AFC BRIEFING

Cross-Sector Fraud Information Sharing

Pathways to Action

March 2026

ACAMS

This paper was presented to the ACAMS International Anti-Fraud and Technology Task Force in February 2026.

Executive Summary

Fraud has emerged as the top anti-financial crime threat globally, with losses continuing to climb despite substantial organizational investment. The fundamental challenge is clear: fraud schemes operate across a vast ecosystem spanning telecommunications, technology platforms, social media, banking, and cryptocurrency exchanges, yet intelligence about these schemes remains siloed within individual sectors and organizations. No single entity sees the complete picture, making real-time disruption nearly impossible.

The ACAMS International Anti-Fraud and Technology Task Force chose to examine private-sector information sharing to identify near-term operational impact potential. Effective fraud disruption requires actionable intelligence to reach parties positioned and willing to intervene, making robust information sharing infrastructure a prerequisite for coordinated prevention and response.

Key Considerations and Discussion Points for the Task Force

- **Critical initiatives:** Based on identified opportunities for action, are there specific initiatives where task force members suggest action is prioritized, such as a deep-dive legal and policy review on current permissions and protections around sectors, privacy, and liability? Who is best placed to advance these?
- **Supporting collaboration:** Which organizations are best suited to partner on initiating the development of an international information-sharing standards framework?
- **Looking ahead:** What are the most critical elements and stakeholders to include as ACAMS supports the task force in (1) hosting the tabletop exercise to focus on information availability, sharing, and actions at each stage of the fraud lifecycle, and (2) developing the Fraud Data Toolkit, including sector-specific high-value data use case templates and priority fraud scenarios (e.g., prevention, interdiction, recovery)?

Existing Frameworks and Critical Barriers

Stakeholder engagements across the United States, Europe, and Asia-Pacific reveal a consistent pattern: effective information sharing is achievable when properly structured, but systemic barriers prevent it from scaling. Where sharing works, such as through financial sector consortia (e.g., Early Warning Services (EWS), Financial Services Information Sharing and Analysis Center (FS-ISAC), technology coalitions (e.g., the Global Signal Exchange, the Tech Coalition's Lantern program addressing child safety), cross-sector initiatives like Hong Kong's FINEST platform and Singapore's Anti-Scam Centre, and bilateral partnerships, success stems from clear governance, focused use cases, reciprocal value, and trusted relationships.

However, the vast majority of organizations are not effectively sharing fraud intelligence. In a series of engagements and roundtables, ACAMS and task force members identified the most critical barriers to scaling the speed, sophistication, actionability, and adoption of information sharing to counter fraud: legal counsel defaulting to "no," perceived liability risks, lack of clear regulatory permission, technical incompatibilities, concerns about data quality and reputational damage, and most fundamentally the limited perceived incentives to invest resources in voluntary sharing that institutions feel may cost significant resources, create potential liability, or even benefit competitors.

- **Legal and regulatory uncertainty:** Existing government-granted liability safe harbors (e.g., Section 314(b) of the USA PATRIOT Act, the Cybersecurity Information Sharing Act) aimed at enabling scaled information sharing are underutilized, with various elements criticized as slow, cumbersome, sector-specific, restrictive in their use case and application, or missing necessary incentives to promote widespread use, even where some feel the government has given broad authorities and protection. Privacy laws (e.g., GDPR, CCPA, GLBA, ECPA) create perceived or actual restrictions, with interpretation varying dramatically across jurisdictions and sectors, which further exacerbates cross-border sharing issues. Organizations report that legal and compliance teams are risk-averse, stopping sharing initiatives before they start.
- **Speed and timeliness:** Fraud infrastructure changes constantly, with criminals continuously monitoring blocklists and rotating domains, phone numbers, and other infrastructure. These patterns make delayed timelines for information sharing ineffective, particularly for short-term prevention and interdiction of fraud and scam proceeds that demand **timely action**.
- **Technical incompatibility and absence of standards:** Organizations use different data formats, identifiers, and systems that make present-day scaled sharing of useful information for combating fraud difficult. Different information is useful to different institutions in the fraud lifecycle. Message formats and data standards vary by country, network, and data type (e.g., financial, digital footprint), challenging effective information exchange.
- **Data quality and actionability:** Organizations frequently receive intelligence without sufficient context. Without confidence scores, investigation details or actionable guidance, recipients cannot justify operational decisions based on shared intelligence. More fundamentally, many organizations also report not understanding what information would be most useful to partner organizations in other sectors. When information has been shared in the past, many organizations expressed concern that it did not appear to be acted upon or produce meaningful outcomes.
- **Reputational risk and competitive concerns**: Organizations fear reputational damage and liability from blocking legitimate customers or being perceived as facilitating "debanking" or denying access to communications or social media platforms.
- **Silos and coverage gaps:** While effective information sharing exists within specific pockets, cross-sector exchange remains minimal, even as fraudsters exploit cross-sector and cross-border technical, communications and financial infrastructure. Breaking down silos within organizations, but especially across industry and internationally, is critical to attain timely and actionable information sharing.
- **Lack of organizational incentives:** In most places and across most sectors, there is very little incentive for organizations to engage in cross-sector information sharing, with many organizations reporting that they feel disincentivized to share because the downsides of sharing in terms of resource expenditure, potential liability, and reputational risk outweigh any benefit.

Next Steps

Addressing the barriers outlined above will require both near-term operational improvements and longer-term structural changes. Several near-term actions could begin to improve cross-sector fraud information sharing: (1) leveraging existing authorities more effectively, including through exploring formal legal reviews of current permissions and protections across sectors, privacy, and liability frameworks; (2) identifying the types of information that are useful for different sectors; (3) sharing low-friction information types, such as typology alerts and hashed identifiers, through automated systems matching the speed at which fraudsters operate; (4) focusing on high-value data with context to turn data into actionable intelligence; and (5) implementing use-case templates and pilots for priority scenarios based on fraud schemes and specific use cases around prevention, interdiction, or recovery. To address longer-term structural challenges, task force members can consider a targeted effort to map and engage public- and private-sector stakeholders to address legal clarifications and safe harbor gaps, drawing on successful international models.

In support of the task force, ACAMS is developing a **Fraud Data Toolkit** to map useful and priority data elements and their utility, and will be hosting a **tabletop exercise** to more fully map out useful data, use case templates, and enabled preventive and disruptive actions throughout the fraud and scam lifecycle. ACAMS will also work through the task force and outside experts to initiate the **development of a fraud information-sharing standards framework** by defining priority use cases, data element requirements, and engaging broader technical and nongovernmental standards organizations, operational organizations, and experts to transition the framework into formal technical specifications for adoption.

Cross-Sector Fraud Information Sharing – Pathways to Action

Background

Fraud has risen dramatically in recent years and was identified as the top anti-financial crime threat globally in the ACAMS Global AFC Threats Report 2026. At the inaugural ACAMS International Anti-Fraud and Technology Task Force, members identified private-to-private intelligence sharing as a foundational priority for coordinated fraud prevention.

One of the fundamental challenges in fighting modern fraud is that different parts of fraud schemes occur across a vast fraud ecosystem that includes telecommunications, technology platforms, social media, banking, cryptocurrency exchanges, and other sectors. This fragmentation leaves individual companies with an incomplete picture of what is happening and makes fraud difficult to identify and disrupt in real time.

Despite substantial investment by individual organizations, fraud losses continue to climb as criminal networks adapt rapidly and operate across organizational and jurisdictional boundaries. Financial institutions, payment providers, technology platforms, telecommunications companies, and other private entities each hold valuable intelligence about fraud patterns, perpetrator infrastructure, and victim targeting, yet this information remains largely siloed. Intelligence is shared inconsistently, often too slowly to enable timely disruption, and frequently only after fraud has already occurred.

A consistent lesson from existing partnerships is that progress accelerates once organizations are explicit about what data needs to be shared, with whom, at what speed, and for what operational purpose. When this clarity is absent, intelligence sharing is perceived as legally risky, operationally burdensome, competitively sensitive, or overly broad, leading organizations to default to caution rather than collaboration.

Current State: What Works and What Breaks Down

Existing Sharing Mechanisms

Evidence from multiple sectors demonstrates that effective private-sector information sharing is achievable when properly structured:

- **Financial sector consortia** such as EWS, the Australian Financial Crimes Exchange, and the FS-ISAC have shown how shared intelligence on threats can reduce fraud losses while respecting competitive boundaries. Their effectiveness stems from several common design features: a focus on specific threat indicators rather than customer data, clear governance structures, and incentives that create mutual value for participants.

> ***Use case spotlight – government-facilitated partnerships:***
>
> *Government-facilitated platforms in Asia-Pacific provide models for scaled cross-sector sharing. Hong Kong's **FINEST** platform, centrally managed by police and now including retail and virtual banks, enables automated many-to-many sharing of money mule and fraudulent account information with measurable impact, reportedly decreasing stop-payment requests since the pilot launched. These platforms succeed through explicit regulatory authorization, centralized technical infrastructure, and clear operational processes.*

- **Technology platform partnerships** have developed bilateral arrangements to share account and content intelligence that disrupts coordinated abuse networks. Platforms share signals about fraudulent accounts, scam content patterns, and coordinated inauthentic behavior that allow partners to take proactive action before fraud scales further.

> ***Use case spotlight – cross-sector tech coalitions:***
>
> *Cross-sector technology coalitions addressing child safety, such as the Tech Coalition's Lantern, demonstrate how shared mission and regulatory requirements (with child sexual abuse material [CSAM] being both universally condemned behavior and legally required to be addressed) drive effective collaboration bringing financial institutions and social media platforms together. The **Global Anti-Scam Alliance** and the **Global Signal Exchange (GSE)** facilitate international coordination on consumer scam intelligence, including the sharing of technical indicators like content hashes and URLs through GSE. These models work because the severity and universal condemnation of the problem, particularly when compounded by legal obligations, incentivize participation.*

- **Anti-money laundering partnerships** such as the U.K.'s **Joint Money Laundering Intelligence Taskforce (JMLIT)** and the **National Cyber-Forensics and Training Alliance (NCFTA)** demonstrate that narrowly scoped, use-case-driven sharing supported by trusted relationships delivers measurable impact. These initiatives work because they emphasize actionable intelligence over comprehensive data sharing.

> ***Use case spotlight – cryptocurrency illicit finance information sharing:***
>
> *Several partnerships across industry, some in partnership with government entities, have arisen to begin operationalizing the sharing of information and even asset recovery related to illicitly derived or scam proceeds denominated in cryptocurrency in order to facilitate recovery, such as the **Illicit Virtual Asset Notification (IVAN)** partnership, the **Security Alliance (SEAL 911)**, **Operation Shamrock and the Crypto Coalition**, and the **T3** Financial Crime Unit Global Collaborator Program.*

- **Informal bilateral arrangements** between individual organizations often move fastest when specific fraud threats emerge, relying on personal relationships and clear mutual benefit rather than formal frameworks.

Where Sharing Breaks Down

Despite these successes, significant barriers prevent broader adoption:

- **Competitive concerns and trust deficits:** As one roundtable participant explained, "trust is difficult to scale." Organizations worry that sharing fraud intelligence could reveal proprietary detection methods, customer behavior patterns, or business vulnerabilities to competitors. Trust deficits between and within sectors limit the willingness to participate, particularly where organizations have different regulatory obligations or business incentives.
- **Legal and regulatory uncertainties:** Privacy laws and regulations (e.g., the EU General Data Protection Regulation [GDPR], the California Consumer Privacy Act [CCPA], the Gramm-Leach-Bliley Act [GLBA], the Right to Financial Privacy Act [RFPA], and the Electronic Communications Privacy Act [ECPA]) and antitrust considerations create perceived or actual restrictions on what can be shared. Stakeholders across engagements consistently reported that legal and compliance teams are risk-averse, stopping information-sharing initiatives before they begin. Even where safe harbors exist, organizations report that they are slow and cumbersome, with limited incentives and practical disincentives — if they share information incorrectly, they face regulatory and reputational consequences, but many feel successful sharing provides no organizational benefit. Other stakeholders, however, highlighted the expansive liability protections already afforded to industry in certain jurisdictions for a range of use cases, such as U.S. examples of **314(b)** for financial institutions sharing information to combat money laundering or the **Cybersecurity Information Sharing Act** for private-sector sharing of cyberthreat information. As one participant noted, "it stops at counsel" due to conservative interpretation of regulations, even when the technical ability and operational desire to share exist.

Disagreements across stakeholders around the clarity and extent of liability frameworks and safe harbor application, as well as liability concerns about sharing information that might be inaccurate or sharing too little or too late, compound hesitation. Liability protections for different sectors and use cases are underutilized due to these perceived or actual restrictions, as well as limited incentives. Different sectors face different legal constraints, making cross-sector sharing particularly complex.

- **Technical incompatibilities:** Data format inconsistencies, API integration costs, and lack of common standards make sharing operationally difficult even where legal and trust barriers are overcome. Organizations use different identifiers for the same entities, maintain data at different levels of detail, and operate incompatible systems. The challenge of compatibility extends globally and across sectors. Even within single sectors like credit cards, dual-message systems between cardholder banks and merchant banks use different formats, with each country having its own networks and standards that do not align even with card network standards. What a small regional bank finds useful differs dramatically from what large institutions need, as the needs of telecommunications and social media platforms differ from those of financial institutions.
- **Data quality, confidence, and actionability concerns:** Organizations question whether shared intelligence will be sufficiently accurate, timely, and specific to justify the operational effort required to integrate and use it. Stakeholders emphasized that raw indicators without context are often of limited value. For example, receiving a Cambodian email address without understanding why it is suspicious or what action to take provides little practical guidance. Organizations stressed the importance of including confidence scores or other clear indicators of reliability so recipients can assess the information and prioritize their response. Without this context, banks receiving intelligence from technology platforms may be uncertain how to use it. False positives erode confidence in shared feeds, while a lack of feedback on outcomes reduces the incentive to continue sharing.
- **Timing delays:** Many existing sharing arrangements operate on daily or weekly cycles that are too slow for fraud prevention. By the time intelligence is shared, fraudsters have already moved funds, closed accounts, or shifted tactics and infrastructure. For information sharing to be effective at preventing fraud rather than merely documenting losses, it must be automated and operate at the speed and scale of criminal activity.
- **Coverage gaps:** Even where sharing works within sectors, cross-sector intelligence exchange remains limited. Banks share with banks, platforms with platforms, but the fraud ecosystem spans all sectors simultaneously.
- **Reputational risk concerns:** Organizations fear reputational damage from blocking or debanking customers based on shared intelligence that might be incomplete or incorrect. The risk of a wrongly exited customer generating negative social media attention is as significant a concern as regulatory or civil liability. This is particularly acute when organizations lack complete information about whether an individual is a victim or perpetrator, making them hesitant to take action without conducting their own investigations. These concerns are amplified in jurisdictions with heightened public sensitivity about financial exclusion.

- **Lack of organizational incentives:** Even when technical capability and individual passion exist, organizations face fundamental incentive misalignment. As some stakeholders reported, "if regulators tell me I must do it, I will, but if they don't, I won't." Voluntary information sharing requires resource investment (e.g., legal review, technical integration, operational processes) with uncertain return, potentially benefiting competitors while exposing the sharing organization to legal and reputational risks. Shareholders question why institutions spend resources on voluntary initiatives. Without clear mandates or competitive advantage, organizations default to minimal compliance rather than proactive sharing.

Prioritizing Information for Sharing

Not all information types are equally valuable or equally challenging to share. Organizations must prioritize extracting and sharing information based on operational impact and implementation feasibility.

Highest-Value Information Types

Based on stakeholder engagement, the information types listed below were identified as high priorities for cross-sector sharing due to their operational impact, cross-sector applicability, and potential to enable timely fraud disruption:

- **Account and destination identifiers:** bank account numbers, originator and beneficiary names, cryptocurrency wallet addresses and payment app identifiers for accounts receiving fraud proceeds. These identifiers help enable proactive blocking and coordinated closures.
- **Phone numbers:** numbers used for scam calls, text messaging or account verification that telecommunications providers can block and other sectors can use for risk signals.
- **Coordinated account networks:** platform account identifiers and behavioral signals showing coordinated fraud activity across social media, dating apps, or other services.
- **Fraud typologies and tactics:** descriptions of current fraud schemes, social engineering tactics, and targeting patterns that allow organizations to update detection rules and warn potential victims.
- **Domains and infrastructure:** URLs, domains, IP addresses, and hosting information for fraud websites and phishing infrastructure that can be taken down or blocked.
- **Device identifiers and digital footprints:** device IDs, suspicious IP address ranges, browser fingerprints, screen resolution, typing pressure patterns, and other device characteristics that enable network analysis.
- **Transaction patterns:** behavioral indicators and transaction sequences that distinguish fraud from legitimate activity without revealing customer identities.
- **Name and national identification numbers:** customer names and official identification numbers, such as passports, used for matching across databases where legally permissible.

Note on name and national identifiers: While organizations emphasized the value of starting with these core identifiers (by some identified as "the most helpful data points" for matching across organizational databases), they recognized that jurisdictional privacy laws create significant variation in shareability. These data points carry high privacy implications and require strong legal justification. Others highlighted challenges with compatibility across regions and languages to support meaningful and timely entity resolution.

Legal Implications by Information Type

Understanding the legal risk profile of different information types helps organizations prioritize what to share first and what requires more careful legal analysis. Not all fraud-related information carries the same privacy or regulatory implications. An initial review based on research and stakeholder engagement enables discussion around tiers of risk for specific information types:

- **Low privacy risk:** Fraud infrastructure indicators, such as domains and IP addresses, fraud typology descriptions, and aggregated pattern information typically involve no personal data and minimal legal barriers.
- **Moderate privacy risk:** Hashed or tokenized account identifiers, phone numbers associated with confirmed fraud, and cryptocurrency wallet addresses involve personal data but can often be shared under fraud prevention provisions in privacy laws with appropriate safeguards.
- **Higher privacy risk:** Unencrypted customer account details, communication content, transaction histories, and linking multiple identifiers to individuals require careful legal analysis and stronger justification under necessity and proportionality principles.

Different jurisdictions and sectors have different baseline permissions for sharing information across borders and with different authorities. Financial institutions operating under the Gramm-Leach-Bliley Act (GLBA) in the United States have clearer authority for fraud-related sharing than many other sectors, while telecommunications providers face stricter constraints under the Electronic Communications Privacy Act (ECPA). In the European Union, GDPR Article 6(1)(f) provides a legitimate interest basis that applies across sectors, but interpretation varies significantly by member state and data protection authority. Singapore's framework explicitly authorizes sharing between banks and telecommunications providers through the Anti-Scam Centre, while Australia's Privacy Act exceptions for fraud prevention remain subject to varied interpretation across sectors. These jurisdictional and sectoral differences mean that a phone number shared by a U.K. telecommunications provider may face different legal considerations than the same number shared by a U.S. financial institution, even when both are acting to prevent the same fraud scheme.

Highest Return on Investment (ROI) for Sharing

Priority information sharing should focus on information that is:

- **Time-critical for disruption:** Real-time or hourly sharing of active fraud infrastructure enables blocking before significant victim harm.
- **Cross-sector relevant:** Phone numbers, wallet addresses, and domains are useful to multiple sectors, maximizing sharing value.
- **Clearly actionable:** Intelligence that enables specific protective actions, such as blocking payment, removing an account, or warning customers, justifies operational investment.
- **Already collected:** Information organizations maintain for their own fraud prevention requires minimal additional cost to share.
- **Legally clearer:** Starting with lower-risk information types builds confidence and operational capability before tackling more complex scenarios.
- **Contextually complete:** Intelligence shared with actionable context like confidence scores, investigative details, and clear guidance on what action recipients can take (e.g., block a payment, freeze an account, remove content, warn customers) justifies operational investment far more effectively than raw data points.

With priorities established around the most valuable and legally viable information types, organizations can take immediate action using existing authorities and low-friction approaches.

Near-Term Opportunities

Several opportunities were discussed that could improve information sharing without requiring new legislation or major technical investment.

Improve Use of Existing Legal Authorities

Many organizations underutilize existing legal permissions that provide various protections and permissions for sharing certain information about and related to fraud:

- **Section 314(b) of the USA PATRIOT Act** provides a safe harbor for financial institutions to share fraud-related information but remains underutilized due to a lack of awareness or overly cautious interpretation.
- **The Cybersecurity Information Sharing Act of 2015** provides cross-sector liability protections for sharing information related to cyberthreats and defensive measures. Unlike Section 314(b), which applies primarily to financial institutions, CISA covers any industry members sharing cyberthreat information. Since most modern fraud is cyber-enabled, this existing safe harbor may provide broader authority for cross-sector fraud intelligence sharing than organizations currently recognize.
- **GDPR Article 6(1)(f) "legitimate interests" basis** permits fraud prevention processing, but organizations often take unnecessarily conservative approaches without seeking legal opinions confirming permissibility.

- **Sector-specific provisions** in telecommunications fraud regulations, payment system rules (such as card network operating regulations), and platform terms of service often permit broader sharing than organizations realize, but they may not be well understood outside their respective sectors.
- **Contractual mechanisms**, including non-disclosure agreements (NDAs), bilateral data sharing agreements, and consortium membership structures, can address many confidentiality and liability concerns without requiring new legislation, although they require legal resources to negotiate and implement effectively.

Organizations could conduct cross-functional legal reviews involving counsel from all relevant jurisdictions to establish shareability baselines documenting what can be shared today under existing frameworks. Regulatory facilitation can accelerate the utilization of existing authorities. In Hong Kong, banking regulators provided explicit letters to participating banks confirming that information sharing for fraud prevention was permissible even before privacy law amendments were finalized, creating the legal comfort needed to launch the FINEST platform. This demonstrates that regulators can enable action within existing frameworks through clear communication and explicit authorization, without waiting for legislative change.

Low-Friction Information Types for Immediate Sharing

Organizations can begin immediately with information types facing minimal legal or operational barriers, which may include:

- **Fraud typology alerts:** Descriptions of current fraud schemes, tactics, and targeting patterns involve no personal data and can be shared freely through existing communication channels.
- **Hashed identifiers:** Phone numbers, account numbers, and wallet addresses hashed using common algorithms provide meaningful matching capability with privacy protection and minimal technical complexity.
- **Infrastructure indicators:** Domains, URLs, IP addresses, and hosting information for confirmed fraud sites can be shared for blocking and takedown coordination.
- **Aggregated patterns:** Statistical information about fraud trends, geographic concentrations, and timing patterns enables improved detection without revealing individual records.

Organizations emphasized that for non-personally identifiable information (non-PII) such as fraud typology alerts, infrastructure indicators, and aggregated patterns, sharing should be automated to match the speed at which criminals operate. Manual processes for reviewing and approving the sharing of domains, IP addresses, and typology information introduce delays that render intelligence obsolete. Automated systems can share these low-risk information types at the necessary speed and scale. These low-risk information types can be shared immediately through informal channels or simple bilateral arrangements, building operational capability and trust for more complex sharing scenarios.

Pilots and Templates

Developing and promoting the adoption of specific templates and guides as part of pilot or wider implementations could provide near-term actionable tools useful to front-line fraud fighters, such as:

- **Use case templates:** detailed documentation for three to five priority sharing scenarios (bank-to-bank mule accounts, bank-to-cryptocurrency wallet addresses, telecommunications-to-all scam phone numbers, platform-to-platform coordinated accounts and dating app-to-bank romance scammers) specifying what data elements to share, legal basis, timing requirements, and enabled actions.
- **Legal guidance documents:** jurisdiction-by-jurisdiction analyses of existing sharing permissions, template data sharing agreements, and explanations of safe harbor provisions.
- **Technical guides:** simple specifications for hashed identifier exchange, API structures for bilateral sharing, and minimum viable data schemas.
- **Governance templates:** model agreements for bilateral, consortium, and intermediary sharing arrangements with standard reciprocity, use restriction and accountability terms.
- **Pilot programs:** the launch of three to five coordinated pilots testing priority sharing scenarios with volunteer participants, documenting implementation challenges and lessons learned for broader replication.

Longer-Term Structural Challenges

While near-term progress is possible with existing authorities, several barriers require more formal frameworks and legislative or regulatory action.

Safe Harbors and Liability Protections

Current gap: Existing safe harbors are sector-specific, primarily for financial institutions, and do not clearly cover cross-sector sharing. Organizations fear liability for sharing inaccurate information, sharing too little, or sharing too late.

Needed: Explicit safe harbor provisions must permit fraud information sharing across sectors, including banks, platforms, telecommunications companies, retailers and cryptocurrency exchanges, under specified conditions. Liability protections for good-faith sharing should be clear and robust enough to reduce organizational hesitation.

Examples of existing approaches:

- **United States:** Section 314(b) of the USA PATRIOT Act provides safe harbor for financial institutions but does not clearly extend to cross-sector sharing with platforms, nor to telecommunications providers or nonfinancial institutions. The Cybersecurity Information Sharing Act of 2015 provides liability protections for any members of industry for sharing information related to cyberthreats and defensive measures, which could extend to cyber-enabled fraud indicators.

- **Australia:** The Australian Privacy Act contains fraud prevention exceptions, but interpretation varies and cross-sector application remains uncertain.
- **Hong Kong:** The Financial Intelligence and Investigation Bureau, through the Hong Kong police, operates the FINEST platform, which received explicit regulatory authorization through Hong Kong Monetary Authority letters to participating banks confirming that sharing was permissible for fraud prevention purposes. The platform now includes all retail banks and virtual banks in a centralized, automated many-to-many sharing system for money mule and fraudulent account information, with a measurable reduction in fraud since implementation.
- **Singapore:** The Shared Responsibility Framework for Phishing Scams creates explicit authority for telecommunications providers and banks to share information through the Anti-Scam Centre.
- **South Korea:** A comprehensive anti-fraud framework led by law enforcement and financial regulators brings together banks, nonbank financial institutions, fintech companies and telecommunications providers with immediate account freezing authority when fraud is identified. The framework demonstrates how legislative action creating clear authority, strong enforcement mechanisms and cross-sector coordination can drive systematic participation.

Key considerations: Develop cross-sector safe harbors that permit sharing of specified fraud indicators, such as account identifiers, phone numbers, wallet addresses, and infrastructure indicators, between designated sectors under appropriate governance, with liability protection for good-faith sharing meeting defined standards.

Privacy Law and Antitrust Clarifications

Potential privacy clarifications:

- Clear guidance that fraud prevention constitutes a legitimate interest or other lawful basis under GDPR and similar frameworks.
- Clear direction on how fraud prevention provisions apply across different sectors, such as financial services, telecommunications, technology platforms, and retail.
- Explicit permission for cross-border fraud intelligence sharing under data transfer regulations.
- Proportionality guidance specifying what data elements are reasonable to share for different fraud scenarios.
- Speed and timeliness provisions recognizing that delayed sharing can render intelligence useless.

Potential antitrust clarifications:

- Confirmation that sharing fraud threat intelligence does not constitute anticompetitive information exchange.
- Guidance on appropriate governance structures for industry consortia.
- Clear boundaries between permissible fraud indicator sharing and impermissible business information exchange.

Examples:

- **European Union:** Data Protection Authorities could issue coordinated guidance on fraud prevention sharing similar to guidance issued for COVID-19 data processing.
- **United States:** The Federal Trade Commission and Department of Justice could clarify antitrust boundaries for fraud information sharing consortia.

Key considerations: Engage with data protection authorities and competition regulators to develop specific guidance clarifying existing permissions and boundaries for fraud intelligence sharing. This will help reduce perceived legal risk that prevents action under existing frameworks.

Cross-Border Data Sharing Authorities

Current gap: Cross-border fraud intelligence sharing faces uncertainty under data transfer restrictions (e.g., GDPR adequacy requirements, Schrems II implications, sectoral data localization requirements). Organizations often default to not sharing internationally even when it is operationally critical. Despite these challenges, there are frameworks and treaty obligations supporting legal cross-border information sharing (e.g., Egmont Group of FIUs, UN Convention against Cybercrime, Mutual Legal Assistance Treaties).

Needed: Mechanisms must enable real-time international fraud intelligence exchange that works within existing data protection frameworks. This could include mutual recognition of fraud prevention as an adequate safeguard, standard contractual clauses specifically for fraud intelligence or multilateral frameworks similar to APEC Cross-Border Privacy Rules.

Examples:

- **APAC:** The FRONTIER+ initiative demonstrates cross-border scam intelligence sharing but lacks a comprehensive legal framework.
- **Europe-U.S.:** The Data Privacy Framework provides a mechanism for transatlantic data transfers, but the application to fraud intelligence sharing remains unclear.

Key considerations: Develop model frameworks for cross-border fraud intelligence sharing that satisfy data protection requirements while enabling operational speed, potentially through multilateral agreements between governments or mutual recognition arrangements between regulators. Propose policy language to organizations such as the Financial Action Task Force (FATF) to integrate timely cross-border sharing of transaction and auxiliary information as critical to combating financial crime and money laundering, such as in Recommendation 16 updates.

Liability, Mandates, and Regulatory Requirements

Several jurisdictions have moved beyond voluntary sharing to create regulatory obligations, fundamentally changing participation incentives.

Challenge: Voluntary approaches may not achieve sufficient participation or investment when competitive pressures discourage action.

How it works: Legal and regulatory requirements create anti-fraud and information-sharing obligations for companies across sectors with significant penalties and liability for failures to meet standards.

Intended effect: Companies increase investment in fraud controls and cross-sector information sharing initiatives, leading to better identification and disruption of fraud, lower fraud losses overall, and greater asset recovery for victims. When companies face significant potential penalties, they invest in their own controls and ensure other participants upstream and downstream are sharing information to mitigate their risk.

Examples:

- **Singapore:** The Shared Responsibility Framework for Phishing Scams creates liability for banks and telecommunications providers that fail to meet specified fraud prevention and information-sharing obligations, incentivizing proactive participation in the Anti-Scam Centre.
- **United Kingdom:** Mandatory reimbursement for Authorized Push Payment (APP) scams creates a financial incentive for payment service providers to invest in fraud prevention and participate in information sharing to reduce their liability exposure.
- **European Union:** PSD2 strong customer authentication requirements and fraud monitoring obligations create baseline standards, though information sharing remains largely voluntary.

Trade-offs: Mandates drive investment and participation but risk being prescriptive and may not adapt quickly to evolving fraud tactics. They work best when combined with industry input on implementation and flexibility for organizations to choose how to meet outcome-based requirements.

Key considerations: In jurisdictions where voluntary approaches prove insufficient, consider outcome-based regulatory requirements (e.g., reducing fraud losses, improving response times, participating in information sharing) rather than prescriptive mandates, allowing organizations flexibility in implementation while creating clear accountability for results.

Voluntary Incentive Mechanisms

Beyond regulatory mandates, several approaches can incentivize participation without legal requirements.

Voluntary Industry Standards and Commitments

Challenge: Enhancing fraud controls and participating in information sharing can create a competitive disadvantage when others in the same sector do not take similar steps.

How it works: Companies voluntarily commit to standards or requirements to promote fraud information sharing. These standards could apply within a sector or across sectors, facilitated by industry associations, government encouragement, or collective action by leading organizations.

Intended effect: If participation is high enough, it reduces the competitive disadvantage. It raises the bar across sectors and pressures companies not otherwise inclined to enhance fraud controls to avoid being perceived by government, regulators, or the public as sector outliers not committed to fighting fraud and protecting customers. This can serve as a first step toward larger information sharing initiatives.

Examples:

- **United Kingdom:** The Telecommunications Fraud Sector Charter brings telecommunications providers together to commit to specific anti-fraud measures and information sharing practices.
- **United States:** Industry associations such as the American Bankers Association promote fraud information sharing through initiatives like EWS and FS-ISAC.
- **Global:** Payment card networks' fraud rules create de facto standards for participating financial institutions, and global organizations enable the sharing of technical indicators (e.g., GSE).

Private Sector Initiatives

Challenge: Cross-sector collaboration is difficult. Navigating legal, regulatory, and operational challenges takes time and resources that individual organizations struggle to justify.

How it works: The private sector forms organizations, associations, or groups to facilitate and execute cross-sector fraud information sharing. Government can recognize, encourage, or endorse these initiatives and may participate.

Intended effect: Having an organization collectively navigate challenges on behalf of members is more effective and efficient. It enables faster and more accurate fraud identification and greater speed in taking disruptive actions across sectors, such as shutting down bank accounts, blocking phone numbers, and taking down online accounts and sites.

Examples:

- **United Kingdom:** CIFAS is a not-for-profit membership organization bringing together banking, insurance, telecommunications, retail, and government, and providing a framework for real-time sharing of fraud risk data and intelligence.
- **United Kingdom:** Stop Scams UK is a member organization of banking, technology, and telecom businesses, facilitating cross-sector collaboration to fight scams.
- **United States:** NCFTA operates as a partnership between industry, law enforcement, and academia to share cybercrime and fraud intelligence.

Government-Led Initiatives

Challenge: Private sector initiatives may lack sufficient authority, specialized insights, or coordination with law enforcement to enable rapid disruption and asset recovery.

How it works: Government creates fusion cells and intelligence hubs that bring public and private sectors together, often physically co-located, to share fraud-related information, insights, and intelligence.

Intended effect: As a trusted intermediary, government leadership can reduce legal and regulatory uncertainty. These initiatives can enable the government to receive and share information more efficiently and align activities with government priorities. They can increase the speed of disruption and asset recovery and make it easier for government to provide feedback to private sector companies.

Examples:

- **Australia:** The National Anti-Scam Centre (NASC) brings together government agencies, law enforcement, banks, telecommunications providers, and technology platforms to share intelligence and coordinate responses in real time.
- **Singapore:** The Anti-Scam Centre (ASC) operates as a joint public-private initiative with co-located representatives from banks, telecommunications providers, and law enforcement to enable immediate information sharing and coordinated disruption.
- **United Kingdom:** JMLIT and the Joint Fraud Taskforce provide models for public-private intelligence fusion.

Each approach has strengths and limitations. Government-led initiatives often offer the benefits of increased priority and authority for more enduring effects while facing challenges related to agility and timeliness needed for more adaptive and near-term threats. The most successful models combine key elements such as baseline legal clarity through safe harbors, voluntary industry leadership through standards and private sector initiatives, government facilitation through fusion centers, and targeted mandatory requirements where voluntary approaches prove insufficient.

Technical and Governance Requirements

Technical Infrastructure

Organizations need infrastructure that balances operational utility, security, privacy protection, and implementation feasibility. For example:

- **Some key requirements for near-term information sharing efforts:**
    - Secure transmission channels (e.g., TLS, VPN)
    - Basic matching capabilities for key identifiers
    - Clear data schemas defining field formats and meanings
    - Access controls ensuring only authorized personnel can query or receive intelligence
    - Audit logging to support accountability
    - Feedback mechanisms to report on actions taken
- **Priority technical standards that could support information sharing infrastructure:**
    - Common identifier formats for account numbers, phone numbers, cryptocurrency wallet addresses, domains, and IP addresses
    - A common fraud typology taxonomy that translates across sectors
    - Confidence and quality indicators for shared intelligence
    - Formats for reporting actions and outcomes
    - API specifications for bilateral sharing
    - Guidance on privacy-preserving techniques (e.g., hashing, tokenization, and when to use each)

Immediate opportunities: Organizations can begin immediately with simple hashed identifiers and by exploring the use of common algorithms. This provides meaningful privacy protection and enables cross-organizational matching without requiring sophisticated infrastructure or legal review.

Governance Requirements

Core governance principles: Information sharing arrangements operate most effectively when they follow a set of principles that foster trustworthiness and security across the sharing environment:

- **Reciprocity:** Organizations receiving intelligence should contribute intelligence and commit to taking appropriate action when sharing information. Tiered participation models can balance fairness with accessibility for smaller organizations.
- **Data handling and retention:** Information-sharing arrangements should establish clear requirements for how long shared intelligence is retained, how it is secured, who can access it, and when it must be deleted.
- **Restrictions on use and onward sharing:** Shared intelligence should be used only for fraud prevention and related purposes. Onward sharing should be permitted only with explicit consent or within the defined sharing community.

- **Audit and accountability:** Participating organizations should maintain logs of intelligence received and actions taken, undergo periodic reviews to verify compliance, and report on aggregate outcomes to help participants assess the efficacy of efforts.
- **Feedback loops:** Recipients should report back on actions taken based on shared intelligence and outcomes achieved.
- **Purpose clarity:** Information-sharing arrangements should explicitly define their operational purpose (e.g., fraud prevention, in-progress interdiction, asset recovery, prosecution support for a specific predicate offense).

Governance model options:

- **Bilateral/peer-to-peer:** This model relies on simple, direct trust relationships but has limited scalability.
- **Consortium:** This approach provides broader reach and pattern detection but requires more complex governance.
- **Third-party intermediary:** This option addresses competitive concerns but introduces operational dependencies.

Organizations should select models based on specific use cases, existing relationships, sector dynamics, and competitive sensitivities rather than pursuing a single prescribed approach.

Key Considerations and Roadmap

The task force should prioritize practical implementation that enables organizations to move from intent to impact without requiring wholesale transformation and then set the foundation to make meaningful progress in partnership with responsible organizations to address longer-term and systemic issues needed for the long-term scaling of counter-fraud initiatives.

Potential Task Force Actions

1. **Develop templates for data sharing agreements and use case templates** for three to five priority sharing scenarios documenting exact data elements, the legal basis, timing requirements, safeguards, contextual information requirements, and enabled actions.
2. **Promote immediate low-friction sharing** of fraud typology alerts, hashed identifiers, infrastructure indicators, and aggregated patterns.
3. **Develop a fraud data toolkit and information-sharing playbook** mapping priority fraud data elements, their utility and source, mechanisms and vectors for sharing, and existing or needed standards for interoperability.
4. **Map gaps in legal clarifications and safe harbor provisions** for cross-border and cross-sector information sharing and engage policymakers to assist efforts to address them.

Conclusion

Private sector fraud intelligence sharing is achievable without waiting for new legal frameworks or wholesale technical transformation. Progress depends on focusing initially on high-impact use cases with clear operational value, specific data elements that organizations can realistically share under existing legal frameworks, and governance models that build trust through transparency and reciprocity.

Organizations should begin immediately with low-friction information types and simple bilateral arrangements, building operational capability and trust for more complex sharing scenarios. The task force's recommendations provide a pathway from current fragmentation toward more systematic, scalable, and sustainable intelligence exchange that delivers measurable reductions in fraud losses.

About ACAMS

ACAMS is a leading international membership organization dedicated to providing opportunities for anti-financial crime (AFC) education, best practices, and peer-to-peer networking to AFC professionals globally. With over 110,000 members across 200+ jurisdictions and territories, ACAMS is committed to the mission of ending financial crime through the provision of anti-money laundering/ counterterrorism-financing and sanctions knowledge-sharing, thought leadership, risk mitigation services, ESG initiatives, and platforms for public-private dialogue.

The association's CAMS certification is the gold-standard qualification for AFC professionals, while the CGSS certification is its premier specialist qualification for sanctions professionals. ACAMS' 60+ chapters globally further amplify the association's mission through training and networking initiatives.