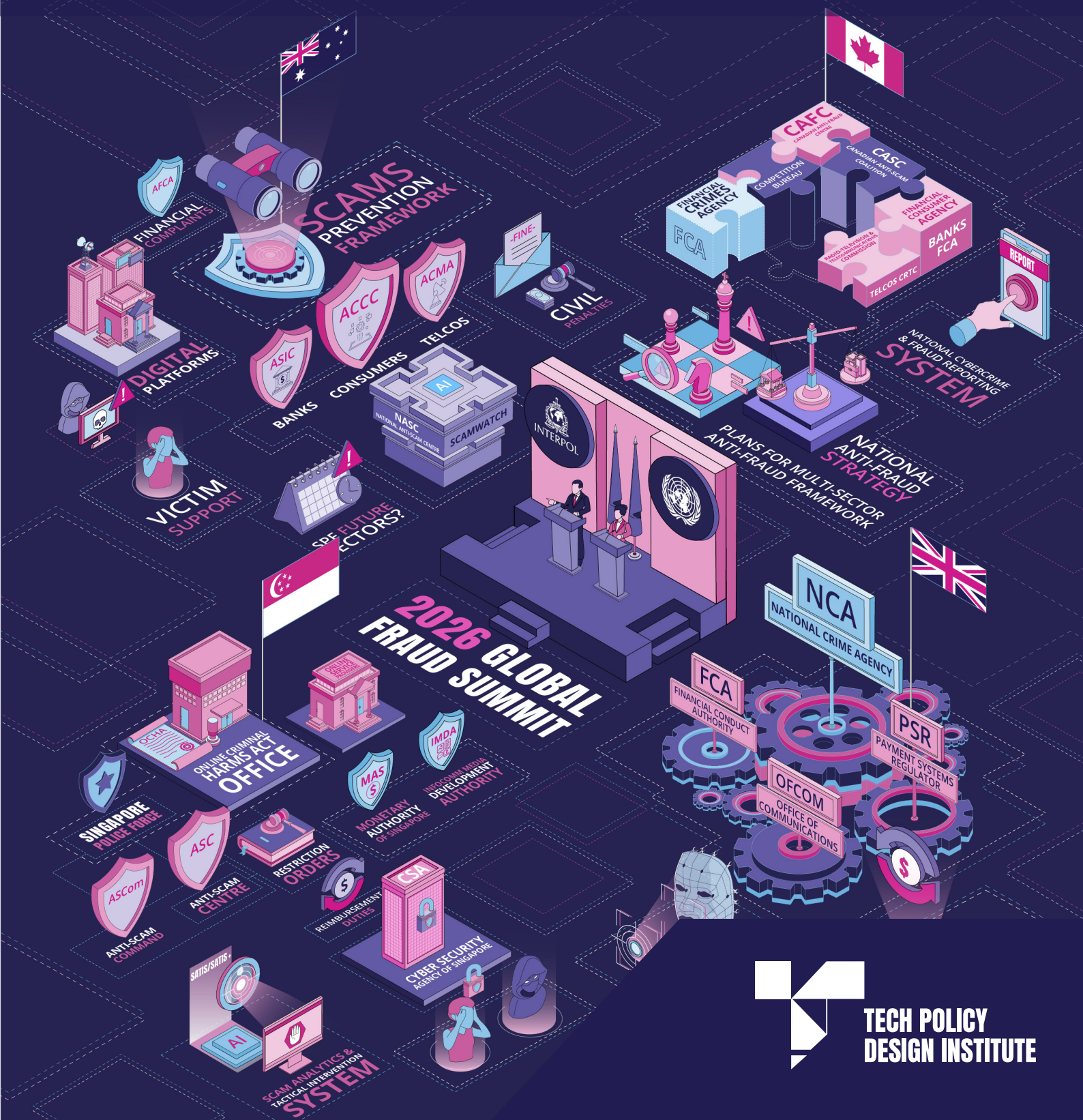
COUNTERING AI-ENABLED SCAMS

NOVEMBER 2026

Insights from Australia, Canada, Singapore & the United Kingdom



TECH POLICY DESIGN INSTITUTE

ABOUT THE TECH POLICY DESIGN INSTITUTE (TPDi)

TPDi is an independent, non-partisan think tank committed to advancing best practice technology policy in Australia and globally. Based in Canberra, TPDi is registered as a not-for-profit with the Australian Charities and Not-for-Profit Commission. TPDi collaborates with all stakeholders in the tech ecosystem. Our mission is to shape technology for the benefit of humanity. We do this through rigorous research, innovative education, evidence-based public commentary, and community building.

Acknowledgements

We are grateful to the 4 country chapter authors of this report (listed below), and to the experts and organisations who contributed their time and expertise to peer review the draft report: Benjamin Ang, S. Rajaratnam School of International Studies; Christiane Gillespie-Jones, Australian Telecommunications Alliance; Ardi Janjeva, Alan Turing Institute; John Matheson, Reset Tech; Australian Competition and Consumer Commission; Australian Government Treasury; Consumer Action Law Centre and Microsoft. While developed through a collaborative process, the final report, assessment, analysis and all outcomes represent solely the views of TPDi and the authors.

This report was made possible by the support of Microsoft. TPDi retains full independence over our research and complete editorial discretion of outputs.

Illustrations are by Guilhermo Clerch. Report typeset and design is by GRiD. Copyediting by The Write Path. Generative AI tools were used in a limited capacity to assist with summary and editing processes. All arguments, analysis, findings and final content in this report reflect the views and work of TPDi and the authors.

Independence statement

TPDi's independence is our most valuable asset. As a registered not-for-profit, our work is supported by external funding. We only accept funding from entities that agree to be disclosed publicly and commit to respect and promote TPDi's independence. TPDi does not represent the views of any of our funders. All outputs represent solely the views of TPDi and/or the authors.

Authors

Thomas van der Valk, Senior Fellow, TPDi

Keldon Bester, Executive Director, Canadian Anti-Monopoly Project & Fellow at Centre for International Governance Innovation and Curtis McCord, Policy Analyst, Canadian Anti-Monopoly Project

Helena Yixin Huang, Associate Research Fellow, S. Rajaratnam School of International Studies

Isabella Wilkinson, Senior Research Fellow, Chatham House

Edited by Zoe Jay Hawkins, Co-Founder, TPDi.

Citation

Hawkins ZJ (ed) (2026). *Countering AI-enabled scams: insights from Australia, Canada, Singapore and the United Kingdom.* Tech Policy Design Institute.

ISBN 978-1-7649583-1-8 (print)

ISBN 978-1-7649583-2-5 (online PDF)

Contact

Tech Policy Design Institute
www.techpolicy.au
hello@techpolicy.au
ABN: 94 681 576 394

Charity status

TPDi is registered as a not-for-profit with the Australian Charities and Not-for-profits Commission.

Copyright

This work is licensed under CC BY-NC-ND 4.0.
To view a copy of this licence, visit:
https://creativecommons.org/licenses/by-nc-nd/4.0/

CONTENTS

FOREWORD iii

EXECUTIVE SUMMARY 1

THEMES AND TRENDS 3

JURISDICTIONS AT A GLANCE 6

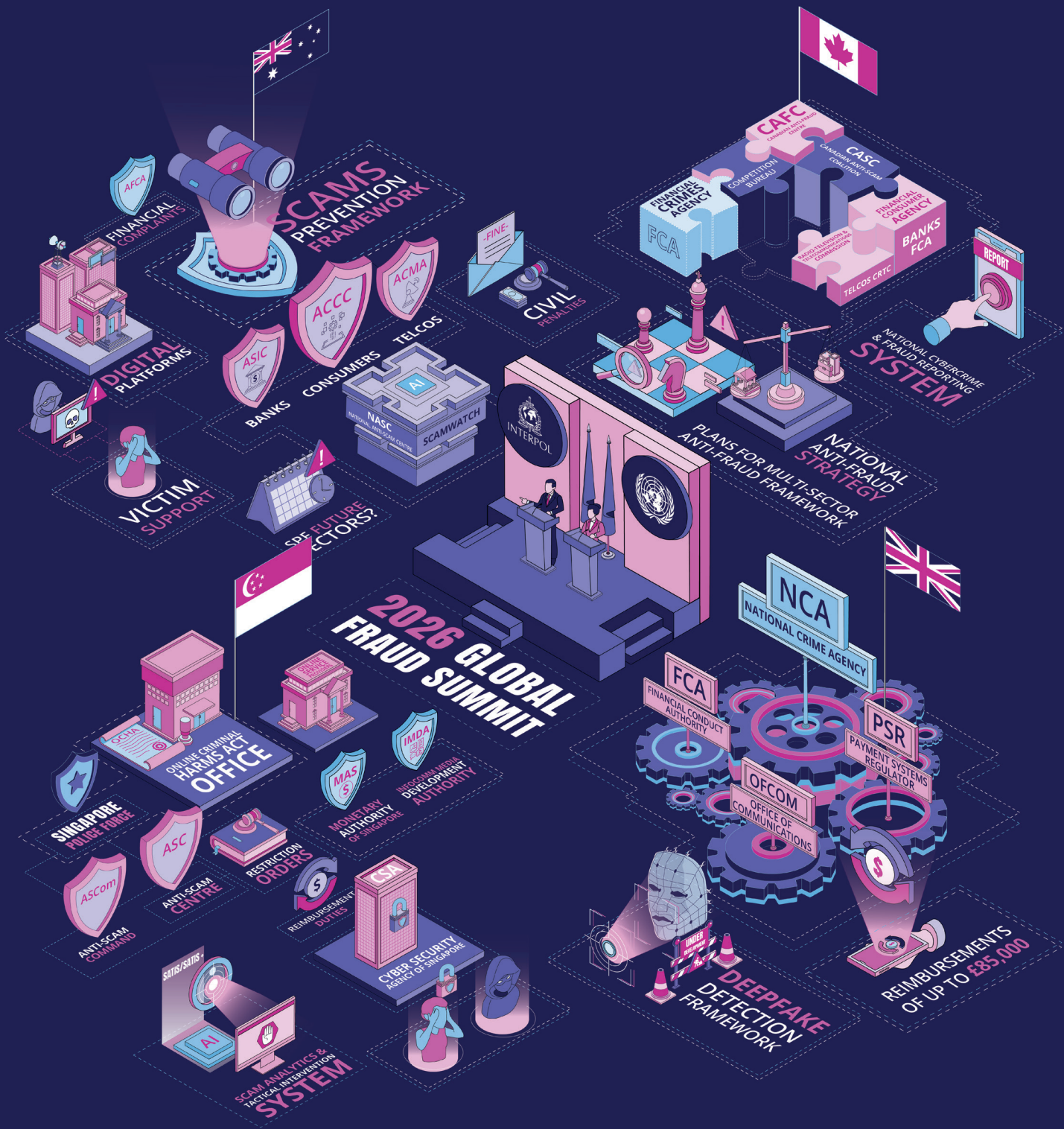
- Australia 7
- Canada 13
- Singapore 18
- United Kingdom 23

CONCLUSION 28

APPENDIXES 29

- Appendix 1: Australia 30
- Appendix 2: Canada 32
- Appendix 3: Singapore 33
- Appendix 4: United Kingdom 35

REFERENCES 36


2026 GLOBAL FRAUD SUMMIT
SCAMS PREVENTION FRAMEWORK
AFCA
FINANCIAL COMPLAINTS
DIGITAL PLATFORMS
ACCC
ACMA
ASIC
BANKS
CONSUMERS
TELCOS
-FINE-
CIVIL PENALTIES
AI
NASC
SCAMWATCH
VICTIM SUPPORT
SPF FUTURE SECTORS?
CAFC
CASC
FINANCIAL CRIMES AGENCY
FCA
COMPETITION BUREAU
FINANCIAL CONSUMER AGENCY
BANKS FCA
TELCOS CRTC
REPORT
NATIONAL CYBERCRIME & FRAUD REPORTING SYSTEM
INTERPOL
PLANS FOR MULTI-SECTOR ANTI-FRAUD FRAMEWORK
NATIONAL ANTI-FRAUD STRATEGY
ONLINE CRIMINAL HARMS ACT OFFICE
SINGAPORE POLICE FORCE
IMDA
MAS
MONETARY AUTHORITY OF SINGAPORE
INFOCOMM MEDIA DEVELOPMENT AUTHORITY
ASCom
ANTI-SCAM COMMAND
ASC
ANTI-SCAM CENTRE
RESTRICTION ORDERS
REIMBURSEMENT DUTIES
CSA
CYBER SECURITY AGENCY OF SINGAPORE
SATIS/SATIS+
AI
SCAM ANALYTICS & TACTICAL INTERVENTION SYSTEM
NCA
NATIONAL CRIME AGENCY
FCA
FINANCIAL CONDUCT AUTHORITY
PSR
PAYMENT SYSTEMS REGULATOR
OFCOM
OFFICE OF COMMUNICATIONS
UNDER SURVEILLANCE
DEEPFAKE DETECTION FRAMEWORK
REIMBURSEMENTS OF UP TO £85,000

FOREWORD

Artificial intelligence (AI) can be a force for good, but it is also supercharging deception at unprecedented speed and scale.

AI-enabled scams are proliferating, with devastating financial and psychological impacts on individuals, communities and businesses around the world.

Cyber criminals use AI tools as force multipliers – creating deepfake videos, voice clones, fraudulent websites, and high-quality spear phishing emails that are harder than ever to detect. AI enables criminals to scale high-quality deceptions and lowers the barriers to entry for scam activity.

No country can fully solve this challenge alone.

These AI-enabled scams are rarely isolated incidents; they are often the work of organised international crime syndicates operating through industrialised 'scam compounds'. These threats are typically transnational, so they require deep international cooperation between law enforcement and intelligence partners.

However, law enforcement is only one piece of the puzzle.

To build resilience to scams, we must answer critical questions. **How can scams be prevented through public, business and governmental awareness and action? How can scams be disrupted? And how should consumers who have become victims be supported?**

As every country grapples with these questions, it is vital to learn from international best practices.

This report provides a comparison of 4 illustrative jurisdictions – Australia, Canada, Singapore and the United Kingdom.

Each jurisdiction chapter in this report has been authored by a policy expert based in that country. Emerging best practices include cross-sector approaches, real-time intelligence sharing and victim reimbursement.

The most effective responses increasingly recognise that combating scams is a shared responsibility. Banks, telecommunications providers, digital platforms, governments and consumers all have a role to play. By collaborating across sectors and borders, we can build scam-resilient societies.

The challenge posed by AI-enabled scams will continue to evolve. The task is to make sure our institutions, industries and policy frameworks evolve with it.

We hope this report serves as both a practical benchmark and a catalyst for action.

Johanna Weaver

Johanna Weaver
Co-Founder
Tech Policy Design Institute

Zoe Jay Hawkins

Zoe Jay Hawkins
Co-Founder
Tech Policy Design Institute

EXECUTIVE SUMMARY

Scams are becoming faster, smarter and harder to detect. The global statistics tell this story. Australians made 481,523 reports of scam incidents in 2025, with financial losses totalling over A$2.18 billion. Scams and fraud cost the UK economy over £14 billion in 2025, with one in 14 individuals and one in 4 businesses becoming victims.[1]

Each jurisdiction has a slightly different definition of scams, detailed in the respective country chapter. A common international conceptualisation centres on technology-facilitated deception. The United Nations Development Programme (UNDP) broadly characterises them as 'deceptive activities that use digital technologies to trick individuals into disclosing sensitive information or transferring funds'.[2]

Scams are a subset of fraud. Generally, a scam has an element of victim deception, whereas fraud can also occur without the victim taking an active part, such as card-not-present fraud, for instance when an unauthorised payment is made with stolen card details. This report is focused on 'scams' and only uses the broader term of 'fraud' when referencing specific a policy approach, legal framework, official report or research that frames it as such. We refer to 'AI-enabled' scams to describe when AI is used to support, scale and accelerate scam development and deployment.

The rapid scaling of generative AI is a force multiplier for scam activity. In their 2025/2026 Annual Cyber Threat report, the Australian Signals Directorate states that recent advancements in AI have amplified the effectiveness of social engineering techniques.[3] Criminals use AI to generate high-quality videos, fake voices, websites, know-your-customer records and spear phishing emails.[4] AI is also used to create fake documents and fake personas on social media and dating platforms.[5] Agentic AI systems can even autonomously plan and execute complete scam campaigns. INTERPOL has warned that AI-enhanced fraud is 4.5 times more profitable than traditional methods of fraud.[6] Part of the policy challenge is that these same AI technologies are also important tools for scam prevention and disruption, helping identify suspicious campaigns at scale and detecting fraudulent account activity. While jurisdictions are investing in specialised capabilities to fight AI-enabled scams, legislative frameworks are generally aimed at tackling scams regardless of the technology used by scammers.

This report identifies **emerging trends and best practices** in scam prevention and disruption through a comparison of 4 illustrative jurisdictions: Australia, Canada, Singapore and the United Kingdom (UK). Each jurisdiction profile has been authored by an **in-country policy expert**, providing an evidence-based assessment of domestic policy settings, implementation challenges and future reform directions. Together, these perspectives reveal where international consensus is emerging and where approaches continue to diverge.

The jurisdiction mapping reveals 3 key emerging focus areas:

- **Multi-sector approaches.** Siloed, reactive law enforcement is no longer sufficient; instead, resilience depends on a multi-sector response that imposes shared responsibilities across sectors such as banking, telecommunications, digital services and potentially others.
- **Public–private cooperation and intelligence sharing.** The most effective models are expanding the focus to intelligence-led disruption across the private and public sectors. Governments, non-government organisations (NGOs) and multinational companies are working to elevate this cooperation to the international level. Operational partnerships and secure information-sharing mechanisms are becoming central to this approach.

- **Victim support.** Jurisdictions are taking different approaches to reimbursing scam victims, including whether reimbursement is mandatory or simply a policy expectation, the losses covered, and the thresholds that apply. The UK has in force a *mandatory* reimbursement regime for eligible authorised push payment fraud, with claims covered up to £85,000. Australia's Scams Prevention Framework introduces reimbursement liability for regulated entities, and the government is proposing a *policy expectation* of automatic reimbursement for verified scam losses below A$3,000. Appropriate safeguards remain important to protect reimbursement processes from abuse and maintain incentives for scam prevention.

The report provides **detailed jurisdiction profiles** laying out the specific approaches and characteristics of each country to tackling AI-enabled scams.

Jurisdiction	Key features
Australia	The **Scams Prevention Framework (SPF)** establishes a whole-of-ecosystem approach with mandatory obligations for banks, telecommunications and designated digital platforms to take effect from 1 March 2027, with other sectors foreshadowed to follow. The National Anti-Scam Centre (NASC) brings together public and private entities as the central coordinator. Separately, Australia operates **fusion cells** that combine government and private sector expertise for rapid intelligence sharing and the disruption of specific fraud types, including scams. The jurisdiction is also proposing a policy expectation that automatic **reimbursement** for verified scam losses under A$3,000 could be appropriate.
Canada	Canada's current approach relies heavily on **criminal law enforcement** but lacks a centralised authority to coordinate across sectors. To address this, the government is developing a **National Anti-Fraud Strategy** to create a multi-sector framework involving banking, telecommunications and digital platforms. While currently nascent and relatively disaggregated, the proposed strategy aims to close **liability gaps** that currently leave consumers with limited recourse.
Singapore	Follows an **ecosystem-based approach** that prioritises **early disruption** through the Anti-Scam Centre (ASC), where bank representatives are co-located with police to freeze bank accounts rapidly. The **Online Criminal Harms Act 2023 (OCHA)** grants the government power to issue Implementation Directives requiring platforms to proactively counter impersonation and fraudulent advertisements. The strategy emphasises **platform accountability** and the use of tools like ScamShield for reporting.
United Kingdom	The UK employs a **multilayered approach** featuring strong industry coordination and a **reimbursement regime** for authorised push payment (APP) fraud up to £85,000. The UK is investing in deepfake detection standards. However, experts note that law enforcement requires better resourcing to handle the **speed and scale** of AI-enabled threats.

The comparison between jurisdictions makes clear that AI-enabled scams are a global systemic threat to trust in the digital economy. This report can be used to identify policy gaps, prioritise cross-sector obligations, and accelerate cooperation between government and industry, both within jurisdictions and at international level.

THEMES AND TRENDS

Emerging international trends

International consensus is emerging that scams should be treated as a transnational organised crime and public–private coordination issue, not merely a domestic consumer protection challenge. As AI supercharges the ability of crime syndicates to scale deceptions, jurisdictions are adopting best practices centred on intelligence-led disruption and shared cross-sector responsibility.

Legislative interventions. International best practice is moving toward comprehensive legislative frameworks with mandatory obligations related to the entire scam lifecycle. Australia's Scams Prevention Framework (SPF) is the most comprehensive framework legislated to date and will impose baseline governance and specific mandatory code obligations on banking, telecommunications and certain digital platform services (taking effect March 2027).[7] Singapore's Online Criminal Harms Act (OCHA) provides the government with the narrower power to issue Implementation Directives to online service providers, requiring them to proactively counter impersonation content and fraudulent advertisements.[8]

Public–private cooperation and intelligence sharing. Effective disruption requires cooperation between government and industry. Operational innovations like Singapore's Anti-Scam Centre (ASC), which co-locates major bank representatives with police officers, can be considered a model for rapid fund tracing and freezing.[9] Australia's 'fusion cells' – agile units that combine government and private expertise to target specific threats like investment or job scams – demonstrate a best practice for high-intensity, intelligence-led disruption.[10] The trend is moving toward high-frequency, secure data-sharing systems that allow for the real-time exchange of scam signals and action across agencies and industries.

International cooperation. Because many scam threats originate from industrialised scam compounds in other jurisdictions, including the exploitation of human trafficking victims, international interoperability is critical from both a human rights and counter-scam perspective. Best practice involves deep integration with INTERPOL mechanisms, such as the Global Rapid Intervention of Payments (GRIP),[11] and participation in regional multilateral initiatives like FRONTIER+, a cross-border platform for real-time intelligence sharing among 14 jurisdictions active across the Indo-Pacific and Canada.[12] Furthermore, jurisdictions are seeking to lead on global standards for deepfake detection to ensure that anti-scam capabilities keep pace with evolving AI techniques.

Victim support. There is a growing trend toward reimbursement models to support victims and to incentivise private sector prevention. The UK's Authorised Push Payment (APP) fraud reimbursement regime requires banks to compensate victims of AAP fraud up to £85,000 under certain conditions.[13] The Australian Government has proposed a policy expectation that entities regulated by the SPF should automatically reimburse scam victims for verified losses under A$3,000 to ensure consumer protection goals while supporting quick resolution and minimising the cost of investigating complaints.[14] More significantly, consumers will be able to seek compensation for their scam losses, regardless of the amount, where businesses have not met their obligations under the SPF.

Singapore's liability system is based on a 'waterfall approach' where financial institutions first, followed by telcos, are expected to bear the full loss if they fail in their obligations such as providing warnings. If they did fulfill their obligations, the consumer bears the liability.[15] Singapore allows for police to issue Restriction Orders to banks to prevent victims of scams from transferring money.[16] Key areas of attention are risks involved with fraudulent claims for reimbursement, follow-on scams where malicious actors impersonate organisations that assist with reimbursements, and a potential for reduced vigilance.

Risks

- **Over-disruption.** Experts caution that these policy approaches must address the risks of over-disruption, where aggressive blocking measures inadvertently harm consumers by stopping legitimate payments or removing valid content. Additionally, Singapore's use of Restriction Orders to temporarily freeze accounts of ongoing scam targets highlights a tension between state intervention and individual financial autonomy. Ultimately, the international trend is towards a focus on early disruption – preventing, detecting and stopping scam activity before losses are fully realised. Purpose limitation for information sharing, accessible review and appeal, and monitoring of false positives are examples of important mitigations against over-disruption.
- **Complexity.** Multi-sector approaches, by definition, bring multiple entities into frame as responsible for preventing and responding to a scam incident. Where duties are allocated without clear thresholds and close coordination between regulators, shared responsibility can raise compliance costs and redistribute liability without a corresponding reduction in consumer harm.
- **Jurisdiction challenges.** A common challenge across countries is ensuring that multinational companies from other jurisdictions, such as digital platforms, effectively comply with local laws. As multinational digital platforms are brought into scope of national laws to counter scams, they will increasingly need to adjust their global policies and practices to requirements specific to the respective jurisdictions they are operating in.

Key multilateral initiatives

Countries are increasingly framing scams as a transnational organised crime challenge that requires multilateral cooperation. Examples of key multilateral forums and cross-sector initiatives involving Australia, Canada, Singapore and the United Kingdom are listed below.

International norm setting

- **UNODC-INTERPOL Global Fraud Summit** (Vienna, March 2026). A pivotal event co-sponsored by country sponsors Canada, Singapore and the UK that resulted in a Call to Action to Combat Fraud and a Public–Private Partnership (PPP) Framework endorsed by over 100 organisations.[17]
- **Industry Accord Against Online Scams and Fraud.** A selection of 11 multinational tech companies signed the voluntary Industry Accord Against Online Scams and Fraud at the UN Summit, to unify collective capabilities in fighting global scammers.[18]
- **G7, Organisation for Economic Co-operation and Development (OECD) and Council of Europe.** These bodies provide international guidance on content integrity and standards for AI.[19]

Operational law enforcement and asset recovery mechanism

- **INTERPOL.** Operates the Global Complex for Innovation based in Singapore and the GRIP mechanism, which has successfully recovered millions in stolen funds.[20]
- **ASEAN.** Singapore and Australia are leading key initiatives to combat the cybercrime and scam syndicates destabilising the ASEAN region.[21]

Cross-sector information sharing

- **Global Signal Exchange.** Launched in 2024, the Global Signal Exchange enables cooperation between business, civil society and government to take on bad actors and protect consumers from scams and fraud through sharing abuse data and related signals.[22]
- **Five Eyes.** Intelligence and law enforcement partners from this network issue specific warnings regarding how AI is rapidly transforming cyber risk, including in Australia, Canada and the UK.[23]
- **FRONTIER+.** A cross-border anti-scam collaboration platform developed by Singapore that facilitates real-time intelligence sharing among 14 jurisdictions, including Australia and Canada.[24]

Key topics looking ahead

Looking ahead into the near future, there are several topics to look out for related to the global fight against scams.

- **PPP Framework implementation.** Over 100 organisations have endorsed and are now beginning to implement the Global Fraud Summit's PPP Framework to enhance global and cross-sector cooperation.
- **Deepfakes and AI countermeasures.** As AI acts as a force multiplier for scams, jurisdictions will prioritise global technical standards for multimedia integrity to tackle deepfakes (for instance through watermarking) and the development of counter-fraud AI to automate the detection of fraudulent content.
- **Balancing risk.** Jurisdictions will be increasingly focused on managing the risks involved with reimbursement models and of over-disruption.
- **Digital identity.** Jurisdictions have digital identity initiatives in place, or are advancing them, to prevent identity theft and support trusted digital transactions. This may extend to AI agent identity in the future.

JURISDICTIONS AT A GLANCE

Policy capability	Australia	Canada	Singapore	UK
Multi-sector legislative framework	■	◪	■	◪
Mandatory obligations for certain digital platforms	◪	◪	■	◪
Mandatory obligations for financial institutions	◪	■	■	■
Mandatory obligations for telecommunication providers	■	◪	■	◪
Central anti-scam coordination body	■	◪	■	◪
Public–private intelligence sharing	■	■	■	■
Real-time operational coordination	■	◪	■	■
Victim reimbursement mechanism	◪	□	■	■
Deepfakes in scope of interventions	◪	◪	■	◪
Digital identity and verification measures	■	■	■	■
International cooperation	■	■	■	■

Note: *This comparison assesses the presence and maturity of policy capabilities as described by authors in the report. It is not an indication of effectiveness of respective capabilities.*

Key:

■ *Established*

◪ *Emerging: scheduled, under consultation or policy proposal*

□ *Limited or not yet evident*

AUSTRALIA

Thomas van der Valk
Senior Fellow, Tech Policy Design Institute

State of play

In Australia, a scam is defined by the Scams Prevention Framework (SPF) as a direct or indirect attempt (whether successful or otherwise) to engage a consumer of a regulated service in a way that it would be reasonable to conclude involves deception and, if successful, would cause loss or harm. A consumer is defined by the SPF as a natural person or small business operation.[25]

In 2025, Australians made 481,523 reports of scam incidents, with financial losses totaling over A$2.18 billion.[26] Scam reports have significantly increased related to job scams, betting scams and identity theft. Young Australians, First Nations communities, people with disabilities, and those from culturally and linguistically diverse backgrounds are particularly at risk.[27]

The Australian Securities and Investments Commission (ASIC) warned Australians that AI is super-charging online scam threats. In 2025, ASIC coordinated the removal of 11,964 phishing and investment scam websites – a 90% increase in takedowns compared to 2024.[28] ASIC has also reported a sharp rise in online scams using deepfake videos of celebrities and politicians, with criminals increasingly exploiting topical issues in the news to deceive consumers.[29]



Policy approach

Legislation. The SPF, which passed Parliament on 13 February 2025, sets out principle-based obligations for businesses in key sectors where scammers operate.[30] This will take effect on 31 March 2027, when banks, digital platforms (designated internet search, social media and instant messaging) and telecommunication services will be required to take reasonable steps to prevent, detect, disrupt and respond to scams, and adopt governance arrangements.[31]

Oversight of the SPF will be shared between several independent Commonwealth statutory authorities:

- the Australian Competition and Consumer Commission (ACCC) for digital platforms and as an overarching regulator
- ASIC for banks
- the Australian Communications and Media Authority (ACMA) for telecommunication services.

Potential sectorial requirements

The SPF will be supported by sector-specific requirements developed in 2 related codes, which set out the minimum steps regulated businesses need to take to meet the SPF principle-based obligations, which will apply from 31 March 2027. The exposure draft lists the following proposed requirements, including:[32]

- **common rules –** adopt governance policies and processes, keep consumer accounts and data secure, proactively search for and take down brand impersonation sites, provide for free 24/7 scam reporting, resolve consumer disputes swiftly, share intelligence, and apportion liability across the sector
- **banks –** payee confirmation, issue warnings, delaying or blocking suspicious payments, and rapid transaction recalls or freezing suspect accounts
- **digital platforms –** verify new accounts and advertisers, pre-screen advertisements, monitor for suspicious activity, issue warnings, suppress suspect content such as deepfakes, and disable scam accounts
- **telcos –** prevent spoofing, deploy automated message filtering to intercept scam links or phone numbers, issue warnings and interrupt scam traffic.

Dispute resolution and compensation. Under the SPF, consumers will be able to seek compensation for their scam losses where businesses have not met their obligations. Entities will be required to have an accessible and transparent internal dispute resolution (IDR) mechanism and to cooperate across sectors for the purpose of IDR. If the business finds it did not meet its obligations under the SPF, the business should provide compensation. Entities are also required to be a member of the Australian Financial Complaints Authority (AFCA), which is an independent external resolution body offering a free service to consumers that are unable to resolve complaints with the regulated entities at IDR stage.

However, the government has signaled that the IDR guidance in the SPF rules may establish an expectation that businesses should provide automatic reimbursement of scam victims for verified scam losses below A$3,000.[33] The Australian Government considers that this could be an appropriate threshold to provide quick, efficient and timely dispute resolution for low-value scam complaints. The proposals may change as they are subject to ministerial sign-off.[34]

Penalties. The SPF is backed by a 2-tier and formula-based system of civil penalties. The maximum penalty for a Tier 1 contravention by a company is the greater of approximately A$52 million, 3 times the total value of any benefit to the company and related entities, or 30% of the adjusted turnover of the company during the breach turnover period. The penalties for Tier 2 contraventions work similarly, but the base penalty cap is set at approximately A$10 million.[35]

Institutional landscape. The Treasury leads the Australian Government's scams policy development. The ACCC, in addition to its enforcement role, plays a central role in scam prevention and response. The ACCC supports educational and awareness raising campaigns across government and operates the NASC, which facilitates collaboration between government and industry, such as information sharing and disrupting scams. NASC also runs Scamwatch, which provides educational material and a tool for consumers to report scams.[36] Law enforcement agencies are responsible for the arrest and prosecution of scammers.

Support. Scam victims can reach out to IDCARE, the national identity and cyber support service. IDCARE assesses the victims' situation and develops a tailored response plan to guide them forward.[37]

Public-private cooperation

Cooperation and information sharing. The NASC coordinates the collaboration between government and industry. The collaboration is focused on sharing insights, opportunities to target scam activity, and mitigating harm. NASC is building a new data-sharing system that will support high-frequency, secure sharing among agencies, industry and organisations.[38] The mandatory requirements under the SPF for reporting of Actionable Scam Intelligence (ASI) to SPF regulators will start to apply by the end of 2027.[39]

Fusion cells. Separate from the SPF, NASC coordinates 'fusion cells', which combine government and private expertise to tackle urgent specific types of scams. Between 2023 and 2025, 3 cells have addressed investment scams, fake job schemes, romance scams and fake online casinos (scambling), focusing on disrupting criminal operations, improving intelligence sharing and enhancing victim support.[40]

Co-regulation. As of 2020, telcos were the only sector regulated specifically in relation to scams through the Reducing Scam Calls and Scam SMS Code, which was revised in 2022. This code was developed by the Australian Telecommunications Alliance, and registered and enforced by ACMA. It requires telecommunications providers to take reasonable steps to prevent and block scam calls and text messages.[41] Since July 2026, telcos are also required to implement the requirements of the SMS Sender ID Register regulations, to prevent the unauthorised use of SMS sender IDs.[42] Examples of relevant measures that are not specific to scams include ACMA rules for telcos requiring the use of multifactor identity verification to protect services from scammer compromise and fraud,[43] and anti-money laundering, counter-terrorism financing and ePayments Code requirements for banks.[44]

Industry self-regulation. In 2023, the Australian Banking Association (ABA) launched an industry-led 'ScamSafe Accord', outlining the anti-scam measures to be implemented across the banking sector to disrupt, detect and respond to scams.[45] This includes the 'confirmation of payee' system.

The Digital Industry Group Inc. (DIGI), an industry association representing technology companies, initiated the Australian Online Scams Code in 2024.[46] This code commits signatories to detect scams, enable fast reporting, take down verified scams, curb scam ads, protect email and messaging, cooperate with law enforcement, share intelligence, inform the public and participate in future-proofing. These initiatives are expected to be supplemented and, where overlapping, effectively overtaken by the mandatory SPF codes.

International cooperation

United Nations. In March 2026, Australia endorsed the Call to Action to Combat Fraud at the UN and INTERPOL Global Fraud Summit in Vienna, driven by the increasing sophistication in scam activity through AI and the industrialisation of criminal syndicates through scam compounds.[47]

Private–public cooperation. At the summit, over 100 organisations endorsed a PPP Framework to enhance global cooperation in the fight against scams, confirming a collective commitment to prevent and disrupt fraud.[48] The Global Anti-Scam Alliance (GASA) – supported by AFCA as a supporting member and NASC as an associate member – endorsed the framework.[49]

Global operations. Australian authorities recovered A$5.5 million scam losses through INTERPOL's GRIP mechanism in a 2024 operation.[50] The Australian Federal Police (AFP) also launched Operation Firestorm in 2024, which focused on scam syndicates and human trafficking targets in South-East Asia and Eastern Europe.[51]

AUSTRAC and Five Eyes. The Australian Transaction Reports and Analysis Centre (AUSTRAC) deploys intelligence staff and shares the advanced financial intelligence TAIPAN system with 10 Pacific nations. AUSTRAC also provides training and is invested in regional networks such as the Pacific Financial Intelligence Community and the Asia Pacific Regional Group.[52]

In June 2026, Five Eyes intelligence and law enforcement partners warned about how AI is rapidly transforming cyber risk, and the need to take comprehensive action.[53]

Critiques of the approach

Reimbursement threshold. The Consumer Action Law Center argues that the proposal of automatic reimbursement of people scammed of A$3,000 or less is well intentioned, but the threshold needs to be higher to avoid the dispute resolution system from grinding to a halt.[54]

New scam risk. The Australian Telecommunications Alliance (ATA) issued concerns about the risk that the A$3,000 automatic compensation could create a honeypot for scammers, where they allow themselves to be deliberately 'scammed' by someone they know and then seek compensation. The ATA has advocated for rigorous checks and balances to validate claims and assess liability.[55] Law firm Gilbert + Tobin raise that, while the Assistant Treasurer and Minister for Financial Services have stated that these risks will be monitored, it remains to be seen whether monitoring alone is sufficient without structural safeguards.[56]

Implementation delay. Consumer organisations object to the 9-month delay of the SPF implementation as it would cause unacceptable harm to consumers during the additional time the framework is not in full force.

Jurisdictional challenge. The Joint Select Committee on Social Media and Australian Society considered the impact of online scams and jurisdictional impediments and recommended that the Australian Government consider options for greater enforceability of Australian laws for social media platforms, including amending regulation and legislation.[57]

Regulatory complexity and over-disruption. Both industry and consumer advocate stakeholders have indicated that the SPF's layered and distributed approach raises questions around regulatory complexity and legal certainty. Examples are the potential for duplication between new and existing codes, consistency of interpretation across the different regulators, and the point at which a regulated entity can be assured it fulfilled its obligations.[58] Gilbert + Tobin also caution against over-disruption, risking consumer harm through the blocking of legitimate payments, accounts, or removing legitimate content.[59]

Future direction

Industry code and sector expansion. The Treasury is currently consolidating stakeholder feedback on the draft common rules, the sectoral requirements for banking, telcos and certain digital platform services, and the internal dispute resolution mechanism including the proposal for automatic reimbursement.[60] The Treasury may designate further sectors in the future.

Content integrity. The Australian Signals Directorate (ASD) has published guidance on how to strengthen multimedia integrity in the generative AI era, including providing transparency such as watermarking and the verification of provenance of content.[61] The G7 and the OECD have provided guidance, and the European Union (EU) AI Act sets a legislative precedent by mandating measures to this end.[62] An increased focus on whether regulated entities apply such measures could therefore be expected.

Digital ID. Digital ID services allow for identity verification in online transactions, taking away the need for people to share personal details with a wide range of businesses and organisations. This is expected to reduce the risk of identity theft and the ability of cyber criminals to create false identities used for scamming activities.[63] From December 2026, the Australian Government Digital ID System will expand to enable private sector parties to implement the government's Digital ID on their services, and to allow accredited digital ID providers to provide alternative digital ID services.[64] This means that Australians will have more opportunities to use digital ID across online services and will have more choice of digital ID service providers.

Key observations

- **Comprehensive framework.** Australia is in the process of setting up a comprehensive whole-of-ecosystem framework to tackle scams. The SPF imposes comprehensive obligations across banking, telecommunications, and designated digital platforms, including intelligence-sharing requirements and a proportionate liability model among entities involved. As an early mover, Australia's implementation will generate evidence on consumer outcomes and workability that other jurisdictions can draw on.
- **Reimbursement.** The government's proposed expectation that businesses should provide automatic reimbursement for verified losses under A$3,000 should allow for quick resolution and minimise the cost of investigating complaints. If this expectation were to be implemented; it should be monitored closely to see if it leads to an increase in scams below the reimbursement threshold.
- **Innovative and future proof.** The NASC fusion cell model combining government and private expertise to target specific scam types demonstrates operational innovation enabling improved scam disruption and victim support. The SPF is also able to adjust to future developments; for instance, through the potential expansion of the scope beyond initial sectors. The framework leaves room for new technological abilities to be applied, such as to detect evolving AI-enabled scam techniques.

CANADA

Keldon Bester
Fellow, Centre for International Governance & Innovation
Executive Director, Canadian Anti-Monopoly Project

Curtis McCord
Policy Analyst, Canadian Anti-Monopoly Project

State of play

In Canada, scams are regulated through the Criminal Code, which defines fraud as 'everyone who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service, is guilty of an indictable offence [...]'.[65]

In the National Anti-Fraud Strategy Discussion Paper, the federal government considers that the following types of fraud could be in scope of the strategy: deception or coercion to authorise the transfer of funds or the exchange of personal or financial information to harm an individual, gaining access to or using an individual's financial account for the same purpose, or impersonating clients to access federal government accounts or to redirect payments.[66]



Scams are a major issue in Canada.[67] Since 2024, over 80% of Canadians have been targeted by some form of online or phone scam.[68] In 2025, over 112,000 instances of fraud were reported, with losses totalling over CA$704 million.[69] However, only 5 to 10% of all fraud cases are reported, so these numbers should be considered as a floor.[70] Reporting also shows that investment scams make up 49% of the overall reported dollar loss in Canada, individuals under the aged 50 are more likely to be victimised, and those over the age of 50 lose more money on average.[71]

Canadian authorities have recognised the role that AI technologies play in scams, allowing more sophisticated and convincing scams at greater scale.[72] Campaigns using deepfake impersonations of public figures to drive investment and cryptocurrency scams were reported around the 2025 federal election; and in one such case, a victim was defrauded of CA$900,000.[73] To date, Canada's approach has not contemplated a dedicated response to AI-enabled scams, framing them more as an intensification of a pre-existing problem. But recent developments in adjacent policy areas indicate this may be changing.

Policy approach

Canada's approach to combatting scams relies primarily on criminal law enforcement without prescribed coordination between the public and private sectors. However, in 2025 the federal government announced its intent to reform Canada's approach to scams with the potential for the introduction of new regulatory frameworks and institutions.

Institutional landscape. Canada's 2 primary law enforcement agencies with a mandate to prevent and disrupt scams are the federal Royal Canadian Mounted Police (RCMP), and the Competition Bureau of Canada, whose mandate defined in the Competition Act covers deceptive marketing practices. Together, the RMCP, the Competition Bureau and the Ontario Provincial Police jointly operate the Canadian Anti-Fraud Centre (CAFC). Other relevant actors include the National Cybercrime Coordination Centre (NC3), a division of the RCMP that works closely with the CAFC, and the Canadian Centre for Cyber Security, a part of the Communications Security Establishment (CSE) with an intelligence gathering role that includes cybercrime such as scams. In 2025, the federal government introduced legislation to establish a new Financial Crimes Agency with a mandate that would include countering scams.[74]

The efforts of these law enforcement agencies are complemented by federal regulators with sector-specific mandates related to scam activity. The Financial Consumer Agency of Canada (FCAC) is responsible for protecting the rights of Canadians when it comes to financial products, and as of 2026, has been given an expanded mandate to mitigate consumer-targeted fraud.[75] Canada's telecommunications regulator, the Canadian Radio-Television and Telecommunications Commission (CRTC), has a responsibility to combat the use of the telecommunications system to commit fraud, including scams.[76]

Policy interventions. The CAFC covers the gamut of anti-scam activity, serving as a central repository for reporting and information sharing between organisations. This occurs through the National Cybercrime and Fraud Reporting System, launched in 2025, serving as an aggregator of fraud and scam reports.[77] The CAFC uses these reports to prevent scams by distributing information on scams, and maintains a repository of educational materials and documented scams. The CAFC also works with other law enforcement organisations to disrupt scam activity by coordinating stakeholders from the public and private sector for enforcement actions.

The proposed Regulations Amending the Financial Consumer Protection Framework Regulations would require banks to obtain express consent from consumers before enabling electronic funds, including wire transfers and global money transfers. If enacted, the proposed regulations would come into force on 1 July 2027, and would, among others, also contain policies and procedures for how banks would investigate suspicious transactions and for notifying consumers of suspicious requests to enable capabilities or increase transaction limits.[78]

Otherwise, Canada has few regulations, codes or standards at the federal level that deal with prevention, disruption or liability for scams. Financial institutions bear some liability for unauthorised access to accounts, but as scams increasingly aim for authorised transfers, victims have limited recourse.[79]

At provincial level, Quebec's Bill 72 introduced an Act that requires a merchant (such as banks), with whom a consumer holds a demand deposit account, must refund the consumer any sum where they are the victim of fraud, unless the merchant raised a warning.[80]

Public-private cooperation

Canadian Anti-Scam Coalition. Cooperation takes places mainly through voluntary and ad hoc initiatives. Canada's financial, telecom and technology sectors, those most implicated in the scam ecosystem, have joined law enforcement and government to form a coalition to share best practices and information to fight scams and protect Canadians. This takes the form of the Canadian Anti-Scam Coalition (CASC), which has been brought into the Canadian Cyber Threat Exchange (CCTX), which operates infrastructure for cross-sector information sharing.[81]

Maple Disruption. In December 2025, the RCMP's NC3 and CAFC coordinated Maple Disruption 2025, an operational sprint bringing together 25 organisations, including those in the private sector, to engage in disruptive actions against tools relied on by those engaged in scam and fraudulent behaviour.[82]

Information sharing limitations. The federal government's discussion paper supporting its consultation on a National Anti-Fraud Strategy suggests that limitations on information sharing presents a hurdle to more formalised public–private cooperation.[83] The consultation notes that established information-sharing procedures could be improved to support more effective identification and disruption of scams, and invites industry to provide input on potential triggers, scope and safeguards for information sharing across private and public sector organisations.

International cooperation

International initiatives. Canada participates in several international anti-scam law enforcement initiatives. Canada is a member of INTERPOL and was notably one of the government sponsors of the 2026 Global Fraud Summit.[84] Several Canadian law enforcement agencies are also part of the Quebec Strategic Partnership, a bilateral cross-border fraud information-sharing and outreach agreement with the United States Federal Trade Commission (FTC).[85]

Joint operations. Since 2024, the CAFC has participated in joint operations as part of the FRONTIER+ anti-scam initiative, alongside law enforcement from Brunei, Indonesia, Hong Kong, Macao, Malaysia, the Maldives, Singapore, South Korea and Thailand. In 2026, the CAFC worked with FRONTIER+ to identify fraudulent bank accounts and websites and disrupt those activities.[86] The operation led to over 3,000 arrests of individuals associated with as many as 138,000 scam cases.[87] Outside of law enforcement, some Canadian financial institutions are members of the GASA.[88]

Critiques of the approach

Liability gaps. One of the major critiques of Canada's current approach to addressing scams from civil society is the lack of liability on the part of the private sector actors implicated in the scam ecosystem.[89] Organisations such as the Public Interest Advocacy Centre (PIAC), Democracy Watch, Option consommateurs, the Canadian Association of Retired Persons (CARP), and the Canadian Anti-Monopoly Project (CAMP) have identified liability gaps at the financial, telecommunications and digital platform level that leave consumers with limited recourse should they fall victim to scams. While there was a proposal in the Canadian House of Commons to reform the burden of liability for scams connected to the financial sector in a 2026 budget implementation bill, the amendment was rejected in the committee process.[90]

Self-regulation of digital platforms. BioCatch, a company specialised in preventing financial crime, has raised that social media platforms currently have no official or mandated role in Canada's counter-scam ecosystem. Their self-regulation prioritises advertiser freedom rather than consumer safety, and there's no sector-wide accountability in Canada tied to their services.[91]

Lack of central authority. A related critique is the lack of a federal framework and regulator tasked with enforcing obligations to address scams across relevant sectors in the Canadian economy. As demonstrated by existence of the CAFC, there are already several law enforcement bodies at the federal and provincial level cooperating on scams under Canada's Criminal Code. Critics argue that Canada needs a central authority with a cross-sector scam framework for the prevention and restitution of scam activity, similar to Australia's approach.[92]

Future direction

National Anti-Fraud Strategy consultation. The National Anti-Fraud Strategy consultation was concluded in April 2026. Though federal consultations in Canada do not indicate either the final form of a policy, or whether policy is adopted at all, the discussion paper guiding the consultation provides potential signals on what a possible future federal response to scams could look like.[93]

The scope of the consultation indicates that federal policymakers understand that private sector players have a role to play in combatting scams. The financial, telecommunications and digital platform sectors are each named as potentially having either general or sector-specific obligations for prevention, detection, disruption and response to fraud, including scams, under the proposed Multi-Sector Anti-Fraud Framework.

Potential obligations. Notably, proposed potential obligations for digital platforms would be new additions, complementing existing obligations for organisations in the financial and telecommunications sector. Potential obligations include advertiser verification, ensuring banned users are unable to bypass verification processes, and screening of fraudulent profiles and malicious links.

In terms of institutional design, the discussion paper suggests that any new framework would likely fall within the remit of a centralised regulator, contrasting with the distributed current state of Canada's anti-scam policy. Some elements of this distributed model are likely to continue, with existing sector-specific regulators (for example, FCAC, CRTC) likely to oversee provisions tailored to their respective sectors.

While the international nature of the organisations and individuals responsible for scams is discussed, international collaboration receives relatively little real estate in the consultation. The role of AI-enabled scams receives little attention as well, meriting a single mention of its potential to enhance the ability of fraudsters to obfuscate their identity.

Digital Safety Act. Adjacent areas of policy are beginning to contemplate the use of AI tools for the purpose of inflicting harm, financial or otherwise, on Canadians. Tabled in 2026, the Safe Social Media Act would enact the Digital Safety Act. While the proposed legislation does not engage directly with scam-related harms, it proposes requirements for the labelling of synthetic content and safeguards for chatbots.

Key observations

- **Federal and provincial coordination.** A virtue of Canada's current approach to combatting scams is that it attempts to knit together the capabilities of federal and provincial law enforcement agencies. The limitation of this approach is that, lacking a centralised institution or policy response, the approach is necessarily disaggregated across organisations and jurisdictions.
- **Nascent policy response.** While the harms of scams continue to generate headlines, Canada's policy response remains nascent, despite the Bill 72 regulations in Quebec. The Canadian federal government appears to be taking an increasing interest in the topic, as one of the country sponsors of the 2026 Global Fraud Summit.
- **Consultation on strategy.** Canada's federal government has concluded a public consultation on its proposed National Anti-Fraud Strategy, which could form the foundation of an effective response to the rise of scams. What remains to be seen is whether scams, especially amid the proliferation of AI tools that increase the scale, sophistication and persuasiveness of scams, receives a more dedicated federal policy response.

SINGAPORE

Helena Yixin Huang
Associate Research Fellow, S. Rajaratnam School of International Studies

State of play

Singapore defines operational and legal concepts such as 'scammer', 'scam victim' and 'scam offence' under the Protection from Scams Act 2025.[94] In practice, most scams in Singapore are understood to be 'self-effected',[95] where victims are manipulated or deceived into transferring money or taking actions that benefit the scammer, but they do not have to be self-effected to be considered a scam.

In 2025, Singapore recorded 37,308 reported scam cases amounting to S$913.1 million in losses.[96] Although the number of reported scam cases decreased by 27.6% from 2024, the median loss of money per scam case has increased by 18.4%, from S$1,389 in 2024 to S$1,644 in 2025.[97] While there is no clear data breakdown showing the number of AI-enabled scams, the figures suggest that although intervention measures may have had some impact on reducing the overall scam volumes, individual scam incidents continue to result in substantial financial harm.



Government Official Impersonation Scams (GIS) were amongst the most notable developments in the Singapore scam landscape, with the total amount lost to GIS increasing by 160%, from S$151.3 million in 2024 to S$242.9 million in 2025.[98] Adults aged 30 to 49 formed the largest victim demographic, accounting for 36.1% of scam victims in 2025. People aged 65 and above suffered the highest average losses, at S$37,053 per reported victim.[99]

Policy approach

Singapore's policy approach to AI-enabled scams is best understood as part of its broader anti-scam architecture. The jurisdiction has not created a standalone approach for AI-enabled scams. Instead, Singapore has strengthened points of intervention across law enforcement, financial regulation, telecommunications governance, online platform accountability and public education. This reflects an ecosystem-based approach to reduce the scammers' ability to establish contact with victims, sustain the deception or to exploit the gaps between different sectors.

Institutional landscape. The institutional landscape is led by the Ministry of Home Affairs (MHA) and the Singapore Police Force (SPF). The Anti-Scam Command (ASCom) consolidates scam investigation and disruption capabilities,[100] while the ASC supports rapid fund tracing and works with co-located bank representatives to freeze suspected scam-linked bank accounts.[101]

Other key agencies in Singapore's anti-scam architecture include the Monetary Authority of Singapore (MAS) and the Infocomm Media Development Authority (IMDA). The Government Technology Agency (GovTech) focuses on scam prevention solutions, and the Home Team Science and Technology Agency (HTX) support the Singapore Police Force with technology tools. The Cyber Security Agency of Singapore (CSA) works with law enforcement, international partners and tech companies to fight cyber-enabled scams, and contributes to public awareness campaigns, for instance through Cyber Tips.

Policy interventions. The Shared Responsibility Framework (SRF) assigns duties to financial institutions and telecommunications operators in relation to scams and establishes expectations for victim reimbursement where prescribed duties are breached.[102]

The consideration of which party will bear responsibility for the losses is based on a 'waterfall approach'. Financial institutions, followed by telcos, are expected to bear the full loss if they fail to discharge their respective prescribed duties. If both have fulfilled their duties, the SRF will not require payouts to be made to consumers.[103]

The OCHA Office administers the OCHA,[104] which allows for implementation directives to be issued to online service providers, entities or individuals where their online activity is suspected of specified offences, including scams. OCHA Codes of Practice for designated online communication services require platforms to put in place systems, processes and measures to counter online harms. This is relevant to AI-enabled scams because social media, messaging and e-commerce platforms may be used to disseminate impersonation content and automated messages at scale.

Deepfake-enabled investment and impersonation scams illustrate the importance of upstream controls, such as the ones undertaken by the OCHA Office. In 2023, a deepfake video of a prominent individual promoting a cryptocurrency scam was published on Meta Platform's services, followed by another deepfake video endorsing an investment scam. The OCHA Office has since issued 2 Implementation Directives to Meta, requiring Meta to 'enhance facial recognition measures' and 'prioritise review of end-user reports from Singapore' by a stipulated date.[105]

Harm mitigation. Singapore has also introduced mechanisms to mitigate harm after an individual has been targeted. The Protection from Scams Act 2025 allows for police to issue Restriction Orders to banks where necessary, to prevent targets of ongoing scams from continuing to transfer money or draw down credit facilities despite police intervention.[106]

IMDA has progressively tightened safeguards to reduce the misuse of local communications infrastructure by scam syndicates. Individuals are now limited to 10 postpaid SIM cards across all telcos,[107] and can use Singpass, their Singapore 'trusted digital identity',[108] to log in and verify the number of postpaid SIM cards registered under their name.[109] MAS has focused on strengthening authentication, fraud surveillance and consumer protection.

Technology tools also reinforce this approach. ScamShield,[110] a mobile application, provides a helpline for checking and reporting scams. Using AI-powered tools, the Scam Analytics and Tactical Intervention System (SATIS) aims to detect and disrupt scam websites and related online infrastructure.[111]

Public-private cooperation

Government-led cooperation. Singapore's approach to public–private partnerships is mostly government-led, with the government setting the legislative and regulatory direction and the industry actors operationalising the safeguards within their respective sectors. The ASC, under the ASCom, co-locates representatives from major banks in Singapore with officers from the Singapore Police Force. This approach reduces delays in information exchanges and enables faster response against suspicious transactions, including the freezing of bank accounts and tracing of scam-related funds. Such arrangements are important because the window for funds recovery narrows exponentially once a victim makes a transfer.

Frameworks such as the SRF have also led to the banking and telecommunications industry taking steps to mitigate phishing scams. Banks have introduced stronger authentication measures, including the phasing out of SMS One-Time Passwords for digital token users.[112] Telecommunication operators support measures such as Sender ID safeguards and provide the option to block international call or international SMS.[113]

Obstacles to cooperation. Despite positive examples, barriers to public–private cooperation can still exist. International companies operating in Singapore may face challenges aligning their global platform policies and internal compliance processes with the local regulatory requirements.

International cooperation

INTERPOL global hub on cybercrime. Singapore is home to INTERPOL's global hub on cybercrime, known as the Global Complex for Innovation.[114] Singapore also participates in wider international platforms and initiatives, including INTERPOL operations such as HAECHI,[115] which supports coordinated action against cyber-enabled financial crime. The ASCom also developed FRONTIER+,[116] a cross-border anti-scam collaboration platform that brings together anti-scam units from 14 jurisdictions for the purpose of facilitating real-time intelligence sharing and coordinated enforcement.

ASEAN. These efforts sit alongside broader regional and international commitments undertaken by the Singapore Government, including ASEAN declarations on combating cybercrime and online scams and mutual legal assistance treaties. Singapore is also ASEAN's Voluntary Lead Shepherd on Cybercrime, which means it is 'responsible for charting ASEAN's initiatives against cybercrime'.[117] In addition, Singapore established the ASEAN Senior Officials Meeting on Transnational Crime (SOMTC) Working Group on Cybercrime in 2013 to 'coordinate the regional approach to cybercrime', 'work together on capacity building, training and the sharing of information', as well as engage ASEAN Dialogue Partners on cybercrime collaboration.[118]

Critiques of the approach

Limited scope. Although the SRF works to reduce phishing scam losses, it is only applicable to the defined scope of phishing scams and does not cover all forms of AI-enabled scams, such as deepfake-enabled impersonation scams or dating scams.

Financial autonomy. The Protection from Scams Act, which allows the police to issue Restriction Orders to banks to prevent targets of ongoing scams from making further transfers or withdrawals, can be seen by some as a significant intervention into their own control over their own finances. The temporary bank account freezes and the lack of access to funds by individuals may also create inconvenience if the transaction was meant to be a legitimate one for emergency purposes.

Compliance cost. Regulatory requirements for the private industry may lead to an increase in the cost of compliance and introduce friction into digital services, which may or may not be cascaded down to the paying consumers.

Future direction

Continued review. In March 2025, Mrs Josephine Teo, Minister for Digital Development and Information and Second Minister for Home Affairs,[119] stated that the government will continue to review its laws and strengthen regulatory frameworks to deal with new forms of cybercrime and the speed at which such crimes are committed.

Prevention and disruption. Singapore's policy direction is likely to continue focusing on scam prevention and disruption. A key recent development is the establishment of the SPF Cyber Command in July 2026, which brings cybercrime and anti-scam capabilities under a unified command.[120] This suggests that Singapore's response will place greater emphasis on intelligence-led disruption, faster operational coordination, and closer integration between scam enforcement, cybercrime investigation and online harms governance.

Private sector expectations. The private sector is likely to face stronger expectations and pressure to embed scam prevention into its business processes. For financial institutions, this may mean stronger authentication, fraud surveillance and transaction safeguards. For platforms, this will likely mean stronger verification, reporting and takedown arrangements. Recent OCHA Implementation Directives to major technology companies indicate a growing expectation that online services should be doing more to prevent impersonation and scam-related misuse of their platforms before the harm occurs.

International cooperation. Singapore is likely to continue expanding its cooperation on cross-border scam-related issues, such as asset recovery, virtual asset tracing and operational coordination, while continuing to perform its duties as ASEAN's Voluntary Lead Shepherd on Cybercrime.

Key observations

- **Ecosystem approach.** Singapore's approach is based on an ecosystem rather than creating a standalone framework to deal with AI-enabled scams. The country has worked to strengthen points of intervention and timely cooperation from across law enforcement and different industry players. Public education remains an important upstream point of intervention in the ecosystem.
- **Deepfakes.** Deepfake scams are being addressed through platform accountability. Singapore's response to deepfake-enabled investment and impersonation scams has focused on requiring platforms to act against scam advertisements, impersonation pages and inauthentic accounts.
- **Early disruption.** Early disruption is a key element of Singapore's approach. Measures such as the OCHA directives, the ASC, ScamShield and SATIS show that an emphasis is placed on detecting and disrupting scam activity before losses are fully realised.

UNITED KINGDOM

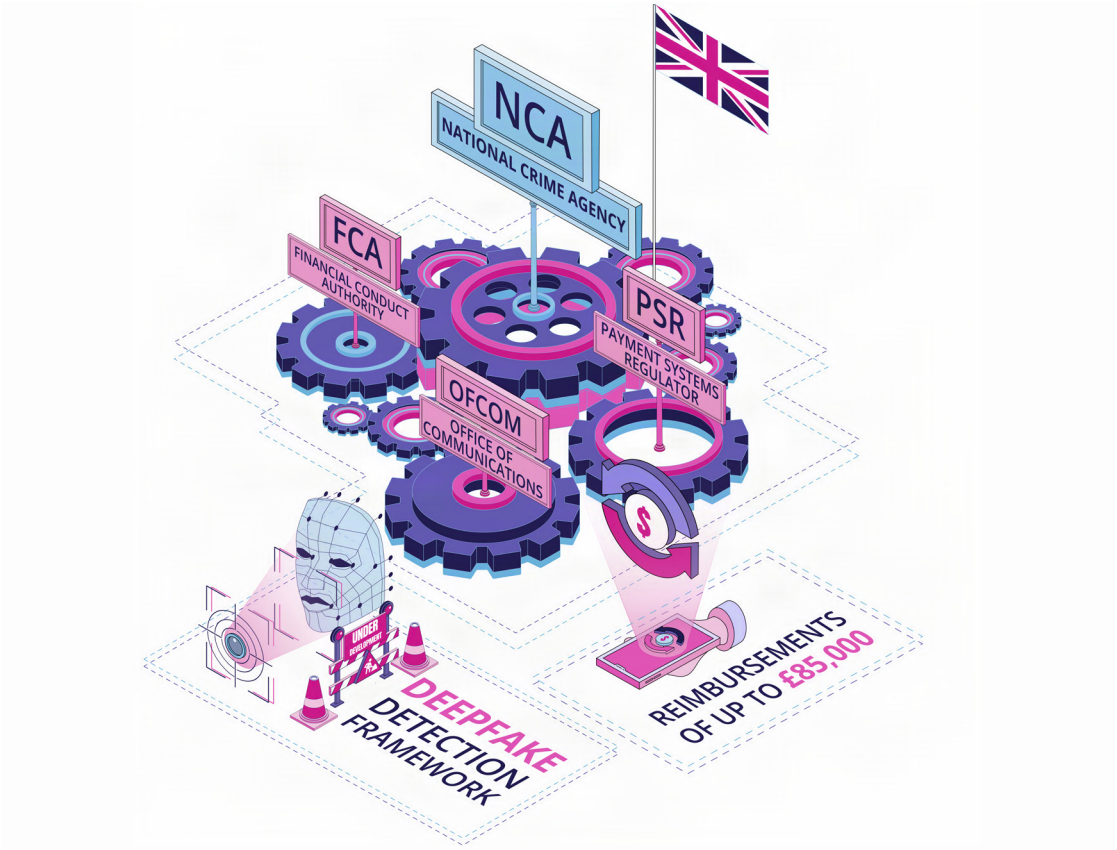
Isabella Wilkinson
Senior Research Fellow, Digital Society Programme Chatham House

State of play

In the UK, scams tend to be understood as a subset of fraud. In legal terms, scams fall under the 2006 Fraud Act, which criminalises fraud by false representation (alongside abuse of power and failure to disclose information). The fraud threat is seen as 'a technology-enabled, hybrid threat'.

The UK has a robust approach to countering deceptive activities such as scams, impersonation, identity theft and actions targeting individuals and organisations for offender benefit. But the scale and complexity of the problems the UK faces, particularly from AI-enabled scams, is growing. Just last year, fraud cost the economy over £14 billion, with one in 14 individuals and one in 4 businesses becoming victims.[121]

Although three-quarters of UK citizens are concerned about AI-driven fraud, less than half trust insurers and banks to protect them from it.[122] Beyond fraud, there is growing recognition in the UK that AI-enabled deception and certain AI-generated material has wider societal impact; it can damage information integrity, undermine trust in public institutions, and – sexually explicit deepfakes in particular – pose risks to women, girls and vulnerable groups.[123]



Policy approach

The UK policy approach to scams is principles-based and collaborative. It relies on co-regulatory instruments, state regulation and some criminal legislation. There are early signs designated institutions are strategising about how to address AI risks.

Institutional landscape. Responsibility for preventing and responding to scams is split across different government departments, ministries, regulators and law enforcement, with many collaborative initiatives.

Front line (disrupt, respond, enforce, prosecute)	**National Crime Agency** (NCA); **Online Crime Centre** (OCC); National Economic Crime Centre; **Home Office**; City of London Police (national lead for fraud); Metropolitan Police; Dedicated Card and Payment Crime Unit (joint Met/London police); local and regional police; National Cyber Security Centre (NCSC); Crown Prosecutor's Service (CPS); PoliceAI (new 2026).
Support (regulate, issue guidance, collect evidence, store information)	**Financial Conduct Authority** (FCA); **Payment Services Regulator** (PSR); Department for Science, Innovation and Technology (DSIT); AI Security Institute (AISI); Ofcom; Companies House; Financial Ombudsman Service (FOS); Report Fraud Service; Foreign, Commonwealth and Development Office (FCDO).
Miscellaneous (other relevant institutions)	HM Revenues and Customs (HMRC); HM Treasury; Bank of England; Public Sector Fraud Authority (Cabinet/HM Treasury); Joint Fraud Taskforce (JFT); National Trading Standards.

Policy interventions. The proliferation of AI in scams stresses the 'traditional' response lifecycle above. It will require adaptations in UK public policy on criminalisation of deceptive behaviour, victim compensation, public information, trusted evidence and accountability.

The 2026–2029 Fraud Strategy, promulgated by the Home Office, sets out the government's plan to mitigate fraud risks, including impersonation by improving deepfake detection capabilities.[124] This includes deepfake detection frameworks and pilots with technology companies and the Electoral Commission.[125] The strategy launched the NCA's Online Crime Centre, with £30 million earmarked for intelligence sharing between mobile network operators, technology companies and law enforcement.[126] This ties into longstanding nation-wide efforts against fraud, like the NCA and City of London police 'Operation Henhouse', resulting in 557 arrests and £9 million worth of account freezing orders last year.[127]

Victim compensation. Consumer protection and victim compensation is a major pillar of UK scam policy. In 2023, the PSR initiated an Authorised Push Payment (APP) protection regime, allowing customers to claim up to £85,000 in compensation from their banks or payment service providers (PSPs) if deceived by fraudsters.[128] This was a world-first, but not a silver bullet: an independent review spotlighted that 'fraudsters are adjusting tactics and moving activity to out-of-scope channels rather than stopping'.[129] Scam techniques and procedures will adapt to bypass bank controls, including through using AI (for example, using 'selfie injections' for identity verification in account takeovers).[130]

Public awareness and reporting. UK anti-scam policy relies on public information (the NCSC and local police provide guidance on phishing and deepfake reporting) and reporting (the City of London operates the national 'Report Fraud' hotline).[131] There are efforts to develop an evidence base and standards: most recently, in an AISI evaluation framework measuring how AI models impact cybercrime and fraud.[132]

Digital platforms. Notwithstanding recent developments in corporate liability for major fraud and sanctions against cybercriminal networks, the country's regulatory regime for scams on Big Tech platforms is still being ironed out.[133] The 2023 Online Safety Act requires platforms to take 'robust action' against illegal content on their platforms, which includes content related to fraud.[134] In July 2026, Ofcom announced companies will face new requirements to deplatform fraudulent ads.[135]

Public-private cooperation

Coordination and information sharing between the public and private sectors is a hallmark of UK scam response.

Two-level model. Anti-scam work is facilitated through a 2-level model: public–private agreements alongside cross-industry coordination and self-regulation. UK Finance is influential as is threat-specific programmatic work funded by industry, like Take Five to Stop Fraud,[136] Stop Scams UK (a group of telecoms, financial and technology platforms working against SIM diversion) and via the Global Signals Exchange (funded by Google).[137]

Recent initiatives. The OCC is a disruption unit launched in 2026, bringing together government, police, intelligence agencies, banks, mobile networks and major tech firms to drive coordinated action against fraud, including scams. At the OCC, police and companies that hold vital intelligence on scams work side by side, sharing data instantly and building a single picture of global fraud networks.[138] Similarly, the Deepfake Detection Framework is a public–private initiative to set an industry standard for deepfake detection.[139]

Information sharing. The UK public and private sectors have information-sharing arrangements in place to counter scams. UK Finance is an illustrative case: a dedicated intelligence-sharing unit, a Banking Protocol Rapid Response Scheme (with tie-ins to local police and training to high street banks) and a Vulnerable Victims Notification system. The UK's financial services industry also directly funds the Dedicated Card and Payment Crime Unit, which reportedly prevented over £273 million from being stolen in 2025.[140] Cifas, a non-profit, operates a comprehensive database of economic crime data and Companies House, a UK executive agency, is a public-facing record and registrar.[141]

International cooperation

Two-thirds of scam offenders targeting UK victims are reportedly based outside UK borders,[142] so it's no surprise the UK anti-scams approach has a strong international component. The National Assessment Centre designates the threat as 'typically overseas, online and tech-enabled'.[143]

Leadership role. The UK co-sponsored the 2026 Global Fraud Summit. The summit's agreed PPP Framework highlights commitments to prioritise research and development and innovations for counter-fraud AI. Many technology and retail companies with UK operations were also signatories to the 2026 Industry Accord Against Online Scams and Fraud.[144]

Deepfakes. The Deepfake Detection Framework mentioned above includes a scenario-based challenge with INTERPOL and Five Eyes representatives, and suggests an ambition to develop consistent standards with allies.

INTERPOL. With INTERPOL, the NCA works to disrupt scam-related activities abroad. The UK also works bilaterally to tackle scam compounds (for instance, in India, Nigeria and Vietnam)[145] and with Europol on serious, organised crime.

Critiques of the approach

Keeping pace with the threat. Researchers at the Alan Turing Institute cautioned that UK law enforcement is 'not adequately equipped to prevent, disrupt or investigate AI-enabled crime', calling for a new NCA AI Crime Taskforce.[146] The newly launched PoliceAI, dedicated to the development of AI in policing, may address this gap.[147]

Legal puzzle. Legal experts warn advances in AI put stress on current approaches to liability, compensation and remediation. The proliferation of booking agents creates liability questions,[148] like what *kind* of payment is within scope for bank or PSP refund. Whether the UK General Data Protection Regulation and broadly principles-based approach is sufficient for post-scam redress and remediation is also the subject of scrutiny, given 'AI-driven financial fraud' *and* AI-based counter-fraud measures raise legal questions about informed consent and automated decision-making.[149]

Illegal fraudulent content is covered by the Online Safety Act. However, some content in the wider ecosystem – especially in malicious advertising, which may enable scams, mis- and disinformation – may be harmful but legal. AI-driven amplification and crypto-based scams may further complicate coverage and enforcement.

Reimbursement cap. Industry shared concerns about the mandatory nature of compensation, and the risk for claim fraud and follow-on fraud by intermediaries. UK consumer champion *Which?* raised the alarm about lowering the compensation cap to £85,000 and risks involved for consumers.[150]

Jurisdictional challenge. Criticism of UK scam responses can be linked to bigger questions about Big Tech accountability, and whether the UK has requisite operational and regulatory agency over the multinational communications infrastructure it relies on. The cross-border nature of globally operated communications infrastructure can complicate domestic enforcement and requires effective cooperation between regulators, law enforcement and service providers.

Future direction

Implementation. The UK's approach is likely to gear towards implementation of the 2026 national strategy and further implementation of its Online Safety Act. Ensuring interoperability between technical and regulatory requirements will be a priority.

Cross-sector collaboration. There is a strong trend towards cross-sector and cross-stakeholder collaboration on methodologies, both in using AI to tackle scams (from monitoring to takedown) and on deepfake detection. The UK designated the former as a priority as early as 2024;[151] the FCA already hosts a sandbox for firms to try out AI-driven processes and recently published a review on how AI will impact the retail financial sector.[152] How the UK works with companies to develop, procure and scale anti-scam AI technologies is an area to watch, particularly amid debates about the UK's dependence on non-sovereign technologies and General Data Protection Regulation (GDPR) risks associated with automated decision-making, including sensitive and identifiable personal data.

Public service media and personhood. On the horizon, other UK policy changes may impact how the UK combats AI-enabled scams. A consultation on the future of public service media may lead to changes in the discoverability of 'trusted' platforms.[153] Meanwhile the Representation of the People Bill may have implications for personhood and registration, 2 scam targets.

Key observations

- **Innovation and best practice.** The UK has a world-leading approach to anti-scams: strong industry coordination, robust public–private partnerships, split responsibilities across parts of the public sector, and a strong international standing for disruption, prevention and response.
- **Limitations.** The UK needs a clear and consistently updated technical evidence base on how advances in AI capabilities impact scammer techniques, tactics and procedures, which demands closer coordination with AISI, technology platforms and AI companies, alongside 'traditional' private sector partners.
- **Implementation challenges.** Two-thirds of scams targeting the UK reportedly originate from outside its borders, which necessitates international cooperation and complicates national-focused disruption, prevention and response.
- **Future policy directions.** The development, deployment and procurement of anti-scam AI is a priority area for the UK, which is already developing guidance on the issue and has recently committed to platforming best practice with industry.

CONCLUSION

AI can be a force for good, but the power of technology to supercharge deception remains a critical challenge. Organised international crime syndicates use AI as a force multiplier to scale high-quality scams, such as through deepfakes and voice clones, that exploit trust across the digital economy. As the 4 jurisdiction chapters show, the central policy challenge is not only to respond after harm occurs, but to prevent, detect and disrupt scam activity before the damage is done.

A common direction of travel is emerging across Australia, Canada, Singapore and the United Kingdom. Jurisdictions are moving toward cross-sector models that place obligations on banks, telecommunications providers, designated digital platforms and government agencies. This shift emphasises real-time operational coordination, intelligence sharing and improved victim support.

This report serves as a practical benchmark for policymakers and regulators. By comparing different models, it identifies where domestic frameworks can be strengthened and where international cooperation must deepen. We invite you to use this report to accelerate evidence-based, internationally aligned responses to disrupt the evolving AI-enabled techniques targeting individuals, communities and business globally.

APPENDIXES

APPENDIX 1: AUSTRALIA

Table 1: Legislation, policy, code or guidance-based interventions to combat scams (Australia)

Intervention name	Intervention type	Objective	Lead agency/ organIsation	Key stakeholders	Status/date
Scams Prevention Framework Act 2025	Regulation	Obligations to prevent, detect, disrupt and respond to scams across banking, telecommunications and certain digital platform services; create reporting/Internal Dispute Resolution /External Dispute Resolution and compensation pathways; enable information sharing and enforcement backed up by civil penalties.	The Treasury for policy setting; implementing roles for the ACCC as general regulator, including for digital platforms, ASIC as banking sector regulator, and ACMA as telco sector regulator.	Regulated entities (initially, banks, telcos, designated digital platforms), consumers (natural persons and small businesses).	SPF Act passed Parliament 13 February 2025.
SPF Rules and sector Codes	Rules under the SPF	Prescribe operational, scope and procedural matters to support SPF principles and sector codes, e.g. designation tests, designation exceptions, statement of compliance, IDR procedural settings, reporting/intelligence-sharing rules to be specified.	The Treasury for policy setting; enforced by designated SPF sector regulators ACCC, ASIC and ACMA.	Regulated entities (initially banks, telcos, designated digital platforms), SPF regulators ACCC, ASIC and ACMA.	The Rules and the Codes commence on 31 March 2027. ASI sharing requirements are to commence in late 2027.
SPF – sector codes (banks, certain digital platforms and telcos)	Codes under the SPF (likely to be included in same instrument as SPF Rules)	Establish baseline, cross-sector obligations on governance, and impose specific mandatory obligations for banks, telecommunication providers and designated digital platforms.	The Treasury for policy setting, with ACCC as general backstop and digital platform regulator, ASIC designated as the banking sector regulator, the ACMA as the designated telco sector regulator.	Regulated entities (banks, telecommunication providers and designated digital platform services), consumers, respective regulators to implement common rules.	Expected to commence 31 March 2027.
Reducing Scam Calls and Scam SMS Code 2022	Registered industry code	Industry requirements for detection, tracing, blocking/ unblocking, reporting and information sharing to disrupt and reduce scam calls and scam SMS.	Code developed by the ATA, registered and enforced by ACMA.	Telecommunication services.	In force since July 2022, first issued in 2020, and expected to be deregistered and relevant obligations to be absorbed by mandatory SPF telco code from 31 March 2027.

Table 1 continued (Australia)

Intervention name	Intervention type	Objective	Lead agency/ organIsation	Key stakeholders	Status/date
ScamSafe Accord	Industry code / voluntary commitment	Sectorwide commitment by banks to implement coordinated measures to detect, disrupt, respond to scams and share intelligence.	Developed by ABA and Customer-Owned Banking Association.	Banking sector.	Launched 2023, ongoing implementation by member banks.
Australian Online Scams Code	Industry code / voluntary commitment	Detect/block suspected scams, enable fast user reporting, promptly take down verified scams, curb scam advertising, protect email and messaging services, cooperate with law enforcement, share threat intelligence, inform the public, and participate in ongoing adaptation to emerging scam threats.	Developed by digital industry trade DIGI.	Signatories include digital platforms, including Discord, Google, Meta, Snap, TikTok, Twitch, X and Yahoo.	Launched on 26 July 2024.

APPENDIX 2: CANADA

Table 2: Legislation, policy, code or guidance-based interventions to combat scams (Canada)

Intervention name	Intervention type	Objective	Lead agency/ organIsation	Key stakeholders	Status/date
Amendments to Canada's Bank Act	Legislative/ regulatory	To impose duties on financial institutions to proactively detect and prevent fraud, give consumers more control over account permissions, create reporting requirements.	FCAC	Canadian Financial Institutions, FCAC.	Received royal assent on 26 March 2026.
Telecommunications anti-fraud measures: universal call blocking and STIR/ SHAKEN caller ID authentication[154]	Regulatory	To require telecommunications service providers to block calls with illegitimate caller IDs and to authenticate caller ID information, reducing fraudulent and spoofed calls.	CRTC	Telecommunications service providers, CRTC, consumers.	Universal call blocking required as of December 2019; STIR/ SHAKEN in effect 30 November 2021.
Regulations Amending the Financial Consumer Protection Framework Regulations	Regulatory (proposed)	Proposed regulations would, among others, require banks to obtain express consent from consumers before enabling electronic funds, and contain policies and procedures for investigations and consumer notifications.	FCAC	Banking institutions, consumers.	If enacted, scheduled to come into force on 1 July 2027.
National anti-fraud strategy	Policy and regulatory reform	To create a framework for a government- and industry-wide approach to combatting scams through regulatory obligations, information-sharing frameworks.	Department of Finance	Public sector and law enforcement, telecommunications, online platforms, financial institutions.	Announced November 2025, consultation ran 30 March to 28 April 2026.
Quebec Bill 72	Provincial-level legislative act	Limitation of a consumer's liability where there is unauthorised use of the consumer's deposit account, and requirement of refund of the consumer where they are the victim of fraud.	Office de la protection du consommateur (OPC)	Merchants, including banks.	Introduced 12 September 2024, passed 7 November 2024, assented to 7 November 2024.

APPENDIX 3: SINGAPORE

Table 3: Legislation, policy, code or guidance-based interventions to combat scams (Singapore)

Intervention name	Intervention type	Objective	Lead agency/ organisation	Key stakeholders	Status/date
Online Criminal Harms Act (OCHA)	Legislation / regulatory framework	Provides legal powers to issue directions to online service providers or other entities to disrupt online criminal content and activities, including (AI-enabled) scams.	MHA / SPF / OCHA Office	Online service providers, digital platforms, social media platforms, e-commerce platforms, users in Singapore.	In force – progressively operationalised from 1 February 2024.
OCHA Codes of Practice for Online Communication Services and E-Commerce Services	Industry code / regulatory obligation	Designated services are required to put in place systems, processes and measures to proactively prevent and disrupt scams and malicious cyber activities.	MHA / SPF	Facebook, WhatsApp, Instagram, Telegram, WeChat, Carousell, Facebook Marketplace, Facebook Advertisements, Facebook Pages, TikTok.	In force – took effect on 26 June 2024. TikTok was designated in September 2025.
OCHA Implementation Directives to online service providers	Regulatory direction / platform accountability mechanism	Targets specific scam trends and platform risks. Relevant to deepfake-enabled impersonation scams as directions were issued to address scam advertisements, accounts, profiles and business pages using videos or images of government office holders.	OCHA Office	Private industry platforms such as Meta, Apple, Google.	Meta received directives in September 2025 and January 2026; Apple and Google received directives in November 2025 to prevent spoofing of 'gov.sg' and government agency names on messaging platforms.155
Protection from Scams Act 2025	Legislation / harm mitigation mechanism	Allows the SPF to issue Restriction Orders to banks to restrict banking and credit facilities of scam victims who remain convinced by scammers.	MHA / SPF	Banks, scam victims.	Passed in January 2025 and operationalised on 1 July 2025.

Table 3 continued (Singapore)

Intervention name	Intervention type	Objective	Lead agency/ organisation	Key stakeholders	Status/date
SRF	Compensation / accountability framework	Assigns duties to financial institutions and telecommunications operators for mitigating phishing scams, and provides expectations for payouts to victims where prescribed duties are breached.	MAS / IMDA	Financial institutions, telcos, consumers.	Implemented on 16 December 2024.
MAS banking safeguards: Money Lock, stronger authentication and transaction friction	Financial sector safeguards/ regulatory supervisory measures	Strengthens authentication, reduces unauthorised access and introduces friction for high-risk transactions.	MAS	Banks, banking customers, digital banking users.	Money Lock was introduced in November 2023 – in place.
Facility Restriction Framework for scam mules	Regulatory / enforcement measure	Restricts banking, mobile subscription, Corppass and Singpass access for scam mules. Addresses the supporting infrastructure that allows scam syndicates to move funds, register lines or misuse digital identities.	SPF, MAS, IMDA, GovTech	Money mules, SIM card mules, corporate entities, banks, telcos, Singpass / Corppass users.	Operationalised on 1 October 2025 and has been implemented in phases since.
Amendments to the Miscellaneous Offences Act on SIM card misuse	Legislation / enforcement measure	Strengthens the enforcement against irresponsible SIM card subscribers, middlemen and errant retailers who facilitate the misuse of local SIM cards for scams.	MHA / SPF	SIM card subscribers, retailers, middlemen, telcos, scam syndicates.	In force since 1 January 2025.
IMDA telecom-munications safeguards: SIM card cap, self-help SIM checker, international call and SMS blocking	Telecom-munications regulation / consumer protection mechanism	Reduces misuse of local telecommunications infrastructure by scam syndicates, including local-looking numbers, mule-linked lines and overseas-originating scam calls or messages.	IMDA, with SPF, GovTech and local telcos.	Telcos, mobile subscribers, consumers, scam victims.	In place – international call and SMS blocking measures implemented progressively since 2024.

APPENDIX 4: UNITED KINGDOM

Table 4: Legislation, policy, code or guidance-based interventions to combat scams (UK)

Intervention name	Intervention type	Objective	Lead agency/ organIsation	Key stakeholders	Status/date
Economic Crime and Corporate Transparency Act	Criminal legislation	Overhaul Companies House with expanded powers, hold large organisations to account (below) and expand corporate liability.	Home Office; Attorney General's Office; National Crime Agency; Companies House; Serious Fraud Office; Crown Prosecution Service	'Large, incorporated bodies and partnerships' with more than 250 employees, more than £36 million turnover, and more than £18 million in total assets.	Act passed in 2023; in force.
Economic Crime and Corporate Transparency Act: Guidance to organisations on the failure to prevent fraud (2024)	Guidance for large organisations	Provide guidance to large organisations for preventing and responding to fraud (including share reasonable fraud prevention procedures and clarify regulatory and legislative regimes).	Home Office; Attorney General's Office; National Crime Agency; Companies House; Serious Fraud Office; Crown Prosecution Service	'Large, incorporated bodies and partnerships' with more than 250 employees, more than £36 million turnover, and more than £18 million in total assets.	Guidance issued in 2024.
Financial Services (Banking Reform) Act; changes to Faster Payment rules through Sections 54–55	Mandatory regulation	Force UK payment service providers to reimburse customers within scope who fall victim to APP fraud, up to £85,000 within 5 days.	Payment Services Regulator	Banks and payment service providers.	Updated 2023; in force 2024.
Insurance Fraud Charter	Voluntary agreement	Reduce fraud by improving data sharing, identifying and disrupting professional enablers of fraud, and better supporting victims of insurance fraud.	Home Office	Insurers; Association of British Insurers; via Joint Fraud Taskforce.	2024
Introduction to AI with a focus on counter fraud	Guidance for counter-fraud professionals	Raise awareness to counter-fraud professionals about AI and its potential uses in the detection and prevention of fraud.	Public Sector Fraud Authority	Counter-fraud professionals in the public and private sectors.	2024
Online Safety Act	Regulation and criminal legislation	Protects children and adults online, placing a range of duties on social media companies and search services, including to protect against illegal content, such as content-related to fraud.[156]	Ofcom	Social media companies and search services.	2023; roadmap to implementation published 2024; illegal content duties in effect 2026.
Deepfake Detection Framework	Standard	Develop an industry standard and approach to detecting deepfakes.	Home Office; DSIT	Technology companies.	2026

REFERENCES

1 UK Home Office, National Crime Agency and The Rt Hon Lord Hanson of Flint, *New disruption unit launched in crackdown on fraud*, UK Government, 9 March 2026. https://www.gov.uk/government/news/new-disruption-unit-launched-in-crackdown-on-fraud

2 M Roberts and V Zakhozhyi, *Countering Digital Scams: Stemming the Tide on an Urgent Development Challenge*, 2 March 2026, accessed 4 August 2026. https://www.undp.org/digital-innovation/blog/countering-digital-scams-stemming-tide-urgent-development-challenge

3 Australian Signals Directorate, *Annual Cyber Threat Report 2025–2026*, Australian Government, 2026, p 18

4 Australian Signals Directorate, *Annual Cyber Threat Report 2024–2025*, Australian Government, 2025, p 25. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025

5 Australian Government, Scamwatch, *How scammers use technology and AI*, Scamwatch website, n.d., accessed 23 June 2026. https://www.scamwatch.gov.au/stop-check-protect/help-to-spot-and-avoid-scams /how-scammers-use-technology-and-ai

6 INTERPOL, Interpol report warns of increasingly sophisticated global financial fraud [media release], INTERPOL website, 16 March 2026, accessed 4 August 2026. https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat

7 J Gibson, 'Scams Prevention Framework Bill 2024', *Bills Digest,* No. 33, 2024–25, Australian Government, p 5. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2425/25bd033

8 Singapore Statutes Online, Online Criminal Harms Act 2023 (No. 24 of 2023), Republic of Singapore, 2023. https://sso.agc.gov.sg/Act/OCHA2023

9 D Dass, 'The Anti-Scam Centre: A Collaborative Approach Against Scams', *Singapore Police Force*, 29 November 2021. https://www.police.gov.sg/media-hub/police-life/2021/11/the-anti-scam-centre---a-collaborative-approach-against-scams

10 National Anti-Scam Centre, *Fusion Cells*, NASC website, n.d., accessed 29 June 2026. https://www.nasc.gov.au/reports-and-publications/fusion-cells

11 INTERPOL, *USD 257 million seized in global police crackdown against online scams* [media release], INTERPOL, 24 June 2024, accessed 30 June 2026. https://www.interpol.int/en/News-and-Events/News/2024/USD-257-million-seized-in- global-police-crackdown-against-online-scams

12 Canadian Anti-Fraud Centre, *Canadian Anti-Fraud Centre supported Operation FRONTIER+III: an international action to disrupt fraud* [news release], Government of Canada, 4 June 2026. https://antifraudcentre-centreantifraude.ca/news-nouvelles/2026/2026-06-04-eng.htm

13 R Bratby, *APP fraud reimbursement: the evidence after one year*, Bratby Law, 6 July 2026. https://bratby.law/app-fraud-reimbursement-evaluation/

14 The Treasury, Scams Prevention Framework codes and rules exposure draft, Treasury website, 2026, accessed 3 September 2026. https://consult.treasury.gov.au/c2026-765133

15 Monetary Authority of Singapore, *MAS and IMDA Consult on Shared Responsibility Framework for Phishing Scams*, Monetary Authority of Singapore, 25 October 2023, accessed 2 September 2026. https://www.mas.gov.sg/news/media-releases/2023/mas-and-imda-consult-on-shared-responsibility-framework-for-phishing-scams

16 Singapore Statutes Online, *Protection from Scams Act 2025*

17 United Nations Office on Drugs and Crime and INTERPOL, *Global Fraud Summit 2026 Outcome documents*, United Nations, 2026. https://www.unodc.org/res/organized-crime/GFS/Global-Fraud-Summit-Outcome-Documents-English.pdf

18 Signatories are Google, Adobe, Amazon, Levi Strauss & Co, LinkedIn, Match Group, Meta, Microsoft, OpenAI, Pinterest and Target. Source: Google, *Industry Accord Against Online Scams & Fraud*, Google website, 16 March 2026, accessed 1 July 2026. https://services.google.com/fh/files/newsletters/industryaccord.pdf

19 OECD, 'G7 Toolkit for Artificial Intelligence in the Public Sector', 2024. https://www.oecd.org/en/publications/g7-toolkit-for-artificial-intelligence-in-the-public-sector_421c1244-en.html **and** OECD AI Observatory, *Policies, data and analysis for trustworthy artificial intelligence,* OECD website, n.d. https://oecd.ai/en/ **and** Council of Europe, *The Framework Convention on Artificial Intelligence*, Council of Europe website, n.d. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

20 INTERPOL, *Towards agile and trusted policing,* INTERPOL website, n.d. https://www.interpol.int/en/How-we-work/Innovation/INTERPOL-Innovation-Centre

21 Ministry of Home Affairs, *Strengthening ASEAN cooperation to combat cross-border scam syndicates*, Ministry of Home Affairs website, 6 October 2026.https://www.mha.gov.sg/media-room/newsroom/strengthening-asean-cooperation-to-combat-cross-border-scam-syndicates/ **and** Australian Transaction Reports and Analysis Centre, *Global impact: From regional leadership to world-wide partnerships,* AUSTRAC website, 15 December 2025, accessed 30 June 2026. https://www.austrac.gov.au/global-impact-regional-leadership-world-wide-partnerships#:~:text=Technology%20remains%20a%20critical%20tool,suspicious%20transaction%20patterns%20warranting%20investigation

22 Global Signal Exchange, About the Global Signal Exchange website, n.d., accessed 4 August 2026. https://www.globalsignalexchange.org/about

23 Australian Signals Directorate, *Five Eyes cyber security agencies statement* [media release], ADS website, 22 June 2026, accessed 30 June 2026. https://www.cyber.gov.au/about-us/view-all-content/news/five-eyes-cyber-security-agencies-statement

24 Singapore Police Force, Operation FRONTIER: A United Front Against Transnational Scams, Singapore Police Force website, 18 August 2025. https://www.police.gov.sg/Media-Hub/Police-Life/2025/08/Operation-FRONTIER-A-United-Front-Against-Transnational-Scams **and** Goh PM (2026) 'Opening ceremony of the Anti-Scam Conference 2026' [speech], Anti-Scam Conference 2026, Singapore, 11 May, accessed 19 October 2026. https://www.mha.gov.sg/media-room/newsroom/opening-ceremony-of-the-anti-scam-conference-2026/

25 J Gibson, 'Scams Prevention Framework Bill 2024', *Bills Digest,* No. 33, 2024–25, Australian Government, p 5. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2425/25bd033

26 National Anti-Scam Centre, *Targeting scams: report of the National Anti-Scam Centre on scams data and activity 2025*, ACCC website, 2026, p 4. https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-reports-on-scams-activity/targeting-scams-report-of-the-national-anti-scam-centre-on-scams-data-and-activity-2025

27 National Anti-Scam Centre, *Targeting scams: report of the National Anti-Scam Centre on scams data and activity 2025,* pp 30–31

28 Australian Securities and Investments Commission, *ASIC ramps-up action to protect consumers from AI-powered online investment scams* [media release], ASIC, 8 April 2026, accessed 21 July 2026. https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-063mr-asic-ramps-up-action-to-protect-consumers-from-ai-powered-online-investment-scams/

29 Australian Signals Directorate, *Annual Cyber Threat Report 2025–2026*, Australian Government, 2026, p 18.

30 The Treasury, Scams Prevention Framework: Protecting Australians from scams, p 1

31 The Treasury, *Scams Prevention Framework: Summary of reforms*, Australian Government, 2024, p 6. https://treasury.gov.au/sites/default/files/2024-09/c2024-573813-summary.pdf

32 The Treasury, *Scams Prevention Framework codes and rules exposure draft*, Treasury website, 2026, accessed 29 June 2026. https://consult.treasury.gov.au/c2026-765133

33 The Treasury, *Scams Prevention Framework codes and rules exposure draft*, Treasury website, 2026, accessed 3 September 2026. https://consult.treasury.gov.au/c2026-765133

34 The Treasury, *Internal Dispute Resolution under the Scams Prevention Framework: Position paper*, Australian Government, 2025, p 3. https://storage.googleapis.com/files-au-treasury/treasury/p/prj38c41037eb554b881caef/page/c2025_715201_pp.pdf

35 Dwyer Harris, *Scams Prevention Framework FAQs*, Dwyer Harris website, 2025, accessed 3 September 2026. https://www.dwyerharris.com/blog/scams-prevention-framework-faqs **and** Gilbert + Tobin, *'Click here': Australia's Scam Prevention Framework takes shape*, Gilbert + Tobin website, 2026, accessed 29 June 2026. https://www.gtlaw.com.au/insights/click-here-australias-scam-prevention-framework-takes-shape

36 Australian Government, *About Scamwatch*, Scamwatch website, n.d., accessed 23 June 2026. https://www.scamwatch.gov.au/about-us/about-scamwatch

37 IDCARE, *National Identity & Cyber Support*, IDCARE website, n.d., accessed 1 July 2026. https://www.idcare.org/

38 NASC receives real-time automated data from ReportCyber, regular scams-related data from the Australian Financial Crimes Exchange (AFCX) and scam reports through Scamwatch. Source: National Anti-Scam Centre, *Collaboration*, NASC website, n.d., accessed 29 June 2026. https://www.nasc.gov.au/what-we-do/collaboration

39 Australian National Audit Office, *Department of the Treasury's Readiness to Implement the Scams Prevention Framework*, ANAO website, 24 June 2026, accessed 15 September 2026. https://www.anao.gov.au/work/performance-audit/department-of-the-treasurys-readiness-to-implement-the-scams-prevention-framework

40 Australian Competition & Consumer Commission, *New taskforce to tackle 'scambling' as fake online casinos target First Nations Australians* [media release], ACCC, 8 July 2026, accessed 31 August 2026. https://www.accc.gov.au/media-release/new-taskforce-to-tackle-scambling-as-fake-online-casinos-target-first-nations-australians

41 Communications Alliance, *Industry Code C661:2022 Reducing scam calls and scam SMS*, Communications Alliance, 2022. https://www.austelco.org.au/wp-content/uploads/2025/06/C661_2022.pdf

42 Australian Communications and Media Authority, *Industry rules - SMS Sender ID Register*, ACMA website, n.d., accessed 11 September 2026. https://www.acma.gov.au/industry-rules-sms-sender-id-register

43 Australian Communications and Media Authority, *Customer identity authentication rules*, ACMA website, n.d., accessed 3 July 2026. https://www.acma.gov.au/customer-identity-authentication-rules

44 Australian Transaction Reports and Analysis Centre*, Changes to AML/CTF obligations: What you need to do*, AUSTRAC website, 1 July 2026, accessed 31 August 2026. https://www.austrac.gov.au/news-and-media/article/changes-amlctf-obligations-what-you-need-do **and** Australian Securities and Investments Commission, *ePayments Code* [ASIC website], n.d., accessed 31 August 2026. https://www.asic.gov.au/regulatory-resources/financial-services/epayments-code

45 Australian Banking Association, *Banks unite to declare war on scammers*, Australian Banking Association website, 24 November 2023, accessed 30 June 2026. https://www.ausbanking.org.au/new-scam-safe-accord/

46 Digital Industry Group Inc., *Australian Online Scams Code*, DIGI website, 2024, accessed 30 June 2026. https://digi.org.au/wp-content/uploads/2025/08/FINAL_-DIGI-industry-led-scams-code-_-July-2024-1-1.pdf

47 Australian Competition & Consumer Commission, *Continued action critical to combat fraud as annual scam losses exceed $2 billion* [media release], ACCC, 30 March 2026, accessed 30 June 2026. https://www.accc.gov.au/media-release/continued-action-critical-to-combat-fraud-as-annual-scam-losses-exceed-2-billion

48 United Nations Office on Drugs and Crime and INTERPOL, *Global Fraud Summit 2026 Outcome documents*, United Nations, 2026. https://www.unodc.org/res/organized-crime/GFS/Global-Fraud-Summit-Outcome-Documents-English.pdf

49 GASA serves as a collaborative platform for coordinated action against scams, and has over 100 member organisations worldwide, including leading financial institutions, technology companies and government bodies. Source: Global Anti-Scam Alliance, *Our members*, GASA website, n.d., accessed 30 June 2026. https://gasa.org/members#associated- organisations

50 INTERPOL, *USD 257 million seized in global police crackdown against online scams* [media release], INTERPOL, 24 June 2024, accessed 30 June 2026. https://www.interpol.int/en/News-and-Events/News/2024/USD-257-million-seized-in- global-police-crackdown-against-online-scams

51 Australian Federal Police, *Operation Firestorm to target cyber scammers cheating Australians* [media release], AFP website, 28 August 2024, accessed 30 June 2026. https://www.afp.gov.au/news-centre/media-release/operation-firestorm-target-cyber-scammers-cheating-australians

52 Australian Transaction Reports and Analysis Centre, *Global impact: From regional leadership to worldwide partnerships*, AUSTRAC website, 15 December 2025, accessed 30 June 2026. https://www.austrac.gov.au/global-impact-regional-leadership-world-wide-partnerships#:~:text=Technology%20remains%20a%20critical%20tool,suspicious%20transaction%20patterns%20warranting%20investigation

53 Australian Signals Directorate, *Five Eyes cyber security agencies statement* [media release], ADS website, 22 June 2026, accessed 30 June 2026. https://www.cyber.gov.au/about-us/view-all-content/news/five-eyes-cyber-security-agencies-statement

54 Consumer Action Law Centre, *Unacceptable Harms: Scam laws delay will see Aussies robbed of billions* [media release], CALC, 28 May 2026, accessed 1 July 2026. https://consumeraction.org.au/unacceptable-harms-scam-laws- delay-will-see-aussies-robbed-of-billions/

55 Australian Telecommunications Alliance, *ATA Statement on Scams Prevention Framework* [media release], ATA website, 28 May 2026, accessed 1 July 2026. https://www.austelco.org.au/ata-statement-on-scams-prevention-framework/

56 Gilbert + Tobin, *'Click here': Australia's Scam Prevention Framework takes shape*., Gilbert + Tobin website, 18 September 2024, accessed 1 July 2026. https://www.gtlaw.com.au/insights/click-here-australias-scam-prevention- framework-takes-shape

57 Parliament of Australia, *Social media: the good, the bad, and the ugly – Final report*, Joint Select Committee on Social Media and Australian Society, 2024. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Social_Media_and_Australian_Society/SocialMedia/Final_report; S Hanson-Young (Australian Greens), Second reading amendment, sheet 3324, Scams Prevention Framework Bill 2025, Senate, Parliament of Australia, 2025, accessed 12 October 2026

58 The Treasury, *Scams – mandatory industry codes*, The Treasury website, n.d., accessed 1 September 2026. https://consult.treasury.gov.au/c2023-464732

59 Gilbert + Tobin, *'Click here': Australia's Scam Prevention Framework takes shape*., Gilbert + Tobin website, section 11.2, 18 September 2024, accessed 1 July 2026. https://www.gtlaw.com.au/insights/click-here-australias-scam-prevention- framework-takes-shape

60 Gilbert + Tobin, *'Click here': Australia's Scam Prevention Framework takes shape*., Gilbert + Tobin website, 18 September 2024, section 13, accessed 1 July 2026. https://www.gtlaw.com.au/insights/click-here-australias-scam-prevention- framework-takes-shape

61 Australian Signals Directorate, *Content credentials: Strengthening multimedia integrity in the generative AI era*, ASD website, 30 January 2025, accessed 2 July 2026. https://www.cyber.gov.au/business-government/secure-design/artificial-intelligence/content-credentials-strengthening-multimedia-integrity-in-the-generative-ai-era

62 Principle 7 reads: 'Develop and deploy reliable content authentication and provenance mechanisms, where technically feasible, such as watermarking or other techniques to enable users to identify AI-generated content'. Source: Government of Japan, *Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI System*, Government of Japan, 2023. https://www.mofa.go.jp/files/100573471.pdf **and** OECD AI Policy Observatory, *Transparency and explainability (Principle 1.3)*, OECD.AI website, n.d., accessed 2 July 2026. https://oecd.ai/en/dashboards/ai-principles/P7 **and** European Parliament Research Service, *Generative AI and watermarking,* European Parliament website, December 2023, accessed 1 July 2026. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI(2023)757583_EN.pdf

63 Digital ID System, *Privacy and security benefits*, Digital ID System website, n.d., accessed 1 July 2026. https://www.digitalidsystem.gov.au/what-is-digital-id/privacy-and-security

64 Digital ID System, *Using Digital ID for your business or organisation*, Digital ID System website, n.d., accessed 12 October 2026. https://www.digitalidsystem.gov.au/using-digital-id-for-your-business-or-organisation#digital-id-providers-and-services

65 Department of Justice, *Canadian Criminal Code R.S.C., 1985, c. C-46*, Government of Canada, last amended 15 June 2026, accessed 11 August 2026. https://laws-lois.justice.gc.ca/eng/acts/c-46/fulltext.html/index.html

66 Department of Finance Canada, *National Anti-Fraud Strategy Discussion Paper*, Government of Canada, 30 March 2026. https://www.canada.ca/en/department-finance/programs/consultations/2026/national-anti-fraud-strategy-discussion-paper.html

67 For the purposes of this chapter the terms 'scam' and 'fraud' are used interchangeably.

68 Canadian Anti-Fraud Centre, *2024 Annual Statistical Report*, Canadian Anti-Fraud Centre, 2025. https://www.cacp.ca/_Library/Alert_Documents/CAFC_Annual_Stats_Report_2024_-_EN.pdf

69 Royal Canadian Mounted Police Government of Canada – Canadian Anti-Fraud Centre, *The rise of fraud*, Canadian Anti-Fraud Centre website, 23 February 23, 2026. https://antifraudcentre-centre-antifraude.ca/features-vedette/2026/02/rise-fraud-montee-fraude-eng.htm **and** Jacqueline Wilson, 'Four-in-Five Canadians Targeted by Scams as Fraud Losses Top $544M', *CTV News*, 15 January 15, 2026. https://www.ctvnews.ca/calgary/article/4-in-5-canadians-targeted-by-scams-as-fraud-losses-top-638m-report/

70 Government of Canada, *Fraud Prevention Month to bring hidden crime into the spotlight*, Competition Bureau, 6 March 2026, accessed 2 September 2026. https://www.canada.ca/en/competition-bureau/news/2026/03/fraud-prevention-month-to-bring-hidden-crime-into-the-spotlight.html

71 Canadian Anti-Fraud Centre, *2024 Annual Statistical Report*, Canadian Anti-Fraud Centre, 2025. https://www.cacp.ca/_Library/Alert_Documents/CAFC_Annual_Stats_Report_2024_-_EN.pdf

72 A Snisarenko, 'Rising number of scams now use AI, Toronto police warn', *CBC News*, 11 March 2026. https://www.cbc.ca/news/canada/toronto/toronto-police-fraud-scams-ai-9.7124459; Canadian Anti-Fraud Centre, *Bulletin: Fraud using deepfakes*, Canadian Anti-Fraud Centre website, 31 July 2024. https://antifraudcentre-centreantifraude.ca/features-vedette/2024/07/bulletin-deepfakes-hypertrucage-eng.htm **and** Competition Bureau Canada, *The rise of AI: Fraud in the digital age* [news release], Government of Canada, 4 March 2024. https://www.canada.ca/en/competition-bureau/news/2024/03/the-rise-of-ai-fraud-in-the-digital-age.html

73 M Lavigne, A Abrahams, M Omar and A Bridgman, 'Social Media Platforms Host and Profit from Scams Using AI and Fake News Websites', *Centre for Media, Technology and Democracy*, 18 April 2025, accessed 30 July 2025. https://www.cdmrn.ca/publications/scam-ai-fake-news **and** P Foran, 'Ontario senior bilked out of $900K after falling victim to crypto scam that used AI deepfake of PM Carney', *CTV News*, 26 June 2026. https://www.ctvnews.ca/toronto/consumer-alert/article/ontario-senior-loses-900000-to-crypto-platform-scam-that-used-ai-deepfake-of-pm-carney/

74 Department of Finance Canada, *Minister Champagne takes aim at financial scams and abuse, announces Anti-Fraud Strategy and new Financial Crimes Agency* [news release], Government of Canada, 20 October 2025. https://www.canada.ca/en/department-finance/news/2025/10/minister-champagne-takes-aim-at-financial-scams-and-abuse-announces-anti-fraud-strategy-and-new-financial-crimes-agency.html

75 Department of Finance Canada, *Government pre-publishes regulations to prevent fraud and facilitate the next phase of consumer-driven banking* [news release], Government of Canada, 26 June 2026. https://www.canada.ca/en/department-finance/news/2026/06/government-pre-publishes-regulations-to-prevent-fraud-and-facilitate-the-next-phase-of-consumer-driven-banking.html

76 Canadian Radio-television and Telecommunications Commission, *How to protect yourself from scammers*, Canadian Radio-television and Telecommunications Commission website, Government of Canada, 18 October 2022. https://crtc.gc.ca/eng/phone/telemarketing/fraud.htm

77 Royal Canadian Mounted Police National Headquarters, *RCMP launches new National Cybercrime and Fraud Reporting System* [news release], Royal Canadian Mounted Police, 6 November 2025. https://rcmp.ca/en/news/2025/11/rcmp-launches-new-national-cybercrime-and-fraud-reporting-system

78 Government of Canada, "*Canada Gazette, Part I, Volume 160, Number 26: Regulations Amending the Financial Consumer Protection Framework Regulations",* Government of Canada website, 27 June 2026, accessed 2 September 2026. https://gazette.gc.ca/rp-pr/p1/2026/2026-06-27/html/reg2-eng.html

79 A Pozadzki, E Alini and M Postelnyak, 'The Scam Industry', *The Globe and Mail*, 5 June 2026. https://www.theglobeandmail.com/business/economy/article-most-common-online-scams-canada-prevention/ **and** Department of Finance Canada, *National Anti-Fraud Strategy Discussion Paper*, Government of Canada, 30 March 2026. https://www.canada.ca/en/department-finance/programs/consultations/2026/national-anti-fraud-strategy-discussion-paper.html

80 Government of Quebec, *Bill 72 (2024, chapter 32) An Act to protect consumers against abusive commercial practices and to offer better transparency with respect to prices and credit*, n.d., accessed 2 September 2026. https://www.publicationsduquebec.gouv.qc.ca/fileadmin/Fichiers_client/lois_et_reglements/LoisAnnuelles/en/ 2024/2024C32A.PDF

81 Canadian Cyber Threat Exchange, *Canadian Anti-Scam Coalition*, Canadian Cyber Threat Exchange website, n.d., accessed 19 July 2026. https://cctx.ca/canadian-anti-scam-coalition/ **and** Canadian Bankers Association, *Canada's major financial services, telecommunication, and technology companies unite with law enforcement and government to target growing threat posed by scams* [news release], Canadian Bankers Association website, 9 September 2025, accessed 19 July 2026. https://cba.ca/article/canadian-anti-scam-coalition

82 Royal Canadian Mounted Police National Headquarters, *Maple Disruption 2025 – Over 3000 disruptive actions taken against fraudsters and cybercriminals* [news release], Royal Canadian Mounted Police website, 17 December 2025. https://rcmp.ca/en/news/2025/12/4348581

83 Department of Finance Canada, *National Anti-Fraud Strategy Discussion Paper*

84 INTERPOL, *INTERPOL-UNODC global summit ends with call to action against fraud surge*, INTERPOL, 17 March 2026. https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-UNODC-global-summit-ends-with-call-to-action-against-fraud-surge

85 Federal Trade Commission, *FTC, Canadian Law Enforcement Agencies Cooperate on Public Outreach to Combat Cross-Border Fraud* [press release], Federal Trade Commission, 22 March 2024. https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-canadian-law-enforcement-agencies-cooperate-public-outreach-combat-cross-border-fraud

86 Canadian Anti-Fraud Centre, *Canadian Anti-Fraud Centre supported Operation FRONTIER+III: an international action to disrupt fraud* [news release], Government of Canada, 4 June 2026. https://antifraudcentre-centreantifraude.ca/news-nouvelles/2026/2026-06-04-eng.htm

87 Anti-Deception Coordination Centre, *Hong Kong Police conducts cross-border anti-scam operation with nine countries and regions under "FRONTIER+"*, ADCC website, n.d., accessed 8 July 2026. https://www.adcc.gov.hk/en-hk/-anti-scam-operation-with-nine-countries-and-regions-under-frontier.html

88 Global Anti-Scam Alliance, *Our members*, GASA website, n.d. https://gasa.org/members

89 T Dawood, *National Anti-Fraud Strategy Consultation: Submission of the Public Interest Advocacy Centre (PIAC)*, Public Interest Advocacy Centre, 2026. https://www.piac.ca/wp-content/uploads/2026/06/National-Anti-Fraud-Strategy-Consultation-PIAC-Comments-FINAL-April-28-2026.pdf

90 A Pozadzki, 'Bloc Québécois proposes banks be held liable for customer fraud losses', *The Globe and Mail*, 19 February 2026. https://www.theglobeandmail.com/business/economy/article-bloc-quebecois-banks-fraud-budget-bill/ **and** Democracy Watch, *Liberals and Conservatives rejected changes to budget Bill C-15 to make bank account fraud measures effective like in Australia*, Democracy Watch website, 26 February 2026. https://democracywatch.ca/liberals-and-conservatives-rejected-changes-to-budget-bill-c-15-to-make-bank-account-fraud-measures-effective-like-in-australia/

91 K Purkiss, *The silent enablers: Social media's role in Canada's growing fraud epidemic*, BioCatch, 28 July 2025. https://www.biocatch.com/blog/social-media-role-canada-fraud-epidemic

92 C McCord, *World of Scams: The Fraud Problem at the Heart of Online Advertising,* edited by K Bester, Canadian Anti-Monopoly Project, 3 February 2026. https://antimonopoly.ca/world-of-scams-the-fraud-problem-at-the-heart-of-online-advertising/

93 Department of Finance Canada, *National Anti-Fraud Strategy Discussion Paper*

94 Singapore Statutes Online, *Protection from Scams Act 2025 (No. 1 of 2025)*, Republic of Singapore, 2025. https://sso.agc.gov.sg/Act/PSA2025

95 Singapore Police Force, *Annual Scam and Cybercrime Brief 2025*, Singapore Police Force, 2026. https://www.police.gov.sg/-/media/SPF/Advisories/Scams/Annual-Scam-and-Cybercrime-Brief-2025.pdf

96 Singapore Police Force, *Annual Scams and Cybercrime Brief 2025*

97 Singapore Police Force, *Annual Scams and Cybercrime Brief 2024*, Singapore Police Force, 2025 https://www.police.gov.sg/-/media/SPF/Media-Room/Statistics/Annual-Scams-and-Cybercrime-Brief-2024/Annual-Scams-and-Cybercrime-Brief-2024.pdf **and** Singapore Police Force, *Annual Scams and Cybercrime Brief 2024* **and** Singapore Police Force, *Annual Scams and Cybercrime Brief 2025*

98 Singapore Police Force, *Annual Scams and Cybercrime Brief 2024* **and** Singapore Police Force, *Annual Scams and Cybercrime Brief 2025*

99 Singapore Police Force, *Annual Scams and Cybercrime Brief 2025*

100 Ministry of Digital Development and Information, *Measures to protect Singaporeans against online scams,* 10 January 2024. https://www.mddi.gov.sg/newsroom/measures-to-protect-singaporeans-against-online-scams/

101 D Dass, 'The Anti-Scam Centre: A Collaborative Approach Against Scams', *Singapore Police Force*, 29 November 2021. https://www.police.gov.sg/media-hub/police-life/2021/11/the-anti-scam-centre---a-collaborative-approach-against-scams

102 Monetary Authority of Singapore, *Guidelines on Shared Responsibility Framework*, Monetary Authority of Singapore, 24 October 2024. https://www.mas.gov.sg/regulation/guidelines/guidelines-on-shared-responsibility-framework

103 Monetary Authority of Singapore, *MAS and IMDA Consult on Shared Responsibility Framework for Phishing Scams*, Monetary Authority of Singapore, 25 October 2023, accessed 2 September 2026. https://www.mas.gov.sg/news/media-releases/2023/mas-and-imda-consult-on-shared-responsibility-framework-for-phishing-scams

104 Singapore Statutes Online, *Online Criminal Harms Act 2023 (No. 24 of 2023)*, Republic of Singapore, 2023. https://sso.agc.gov.sg/Act/OCHA2023

105 Ministry of Home Affairs, *Issuance of Implementation Directive to Meta Under the Online Criminal Harms Act* [press release], 25 September 2025, Singapore Government. https://www.mha.gov.sg/media-room/newsroom/issuance-of-implementation-directive-to-meta-under-the-online-criminal-harms-act/

106 Singapore Statutes Online, *Protection from Scams Act 2025*

107 Infocomm Media Development Authority, *Tightening of limit on number of postpaid SIM cards* [press release], 23 January 2026, Singapore Government. https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2026/tightening-of-limit-on-number-of-postpaid-sim-cards

108 Government Technology Agency, *Singpass*, Govtech website, 9 June 2026, accessed 10 July 2026. https://www.tech.gov.sg/products-and-services/for-citizens/digital-services/singpass/

109 S Koh, 'New SIM card checker tool rolled out in Singapore to combat scams', *The Straits Times*, 2 March 2026. https://www.straitstimes.com/tech/new-tool-lets-sporeans-check-the-number-of-postpaid-sim-cards-registered-to-their-name

110 Government of Singapore, *What Is ScamShield*, ScamShield website, last updated 21 May 2026, accessed 9 July 2026. https://www.scamshield.gov.sg/about-scamshield/what-is-scamshield/

111 Government Technology Agency, *Scam Analytics and Tactical Intervention System (SATIS)*, Govtech website, last updated 12 May 2026, accessed 9 July 2026. https://www.tech.gov.sg/products-and-services/for-citizens/scam-prevention/satis/

112 TODAY, 'Banks in Singapore to phase out login OTPs for digital token users', *Channel NewsAsia*, 9 July 2024. https://www.channelnewsasia.com/singapore/banks-in-singapore-phase-out-login-otps-digital-token-users-5573601

113 Infocomm Media Development Authority, *As part of anti-scam measures, Telcos to introduce option for mobile subscribers to block calls from international numbers* [press release], Singapore Government, 4 January 2024. https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/opt-to-block-incoming-international-calls

114 INTERPOL, *Towards agile and trusted policing,* INTERPOL website, n.d. https://www.interpol.int/en/How-we-work/Innovation/INTERPOL-Innovation-Centre

115 INTERPOL, *USD 439 million recovered in global financial crime operation* [news release], INTERPOL website, 24 September 2025. https://www.interpol.int/en/News-and-Events/News/2025/USD-439-million-recovered-in-global-financial-crime-operation

116 Singapore Police Force, *Operation FRONTIER: A United Front Against Transnational Scams*, Singapore Police Force website, 18 August 2025. https://www.police.gov.sg/Media-Hub/Police-Life/2025/08/Operation-FRONTIER-A-United-Front-Against-Transnational-Scams

117 Ministry of Home Affairs, *Strengthening ASEAN cooperation to combat cross-border scam syndicates*, Ministry of Home Affairs website, 6 October 2026.https://www.mha.gov.sg/media-room/newsroom/strengthening-asean-cooperation-to-combat-cross-border-scam-syndicates/

118 Council of Europe, *Singapore: Cybercrime policies/strategies*

119 J Teo, *Committee of Supply Debate 2025 on 'Building a Future-Oriented and Trusted Home Team'* [speech], Ministry of Home Affairs, Singapore, 4 March 2025. https://www.mha.gov.sg/media-room/newsroom/committee-of-supply-debate-2025-on-building-a-future-oriented-and-trusted-home-team/

120 Singapore Police Force, *SPF Forms New Cyber Command To Prevent, Deter And Disrupt Online Criminal Threats*, [news release], 3 July 2026. https://www.police.gov.sg/Media-Hub/News/2026/07/20260703_spf_forms_new_cyber_command_to_prevent_deter_and_disrupt_online_criminal_threats

121 UK Home Office, National Crime Agency and The Rt Hon Lord Hanson of Flint, *New disruption unit launched in crackdown on fraud*, UK Government, 9 March 2026. https://www.gov.uk/government/news/new-disruption-unit-launched-in-crackdown-on-fraud

122 Barclays, *Three in four shoppers believe AI advances have made scams more convincing, fuelling Black Friday fraud fears* [media release], Barclays website, 21 November 2025. https://home.barclays/news/press-releases/2025/11/three-in-four-shoppers-believe-ai-advances-have-made-scams-more-/

123 UK Home Office, The Rt Hon Liz Kendall MP and Jess Phillips MP, *Government leads global fight against deepfake threats*, UK Government, 5 February 2026. https://www.gov.uk/government/news/government-leads-global-fight-against-deepfake-threats

124 UK Government, *Fraud Strategy 2026–2029,* 2026, Government of the United Kingdom Home Office. https://assets.publishing.service.gov.uk/media/69aea29d917847c0a4c8999e/E03551200_Fraud_Strategy_2026__English__ELAY.pdf

125 UK Home Office, The Rt Hon Liz Kendall MP and Jess Phillips MP, *Government leads global fight against deepfake threats*

126 UK National Crime Agency, *Fraud Strategy supports National Crime Agency's commitment in fight against fraud*, UK National Crime Agency, 9 March 2026. https://www.nationalcrimeagency.gov.uk/news/fraud-strategy-supports-national-crime-agency-s-commitment-in-fight-against-fraud

127 UK National Crime Agency, *Operation Henhouse: Strongest year yet in fight against fraud led by NCA and City of London police*, UK National Crime Agency, 24 March 2026. https://www.nationalcrimeagency.gov.uk/news/operation-henhouse-strongest-year-yet-in-fight-against-fraud-led-by-nca-and-city-of-london-police

128 J Sullivan, *APP fraud: The UK's mandatory reimbursement requirement*, Thomson Reuters Institute, 2 April 2024. https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/app-fraud-uk/

129 R Bratby, *APP fraud reimbursement: the evidence after one year*, Bratby Law, 6 July 2026. https://bratby.law/app-fraud-reimbursement-evaluation/

130 UK Finance, *Annual Fraud Report 2026*

131 UK National Cyber Security Centre, *Respond to a cyber attack: Phishing*, UK National Cyber Security Centre website, n.d. https://www.ncsc.gov.uk/section/respond-recover/phishing **and** UK North Yorkshire Police, *Deepfakes,* UK North Yorkshire Police website, n.d. https://www.northyorkshire.police.uk/advice/advice-and-information/online-safety/online-safety/deepfakes-what-is-a-deepfake/ **and** UK Police, *Report Fraud*, Report Fraud website, n.d. https://www.reportfraud.police.uk/

132 UK AI Security Institute, *An evaluation framework for AI misuse in fraud and cybercrime*, UK AI Security Institute, 26 February 2026. https://www.aisi.gov.uk/blog/an-evaluation-framework-for-ai-misuse-in-fraud-and-cybercrime

133 UK Home Office, *Offence of 'failure to prevent fraud' introduced by ECCTA*, UK Home Office website, 6 November 2024. https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta **and** A recent example: UK Foreign, Commonwealth & Development Office and The Rt Hon Yvette Cooper MP, *UK and EU strike Russian cyber networks with new sanctions* [press release], UK Government, 13 July 2026. https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions

134 UK Department for Science, Innovation and Technology, *Guidance: Online Safety Act: explainer*, UK Government, updated 24 April 2025. https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

135 D Milmo, 'Big tech platforms will have to ban scam ads under UK plans to tackle fraud', *The Guardian,* 11 July 2026. https://www.theguardian.com/media/2026/jul/10/online-platforms-ban-scam-ads-uk-fraud-ofcom-online-safety-act

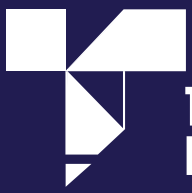
136 Take Five to Stop Fraud, *Homepage*, Take Five to Stop Fraud website, n.d. https://www.takefive-stopfraud.org.uk/

137 Global Signal Exchange, *About*, GSE website, n.d. https://www.globalsignalexchange.org/about

138 UK Home Office, National Crime Agency and The Rt Hon Lord Hanson of Flint, *New disruption unit launched in crackdown on fraud*

139 UK Home Office, The Rt Hon Liz Kendall MP and Jess Phillips MP, *Government leads global fight against deepfake threats*

140 UK Finance, *Annual Fraud Report 2026*
141 Cifas, *Homepage*, website, n.d. https://www.cifas.org.uk/ **and** UK Government, Companies House, UK Government website, n.d. https://www.gov.uk/government/organisations/companies-house
142 UK Home Office and The Rt Hon Lord Hanson of Flint, *Global taskforce launched to hunt down overseas scammers*, UK Government, 17 March 2026. https://www.gov.uk/government/news/global-taskforce-launched-to-hunt-down-overseas-scammers
143 UK Home Office, *National Assessment Centre Fraud assessment 2025*, UK Government, 9 March 2026. https://www.gov.uk/government/publications/national-assessment-centre-fraud-assessment-2025/national-assessment-centre-fraud-assessment-2025
144 Adobe, Pinterest, Google, OpenAI, LinkedIn, Match Group, Meta, Amazon, Microsoft, Target and Levi Strauss & Co are signatories. Source: *Industry Accord Against Online Scams & Fraud*, 2026. https://services.google.com/fh/files/newsletters/industryaccord.pdf
145 UK Home Office, *National Assessment Centre Fraud assessment 2025*
146 J Burton, A Janjeva, S Moseley and Alice, *AI and Serious Online Crime*, The Alan Turing Institute, March 2025. https://cetas.turing.ac.uk/sites/default/files/2025-03/cetas_research_report_-_ai_and_serious_online_crime_0.pdf
147 UK Home Office and Jones S MP (10 June 2026), 'PoliceAI to speed up investigations and fight crime', *UK Government*, https://www.gov.uk/government/news/policeai-to-speed-up-investigations-and-fight-crime
148 D Tilbury, *What new rules for agentic AI in payments might look like*, Pinsent Masons website, 8 July 2026. https://www.pinsentmasons.com/out-law/analysis/what-new-rules-agentic-ai-payments-look-like
149 V Shpachuk, O Markova and B Adamyk, 'AI-driven financial fraud: key risks and legal protections for financial institutions', *Journal of Banking Regulation,* 20 July 2026, 27(6). https://link.springer.com/article/10.1057/s41261-025-00304-y
150 C Smith C and J Meierhans, 'Banks must refund fraud up to £85,000 in five days', *BBC News,* 25 September 2024. https://www.bbc.co.uk/news/articles/cy94vz4zd7zo
151 UK Public Sector Fraud Authority, *Introduction to AI Guide with a focus on Counter Fraud*, UK Government, 18 March 2024. https://www.gov.uk/government/publications/introduction-to-ai-with-a-focus-on-counter-fraud/introduction-to-ai-guide-with-a-focus-on-counter-fraud-html
152 Financial Conduct Authority, *Supercharged Sandbox*, FCA website, last updated 22 July 2026. https://www.fca.org.uk/firms/innovation/supercharged-sandbox **and** S Mills, *AI and the future of retail financial services (The Mills Review)*, Financial Conduct Authority, last updated 6 July 2026. https://www.fca.org.uk/publications/corporate-documents/mills-review
153 E Cox, *UK looks to reshape public service media as tech platforms face demand to showcase 'trusted' news*, Pinsent Masons, 8 July 2026. https://www.pinsentmasons.com/out-law/news/uk-public-service-media-tech-platforms-trusted-news
154 Canadian Radio-television and Telecommunications Commission, Implementation of Universal Network-Level Blocking of Calls with Blatantly Illegitimate Caller Identification, *Compliance and Enforcement and Telecom Decision CRTC 2018-484*, Government of Canada, 19 December 2018. https://crtc.gc.ca/eng/archive/2018/2018-484.htm **and** Canadian Radio-television and Telecommunications Commission, *Canadians to benefit from new caller ID technology to combat spoofed calls* [news release], Government of Canada, 30 November 2021. https://www.canada.ca/en/radio-television-telecommunications/news/2021/11/canadians-to-benefit-from-new-caller-id-technology-to-combat-spoofed-calls.html
155 Singapore Police Force, *Annual Scams and Cybercrime Brief 2025*
156 UK Department for Science, Innovation and Technology, *Guidance: Online Safety Act: explainer*, UK Government, updated 24 April 2025. https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer



TECH POLICY
DESIGN INSTITUTE