ACAMS

Anti-Scam Centers and Private-Public Partnerships Toolkit for Financial Institutions:

Day One Readiness

Table of Contents

Introduction

Global fraud losses are rising as criminal networks continue to increase the scale and sophistication of their schemes. Developing a robust anti-scam ecosystem requires strategic coordination and engagement among government, law enforcement and the private sector. Recent global discussions, including work by the United Nations Office on Drugs and Crime and the Interpol Global Fraud Summit, have advocated for the establishment of anti-scam centers (ASCs) and similar public-private partnerships (PPPs) as a means to tackle the proliferation of fraud and scams along with cross-sector and cross-border data sharing, an enhanced preventative approach and targeted awareness campaigns.

ASCs/PPPs — collaborative mechanisms that integrate intelligence sharing, operational coordination, victim assistance and threat mitigation — are proving to be highly effective national responses. ASCs/PPPs can help institutions identify mule accounts faster, improve interdiction at the point of payment, strengthen transaction monitoring, inform onboarding controls, enhance customer warnings and recovery processes, and generate practical lessons that feed back into fraud, anti-money laundering (AML) and anti-financial crime frameworks.

Countries with established ASCs/PPPs have seen clear benefits, with significant potential for further development. As a result, many countries are aiming to launch or improve ASC/PPP initiatives. Financial institutions invited to join ASCs/PPPs have a valuable opportunity. By participating in an ASC/PPP, they gain access to intelligence that allows them to detect fraud within their institutions more quickly. The lessons learned can also strengthen their overall controls, thereby enhancing protection for both the institution and its customers.

ACAMS created this toolkit to help financial institutions prepare for and participate effectively in ASCs/PPPs. As part of the ACAMS International Anti-Fraud & Technology Task Force work, we organized a series of roundtables and interviews with industry experts from around the world who are actively engaged in ASCs/PPPs. This toolkit compiles key lessons learned and practical insights, and provides guidance from industry leaders across each stage of a financial institution's involvement in an ASC/PPP — from initial preparations to information sharing and achieving long-term success. Its purpose is to help institutions answer three practical questions:

- **What do we need in place before joining an ASC/PPP?**
- **How do we operate effectively once inside it?**
- **How do we convert participation into measurable disruption, customer protection and control improvement?**

Established ASC Initiatives

Singapore
Anti-Scam Command (ASCom)

Australia
National Anti-Scam Centre (NASC)

South Korea
National Counter Scam Bureau

Canada
Canadian Anti-Fraud Centre (CAFC)

Malaysia
National Scam Response Centre (NRSC)

United Kingdom
Online Crime Centre

Hong Kong SAR
Anti-Deception Coordination Centre (ADCC) and Anti-Deception Alliance

FRONTIER+ is also a cross-border alliance that operates across multiple jurisdictions, including: Australia, Brunei, Canada, Hong Kong SAR, Indonesia, South Africa, Macao SAR, Malaysia, Dubai, Singapore, South Korea and Thailand.

Although joining an ASC/PPP offers many benefits, it demands careful planning, resources and execution. Financial institutions must ensure compliance with relevant laws and regulations, respond promptly and effectively to ASC/PPP requests, and make the most of the broader insights gained.

Practical Benefits and Outcomes

For a financial institution, ASC/PPP participation has five practical dimensions:

1. **Rapid disruption:**
Institutions can identify and freeze suspect accounts, trace proceeds, escalate to counterpart institutions, support fund recovery and move faster against mule activity. ASCs/PPPs typically have service-level agreements (SLAs) to ensure that participants act swiftly on freezing and tracing requests.

2. **Intelligence exchange:**
Institutions both contribute and receive signals such as linked accounts, scam typologies, beneficiary patterns, wallet addresses, phone numbers, domains, device markers and behavioral indicators.

3. **Control enhancement:**
Intelligence from an ASC/PPP should strengthen onboarding, transaction monitoring, interdiction lists, mule detection, customer risk treatment and fraud rule design.

4. **Customer and victim protection:**
Participation should improve warnings, intervention and signposting, especially where customers are vulnerable or at risk of repeat victimization.

5. **System improvement:**
Mature ASC/PPP participants often help shape typologies, prepare strategic intelligence products, enhance escalation mechanisms, amplify information-sharing norms and improve public messaging and cross-sector good practice.

Preparing for Day One – Legal and Data Readiness

Before an institution starts exchanging information through an ASC/PPP, it needs to understand whether there are existing safe harbors, memorandums of understanding (MOUs), statutory gateways, supervisory expectations or other mechanisms that support lawful sharing for fraud prevention, detection, disruption and victim protection.

The following conversation starters are designed for relevant teams to discuss and operationalize before engaging in ASC/PPP information sharing.

Key Considerations

Legal

- What is the legal basis for sharing information to address privacy, customer confidentiality, bank secrecy and other legal or regulatory restrictions?
- Are there safe-harbor provisions, formal information-sharing agreements, MOUs or other mechanisms to facilitate the legal sharing of information?
- Will there be cross-border sharing, internally or externally? What is the legal basis for this cross-border sharing?
- At what speed does the legal framework allow the institution to operate and share? Is it clear enough to allow for automated sharing, or will sharing need to be manual to allow for potential legal review?

Data

- What types of data can and cannot be shared?
- Is there any data that the institution will intentionally not share?
- Who will have access to the information sent or received at the institution? What access rights or other controls are needed?
- What is the protocol for requesting data, and who can share it internally or externally? Can data be shared only with the government, among participants, within a sector or across sectors?
- In what format will data be received and sent?
- Is the data structured in a compatible way with partners?
- Can the data be structured in a way that supports automated operations?
- What retention, deletion and audit rules will apply?

Tips from Industry Leaders

- **Prepare for legal and privacy reviews to take time.** Legal and privacy reviews will take longer than expected – both before joining an ASC/PPP and as questions arise during participation. Expect more questions and interventions from legal and privacy teams where participation in an ASC/PPP and the associated information sharing is voluntary.
- **Develop a step-by-step legal analysis.** To expedite the review and approval process, consider preparing a detailed, step-by-step legal analysis covering what data can be shared and with whom, both internally and externally. For each step in the process, note the legal authority that allows the information to be shared and what, if any, limits exist. Mapping the process in this way can help make stakeholders across the institution comfortable with the sharing that will occur.
- **Consider internal cross-border data-sharing legal challenges.** For institutions with operations in more than one country, consider the implications of any potential internal cross-border, even if the ASC/PPP itself is purely domestic. This can occur when internal operations, investigations, financial intelligence units, legal, audit or other teams are in a different country from the ASC/PPP. Consider both the legal basis for sharing the information and whether the ASC/PPP permits it. If the institution cannot share information internally as it normally would, it will need to produce an alternative staffing and operational plan.
- **Address cultural barriers to information sharing.** Beyond the legal assessment, some industry leaders noted the need to address long-standing cultural norms around information sharing. In some institutions, information has historically been shared only when legally required. Overcoming this mindset often requires building a clear case for relevant parties and senior leaders by articulating the strategic value and benefits of joining an ASC/PPP.
- **Define data capture and exchange requirements.** Financial institutions should know how they will capture and exchange core fields such as event time, scam typology, account identifiers, payment rail, transaction value, linked indicators, urgency, requested action and eventual outcome.
- **Assess data compatibility at the outset.** Several industry leaders reported that data compatibility is a significant challenge. Governments might request data in a particular format, different institutions might have different data standards, and harmonizing data within an institution can be difficult. Bringing technology and data teams in early to figure out how to structure data and get it in the right format is important. Making any necessary enhancements will take time and may involve additional costs.
- **Engage regulators early.** Explain the ASC/PPP to regulators, including what the institution will be doing, the legal basis for information sharing and the controls it has put in place. Proactive engagement can help build regulatory confidence and reduce friction later.

A useful approach is to classify information into three broad categories.

- **Strategic intelligence:**
  typologies, trends, red flags and fraud-chain insights.
- **Operational indicators:**
  account details, phone numbers, domains, device signals, beneficiary patterns, wallet addresses and linked entities.
- **Customer- or case-level information:**
  customer identifiers, transaction histories, know your customer (KYC) records, investigation notes and other sensitive data..

This tiering helps legal, privacy and operational teams make consistent decisions about speed, recipients and controls.

Participating in an ASC/PPP – Staffing and Operational Readiness

After legal approvals are in place and data is ready to share, the next step is building the right staffing and operational model. That model should reflect the institution's internal needs, the ASC/PPP's requirements and the pace of information sharing. Done well, it will help the institution manage requests efficiently and gain the greatest value from participation.

Key Considerations

Staffing

- Will staff be physically embedded, seconded full time or part time, or participating virtually?
- Which teams and operational functions will need to support the ASC/PPP, including fraud, AML, financial intelligence units, transaction monitoring, account restrictions and closures, legal and investigative teams? Will sharing be automated or manual? What is the expected frequency and volume?
- Who will have the authority to act on accounts, including freezing, restricting or escalating activity?
- Will resourcing require year-round and 24/7 coverage?
- What is the process from the initial inbound request or information sharing through the final response to the ASC/PPP?
- What response times are required? What needs to happen within minutes, hours or days?
- Is the ASC/PPP built around real-time disruption or information sharing only?
- What internal approvals are needed to act based on ASC/PPP intelligence? What is the escalation process for unusual or urgent requests?
- How is ASC/PPP work prioritized?
- How will information be shared securely (e.g., shared platform, secure email, calls, API)?
- What are the operating procedures for account freezing, counterparty bank outreach and victim engagement?
- Which other internal teams need to receive briefings or training on ASC/PPP work?

Victim Outreach

- Who contacts the customer?
- When will a warning be triggered?
- What outreach messages are used?
- How are vulnerable customers managed?
- How is onward support provided or communicated?

Tips from Industry Leaders

- **Plan for staff vetting.** Certain ASCs/PPPs require participants to undergo government vetting. This process may apply only to a primary staff member, but it can also extend to additional personnel. All relevant staff must consent to this screening, which can present HR challenges if employees refuse or are disqualified because of their background. Staff vetting often takes more time than anticipated.
- **Assess how information sharing will affect staffing.** The manner, type and volume of information shared will all have an impact on staffing. If information is shared manually and tends to be more strategic, rather than tied to specific identifiers, it will take longer and require more resources to analyze. Automated sharing and concrete indicators can be analyzed more quickly by fewer people. The larger the institution, the more likely it is to have responsive information. As a result, larger institutions are likely to need more resources.
- **Decide whether to use a stand-alone team or existing processes.** While operational models vary, more institutions appear to leverage existing operational processes for ASC/PPP work rather than creating a stand-alone, end-to-end ASC/PPP team. Industry leaders said using existing processes allowed institutions to better manage fluctuations in the volume of ASC/PPP work. However, institutions that leverage existing processes still typically have a specific point person for the ASC/PPP and sometimes a broader ASC/PPP group or committee to oversee the work. When using existing processes and shared resources, other groups should understand the importance of ASC/PPP work so that it is appropriately prioritized, triaged and, where necessary, compartmentalized.

- **Build accountability into roles and performance expectations.** ASC/PPP work is often not someone's sole responsibility. When it is only one part of an employee's role, the institution should include those duties in the employee's job profile, goals and performance review so the work is not neglected.
- **Prepare for operational complexity.** For many institutions, executing ASC/PPP work will involve multiple teams and operational processes. This could include data teams, various operational teams, analysts, investigators, financial intelligence units, account restriction and closure teams, transaction monitoring and detection, and more, which may be located across fraud, AML or other groups within the organization. To manage this complexity, institutions should map and document all upstream and downstream impacts of ASC/PPP work.
- **Establish governance over the operating model.** Institutions should define clear handoffs, ownership and oversight across the groups involved in ASC/PPP work. Industry leaders track case volumes and monitor service-level agreement compliance within teams and with the ASC/PPP. Missed SLA deadlines could indicate an operational breakdown, a lack of prioritization or the need for more staff. Many institutions leverage existing governance processes for operations but may develop ASC/PPP-specific reporting within those forums.
- **Use secure data-sharing channels from the start.** One industry leader reported that their biggest regret was not using a more formal, secure system for sharing data from the outset, such as encrypted email. If data is not sent in a safe, secure manner, the consequences can be significant. Some ASCs/PPPs set up dedicated email platforms to enable secure communications between public- and private-sector organizations.
- **Create an internal feedback loop.** ASC/PPP insights should not remain limited to the teams handling operational requests. Institutions should share relevant insights with teams that can use them to enhance controls, update customer and enterprise-wide risk assessments, support proactive investigations and develop training materials. A structured feedback loop helps ensure those insights are disseminated appropriately and that the institution gains the full value of its participation.

In practice, most financial institutions fall into one of four models:

- **Liaison model:** relies on a named point of contact to coordinate requests across existing teams.
- **Hub-and-spoke model:** uses a central coordination function to triage inbound and outbound work and route it to fraud, AML, investigations, legal and account control teams.
- **Embedded model:** places staff within the ASC or law enforcement environment, physically or virtually, to support faster decision-making.
- **Fusion-cell model:** supports time-bound operational teams built around a priority threat, such as investment scams, impersonation scams or mule networks.

Ensuring Success – Governance and Measuring Effectiveness

ASCs/PPPs carry legal, regulatory, operational and reputational risks, making strong governance crucial. With proper risk management, the advantages of participation usually far exceed the risks. However, articulating the value of an ASC/PPP and demonstrating its benefits to internal stakeholders can be challenging. Developing metrics to assess and demonstrate the success and impact of the institution's involvement in an ASC/PPP, both internally and externally, is essential.

Key Considerations

Governance

- Who is accountable for decisions made through the ASC/PPP, and who owns the relationship internally?
- What governance forums will oversee participation?
- How will conflicts or potential conflicts between the ASC/PPP and internal policy be resolved?
- How will false positives, customer complaints and overly conservative restrictions be handled?
- How will reputational risk be managed?
- How will actions taken through the ASC/PPP be documented for audit and regulatory review?

Measuring Effectiveness

- What are the institution's key performance indicators (KPIs), and which matter most?
- How will the success of the institution's participation in an ASC/PPP be measured and demonstrated internally?

Tips from Industry Leaders

- **Secure senior-level buy-in.** Executive and senior leadership commitment is critical to the institution's effective participation in an ASC/PPP. It helps ensure access to resources, appropriate prioritization within the institution and the ability to address potential resistance. Institutions also should designate an executive with suitable authority to oversee the ASC/PPP and maintain oversight through established senior governance forums. Over time, maintaining senior-level support will depend on the institution's ability to demonstrate the value of its participation.

- **Measure return on investment.** Return on investment can be one of the most compelling ways to demonstrate the value of ASC/PPP participation. It compares the total cost of participation with the amount of fraud losses prevented for the institution and its customers. One institution reported that for every $1 spent on participating in an ASC/PPP, it prevents $11 in fraud losses. This can be a powerful way to support continued investment in an ASC/PPP.

- **Plan for reputational risk.** While ASCs/PPPs aim to share high-quality information, the intelligence shared is not always perfect or complete. False positives can result in overly conservative restrictions or account closures. In those cases, there can be reputational fallout. Affected customers may post about their experiences on social media, attracting wider attention. The institution should have a plan or process in place to handle these situations should they occur.

- **Define success metrics.** Demonstrating the success of the institution's participation in an ASC/PPP can be challenging. Institutions will often have imperfect information and feedback about the results of their work. The data available might not easily fit into the types of governance dashboards that the institution normally uses. Demonstrating success may require a mixture of qualitative information and quantitative data. Some of the metrics industry leaders have used to demonstrate the success of their ASC/PPP participation include:
  - Money mule or fraudulent accounts identified
  - Money mule or fraudulent actors the institution has already proactively identified
  - Comparisons to other institutions, when data is available
  - Funds frozen
  - Accounts restricted or closed
  - Victims helped
  - Money recovered
  - Fraud against the institution prevented
  - Fraud against customers prevented
  - Speed to action, across various categories
  - Suspicious activity reports, suspicious transaction reports or suspicious matter reports filed
  - Cases that led to arrests, convictions and seizures
  - Adjustments to customer risk ratings
  - Interdiction list updates
  - Controls updated
  - Speed of adjustments to controls
  - Adjustments to the enterprise-wide risk assessment

Conclusion

By emphasizing legal and data readiness, thoughtful staffing and operational planning, robust governance and clear effectiveness metrics, institutions can maximize the value of their participation while mitigating risk. Collaboration and information sharing are central to combating fraud and protecting both organizations and their customers. The insights and strategies shared by industry leaders can help financial institutions take confident, proactive steps toward building a safer, more resilient anti-scam ecosystem.

Appendix 1

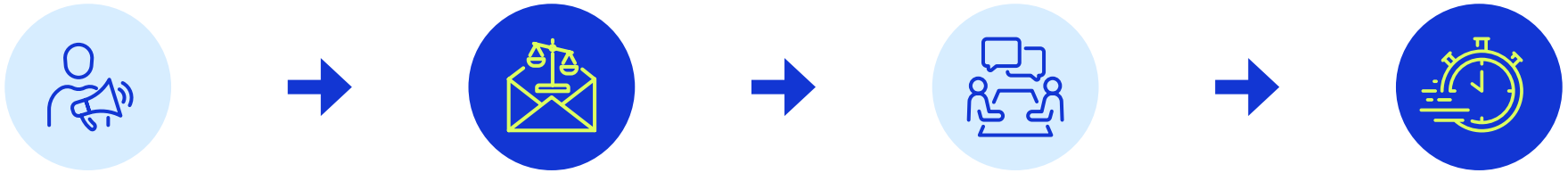
Day One Readiness Checklist for Financial Institutions

Before joining an ASC/PPP, institutions should be able to answer “yes” to the following:

- ☑ Do we have an executive sponsor and operational owner?
- ☑ Have we mapped the legal basis for participation and data sharing?
- ☑ Have we defined what data can be shared, at what level and with whom?
- ☑ Have we standardized a minimum operational data set?
- ☑ Do we have a secure and auditable exchange mechanism?
- ☑ Have we defined service levels and escalation routes?
- ☑ Do we know who can approve urgent account or payment actions?
- ☑ Have we prepared customer and victim communication plans?
- ☑ Have we assessed the implications of cross-border internal information sharing?
- ☑ Have we briefed relevant regulators or supervisors where appropriate?
- ☑ Do we have metrics for operational performance, disruption and customer outcomes?
- ☑ Do we have a formal process for feeding ASC/PPP insights back into control frameworks?

Appendix 2

Intake Decision Tree



Is this a strategic insight or an urgent operational request?

Does it require account action, customer contact or law enforcement escalation? Is it domestic or cross-border?

Can it be handled automatically, reviewed by an analyst or escalated to legal and privacy teams?

What response time applies – minutes, hours or days?

Appendix 3

Further Resources

- PUBLIC-PRIVATE PARTNERSHIP TOOLKIT AGAINST ORGANIZED FRAUD, UNODC, 2026
- UK Member State Initiative Operationalizing a Global Public-Private Partnership on Fraud, 2026
- Cross-Sector Fraud Information Sharing, ACAMS International Anti-Fraud and Technology Task Force, 2026
- Uniting Against Fraud, PWC and Global Anti-Scam Alliance, 2025
- AFC Briefing: Fraud Planning Assumptions 2026-2030, ACAMS, 2025
- Policy Discussion Paper: A new era of private sector collaboration to fight economic crime; Future of Financial Intelligence Sharing (FFIS), 2025
- AFC Toolkit: Protecting Your Customers from Exploitative Scams, ACAMS, 2025

About ACAMS

ACAMS is the leading international membership organization dedicated to providing opportunities for anti-financial crime education, best practices, and peer-to-peer networking to AFC professionals globally. With over 120,000 current members across 200+ countries and territories, ACAMS is committed to the mission of combatting financial crime through the provision of anti-money laundering/counter-terrorist financing, anti-fraud and sanctions knowledge sharing, thought leadership, risk-mitigation services, and platforms for public-private dialogue. The association's CAMS certification is the gold-standard qualification for AFC professionals. It also offers the CGSS certification for sanctions professionals, the CAFS certification for anti-fraud professionals, and the CCAS certification for AFC practitioners in the crypto space. ACAMS' 65+ worldwide chapters further amplify the association's mission through training and networking initiatives.

Legal Disclaimer:

ACAMS strives to only use reliable information in the preparation of its materials. The content contained herein is for general information purposes only. This publication has been prepared using information believed to be reliable and accurate after reasonable inquiry and diligence, but in any event is provided "as is" and ACAMS does not represent it to be error free. This toolkit is neither legal nor tax nor business advice, nor should it be relied upon as such. ACAMS has no obligation to update the information included herein. Please consult your legal, tax, and business advisors with any questions regarding applying this information to your circumstances. This report may contain links to third-party sites which are provided as convenient. The inclusion of such links should not be taken as an endorsement of these sites or their content.