ACAMS International Anti-Fraud & Technology Task Force
Launch Agenda and Discussion Paper

Date: 24 November 2025

Task Force Leadership:

- Co-Chairs: Scott Rembrandt, *US Treasury,* Giles Thomson, *HM Treasury*
- Coordinated by ACAMS Secretariat

Task Force Membership: ~40 members represented across international governments (regulators, law enforcement), NGOs, civil society, and industry (financial, technology, social media, telecommunications sectors) *(Refer to Appendix A for membership list)*

Meeting Cadence: Quarterly full-Task Force meetings, virtual/hybrid format *(ref. App. B)*

Strategic Objective: The Task Force will enhance collective responses to the evolving fraud threat environment, help develop effective policy and technological responses, identify ways for financial institutions and other stakeholders to operationalize effective cross-sector and organizational mitigation responses, including information sharing, reporting frameworks, detection and disruption efforts. *(Refer to Task Force Terms of Reference)*

AGENDA (Annotated)

09:00-09:15 EST — Welcome & Task Force Co-Chair Introduction

- *ACAMS (Justine Walker) and TF Co-Chairs welcome all membership, remind the TF of operation under the Chatham House rule, and give brief opening remarks on context and purpose of TF as set out in the Terms of Reference.*

09:15-09:30 EST — Task Force Member Introductions

- *TF members will introduce themselves and their role in the fraud/counter-fraud ecosystem.*

09:30-09:50 EST — Fraud Threat Landscape Overview

- *ACAMS will give a brief overview of the fraud threat landscape and key obstacles in addressing fraud (Carole House and Joby Carpenter)*

09:50 - 10.50EST— Cross-Sector Perspectives and Open Discussion of Task Force Priorities

- *Select organizations across each sector will offer 2-minute interventions sharing what is and is not working in their sectors to combat fraud, and what they feel is needed from other sectors to best enable fighting fraud.*
- *Co-chairs will moderate open discussion among Task Force members on the workstream structure and discuss key initiatives that would be most useful to prioritize.*

10:50 -11:15EST — Integrated Counter-Fraud Framework Development

- *ACAMS will present a proposed workstream structure for input for priority initiatives that will be advanced under the auspices of the Task Force. Discussion on how Task Force initiatives can be advanced to support other domestic/international activities.*

11:15-11:30EST — Conclusions and Next Steps

- *Co-chairs and ACAMS will summarize key points and any conclusions from discussion*
- *Co-chairs ask Task Force:*
    - *To approve cadence of full Task Force meetings*
    - *To seek views on membership gaps and further contributors*
    - *To approve (or provide input within 2 weeks to refine) workstream structure*
    - *To provide input within 2 weeks on top priority initiatives for the Task Force to pursue and the proposed first engagement sessions (ref. App. C)*

ACAMS

DISCUSSION PAPER

I. Fraud Landscape Overview

For too long, fraud has been seen as a cost of doing business, a nuisance to be absorbed by banks and consumers. That perception is a dangerous relic. Modern fraud is a combination of geopolitics and technical edge conducted via criminal proxies, targeting businesses and the public. Yet the global response has remained largely piecemeal and reactive.

Industrialization has morphed fraud from petty crime into a strategic tool used by criminal organizations and illicit state actors. Fraudsters leverage global, industrial-grade tools — bot farms, malware, cryptocurrencies — alongside old-fashioned social engineering, while nations and consumers must guard every vulnerability across financial and technical platforms that are exploited in these schemes.

Fraud subsidizes transnational organized crime and rogue states, undermining the integrity of the global financial system. North Korea weaponizes cyber-enabled fraud networks to circumvent sanctions and generate revenue, maximizing economic damage while minimizing attribution risk. Global syndicates operate romance and investment scams from enclaves in Myanmar and Cambodia, partnering with militias and corrupt elites and funneling proceeds from victims who invest their emotional and financial capital. Sophisticated and capable fraud networks target vulnerable young people with devastating schemes.

Frauds manifest across a spectrum of damaging schemes with costs amounting to hundreds of billions, for example:

- Business email compromise (BEC) frauds where criminals hijack corporate communications to redirect payments (~$6.7 billion in global annual losses in 2023).
- Account takeover (ATO) frauds, leveraging stolen credentials and SIM-swap attacks (~16 billion in global losses in 2024).
- Synthetic identity fraud, where criminals combine real and fake personal information to create a new identity to use in fraud (estimated $20-40 billion losses annually).
- "Pig butchering" scams combining romance fraud with cryptocurrency investment schemes that steal billions from victims annually and drive devastating human costs.
- Benefits fraud that exploited pandemic relief programs for an estimated $163 billion in losses.
- Healthcare fraud potentially amounts to hundreds of billions in losses each year, leading to increased consumer costs and reduced coverage.

Fraud is an international security threat. The ACAMS Anti-Fraud and Technology Task Force is forming to reinforce global authorities' ability to treat it like one.

II. Key Challenges in Combating Fraud

Strategic and operational challenges hinder government authorities' and industry's ability to effectively combat fraud and restore losses to victims:

Prevent: Criminals exploit limitations across shared fraud intelligence and identity verification checks across financial institutions, using the same schemes and often emerging tech capabilities repeatedly at different institutions while targeting vulnerable people with increasingly sophisticated scams.

Detect: Fragmented, non-standardized data collection, legacy technology, and limited real-time information sharing across sectors and public-private authorities challenge the ability to identify cross-institutional fraud patterns, and related money laundering such as muling, before funds are transferred.

Disrupt: Insufficient speed and cross-sector coordination means that fraudulent proceeds are not interdicted quickly enough. Criminals also exploit common devices and digital infrastructure in accessing financial, social media, and technological platforms and infrastructure—there is no sufficiently timely mechanism for coordinating detection, denial, and disruption of these networks and payment flows at scale across global sectors and authorities.

Redress: Unclear liability frameworks, inconsistent reimbursement policies, and inadequate and slow dispute resolution mechanisms leave victims, particularly those of authorized push payment scams, without clear pathways to timely recovery or compensation.

III. Counter-Fraud Framework and Potential Initiatives

The Anti-Fraud and Technology Task Force will pursue priority initiatives to drive tangible outcomes across several workstreams that will assist public and private sectors in meaningfully improving the ability to combat fraud. Each workstream may convene discussions with outside experts, authorities, and victims as appropriate, as well as convene sector-specific discussions (e.g., targeted meetings among fintechs, technology platforms, government, etc.) to support their effort:

- **Policy** – Develop a policy roadmap for fraud-prevention measures across jurisdictions and sectors.
    - *Ex. potential initiatives: Mapping policy gaps and obstacles with library of policy recommendations and templates; globally applicable fraud taxonomy*
- **Information Sharing** – Develop frameworks for enhanced timely and actionable information sharing of fraud networks and activities.
    - *Ex. potential initiatives: Emerging typology deep-dive reports, map of fraud data and reporting channels and metrics; data schema for useful fraud data*
- **Capacity Building** – Build and conduct training and operational capacity building materials and frameworks.

  - *Ex. potential initiatives: Counter-fraud toolkit and training; incident response playbook and tabletop exercise; rapid coordination protocols and best practices; compendium of activity promoting effective initiatives*
- **Technology Advancements** – Develop a roadmap of priorities for technology solution developments in countering fraud.
  - *Ex. potential initiatives: Develop a pilot architecture for training AI-enabled fraud detection models; build a tech-enabled fraud threat profile; build common frameworks and practices for cross-platform identity verification*
- **Public Engagement and Education** – Enhance and elevate consumer awareness and victim support efforts across Task Force membership
  - *Ex. potential initiatives: Survey consumer-focused awareness and victim support methods and best practices by sector*

In support of these workstreams, the Task Force will also host workstream-aligned **engagement sessions** between full Task Force meetings to allow for engagement with a broader community of experts, companies, and authorities to more deeply examine key issues for countering fraud.

IV. Key Discussion Questions

The Task Force will engage in open discussion, facilitated by the Co-chairs, around what initiatives should be prioritized based on their potential to achieve high impact as well as tangible near-term progress. The following questions can help stoke and guide discussion:

- **Policy:**
  - What are the highest-impact policy gaps across each sector needed to better combat fraud? What are the greatest obstacles to addressing them?
  - What does the asymmetry in the trillions in losses to fraud versus the millions spent on defenses by nations tell us about what interventions could best achieve strategic impact versus tactical wins?
  - What is the state of mapping of existing standards in addressing fraud? Where are weaknesses based on a gap in implementation of existing standards that aren't known or implemented, or a gap in development of new effective responses?
- **Information Sharing:**
  - How real-time and comprehensive is our intelligence picture and data sharing on fraud? Which causes (e.g., legal, policy, technological) are most addressable now? Which ones would be the highest impact to address?
  - The most effective fraud operations exploit jurisdictional and cross-sector gaps. How do we build toward more effective international coordination and harmonization, which can be very difficult to achieve, but also focus on achieving near-term outcomes even with limited cooperation?
  - How do we measure or characterize success in countering fraud? (e.g., capturing fraud losses; time to detection or disruption; criminal prosecutions; network disruptions; something else?)

- **Capacity Building:**
  - What are the most impactful areas of capacity needed by tools and workforce to better counter fraud?
  - What training is needed to be better, more widely accessed, or operationalized across specific sectors or jurisdictions?
- **Technology Advancements:**
  - What artificial intelligence, advanced computing, digital identity, blockchain, or other emerging technology developments would best enable institutions to combat fraud? How quickly can they be developed and fielded?
- **Public Engagement and Education:**
  - What touchpoints and strategies for educating consumers are the most effective?
  - In consideration of complex issues like liability and accountability as well as practical implementation, how much prioritization should be placed on educating potential victims versus focusing on centers of gravity and chokepoints across the wider fraud ecosystem?

Appendix A – Tentative Calendar
Appendix B – Engagement Sessions Outline

APPENDIX A: TENATIVE TASK FORCE CALENDAR

Key Dates

- **Full Task Force Meetings (Virtual)**
  - November 19, 2025 – Launch
  - February 2026
  - May 2026
  - September 2026
  - December 2026
  - March 2027

Expert Level Deep Dive Engagement Session Workflow

The ACAMS International Anti-Fraud & Technology Task Force will hold engagement sessions between full Task Force meetings to support its workstreams. These sessions – thematic and regional – will bring in a broader network of experts and organizations with relevant insights into the fraud ecosystem. Their input will help strengthen and inform the task force's efforts to combat fraud.

Task force members are welcome to participate, co-chair, or nominate colleagues to join these sessions. Attendance is optional.

Note on Outputs:
Each engagement session will produce two key outputs: ***(1)*** *a concise report submitted to the Task Force highlighting strategic policy considerations and/or fraud-related issues that warrant attention within the context of the global anti-fraud framework, and* ***(2)*** *a practical ACMAS resource – such as a toolkit, playbook, or similar deliverable – designed to support implementation and operational effectiveness.*

- Thematic Engagement Sessions (January – April 2026)
  - January 27, 2026 *(DC, Hybrid)* – AI-Enabled Fraud and Digital Identity Policy
  - February 2026 (*Virtual*) – PPP: Anti-Scam Centers, Building a Collaborative Model
  - Late March 2026 *(DC, Hybrid)* – Fraud Ecosystem and Response Mapping Tabletop Exercise
  - Early April 2026 *(Virtual)* – Vision for Visibility: Examining and Optimizing Reporting
  - April 20-22 - Senior AFC Leaders Strategic Vision Dialogue – Hollywood Assembly, Florida, US

- Regional Engagement Sessions (December 2025 – May 2026, in-person)
  - December 2025 *(Tokyo)* – Assembly Japan
  - April 2026 *(Singapore)* – Assembly APAC
  - May 2026 *(Frankfurt)* – Assembly Europe
  - Further dates in planning (Mexico, Hong Kong, Australia, MENA)

APPENDIX B: TASK FORCE ENGAGEMENT SESSIONS OVERVIEW

Below is a detailed description of the potential engagement sessions that ACAMS proposes for Task Force membership consideration, input, and prioritization:

Date	Engagement Session	Possible Long-term Outputs	Potential External Participants
January 27, 2026 (DC, *Hybrid*)	**AI-Enabled Fraud & Digital Identity Policy** *Policy* Build a coordinated, cross-sector understanding of AI-enabled fraud and deepfake threats. Identify actionable pathways for detection, mitigation, and intelligence sharing.	• Building an AI Fraud Defense Playbook • Explore regulatory, industry, and technology enablers for systemic defense • Establish authenticity verification standards and techniques to differentiate between legitimate and fraudulent AI applications	Industry (financial, banking, credit card companies), technology, AI, identity verification
Late March 2026 *(DC, Hybrid)*	**Fraud Ecosystem and Response Mapping Tabletop Exercise** *Capacity Building* Adopt a unified strategy to disrupt the systems that enable fraud through rigorous, cross-sectoral tabletop exercises across key sectors. These exercises will uncover critical vulnerabilities and services that fraudsters exploit. The insights will identify top priorities and drive the development of coordinated and actionable plans to reduce fraud.	• A walkthrough step by step of several fraud schemes with all ecosystems represented • Mapping of the visibility and authorities at each step; best practices of actions that can/should be taken at each step and intervention point • Development toward a fraud response playbook for cross-sector and public-private response	Industry (financial – banking, payments, fintech, cryptocurrency), technology/social media/dating platforms, fraud experts and response groups, victim and consumer advocacy
February 2026 *(Virtual)*	**PPP: Anti-Scam Centers, Building a Collaborative Model** *Capacity Building* To strengthen the anti-scam and fraud ecosystem	• Identify effective and ineffective practices. • Align the structure and content of a toolkit to help stakeholders build robust, operational, tactical, and	Government and regulatory authorities (FIUs, law enforcement),

	through practical, cross-sector collaboration through the development and enhancement of anti-scam centers.	strategic frameworks for collaboration.	payment service providers, fintech
Early April 2026 *(Virtual)*	**Vision for Visibility** *Information Sharing* Examine reporting channels and repositories, SAR/STR requirements and data schemas. Discuss what is needed to create structures for real-time visibility and coordination	• Map of key reporting channels • Data schema critical to combating fraud • Red teaming operational, tactical and strategic intelligence sharing opportunities • Legal data and intelligence sharing assessment • Leading to codification of principles for data sharing, legal gateways, and operational trust, confirming institutional commitment	FIUs, other law enforcement, regulatory, and civil society reporting streams and repositories
April 20-22, 2026 (Hollywood, Florida, USA *In-Person*)	**Senior AFC Leaders Strategic Vision Dialogue** *Policy* To establish a unified, cross-sectoral framework for mapping global fraud threats and aligning policy responses across jurisdictions and industries.	• Examination of cross-jurisdictional case studies and successes to fighting fraud; • Mapping of int'l financial and tech standards that address fraud; • Identifying frameworks and mechanisms to improve int'l coordination • Toolkit outlining different fraud types and prevention and disruption approach • International taxonomy for classifying and recording fraud types	Regulators, law enforcement, FIUs, industry, payments, technology leaders
TBC	**Victim Experience and Redress** *Public Engagement and Education* Foster a collaborative environment for testing	• Invite to hear from victims and consumer groups the issues on the victim's side; • Mapping challenges for redress;	Victims, consumer advocacy and victim support services

	and refining public–private campaigns that build fraud awareness and strengthen self-protective behaviours among individuals, businesses, and civil society organisations.	• Examination of best practices for education and awareness initiatives and how to improve efficacy	
TBC	**Tech Showcase and Sandbox** *Technology Advancements* Build collaborative sandbox environment where public and private sector participants can safely test, explore, and evaluate emerging technologies used both for harm and for protection. The session will feature live demos of tools used by fraudsters—such as deepfakes, cyberfraud techniques, and account takeovers—alongside cutting-edge regtech and fraud detection solutions designed to counter them.	• Tech Showcase with demos from companies showing tech used for bad (deepfakes, cyberfraud and ATOs) and for good (regtech solutions to detect and defend against); • Discussion of capability gaps in market and what is needed across institutions	Regtech solutions (AI, deepfakes, identity solutions, fraud monitoring)