pwc

GASA
Global Anti-Scam Alliance

Uniting against fraud

How anti-scam centres can strengthen national fraud defences
October 2025

Contributors

At the heart of the national anti-scam centre concept explored in this paper lies a core principle: that only through collaboration can fraud be tackled effectively.

No single organisation or group holds all the necessary data or has all the capabilities needed to tackle fraud completely. Instead, it is by combining the data, intelligence, resources, skills and insights of multiple organisations that a response greater than the sum of its parts can be built and which matches criminals' ability to operate across platforms, services and borders.

The development of this paper reflects the very same principle: We have collaborated with the Global Anti-Scam Alliance (GASA), Euroconsumers, Cifas, and a range of other industry organisations to shape shared thinking on the role national anti-scam centres could play in strengthening fraud defences as part of a broader whole-system approach.

Contributors have shared their perspectives on priority areas of focus and successful international practices, helping to inform possible paths forward towards greater collaboration.

We are grateful to all the organisations that have contributed to the development of this paper, bringing together cross-industry and international perspectives, and demonstrating the power of collective action in the fight against fraud.

Contents

Foreword

Jorij Abraham

Managing Director, GASA

Els Bruggeman

Head of Policy, Enforcement and Communication, Euroconsumers

Simon Miller

Director of Policy, Strategy and Communications, Cifas

Fraud has become one of the most pervasive and damaging threats facing individuals and businesses around the world. According to GASA's latest Global State of Scams report, the scale of the challenge is staggering: scams cost consumers over US$1 trillion worldwide in 2024[1]. And losses are not just financial, fraudsters exploit the vulnerable, erode trust and undermine the integrity of digital and financial systems globally.

International Organised Crime Groups (OCGs) have embraced fraud as a low-risk, high-reward opportunity. The anonymity enabled by digital platforms, the speed of cross-border transactions, and the sheer volume of potential targets have created an environment in which criminals can operate with impunity. These actors are not lone opportunists, they are part of well-resourced, agile criminal networks that adapt quickly to exploit weaknesses across systems and jurisdictions.

To counter this threat, our defences must be equally coordinated and dynamic. We must deploy a range of interventions (prevention, detection, disruption and enforcement) including raising awareness, improving the detection of fraudulent content and communications, enhancing payment monitoring and interventions, increasing the use of disruptive tactics and prosecutions, accelerating the blocking and seizure of the proceeds of fraud and ensuring better victim support.

Encouragingly, there is no shortage of innovation. Across sectors and countries, promising new initiatives and technologies are emerging. Financial institutions are investing in better detection. Tech platforms are developing smarter content moderation and data sharing initiatives. Law enforcement agencies are delivering new investigative techniques. Civil society groups are leading impactful awareness campaigns and providing victim support. But these efforts, while valuable, often operate in silos.

What is often missing is a mechanism to bring capabilities together and build a holistic response. This is why every country needs a national anti-scam centre: to facilitate collaboration, coordinate across the ecosystem and to enable collective responses.

Anti-scam centres can take many forms, but crucially they unite expertise, data and operational capabilities from across sectors. Several countries have already established such collaboration centres and there is no single answer to what an anti-scam centre can be or what it should do. By establishing collaboration centres at a national level and linking them together internationally a global web can be established to create a network of allied units. Such a network could not only enhance capabilities within countries but also help to block the flow of criminal proceeds across borders and disrupt transnational criminal networks that profit from fraud.

We are delighted to have worked with PwC on this report exploring how national anti-scam centres can serve as a cornerstone of a more integrated and effective response to scams. The paper draws on insights from across industries and geographies, and we hope it contributes to the growing momentum for collective action. Because only together through shared purpose, shared intelligence, and shared responsibility can we turn the tide against fraud.

[1] https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai

Introduction

In March 2025, London hosted the Global Anti-Scams Summit (GASS). Organised by GASA in partnership with the UK Home Office, Cifas – the UK's leading fraud prevention service – and Euroconsumers, the event brought together almost 800 anti-fraud specialists from across industries and countries. The summit served as a powerful reminder of the scale and complexity of fraud threats, and the need for coordinated action both at a national-level and globally.

PwC worked with GASA to convene a panel at the summit with representatives from organisations including the European Commission, Cifas and Euroconsumers to discuss the potential role of national anti-scam centres in improving collaboration and driving greater coordination across sectors. The panel discussed the growing drive for coordinated national responses to fraud, including Euroconsumers call for national fraud hotlines following their international consumer forum in Brussels in 2024[2]. Euroconsumers also hosted a panel at GASS focused on the importance of collaboration to deliver support for fraud victims.

These panels explored the organisational models that could be established to bring together data, technology, and expertise from across the public and private sectors to enable a more unified response to fraud. The panels also discussed approaches already in place globally including in the UK, Australia, Singapore, Netherlands and Taiwan and how learnings from these could help create a blueprint for success elsewhere.

This paper builds on the discussion at GASS London 2025, summarising the panel's perspectives, supplemented by additional research on how anti-scam centres could function, what value they can deliver, and how they might be structured to support a whole-system fraud response.

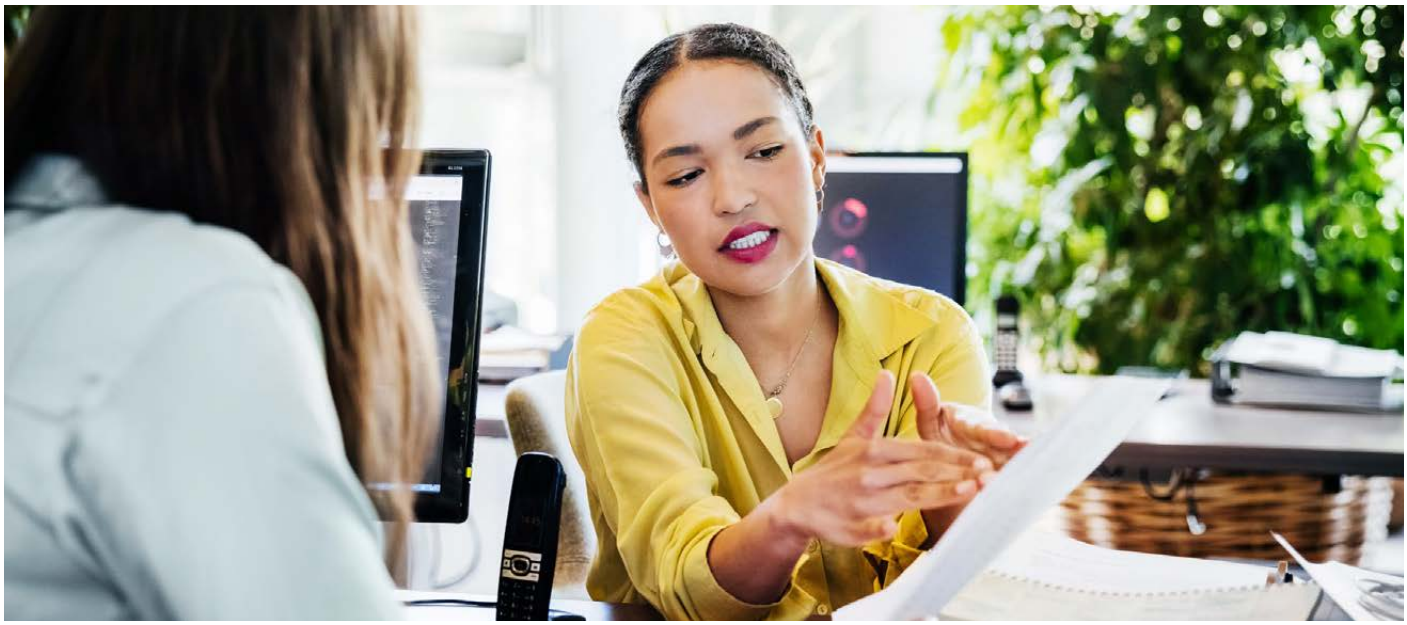
[2] https://www.euroconsumers.org/wp-content/uploads/2024/12/Scam-victims-need-backup-Euroconsumers-and-GASA-call-for-national-fraud-hotlines-.pdf

Understanding the current anti-scam centre landscape

National responses to fraud have evolved organically over many years. The structure of existing national anti-fraud organisations and their respective roles varies significantly by country, shaped by distinct national contexts, institutional legacies and histories of cross-sector and public-private collaboration. While these factors mean that no two countries have quite the same setup, there are three broad models that typically apply:

1. Fragmented fraud response

- No centralised coordination of national anti-fraud response with anti-fraud capabilities being developed in silos based on individual industry and/or organisational priorities and incentives.
- While this model often gives rise to a highly dynamic and innovative anti-fraud ecosystem, the lack of central coordination can hinder rapid, unified responses to fraud.
- Organisations can be highly successful in delivering their individual objectives, but with greater potential for gaps to arise in the framework with potential benefits of joined up action being missed and greater potential for duplication of effort across the system.
- This model does not preclude collaboration, whether bilaterally, within industries or across sectors, but it can be harder to scale or industrialise initiatives to deliver a system-wide approach leading to gaps in defences that can be exploited to the detriment of the system as whole.

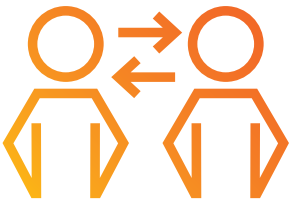


2. Anti-fraud organisation with focused remit

- Some jurisdictions have developed centralised anti-fraud centres that facilitate cross-organisation collaboration, but with remits that are focused on a particular type of fraud.
- These organisations have typically been established to tackle a specific fraud issue at a point in time, for example criminal activity across a specific border between two countries or a particular type of fraud like identity theft or online shopping scams.
- While these organisations often have existing technical capability and well-established pathways for collaboration across different organisations, both public and private, they may not have the breadth of capabilities or the organisational mandate to expand their remit into other areas.

3. National anti-scam centre

- The scale and impact of fraud in some countries has led to the establishment of dedicated anti-fraud centres with broad remits to drive improved prevention, detection and response across the ecosystem.
- Organisational models vary from country to country, but the core principle is to establish a centralised coordinating organisation to act as a focal point for collaboration across the wider anti-fraud ecosystem.
- The roles and activities of an anti-scam centre will vary, but the guiding principle is to break down silos and facilitate the sharing of data, intelligence, capabilities and resources across organisations involved in the fight against fraud.
- Anti-scam centres help to knit together fragmented national capabilities and provide businesses and consumers with a clearly defined and visible point of contact in relation to fraud.



Most countries globally operate with a fragmented model where different law enforcement agencies, and public and private sector anti-fraud groups operate in silos. There can still be extensive collaboration across this fragmented structure, but this is often driven more informally with greater reliance on the different stakeholders across the ecosystem finding ways to work together. The next section of this paper outlines the benefits that can be delivered by transitioning towards a national anti-scam centre model, which could be achieved in a number of different ways:

Transition approach	Benefits	Potential challenges
1. Establishing an anti-scam centre as a new organisation to knit together existing organisations.	• Roles and responsibilities could be clearly defined at the outset minimising the risk of overlapping remits. • Opportunity to reset a fragmented approach and lead with a more coherent national strategy. • A new organisation could be designed from scratch to be fit for the future, less hindered by legacy structures, mindsets and tooling.	• Risk of creating another organisation to add to an existing 'alphabet soup' of agencies and organisations tackling fraud. • Establishing a new organisation's authority, credibility and consumer recognition could take time. • Success of the organisation will rely on stakeholders buying in to its objectives and collaborating effectively. • Establishing new funding can be complex. • The ability to establish public-private partnerships will depend on the influence the new organisation is able to exert across relevant organisations.
2. Expanding the role and remit of an existing anti-fraud organisation.	• Opportunity to leverage technical capabilities and expertise within existing organisation. • Maximises impact by strengthening a well-established agency, rather than creating additional structures. • Established organisation can bring existing credibility and authority across the ecosystem, as well as existing relationships with other organisations.	• May be harder to adapt existing organisation to its expanded remit. • Can be difficult to overcome existing biases and perceptions of the strengths and weaknesses of an existing organisation, which may impact the ability to drive successful public-private partnerships. • Inter-organisational politics and competing remits can stifle support for the organisation's expanded role. • Can be difficult to adapt existing funding models to support expanded remit.

Routes to establishing anti-scam centres would need to reflect specific country structures and nuances. Every country will have distinct political contexts and narratives around public-private partnership that will influence what anti-scam centre structures are achievable and governments in different countries will have varying abilities to influence private sector participation in anti-scam centres. Establishing anti-scam centres in countries with more well-established anti-fraud organisations and mature collaboration networks will involve navigating greater complexity to design a structure that compliments and integrates effectively with existing approaches.

Conversely, while building more 'from scratch' may appear simpler, more foundational work to establish pathways for collaboration may be needed.

Establishing an anti-scam centre would likely require an initial group of organisations to provide seed funding and to drive initial organisational design and set up. This could be led by any combination of organisations across the private sector, or through a public-private partnership or by central government.

What challenges can national anti-scam centres address and what improved outcomes could they deliver?

There is increasingly widespread international recognition that fraud is a serious societal issue with governments, regulators and industry leaders elevating the topic on their agendas. In several jurisdictions, organisations are already working together to share data and insights, recognising that collective action is key to staying ahead of increasingly sophisticated fraud tactics. While the direction of travel has been positive, there is still considerable room for improvement. In this section, we summarise the challenges inherent in the typically fragmented fraud response that we see across many jurisdictions and the beneficial outcomes that national anti-scam centres could realise.

01

Siloed ecosystem

▼

Networked system response

One of the most significant barriers to tackling fraud is the siloed nature of the anti-fraud ecosystem, both within individual countries and globally. Each organisation, whether a bank, telecom operator, tech platform, law enforcement agency or victim organisation, has visibility over only a narrow slice of the fraud landscape. This limited perspective makes it difficult to understand the full picture and to anticipate how fraudsters are adapting across channels. Innovation is common and there are a wide range of initiatives at both a national and global level for sharing intelligence and data, collaborating on consumer education, and in support of law enforcement investigations but it can be difficult to achieve a critical mass of support making them harder to scale, join up and to industrialise outputs.

How anti-scam centres could help

National anti-scam centres can create a shared space for collaboration. By bringing together representatives from across sectors, these centres can enable better understanding of what data, capabilities, and insights exist and how they can be combined to strengthen defences. By providing system-level leadership, anti-scam centres can also drive strategic choices about which initiatives to scale and offer a guiding picture to align them into a cohesive and mutually supporting set of national capabilities.

Outcomes

- Increased collaboration and more networked ecosystem, nationally and across borders.
- A system-level strategy and strategic capability development.
- Critical mass participation in anti-fraud initiatives.
- Better scaling of successful initiatives to industrialise outputs.

02

Misaligned standards and investment decisions

System-level decision making and standard setting

Linked to siloed nature of the ecosystem, in fragmented models each individual organisation, whether public or private, develops capabilities to address their individual risks and organisational mandates. While this means that capabilities are effectively tailored to specific use-cases, it can mean that the resulting ecosystem-wide response contains high levels of duplication, overlapping initiatives and inefficiency. Choices about where to construct strategic data and technology capabilities, such as sector-level or national tooling, or where to locate skills and resources are made in the context of each individual participant rather than the system a whole. As a further consequence, policies and standards vary across the ecosystem making it both harder to link disparate processes together from a technical perspective but also creating blockers to collaboration due to the need for alignment of processes and governance.

How anti-scam centres could help

National anti-scam centres have the potential to play a transformative role in shaping the broader system response to fraud. By convening key stakeholders from across sectors (financial services, telecom operators, technology, law enforcement, and consumer advocacy) these centres can serve as a focal point for joined-up decision-making and coordinated action. These centres could offer a mechanism to establish leadership rather than relying on individual organisations or sectors to act in isolation, a national anti-scam centre could provide a structured forum where diverse perspectives are brought together to inform strategy, align priorities, and drive collective progress. Done well, a national anti-scam centre could become the strategic brain of the anti-fraud ecosystem guiding investment, aligning efforts, and ensuring that the response to fraud is as coordinated and adaptive as the threats themselves.

Outcomes

- More strategic-level decision making on where resources, data and technology can be most effectively deployed to disrupt frauds and protect consumers
- Policy and operational responses that are informed by real-time insights from across the whole ecosystem
- Coordinated development of cross-sector tools, data infrastructure, and response mechanisms that no single organisation could build alone.

03

Slow and incomplete data and intelligence sharing

Fraudsters move quickly, often exploiting new vulnerabilities before defences can catch up. But the pathways for sharing data and intelligence across the ecosystem are often slow, unclear, or incomplete. Organisations may not know what information would be valuable to others, or how to share it securely and appropriately. In some cases, information may be shared only in summarised form, stripping it of the detail needed to drive meaningful intervention. Legal risk and data privacy obligations can be actual or perceived blockers to data and intelligence sharing, creating additional compliance and governance burdens that can discourage cross-sector collaboration.

Accelerated interventions powered by shared insight

How anti-scam centres could help

National anti-scam centres can serve as a central hub for intelligence coordination helping to define what types of data and intelligence are most useful, and establishing streamlined, governed routes for dissemination that address data privacy concerns. They could also support the sharing of best practice across the ecosystem and work with national authorities to clarify or update interpretations of data sharing 'safe harbours'. Centralising some types of data and intelligence sharing could also reduce the need for bilateral data sharing agreements, supporting faster networking of data and standard industry-accepted terms. A centralised model could also reduce the burden on law enforcement to manage multiple bilateral relationships, allowing them to focus on high-impact interventions while ensuring intelligence is shared with the right partners under a clear governance framework. They could also help to ensure that intelligence is made available to all relevant organisations, avoiding the situation where data providers' commercial models make accessing data unaffordable for smaller industry players.

Outcomes

- Greater clarity and understanding of data available across the ecosystem.
- Development of updated, or clarified, data privacy standards in the context of fraud prevention and detection.
- Consistent and governed routes for data and intelligence sharing that address data privacy concerns.
- Faster dissemination of valuable information to support disruption, blocking and seizure of proceeds of fraud.
- More consistent access to valuable information regardless of organisational scale.
- Faster, smarter, and more coordinated responses to fraud.

04

Confusing and inconsistent fraud reporting

‘Report it once’ model

In many countries, the landscape of organisations and authorities involved in fraud prevention, detection, enforcement and redress is complex and fragmented. This can make it difficult for individuals to know where to report fraud or they may be urged to report it multiple times to multiple different stakeholders. A recent Euroconsumers’ survey showed that more than half of fraud victims did not seek help at all and when they did reach out only one out of three decided to report to the police or their bank[3]. This situation results in patchy data, missed opportunities for intervention, and a lack of coordinated response. Phishing, smishing and vishing calls might be reported to one, or in some jurisdictions, multiple different authorities as well as to the different communication platform operators. Fraudulent online adverts might be reported to different trading standards-focused organisations, or to the online platform carrying the advert, or possibly to law enforcement or to a bank by a customer that has become a victim of a fraud. This inconsistency leaves many consumers uncertain about where to report different types of frauds, leading to underreporting and a sense of futility and a perception that authorities are indifferent or inactive when it comes to tackling fraud.

How anti-scam centres could help

A single, unified reporting mechanism could change this situation giving victims clarity, confidence, and a greater sense of agency in the fight against fraud. A national anti-scam centre could support a “Report Once” model for fraud. Regardless of how or where a consumer reports a fraud, the information would be routed to a central hub and shared with the appropriate organisations. To be effective, this system would require strong data infrastructure, secure intake channels, and clear governance protocols. Crucially, it would also need to demonstrate that action is being taken building public trust by showing how reports lead to real-world outcomes.

Outcomes

- Clarity for victims on where to report fraud.
- Reduced stress and emotional toll on victims caused by the need to navigate confusing reporting processes.
- Consistent and more complete data capture and insight into incidence of fraud.
- Enable dissemination of insights derived from reporting fraud more consistently across the wider ecosystem.

[3] Euroconsumers (2024), Caught in the web: Navigating the digital maze of scams, https://www.euroconsumers.org/wp-content/uploads/2024/12/Caught-in-the-web-Navigating-the-digital-maze-of-scams.pdf

05

Lack of support for victims

Joined up victim care

Victims and consumer organisations regularly highlight that there is often a lack of understanding of the collateral damage that fraud can cause including emotional and psychological harms but also practical challenges of reclaiming access to online accounts and profiles, rebuilding credit profiles and regaining confidence to use online and digital banking services. The level of care a victim receives can depend entirely on which organisation they report to and whether that organisation has a regulatory obligation to help. In many cases, no support is offered at all. Where help is available, it is frequently delivered by charities or non-profit organisations whose capacity is constrained by limited funding and regional reach. This patchy landscape can deepen the trauma of being scammed, leaving victims feeling isolated and unsupported.

How anti-scam centres could help

National anti-scam centres can facilitate better responses for fraud victims, providing referrals to services that provide consistent, high quality care. They can provide a central point of contact to direct consumers to the wide range of different support services that can be needed in the wake of fraud. By simplifying the landscape, understanding victim needs and improving coordination, these centres can help build public trust and ensure that support reaches those who need it most. Having specialists in fraud victim support would also provide the anti-scam centre with a comprehensive picture of how best to support victims, providing valuable insight to refine how fraud prevention work is resourced and prioritised.

Outcomes

- Clear pathways for the reporting of fraud, leading to higher reporting rates and increased insight into fraud threats and trends.
- Simple, centralised point of contract for victims to access high-quality anti-scam advice and support .
- Victim centric insight to inform refinement of anti-fraud measures and upstream intervention strategies.

06

Inconsistent and public awareness campaigns

Inclusive and insight-driven education

Globally, public knowledge of fraud threats is patchy, and awareness campaigns are spread across multiple agencies and industries with inconsistent messaging. Education campaigns can be costly and organisations with greatest potential ability to reach and engage the public may not be incentivised to invest in impactful fraud awareness content. Multiple overlapping campaigns delivered through the same mediums and targeting the same audience can lead to duplication of effort and a lack of consistency in themes and advice being delivered.

How anti-scam centres could help

Fraud and scams awareness and education is not something that a single organisation can ever deliver on its own, it is the work of many different organisations, each of whom may have access and be able to reach a different group of people. However, having a central point of collaboration for public fraud and scams awareness can facilitate the sharing of best practices and elevate bottom-up initiatives. By acting as a centre of excellence, a national anti-scam centre could facilitate and align awareness efforts.

Outcomes

- Elevated public awareness campaigns with increased engagement based on insight of victim experiences.
- Education materials contain consistent messaging across sectors and platforms
- Inclusive education that reaches all age groups and demographics by ensuring content is delivered through appropriate communication channels.
- Education materials are responsive to emerging fraud tactics and trends.
- Processes to measure education campaigns against clear success criteria to evaluate impact and effectiveness.

07

Limited scope for disruption

Coordinated disruption across the whole ecosystem

Tackling fraud is a constantly evolving cat and mouse game and historically, approaches have necessarily focused on a limited number of key moments in a fraud lifecycle, validating information at onboarding, protecting access to a customer account, screening a payment, etc. However, fraud lifecycles often start far upstream of these events with criminals needing to set up profiles, accounts and infrastructure to support fraud tactics and with early contact and communication with the victim often long before a transfer of funds occurs. While it is obviously sensible to concentrate prevention and detection activities at these crucial points in the fraud lifecycle, earlier opportunities to disrupt criminal activities can often be missed.

How anti-scam centres could help

In addition to their coordination role, anti-scam centres could play a proactive and disruptive role in the fight against fraud. These centres would be empowered to take direct action to identify, interrupt, and dismantle scam operations through a range of strategic capabilities and working in partnership with other public sector organisations and law enforcement agencies. By leveraging integrated datasets, they could detect emerging trends and behavioural patterns to triangulate the identities or locations of fraudsters. They could also deploy time-wasting tactics, so called honey-potting, to divert criminals' efforts and reduce harm to the public. Operational capabilities could include the takedown of fraudulent websites, phone numbers, and fraudulent online identities or profiles. Anti-scam centres could also coordinate the freezing of accounts across multiple banks and organisations, ensuring a swift and unified response to active threats. To support law enforcement, these centres would offer technical expertise, advanced data analytics, and actionable intelligence to aid investigations and interventions. International collaboration would be key, enabling coordination with overseas counterparts to disrupt cross-border fraud networks.

Outcomes

- Use of joined-up datasets to identify fraud patterns and triangulate the identity or location of criminals.
- Disruption and distraction initiatives like honeypots to waste fraudsters' time and reduce their effectiveness.
- Enhanced takedown operations to support removal of fraudulent websites, phone numbers, and fraudulent online profiles.
- More coordinated and rapid freezes across multiple banks and organisations to block fraud-related transactions.
- Delivery of covert and technical expertise, intelligence, and analytics to aid investigations and interventions.
- Collaboration with global counterparts to target and dismantle overseas criminal fraud operations.

08

National responses

Networked international response

While there are well established mechanisms for international cooperation between national law enforcement agencies, historical responses to fraud have primarily been driven at a national level. However, the ease with which money can move across borders and the growth of transnational online platforms has meant that fraud is now a truly international enterprise. Tackling fraud requires close cooperation between international governments and law enforcement agencies and joined up action by global industry players who have footprints across multiple countries affording the best possible protections to their users wherever they are located.

How anti-scam centres could help

Establishing anti-scam centres at a national level would provide a clearly defined and centralised point of engagement for other similar organisations based in other countries. These centres could foster closer cooperation across borders and help to accelerate responses to changing fraud patterns and modus operandi. In the longer term, there may be benefit in establishing international agencies to support international standard setting and connectivity, following the model that has been adopted for international action against money laundering.

Outcomes

- Joined up network of national centres that coordinate cross-border anti-fraud activities.
- Clearer pathways for sharing of best practice and insight.
- Support raising of global standards to tackle fraud.

Principles for building a national anti-scam centre

There is no one size fits all model for an anti-scam centre and each country's approach would need to be shaped considering the existing national situation, the constellation of different organisations involved in the fight against fraud, and the different objectives and roles that a national anti-scam centre might perform. Developing an anti-scam centre would require careful consideration of this environment and how best to bring together existing capabilities to deliver its objectives. Defining objectives and linked organisational design principles at the outset would be critical for this journey. In this section, we set out some of the key principles that would require consideration when designing an anti-scam centre.

01

Embed credible, empowered leadership

Effective leadership will be foundational. The anti-scam centre would need to be led by a team with credibility across sectors, people with a track record in tackling fraud. Leadership could not only set strategic direction but also act as visible advocates, using their networks to convene stakeholders and build momentum. Trust will be critical.

Leadership structures should be designed to ensure representation and voice across sectors. An elected oversight board, where relevant industries nominate sector representatives, could help build this trust. In practice, the centre may need to start with a small group of committed organisations and scale as credibility and impact grow.

02

Establish a clear mandate, define objectives and demonstrate impact

A clear mandate and defined objectives would be essential for the success of the anti-scam centre, both to ensure alignment between participating organisations but also to ensure the role of the organisation is understood across the wider ecosystem. Objectives would need to be tied to measurable outcomes so that the success of the anti-scam centre could be monitored. Ambitions and objectives would need to be defined through a set of strategic goals and KPIs, such as reductions in fraud losses, increased prosecutions, improved consumer outcomes, or enhanced cross-sector collaboration.

Objectives and linked metrics would need to be defined tightly and agreed across relevant stakeholders to help focus activity on an agreed set of priorities. Metrics would need to be underpinned by quality data and robust evaluation. Feedback loops would need to be built in to assess impact and adapt strategy. This would include both quantitative indicators and qualitative insights, such as consumer confidence or stakeholder satisfaction. Having clear targets and monitoring of metrics would help to focus efforts and help decision making in relation to multiple, potentially conflicting, priorities.

03

Establish robust inclusive governance

Robust governance will be essential to ensure accountability, transparency, and strategic alignment. A joint strategy board, comprising public and private sector stakeholders, could provide oversight and advise on priorities, ensuring the centre remains focused and responsive. To maintain trust, governance would need to balance agility with checks and balances. A clearly defined mandate, subject to regular review, could help achieve this.

Independent review mechanisms should be built in to assess whether the anti-scam centre is delivering against its objectives and operating within its remit. Participation from sector regulators will also be important: their involvement could reassure stakeholders that the anti-scam centre's actions are aligned with broader regulatory frameworks and national strategies.

04

Ground operations in legal frameworks that enable collaboration

The anti-scam centre's ability to share insight and data effectively will depend on the legal frameworks that underpin it, particularly in relation to data privacy. Clear pathways could be established to enable lawful and secure sharing of information across sectors, while respecting privacy and confidentiality. Existing or new 'safe harbours' for sharing certain types of data could enable institutions to share information and an anti-scam centre could act as a centre routing authority, maintaining technology that enables compliance with privacy standards.

It would be critical to address civil liability fears by providing reasonable and transparent guardrails for information sharing. In some jurisdictions, new legislation may be required to support this, particularly where enforcement powers or cross-border collaboration are involved, or it may be necessary for authorities to clarify or update their interpretations of data privacy rules to alleviate institutions' fears of penalties when sharing data for the purpose of fraud prevention and detection. Guardrails will also be needed to manage the sharing of sensitive data, including data such as customer information or proprietary intelligence.

05

Design for agility through a modular organisational mode

The anti-scam centre would need to be designed for flexibility. A modular structure could allow it to adapt to emerging threats and policy priorities. Specialist teams, sometimes referred to as fusion cells, could be formed, focused on intelligence, disruption, victim support, or communications, scaling up or down as needed.

Rotating roles, particularly from the private sector, could help build networks, share knowledge, and foster a sense of joint ownership. To attract talent, these roles would need to be positioned as valuable development opportunities.

06

Resource for multi-disciplinary excellence and continuity

The skills required will depend on the centre's role, but are likely to include data science, legal and regulatory expertise, customer service, victim support, communications, and law enforcement. This diversity of capability is essential to understanding and disrupting the full fraud lifecycle. A blended resourcing model is likely to be most effective.

The strength and success of anti-scam centre will lie first and foremost in its ability to the connect different (existing) stakeholders fighting fraud and bring in the specialist expertise of each and every one of them. Training and development pathways should be built in from the start. Participation in the anti-scam centre should be seen as a career-enhancing opportunity, an experience that builds skills, networks, and purpose.

07

Build and integrate system-level capabilities

The anti-scam centre would need to be clear about which capabilities it builds in-house and which it integrates from existing initiatives. In an ideal world, it would sit at the centre of a whole-system response. In practice, it would need to work alongside and sometimes through existing structures. Duplication of capability between the anti-scam centre and existing initiates should be avoided but may be inevitable at the outset.

Over time, the centre should focus on scaling what works and integrating with other organisations to eliminate duplication and avoid fragmentation. Strategic capabilities, such as data analytics or disruption operations, could be added incrementally as the centre matures. System-level design will be critical. The anti-scam centre would need to be positioned not as a competitor, but as a coordinator amplifying and aligning the efforts of others.

08

Secure sustainable diversified funding

Sustainable funding is essential. Initial seed funding from the government or industry could demonstrate commitment and de-risk early development. But over time, funding would need to be diversified. Options include direct contributions from industry, in-kind support by participating organisations (e.g. provision of technology infrastructure, office space, seconded personnel etc.), third-party funding from anti-fraud organisations and foundations, and joint investment in shared capabilities. Outcome based funding models could also be explored, linking investment by the government to measurable impact.

Investment could itself be sourced through a direct fraud levy on relevant sectors or organisations (e.g. a so called 'polluter pays' model) or it could be provided by utilising funds seized from fraudsters (likely requiring legislative change in some jurisdictions to enable this). Whatever the model, long-term commitments would be needed. An anti-scam centre would take several years to establish and embed effectively. Operating hand-to-mouth would not be conducive to long term, strategic planning. Multi-year funding, ideally on a 3–5 year cycle would be needed to provide the stability needed to plan, invest, and deliver.

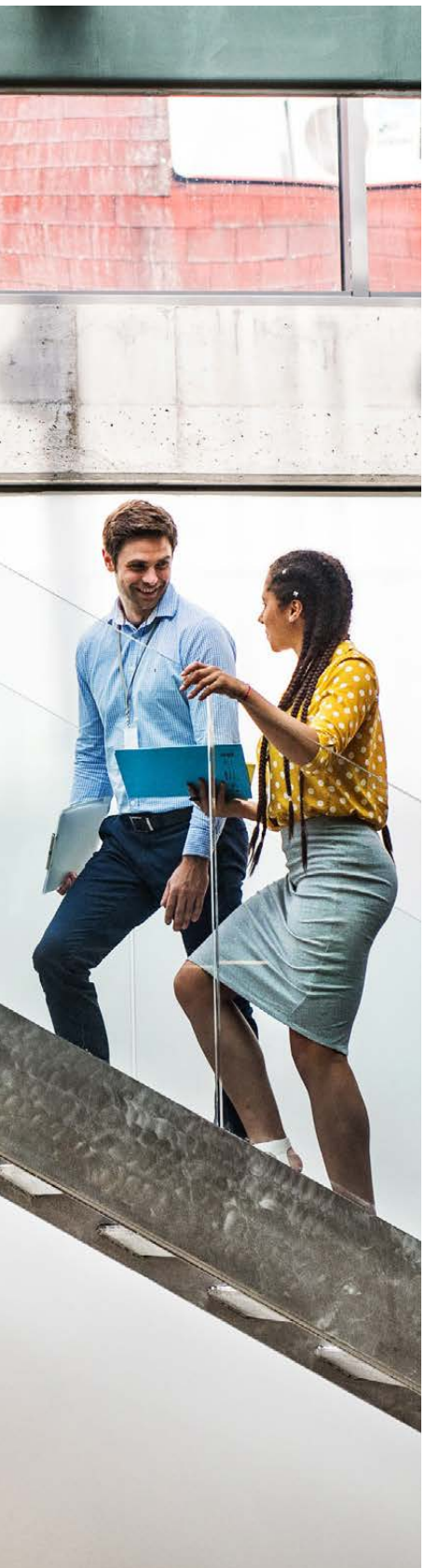
09

Cultivate an experimental, innovative culture

Finally, an anti-scam centre would need to foster a culture of innovation, experimentation, and shared purpose. It should be a place where ideas are tested, where failure is accepted as part of learning, and where collaboration is the norm. A distinct organisational identity could help build this culture creating a sense of unity and mission across diverse participants.

Values such as transparency, agility, and public service should be embedded from the start. Above all, the anti-scam centre would need to be seen as a place where people want to work, where organisations want to contribute, and where meaningful change is made possible.

Examples of international organisations



Australia – National Anti-Scam Centre

The national anti-scam centres (NASC) in Australia was launched in July 2023 as a three-year phased programme to strengthen national scam prevention and disruption. It coordinates government, law enforcement, and private sector efforts through intelligence sharing, public awareness campaigns, and targeted 'fusion cells' which are time-bound public-private taskforces tackling the most harmful scam types. In its first year, NASC created three fusion cells targeting investment, employment, and romance scams, achieving a 41% reduction in scam losses, driven largely by a decline in investment scams.

The centre has engaged over 500 stakeholders across financial services, telecommunications, and digital platforms to identify collaboration opportunities and enhance customer protection. Cross-sector data and intelligence sharing have enabled earlier detection of scam trends and faster disruption responses. These efforts have included the takedown of 5,000 malicious websites in partnership with Optus and rapid public education on emerging threats.

Canada – Canadian Anti-Fraud Centre CAFC

The Canadian Anti-Fraud Centre (CAFC) was established in January 1993 in North Bay, Ontario, and is jointly operated by the Royal Canadian Mounted Police, Ontario Provincial Police, and the Competition Bureau to serve as Canada's national anti-fraud call centre and central repository for fraud intelligence. It focuses on cross-border coordination by gathering and analysing fraud reports, including mass marketing scams, identity theft, and telemarketing fraud, and disseminating actionable intelligence to law enforcement across Canada and internationally.

In 2024, the CAFC received approximately 108,878 fraud reports, associated with more than CAD 638 million in losses, with only an estimated 5 to 10 percent of actual fraud being reported. The centre supports timely cross-border fund recovery, for example helping recover CAD 2.3 million in a case in partnership with Hong Kong authorities. It also guides national disruption efforts, freezing and recovering over CAD 2.9 million in 2022 and coordinating fraud investigation deconfliction via the National Financial Crime Intelligence Sharing Group. Public outreach and prevention remain core functions through campaigns such as Fraud Prevention Month and targeted fraud education across demographics.

Singapore – Anti-Scam Command/Scam Shield

Singapore's national scam response integrates public-facing tools with centralised operational disruption. ScamShield, jointly developed by the Ministry of Home Affairs, the Singapore Police Force, Open Government Products, and the National Crime Prevention Council, enables citizens to check suspicious calls, messages, and websites, report scams, and block malicious entities. Since its 2024 upgrade to include platforms such as WhatsApp and Telegram, adoption has grown to over 1.19 million users, with more than 120,000 scam entities blocked. These capabilities are complemented by the Police Anti-Scam Centre (established in 2019) and the Anti-Scam Command (operational since 2022), which integrate investigation, intelligence, enforcement, and financial-sector partnerships to rapidly freeze accounts and recover funds. In 2024, these efforts recovered more than S$182 million and prevented an additional S$483 million in potential losses.

Taiwan – Anti-Fraud Command Centre

Taiwan's anti-scam architecture combines a public reporting hub with a centralised command for operational disruption. The 165 Anti-Fraud and Internet Scam Hotline, operated by the Criminal Investigation Bureau, is the main point of contact for victims to report scams and receive advice. The Anti-Fraud Command Centre, established in June 2023, coordinates cross-agency enforcement and has blocked more than 16.97 million spoofed calls and 12.29 million malicious text messages, while recovering over NT$20 billion in scam proceeds. To strengthen prevention and oversight, Taiwan has introduced the Next-Generation Anti-Fraud Strategy Guidelines 2.0 (2025–2026), expanded the Fraud Crime Hazard Prevention Act, and mandated real-name systems for online advertising to reduce scam exposure. Recent initiatives include extensive public outreach targeting high-risk groups to raise awareness, with goals such as 50 million online views, 500 educational lectures and 140 million anti-fraud text messages to help prevent losses.

Australia

Centre/Programme
National Anti-Scam Centre (NASC)

Lead agencies
Australian Competition and Consumer Commission (ACCC)

Core functions

- Coordinate national scam prevention and disruption.
- Intelligence sharing.
- Awareness campaigns.
- Targeted 'fusion cells'.

Notable mechanisms
Fusion cells (time-bound public-private taskforces) targeting priority scams

Singapore

Centre/Programme
ScamShield and Anti-Scam Command

Lead agencies
Ministry of Home Affairs, Singapore Police Force, National Crime Prevention Council

Core functions

- Public reporting.
- Scam blocking.
- Intelligence sharing.
- Public-private disruption operations.

Notable mechanisms
ScamShield app, Anti-Scam Centre co-located with banks, Anti-Scam Command integrates all enforcement functions

Canada

Centre/Programme
Canadian Anti-Fraud Centre (CAFC)

Lead agencies
Royal Canadian Mounted Police, Ontario Provincial Police, Competition Bureau

Core functions

- Central repository for fraud reports.
- Intelligence sharing.
- Cross-border fund tracing.
- Public education.

Notable mechanisms
National Financial Crime Intelligence Sharing Group supports international coordination on fund recovery

Taiwan

Centre/Programme
165 Anti-Fraud Hotline, Anti-Fraud Command Centre

Lead agencies
Criminal Investigation Bureau (CIB), National Police Agency

Core functions

- Public reporting via hotline.
- Centralised cross-agency enforcement.
- Scam blocking.
- Legislative prevention measures.

Notable mechanisms
Fusion cells (time-bound public-private taskforces) targeting priority scams

Conclusions

The scale and sophistication of fraud today demand a coordinated, agile, and cross-cutting approach and existing models have shown how anti-scam centres can play a key role in providing this. Most critically, the anti-scam centre model can work as part of existing national efforts and organisational structures, avoiding the need for wholesale system redesign (which is often unfeasible given the embedded nature of current structures) by acting as a bridging point rather than as a replacement of existing capabilities.

The anti-scam centre concept is new and, so far, there are only a few working examples globally. Models are continuing to evolve and there is no single 'best practice' approach. Instead, where anti-scam centres have been established, approaches have been tailored to fit with existing local structures and organisation models.

While the exact roles of anti-scam centres and how they integrate with other organisations will vary from country to country, there are certain functions that are likely to be intrinsic to the anti-scam centre model's objective of driving coordination and collaboration across the ecosystem. These 'core' functions may include:

- Facilitating centralised fraud reporting and case analysis.
- Enabling public-private collaboration on anti-fraud strategy, standards and best practices.
- Facilitating intelligence and data sharing at various levels across the ecosystem (public-private and private-private).
- Supporting public awareness initiatives.
- Enabling access to consistently high-quality victim support.

In some countries, in the long term there may be potential to build beyond these core functions with capability to lead disruption initiatives, to support intensified law enforcement operational activity, to enable recovery of lost funds and to enable enhanced cross-sector data analysis capabilities. Establishing anti-scam centres and integrating them into existing structures will take time and starting small with tightly defined objectives and an organisational mandate will be key.

The pathway to transition to an anti-scam centre model will depend on individual national characteristics but could be achieved by transforming the role of an existing trusted organisation or by establishing a new structure across the existing ecosystem. Either way, public-private buy-in will be key which in turn will require clearly defined objectives and shared belief in the anti-scam centre model as a way to achieve them.

Ultimately, anti-scam centres could represent more than a new organisational model. They could be a call to collective action and an opportunity to turn shared purpose into shared impact. By working together, a more resilient, responsive, and trusted system to protect individuals, businesses, and society from the harms of scams could be developed.

PwC contacts

Alex West

Partner, PwC UK, Banking and Payments Fraud

alex.e.west@pwc.com

+44 7841 567 371

Penny Dunn

Partner, PwC Australia, Risk Advisory

penny.dunn@au.pwc.com

+61 407 367 561

Brian Castelli

Partner, PwC US, Fraud Risk Management Leader

brian.castelli@pwc.com

+1 917-562-5882

RITM0284867