ACAMS International Anti-Fraud & Technology Task Force
February Meeting – Summary Brief

24 February 2026

This briefing provides an overview of the February meeting of the ACAMS International Anti-Fraud & Technology Task Force. It outlines strategic updates, key themes, and priority actions focused on strengthening global anti-fraud capabilities across sectors.

Overview

The February meeting advanced the Task Force's work toward improving cross-sector fraud information sharing, data visibility, and operational collaboration across financial institutions, technology platforms, law enforcement, and other stakeholders. Members reviewed emerging risks and aligned on practical steps to accelerate progress through targeted pilots, toolkits, and coordinated engagement.

Strategic Update

Task Force co-chairs provided an overview of ongoing anti-fraud developments across key jurisdictions, including upcoming national risk assessments, increased global focus on fraud within standard-setting bodies, and continued efforts to establish or enhance anti-scam centers. These developments highlight the urgency of building consistent, collaborative approaches across sectors and borders.

Key Themes: Advancing Cross-Sector Fraud Information Sharing

1. Establishing Clear Legal Pathways

Legal uncertainty remains a central barrier to effective information sharing. Clear legal mechanisms, harmonized permissions, and well-defined governance frameworks are essential for enabling institutions to exchange fraud-related data with confidence and consistency. The UK's model — leveraging GDPR Article 6 "legitimate interest" alongside specific fraud-sharing allowances — illustrates a structured approach, though similar frameworks have taken years to develop in other jurisdictions.

2. Identifying High-Value Data for Detection

Participants emphasized the need to identify a narrow, high-impact set of data elements — such as URLs, IP addresses, and account identifiers — that deliver the greatest operational value across the fraud lifecycle. Mapping data availability, relevance, and gaps across sectors is a foundational step toward building a coherent information-sharing framework.

3. Targeted Pilots to Demonstrate Practical Impact

There was strong support for small, focused pilots tied to specific typologies, particularly those involving the social-media-to-payments fraud pathway. Pilots that test real-time sharing of known fraud indicators can help demonstrate value, reduce friction, and build trust across participating organizations. The Global

Signal Exchange's success with small pilots — now facilitating the sharing of more than one million signals daily — illustrates the potential impact of this approach.

4. Strengthening the Technology and Trust Infrastructure

Persistent fragmentation across systems and datasets continues to impede rapid fraud detection. Participants underscored the need for secure, interoperable platforms that support real-time analytics, shared detection logic, and coordinated interventions. Many institutions operate systems containing hundreds of data fields. While they may only use a small subset of these data fields for their own fraud detection, it may be that other data fields are useful to institutions in other sectors. This indicates the need to identify what data different institutions/sectors collect and what would be the most operationally relevant for other sectors.
Equally critical is the underlying trust infrastructure, including transparent data-accuracy standards, clear usage boundaries, robust security protocols, and alignment across jurisdictions. Technology is foundational, but trust-driven governance ultimately determines whether cross-sector sharing can scale.

5. Integrating Scam-Response Centers into the Data-Sharing Ecosystem

Anti-Scam Centers (ASCs) can serve as operational hubs within broader information-sharing networks. Scalable, capability-based ASC models can support forward- and backward-tracing of funds, accelerate disruption of mule networks, and accommodate differing legal and supervisory environments.
ASCs are not a one-size-fits-all solution; instead, they provide a flexible, centralized model that can be adapted to each jurisdiction's legal, operational, and technological context.
Upcoming international guidance presents an opportunity for greater global alignment and shared implementation pathways.

Conclusion & Next Steps

Members expressed strong interest in accelerating the Task Force's transition from analysis to operational execution. Immediate next steps include:

- Advancing a **legal permissions paper** through collaboration between ACAMS and GASA to clarify pathways for cross-sector and cross-border sharing.
- Producing an **operational data-sharing toolkit**, aimed at low-friction opportunities to advance practical implementation.
- Developing and prioritizing **small-scale pilots** focused on high-value data and targeted typologies.
- Conducting the **Fraud Ecosystem and Response Mapping Tabletop Exercise** planned for late March/early April 2026.