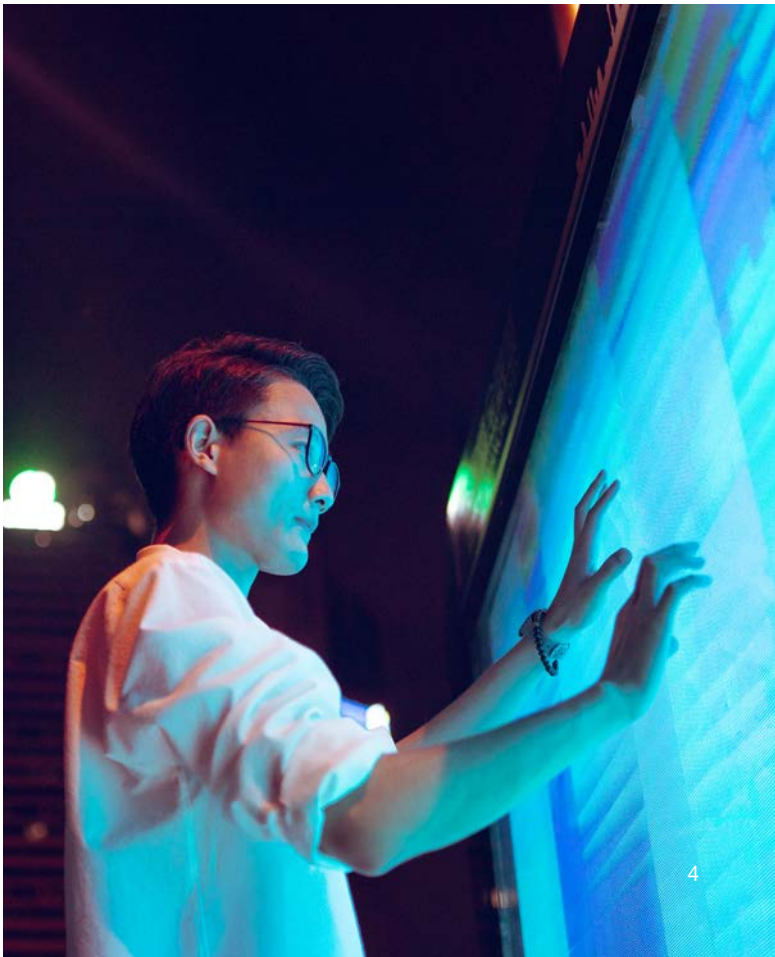
In 2024, fraud has been on leaders' agendas like never before. Banking and payments firms are preparing for the planned implementation of the Payment Systems Regulator's reimbursement regime on 7 October. Tech companies and telcos are delivering on commitments made in sector fraud charters. Across all industries, businesses are responding to new economic crime-related laws including the Online Safety Act and the Economic Crime and Corporate Transparency Act. In the UK, we also have a new government that made manifesto commitments to introduce an expanded strategy to tackle fraud threats.

In this milestone year, we have taken the opportunity to look to the future and consider what the next phase of such a UK fraud strategy might look like. In June 2024, in collaboration with Stop Scams UK, we hosted an event bringing together leaders from across industry sectors to discuss how fraud threats will likely evolve in the next decade and the ways that the cross-sector response needs to change. Our ambition for the event was to look beyond short term priorities and start to shape a view of what a holistic anti-fraud approach might look like.

While a lot of progress has been made to tackle fraud in recent years, there is a long way to go to solve the problem: nearly a quarter of a million people in the UK became victims of authorised fraud in 2023, with £459.7m getting into the hands of fraudsters[1]. If these statistics weren't troubling enough, evidence suggests that many frauds go unreported - as much as 86% according to the National Crime Agency. The objective of the event was to identify priority areas for change, recognising that the threat landscape will continuously evolve around us as fraudsters adapt their tactics, adopt emerging technologies and exploit new vulnerabilities.

The first section of this paper plays back the key themes discussed at the event to provide an industry view of priority changes.

The second half of the paper builds on the industry view and presents a hypothetical vision of the future threat landscape and what an ambitious but achievable national response to authorised fraud might look like in the 2030s. The intention of our imagined future is not to try and cover everything, but to pose ideas that provoke debate, many of which apply broadly across economic crime as a whole rather than just APP fraud. We hope that this paper sparks wider discussion, supports long-term thinking and contributes to debate on how the national response to fraud and economic crime can continue to be improved.



[1] https://www.ukfinance.org.uk/system/files/2024-06/UK%20Finance%20Annual%20Fraud%20report%202024.pdf

Industry perspective on the next decade

In June 2024, Stops Scams UK together with PwC's UK banking and payments fraud team convened a group of senior leaders from across industry to start to share a vision for a future-ready UK anti-scam framework. The event brought together 30 representatives from banks, technology companies and telcos as well as fraud experts and specialists from academia. Also attending were representatives from civil society groups and from government.

The aim of the event was to gather expert insight on the possible future fraud environment and to identify what changes will be needed in anti-scam approaches to meet future challenges effectively. A keynote address by Baroness Morgan of Cotes highlighted the importance of maintaining momentum in the fight against scams and cautioned against letting recent reductions in reported fraud lead to complacency, highlighting the issue of under-reporting and the speed at which threats are evolving.

Following the event, PwC and Stop Scams UK have worked together to draw out the key themes that were discussed. This section provides an overview of these key themes, focusing on ideas and solutions, to present an industry view of the areas of consensus to take forward into future strategy discussions.

A cross-sector conversation on the future of fraud threats

Industry and fraud experts attending the event agreed that the fraud threat landscape will evolve rapidly over the next decade, driven by the adoption of increasingly sophisticated technologies by fraudsters. Discussion focused on two key ways through which this evolution will manifest:

- Volume – The growing adoption of automation and generative AI tools by fraudsters will lead to an increase in fraud threat volumes over the next half of the 2020s. Technology will amplify fraudsters' ability to operate at scale, with fraud attacks deployed in volume using a range of channels simultaneously to reach potential victims.
- Sophistication – Technology will allow fraudsters to develop sophisticated scams that will become harder for consumers to recognise as malicious. Criminals will be able to create highly personalised approaches, using hyper-realistic deep fakes and voice clones and tailoring tactics based on personal information found online. Technology will also allow criminals to proactively probe business systems and processes to find weak links in the chain that can be rapidly exploited.

In combination, participants agreed that evolution across both these dimensions will make it harder for consumers to differentiate scams from legitimate content and that this will likely require service providers across all industry sectors to take more interventionist protective measures informed by detection techniques that can adapt rapidly to changing threats and scammer MOs.

Participants also highlighted how quickly criminals adapt to exploit new vulnerabilities, calling out risks around new payment methods and stores of value and the importance of building in safety by design. With protective measures on banking services becoming stronger, participants highlighted the risk that criminals will diversify their approaches to target other platforms that may be less well prepared, citing the rise in account takeovers in 2023 and the potential for fraudsters to target, for example, crypto-wallets where value can be quickly transferred into a scammer's control. Participants also discussed that while criminals have typically favoured targets in English-speaking countries due to more prevalent English language skills globally, highly accurate translation tools in combination with generative AI will make it easier to approach targets in other countries where scam awareness and defences may be less well developed.

Notwithstanding these agreed areas of evolution, participants highlighted that scam threats will continue to play on the same human vulnerabilities and that many existing protective measures - in particular scam awareness - will remain effective. Participants were confident that by building safety into platforms by design and developing a more cohesive whole system response, powered by collaboration and data sharing, it will be possible to significantly reduce scam losses.

Consensus areas for priority development

Throughout the discussion there was recognition of the successes that have been achieved to date, in particular the step change in collaboration across industry sectors that has been achieved since the start of the decade driven by organisations like Stop Scams UK as well as the government.

All participants agreed that a wide range of changes and interventions were needed and that the approach should be to support and incentivise the improvement of individual organisation's defences as well as strengthening industry level capabilities and hardening the ecosystem as a whole.

Three key themes ran across the industry discussion

01 A holistic response will be critical to building a secure anti-scam perimeter

Throughout the event, participants reiterated the importance of a whole system response and called out the importance of taking a 'whole of economic crime' perspective. A national response should bring together capabilities across all aspects of economic crime prevention, recognising that criminals do not operate within a scam 'silo'.

Coordinated centralised leadership will be required to deliver a cohesive overall response with participants highlighting the importance of private sector involvement in the design of the response as well as its implementation. Participants recognised the importance of government leadership and called out the need for genuine public-private partnership to tackle this challenge and for collaboration to expand at all levels of the ecosystem, including across international borders.

Key changes needed:

- System level leadership from government to drive a cohesive vision of a future-ready economic crime framework.
- Development of a longer term roadmap to develop national capabilities through public-private partnership, providing greater certainty on the direction of travel to support long-term private sector investment.
- Public-private partnership in the development of economic crime strategy and the design of anti-scam capabilities.
- Formal structures for collaboration across international borders, creating consistent channels to support intelligence exchange and cross-border interventions.

02 Data sharing will be central to powering interventions

Participants recognised the ongoing work to enhance data sharing initiatives, both between individual private sector organisations, across sectors and between public and private bodies. All participants agreed that this will be a critical enabler of impactful interventions. Participants recognised the good work that had been done to date to develop pilot schemes and build data sharing initiatives, but called out the need for a clearer vision for a target state set of future data capabilities and a roadmap to deliver these in a practical timeline. There was a recognition that this will require central system-level leadership and system design choices to be made by the government.

Key changes needed:

- Clear vision for system-level data sharing, including clarity around where strategic capabilities will be housed and how data will be made accessible to relevant organisations.
- Leadership by government and investment to build strategic data sharing capabilities designed so that they can be used by both public and private sector, across a range of use cases, to support secure and efficient operations to drive economic growth.
- Clearer guidance and principles to govern data sharing between institutions to give organisations greater confidence in safe channels of data exchange.
- Coordinated strategy to develop digital identity tools and standardised platforms to safely share information across institutions using privacy enhancing technologies.
- Investment in data science skill sets across the whole ecosystem and particularly in key institutions and law enforcement agencies that will act as hubs for the collection of economic crime data.
- Greater collaboration between law enforcement and the private sector to power effective interventions across the scam lifecycle, recognising that sharing of insights and intelligence will need to be two-way to create a force-multiplier effect.

03 Interventions will be required across the whole scam lifecycle

Following similar themes around the importance of a holistic response, participants raised the importance of everyone in the ecosystem playing their part to tackle scams.

Key changes needed:

- Interventions at every stage of the scam life cycle with all organisations represented having a role to play in terms of educating consumers, removing and blocking scam content, detecting suspicious activity and intervening to protect consumers where needed.
- Coordinated and cooperative efforts from online platforms, telcos, banks, payment firms and law enforcement to enable interventions that protect customers and disrupt fraudsters.
- Ensuring there are real consequences for criminals perpetrating scams, with international cooperation needed to ensure those operating abroad can not do so with impunity.
- Delivery of whole-life education to consumers to strengthen scam awareness with increased focus on digital and financial literacy tailored to different demographics and deployed across multiple channels.
- A more nuanced approach to assessing vulnerability to scams to allow organisations across both the private sector and law enforcement to make more targeted and effective interventions to protect individuals.
- Processes to ensure that new products, platforms and services provide fraud protections to users by design and allow for data and intelligence sharing across organisations.
- A greater focus on deterrence to discourage participation in economic crime activities, with the effectiveness of interventions being evidence-based and supported by academic research to ensure that protective measures and deterrents achieve their desired objectives.

Running across the changes proposed by the participants was the concept of putting pressure on fraudsters' margins by limiting their room for manoeuvre and forcing them to adopt increasingly complex and sophisticated methods to avoid detection. Participants agreed that, wherever possible, the ambition should be to place whole platforms and systems off limits to fraudsters to provide safe environments where businesses and consumers can operate with confidence, driving investment and growth.

Participants were optimistic that digitalisation of processes across all aspects of economic activity will support increasingly effective economic crime interventions by making more data available in real time and enabling interventions at greater scale through automation.

A hypothetical view from the 2030s

Introduction

In this section we envision how the scam threat landscape may evolve and we provide our perspective on key features of what an ambitious whole system response might look like by the 2030s. This section is fictional and is written from the perspective of the 2030s looking back on what could be achieved if we imagine that the changes recommended by industry at the June event are delivered. Our aim of writing from a future perspective is to focus on what could be achieved rather than the steps needed to get there.

Our imagined future is hypothetical, but has been informed by discussions at the June event as well as our wider conversations with clients and by our work to tackle fraud and scams in both the public and private sectors. We recognise that this is a highly complex problem and that we don't have all the answers, but we hope that our imagined future sparks ideas and provokes debate about the next stage of anti-scam strategy.

A new decade, evolved threats – Headlines from the 2030s

01 **Scam losses are in decline but still high**
In the early 2030s, scam losses reported by the finance industry have been c.£310m, down 50% compared to 2023 adjusting for inflation. Reported scam case numbers have fluctuated between 120,000 and 160,000 per year. Although the downward direction of travel has been positive, fraud is still the most commonly reported crime. The diversification of threats outside of traditional banking and payments has made capturing reliable data on fraud losses more complex. Victim support groups argue that fraud hasn't declined as much as the data suggests, it's just become harder to measure.

02 **Low value, high volume scam tactics**
Industry has been very successful at stopping high value scams, but has had to develop new approaches as fraudsters have adapted to high volume, low value tactics and micro-frauds. Low value frauds have proved hard to distinguish from normal customer spending with interventions being more difficult as customers demand low friction payment experiences. Operational costs of intervening in individual low value transactions are not always proportionate, but fraud losses across multiple payments can add up quickly.

03 **Platform choice determines exposure to threat types**
Criminals deploy different tactics for different groups in society based on how they behave online and the platforms they choose to use, often closely linked to age. Younger users typically favour platforms with anonymous online personas and criminals use tactics that encourage algorithms to promote highly personalised malicious content. Middle aged users typically use multiple platforms with public profiles kept separate from private profiles that are restricted to friends and family. Criminals use deepfakes to infiltrate these private personas and socially engineer victims from there. Older users more often document their lives online in public profiles and are more susceptible to personalised scams where fraudsters tailor content based on individual interests and recent experiences.

04 **Criminals expand activities on unregulated communications platforms**
The emergence of new fully virtual meeting places and metaverse spaces has also created new unregulated channels where criminals can approach potential victims adding to the highly diverse existing set of messaging channels further complicating monitoring activities.

05 **Criminals target diverse stores of value**
As protections around banking services have strengthened, scam threats have shifted to other stores of value and online platforms with digital wallets. Social media platforms and online shop fronts have integrated with non-traditional payment providers including 'points to pay' and earned content tokens. Professional and casual content creators earn points or create other stores of value online which can be redeemed for in app purchases, or cashed out at certain thresholds. Criminals targeted these stores of value through social engineering and account takeover.

06 **Business in the crosshairs**
Criminals have increasingly targeted businesses seeking larger returns. Professional fraudsters invest months researching a single business to locate points of vulnerability, using cyber attacks to gather information that can be used to tailor attacks. Continued cost of living pressures have presented opportunities for criminals to offer incentives to insiders for divulging confidential information. There have been a number of cases in the media where insiders have facilitated scams against their employers, underscoring the importance of insider threat monitoring and employment screening.

07 **Deepfakes and clones are pervasive in scams**
Deepfakes and voice clones have become pervasive across scams with fraudsters using cloned voices of known friends or family members. Older customers are particularly vulnerable as they have less exposure to the voice distortion and voice cloning that is commonplace on social media platforms with younger users.

08 **Fraudsters exploit real world events in near real-time**
Automation has also allowed criminals to respond to current events almost instantly. Criminals use automated monitoring to scan international news to identify current events that can provide a launchpad for a scam. Scam approaches are tailored to events and focused on specific groups and communities that may be vulnerable.

09 **Low barriers to entry have led to rising synthetic identity fraud**
Fraudsters combine identity theft techniques with the use of AI-powered document manipulation tools to fabricate fake identities to access services and lines of credit and to build covers for scams. Identity fraud 'how to' guides are easily accessible online, with automation enabling fraudsters to more quickly build credit histories and online profiles to establish genuine looking data footprints.

Consumer fraud awareness in the 2030s

01 **Aware, but apathetic**
Scam awareness is a mandatory part of the PSHE curriculum and there has been sustained public awareness campaigning with multiple initiatives being delivered by industry and the Government. Despite these campaigns, use of protective tools is uneven and consumer caution varies significantly. Some consumers, particularly those that have grown up with scam protections, are typically less cautious and willing to take a risk to get a good deal with low value purchase scams being rife.

02 **More than financial impacts**
Reimbursement and automated reporting has meant victims are more comfortable coming forward and reporting scams. Affected customers can report a scam and be reimbursed without ever interacting with a real person. This has speed up reimbursement timelines and reduced operational costs, but has led to more limited opportunities for personalised advice and education around avoiding future scams. Banks and other providers work with specialist service providers that can help customers address the emotional and psychological harm victims can experience, which have been exacerbated by the increasingly personalised nature of scammer tactics.

03 **Distorted reality**
Fully synthetic content and AI-enhanced media are ubiquitous across all aspects of society. Consumers expect to interact with synthetic content, and the use of deepfakes in itself is no longer a scam red flag. While consumers are more aware of synthetic content and platforms warn customers when it is detected, its ubiquity has made it harder to distinguish legitimate from malicious use.

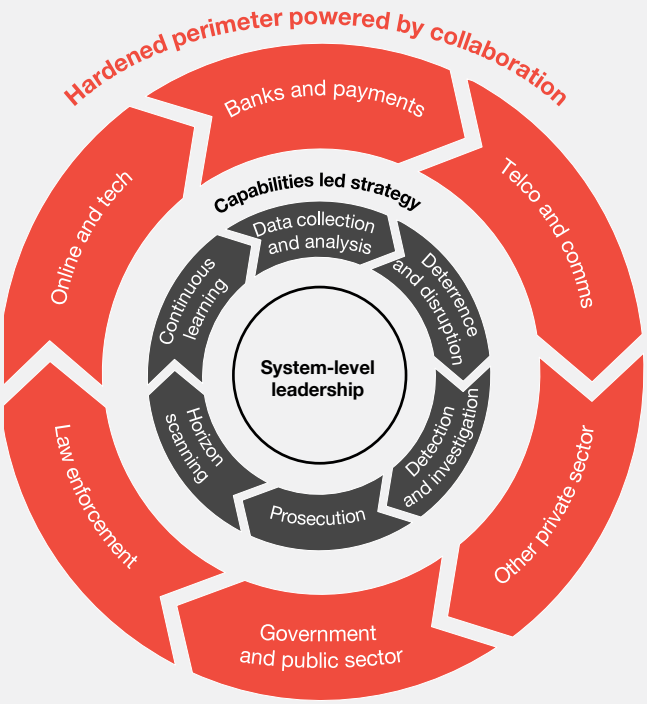
04 **Is the message getting through?**
Consumers are regularly warned about fraud risks when they are operating online and making payments, but this has led to 'message fatigue', and scrolling past generic cautions. Platforms have been trying innovative techniques, using behavioural science, to engage customers and trigger a response.

05 **Personalised banking**
Customers are encouraged to be proactive in communicating about upcoming payments and changes in their personal circumstances. Some banks have instituted 'warming in' periods for very large payments where notice needs to be given in advance to address the urgency tactic used by scammers. Service providers routinely check-in with customers through synthetic relationship managers to deliver a tailored customer experience and to support predictive modelling around vulnerability to scams.

A whole system response

The 2025 Economic Crime Strategy set out a vision for a future anti-scam framework built on a foundation of public-private partnership. Building on the achievements in the earlier half of the decade, the strategy sought to centralise leadership and oversight while also encouraging innovation and enabling the development of capabilities across every part of the ecosystem. The strategy defined the key capabilities needed to tackle present and emerging threats and set out a cohesive five-year roadmap to develop these building on existing systems, agencies and expertise.

The 2025 economic crime strategy



01 A national economic crime defence council provides system level leadership

The 2025 strategy announced the formation of a new public-private national Economic Crime Defence Council ('ECDC'). The objective of the ECDC has been to provide overall system leadership and to coordinate across the wide range of law enforcement agencies, government departments and private sector organisations involved in the anti-scam ecosystem.

A non-departmental government minister for Economic Crime chairs the ECDC, expanding on the 'Fraud Champion' role of the early 2020s. The ECDC provides governmental leadership and authority to drive change, but as a public-private partnership, recognises the importance of bringing industry into decision making about the national level response.

Fully operational by 2027, the ECDC consists of a permanent group of public sector and government representatives with members also drawn from a range of private industry sectors. Private sector representatives are nominated on an industry basis by the organisations they represent with new industries being brought into the ECDC as they grow in importance to the ecosystem.

Organisations like Stop Scams UK continue to provide forums where all relevant industry stakeholders can come together to share ideas and collaborate, feeding thinking into the ECDC via industry council members.

The ECDC also leads efforts to strengthen international collaboration. A biannual Global Fraud Summit has become a standing feature within the international community following the success of the first one held in the UK in 2024. The recurring summit meetings have been key to keeping open lines of dialogue between national governments and creating consistent lines of communication between responsible authorities.

By the early 2030s many other countries have established equivalent versions of the ECDC, providing clear lines of communication into national authorities responsible for coordinating anti-scam activities. This coordination has led in turn to cross-border intelligence sharing initiatives and joint policing operations targeting the largest international scams groups.

02 Strategic data capabilities are delivered through utilities built on a federated data model

The 2025 strategy set out a vision for a federated data model with key data capabilities provided by centralised utilities, operated by a range of public and private sector organisations. The federated data model allows for the proliferation of data sharing initiatives and platforms, tailored to the needs of different use cases and user groups. This approach has encouraged innovation and for players of all sizes to develop solutions to address specific challenges. This in turn has powered the growth of a world-leading economic crime data analytics and technology industry in the UK.

An open API model allows authorised public and private sector users to access relevant data sets and apply tailored analytics to support a wide range of use cases. Accessing the wide range of data points available to authorised public and private organisations through this collaborative framework supports fraud prevention and security while also reducing costs for individual organisations freeing up resources to invest in business growth.

Consistent standards and codes of practice for data sharing have been developed through the ECDC in collaboration with the Information Commissioner's Office. This has ensured that consistent principles for data sharing and standards of data security and governance apply across the ecosystem regardless of the different organisations that operate data sharing capabilities. This has supported consumer and industry trust in the overall framework and provided greater transparency as to how data is shared and the uses it is put to.

03 An economic crime command centre brings together private sector data capabilities and law enforcement to drive innovation

At the centre of the federated data model is a new Economic Crime Command Centre ('E3C'). Operated as an arms-length government body overseen by the ECDC, E3C brings together data science and analytical experts from a range of industries and law enforcement. E3C was established on the principle that bringing technical experts from different organisations together would encourage cross-pollination of ideas, a better understanding of what data each organisation holds and how it might be useful to others and the creation of trusted relationships that would create stronger longer-term connectivity across sectors.

Tech companies, telcos and banks have supported the formation of E3C by providing expert staff on rotating secondments. Funding for E3C is drawn from money that has been frozen due to economic crime concerns and by contributions by private sector organisations through the provision of resources, technology and infrastructure.

Consistent leadership is provided by a permanent team drawn from the National Crime Agency and City of London Police. E3C has acted both as an investigation hub as part of the pursuit of large scale criminal gangs, and also as an innovation centre identifying new ways to combine data to enable rapid responses to emerging risks and to provide insight to the wider anti-scam ecosystem.

04 Policing and the criminal justice system

Funded through a ring-fenced budget, an expanded national fraud force provides specialist support to anti-fraud policing. Led by the City of London Police, the national fraud force has teams deployed alongside the Regional Organised Crime Units. Specialist anti-fraud officers coordinate policing action with performance measured against national fraud crime statistics.

Police responses to fraud have become increasingly data-led, powered by the analytical capability within the Fraud Intelligence Bureau ('FIB'). The FIB operates the national fraud reporting system which contains powerful analytical capabilities to surface intelligence and support prioritisation of targeted policing activity.

Combined with the data science expertise with E3C, specialist fraud investigators have been able to take precision actions to target criminal gangs to disrupt their business models.

A network of specialist economic crime courts have been established across the UK building on the model of the Central London Economic Crime Court. Specialist judges oversee fraud cases with legislation to modernise fraud offences enacted in the late 2020s following the Fisher Review. This has led to accelerated outcomes and more consistent sentences in fraud cases.

Evolving capabilities in the private sector

Banks and payment firms

Banks and payment firms have committed sustained investment over more than a decade to transform their capabilities to prevent and detect fraud and scams. Regulators are increasingly assertive in their supervisory capacity when monitoring fraud capabilities and have increasingly taken enforcement action where performance information indicates that firms are not effectively protecting their customers.

While spending on counter-fraud increased during the mid-2020s as firms replaced legacy systems and prepared for the new regulatory regime, new technologies leading to better prevention and detection rates have delivered positive returns on investment in the latter half of the decade as reimbursement costs have declined.

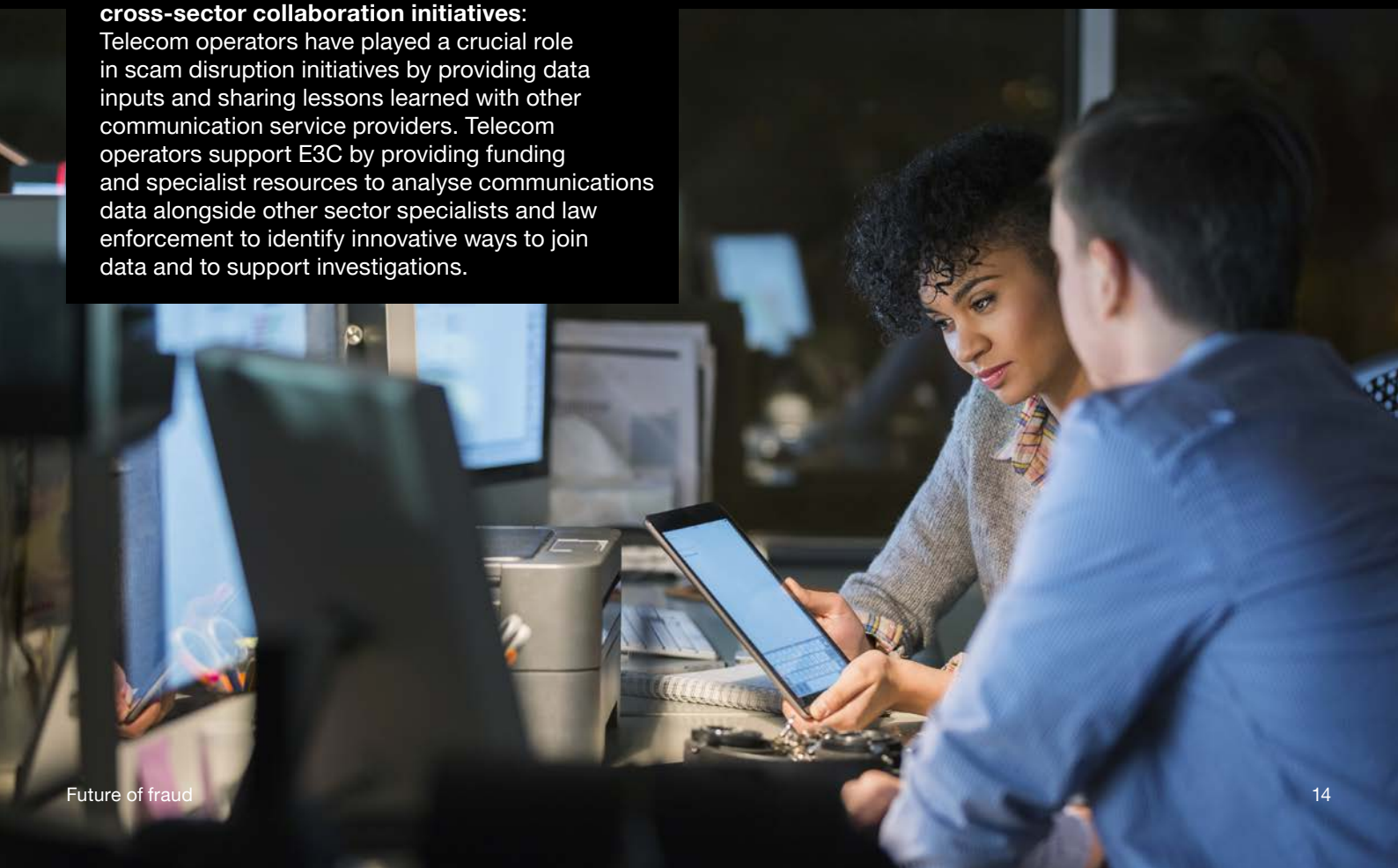
- **Increasingly sophisticated scam detection models**:
  Banks are deploying increasingly sophisticated risk detection systems that identify scam risk at the point of payment based on individual customer behaviours. Banks draw on a range of data sets available through the federated data model and provided by data utilities to enrich risk detection. Investment has concentrated in this area with the aim of providing the best possible protections to customers and as the most effective way of managing downstream fraud reimbursement claim costs.
- **Cross-industry data sharing through the federated data model:**
  Working through the ECDC and driven by innovation led by E3C, banks increasingly ingest data from tech companies and telcos to detect risks of certain scam types. Following a successful pilot in the mid 2020s, social media platforms now share scam signals and information about users that have accessed suspected scam content which is matched to bank account holder details to inform payment risk modelling. Privacy-enhancing technologies are used to securely share information between institutions.
- **Leveraging the payments architecture to tackle economic crime**:
  The phased introduction of the new payments architecture and the adoption of ISO20022 has standardised enhanced payment messaging across UK payment systems. Building on the enhanced fraud data standard, vendors now offer a suite of overlay services that provide analytics capabilities over networked money flows across multiple institutions. An open API model enables banks and payments firms to access payments data analytics to support transaction risk scoring, the investigation of suspect payment flows and funds tracing and recovery. In combination with existing bilateral and consortia data models, this approach has driven significant improvements in the detection and interdiction of the money flows that follow a successful scam.
- **Increasing interventions in payment journys:**
  Risk detection systems are now used to drive precision warning messages to customers at the point of payment. Warning messages, designed by behavioural scientists, are interactive and delivered through a range of means, tailored to each customer to drive maximum engagement. Virtual service agents are used to speak with the customers where payments are flagged as risky, with a range of risk detection techniques such as voice analytics used to enable decisions to be made to either clear payments for release or directing customers to speak to human fraud specialists.
- **Money mules under pressure:**
  Banks have invested in capabilities to model payment networks to detect flows of fraudulent funds through money mule rings. Network analytics tools are in widespread use, drawing on transaction information made available either through consortia models and access to centralised payment scheme data. Growing adoption of data-driven ‘perpetual KYC’ approaches has led to better quality data about bank customers, in turn driving better monitoring for money mule activity.

Communications systems

- **Telecom networks increasingly off-limits to fraudsters**:
  Telecom operators have continued and extended their efforts to identify and block fraudulent calls and messages over their networks, with increasingly sophisticated capabilities deployed to identify malicious content and communications patterns. Coordinated action by network operators, law enforcement and the National Cyber Security Centre has led to highly effective blocking of mass smishing attacks and scam calls on telephone networks. Criminals continue to probe for weaknesses in spam filtering logic, using automation to pressure-test defensive systems to locate and exploit weaknesses.
- **Mobile handsets provide built-in security features for consumers:**
  Handset providers increasingly offer built-in functionality to analyse incoming calls to alert users where voice calls or messages may be fraudulent. Handsets incorporate authentication functionality whereby inbound calls are 'signed' by the caller using the biometric security features on their devices. This signature is recognised by the receiving handset giving the user confidence that the caller is genuine.
- **Businesses deploy surveillance technology to screen communications for scams**
  Large organisations deploy added surveillance tools across certain employee communications devices to detect patterns that may be indicative of scams. Alerts are routed to Monitoring and Compliance functions for review and intervention where required.
- **Communications platforms support cross-sector collaboration initiatives**:
  Telecom operators have played a crucial role in scam disruption initiatives by providing data inputs and sharing lessons learned with other communication service providers. Telecom operators support E3C by providing funding and specialist resources to analyse communications data alongside other sector specialists and law enforcement to identify innovative ways to join data and to support investigations.

Online platforms

- **Measures to block fraudulent content online improve:**
  Larger online platforms have continued to invest in capabilities to identify and block suspect content. They employ sophisticated machine learning models trained on historical scam data to recognise patterns and characteristics common to fraudulent activities. These models enable real-time detection and response, allowing immediate action to warn users or block suspect content. Platforms prevent users from creating new accounts where they have previously been removed due to fraud.
- **Identity verification increasingly integrated into platforms**:
  Online platforms have integrated digital identity solutions to allow users to verify their identity and appear as trusted users, regardless of whether they present online under a persona, or themselves.
- **On-platform payments:**
  To provide a secure transaction environment, tech companies have introduced in-platform, closed-loop payment systems. These systems offer a secure way for customers to make payments within the platform. While the use of these payment systems remains optional, their adoption rate has been impressive. Despite their security benefits, these systems are not immune to fraud. There have been instances where criminals have targeted these payment systems, attempting account takeovers to access stored credit. Criminals also commonly use social engineering techniques and promises of 'better deals' if targets send payments directly, often through crypto exchanges or using non-traditional payments such as exchanging metaverse coins.



Conclusions

Developing an effective scam response is both an ethical and economic imperative. As well as protecting consumers from the significant emotional and psychological harms that scams can cause, more effective scam responses will support trust and build confidence in business process, prevent money from being lost from the legitimate economy and drive efficiencies by leveraging the force-multiplier effect of many organisations working together in concert to tackle economic crime.

While we can be sure that scammers will continue to try to steal money and that they will use ever more sophisticated techniques to do so, we can also be sure that industry will continue to innovate and develop ever more powerful anti-scam capabilities. Collaboration across industries has never been greater and while current and emerging threats are severe, we should be confident that it is possible to turn the tide on scams and place whole systems and platforms off-limits to fraudsters.

Below we set out our view of priority areas of focus for government and industry to develop strategies to deliver this ambition:

Government

There is an opportunity for the next phase of national fraud strategy to set out a cohesive vision for a whole system response to economic crime and a roadmap to achieve it. Such a strategy should:

- Define how system-level leadership will be provided to bring together the diverse stakeholders involved in the fraud ecosystem.
- Set out how collaboration across public and private sectors will be supported and expanded and how everyone in the ecosystem can be best encouraged to play their part to tackle scams.
- Articulate the capabilities needed now and into the future to tackle current and emerging threats and how these will be developed and continually evolved.
- Accelerate data sharing to support economic crime prevention and the development of best-practice system-level data sharing design choices to support private sector investment.

Industry

Individual organisations equally need to develop long-term strategies to ensure they have the capabilities to protect their customers and their organisation from fraud now and into the future. Organisations need to consider how to:

- Monitor fraud risks in the context of changing business processes, evolving customer behaviours and emerging threats.
- Create joined-up capabilities that break down internal data silos to provide richer insight across the organisation to improve fraud detection.
- Leverage technology and automation to improve efficiency and enable specialist resources to be concentrated on the highest impact areas.
- Participate in industry collaborations to share insight, learn from leading practice and connect into technology and data initiatives.

The authors

PwC UK's banking and payments fraud team

Harry Holdstock

Fraud & Regulatory Protection leader

harry.g.holdstock@pwc.com

Alex West

Banking and payments fraud leader

alex.e.west@pwc.com

Francesca Belletty

Fraud and financial crime specialist

francesca.belletty@pwc.com

Hannah Bergin

Banking fraud specialist

hannah.f.bergin@pwc.com

Isla Hamilton

Banking fraud specialist

isla.hamilton@pwc.com

RITM0094968