FINTECH ASSOCIATION of HONG KONG
香港金融科技協會

Hong Kong Digital Asset Integrity Forum
Tackling Cross-Sector Fraud: A call to action

FEB 2026

FTAHK.ORG

CONTENTS

The FinTech Association of Hong Kong (FTAHK) is a **member-driven, independent, not-for-profit, & diverse** organisation that is the voice of the FinTech community in Hong Kong. It is organised and led by the community, for the community, through a series of committees and working groups.

Our objective is to promote Advocacy, Communication and Education in the wider FinTech ecosystem.

Build the community.

Be the connector.

A. FOREWORD

To the Stakeholders of Hong Kong's Financial Ecosystem:

The Fintech Association of Hong Kong (FTAHK) is proud to introduce the **Digital Asset Integrity Forum (DAIF)**, a premier quarterly assembly designed to fortify the nexus between traditional finance (TradFi), the rapidly evolving digital asset sector, and the public sector, including regulators and law enforcement authorities (LEAs). By bringing together this holistic financial services ecosystem—spanning global systemic banks, digital asset-native firms, specialized consultants, and intergovernmental bodies—the Forum serves as a central engine for tackling today's most pressing challenges in financial crime compliance and fraud.

In an era where illicit flows move seamlessly across borders and asset classes, our defence must be equally integrated, ensuring that every relevant stakeholder has a seat at the table to drive meaningful systemic change in Hong Kong.

As Hong Kong cements its position as a global premier hub for digital finance, the DAIF serves as a critical **Public-Private Partnership (PPP)**. Our mission is to move beyond high-level discussion toward the design of actionable, cross-sector solutions that safeguard the integrity of our financial markets.

Our Foundation and Evolution

The Forum was established on the principle that systemic risks—such as financial crime, market manipulation, and fraud—cannot be mitigated in isolation. Just as criminals move assets now between the TradFi and digital asset sectors, the industry must now also respond to protect the financial services ecosystem holistically. The inaugural session of the DAIF last November set a high benchmark for this collaborative spirit, conducted in coordination with the **Wolfsberg Group**. This initial session focused on creating dialogue amongst all parties and represented the first time that Compliance Officers from Banks, Payment Services Providers, VASPs, regulators, and law enforcement authorities sat together to discuss the financial crime challenges impacting Hong Kong today.

The Purpose of the Forum

The DAIF acts as a neutral, expert-led platform where the public and private sectors meet to:

- **Identify Emerging Financial Crime Typologies;**
- **Bridge Information Gaps across Industries;**
- **Design Interoperable Standards (processes)**;

- **Align & develop solutions that reduce Fraud and other Financial Crime in HK.**

A Community of Leaders

The strength of the DAIF lies in its participants. Our working groups comprise senior leaders from the world's largest custodial banks, global Tier-1 investment banks, leading regulated digital asset exchanges, and top-tier professional services firms, alongside key representatives from local authorities and the Bank for International Settlements (BIS).

A Call for Engagement

The complexity of modern financial crime requires a unified front, particularly as the speed of digital asset transactions combined with markets operating 24/7 leads to a higher risk of crime being perpetrated. The DAIF is not merely a discussion group; it is a laboratory for the future of financial oversight. We invite you to review the enclosed Q1 Report on Cross-Sector Fraud, which outlines our latest strategic recommendations for the Hong Kong ecosystem.

Together, we are ensuring that innovation in Hong Kong is built upon a foundation of security, transparency, and trust.

Sincerely,

The Digital Asset Integrity Forum

Priscilla Adams, Board Member of the Fintech Association of Hong Kong

B. POST-EVENT REPORT: Q1 2026 DAIF Meeting

Post-Event Report: Digital Asset Integrity Forum (Q1 2026)

Host: Fintech Association of Hong Kong (FTAHK)

Chair: Priscilla Adams, Board Member, FTAHK

Participants *(in alphabetical order)*: Alix Partners, BIS, BNY Investments, Bullish, Chainalysis, DBS, EY, HashKey, HSBC, Standard Chartered, Starling Global, Stratford Finance, VerifyVASP, 3Points Compliance.

Executive Summary

On 10 February 2026, the FTAHK convened senior leaders from traditional finance (TradFi), virtual asset service providers (VASPs), and the public sector to address the escalating threat of cross-sector fraud. As the boundaries between fiat and digital assets blur, criminals are exploiting communication gaps and the disparate speeds of institutional response to exploit the general public.

The forum moved beyond theoretical discussion to identify structural vulnerabilities and design a collaborative framework for information sharing, prevention, and asset recovery.

The Evolving Fraud Landscape in Hong Kong

Fraud is a primary predicate offense for money laundering in Hong Kong, with deception cases accounting for **48.5% of all crime** in the SAR[1]. The evolution of these threats has been rapid:

- **The "Pig Butchering" Evolution:** Schemes have moved from simple crypto scams to industrialized operations involving complex Hong Kong-linked money flows.
- **The AI Era:** Impersonation frauds with deepfakes and synthetic identities have caused a surge in sophisticated "Authorized Push Payment" (APP) fraud. Fraudulent websites, and money mule accounts are also expanding and the average loss per victim is now significantly increasing.

[1] Press Release by the Hong Kong Police Force on 2026-02-11 "Law and Order Situation in Hong Kong in 2025" available at: https://www.police.gov.hk/ppp_en/03_police_message/pr/press-release-detail.html?refno=P202602110004.

- **Total Losses:** Deception cases resulted in financial losses of **HK$8.1 billion** in the most recent reporting cycle, highlighting the urgency for intervention.[2]

Key Challenges and Systemic Gaps

The working group identified critical "friction points" that benefit illicit actors:

- **Velocity Mismatch:** While money moves between market participants via digital assets in mere minutes or hours, investigative processes remain anchored in a "before digital assets" world. Investigations start after a formal complaint has been lodged with Law Enforcement (LE), with LE acting as a central go-between between banks and VASPs. Similarly, banks frequently require T+3 days to intervene in authorized transfers unless they are willing to assume the recovery risk themselves. Information received by VASPs often arrives far too late to prevent the further movement of illicit funds.

- **Information Silos:** Banks require safe harbours to navigate the secrecy provisions of the Banking Ordinance, which currently restrict their ability to disclose client or transaction information to non-bank entities like VASPs. While VASPs are not bound by the same Ordinance, there is no formal, reciprocal framework for real-time intelligence exchange.

- **The Centralized Challenge:** LEAs are currently the only authority which can obtain information from and communicate across all parties (Banks, VASPs, OTC desks). This need to act as a go-between means that information is kept safe, but the time window for freezing assets that often move in hours, can be lost. Successful recovery of assets continues to remain a challenge.

Progress and Strategic Tools

The forum highlighted existing mechanisms that can be leveraged for both preventing frauds and facilitating asset recovery, distinguishing between local innovations and the global enforcement landscape:

Hong Kong Specific Innovations:

- **Scameter & Scameter+:** The Scameter series, managed by the Hong Kong Police Force, has become a vital first-tier defense by providing a real-time search engine for suspicious accounts, URLs, and payment

[2] Press Release by the Hong Kong Police Force on 2026-02-11 "Law and Order Situation in Hong Kong in 2025" available at: https://www.police.gov.hk/ppp_en/03_police_message/pr/press-release-detail.html?refno=P202602110004.

details. The upgraded Scameter+ leverages AI-driven risk analysis to provide instant color-coded warnings, a development that now specifically includes virtual asset wallet addresses to aid in tracking illicit flows. This database is increasingly integrated into bank-led fraud monitoring systems, moving the ecosystem toward a more dynamic and automated detection model. In the first 9 months of 2025 alone, the tool was instrumental in intercepting over HK$1.57 billion in fraudulent transfers, proving its efficacy in reducing the average loss per victim by intervening at the earliest possible stage of the transaction chain.[3]

- **Tokenized Injunctions:** Hong Kong courts are pioneering Tokenized Injunctions as a groundbreaking legal remedy to bypass the anonymity of blockchain participants. This mechanism involves the "airdropping" of court orders via NFTs directly into suspect cryptocurrency wallets, effectively "tainting" the address and providing public, immutable notice of a legal claim to any secondary exchanges or future transactors. While this remains an emerging application that requires further exploration to become a standard market practice, 2024 and 2025 saw landmark precedents where the High Court granted these orders to freeze assets in non-custodial wallets. By leveraging established jurisprudence that recognizes virtual assets as property, this tool allows for legal intervention at the speed of the blockchain, though its scalability across different types of custodial and non-custodial architectures remains a key focus for the Forum's future technical workstreams.

The Global Enforcement Context:

- **Interpol Silver Notice:** On an international level, the "Silver Notice" serves as a critical pilot program (extended through 2026) specifically designed to identify, monitor, and freeze assets linked to financial crime across both fiat and crypto denominations globally. This tool is a direct response to the jurisdictional challenges of modern fraud, allowing law enforcement to issue international alerts to seize illicit proceeds before they are laundered through complex multi-party transaction chains. By focusing on assets rather than just the person, it provides a vital global mechanism to disrupt the financial incentives behind industrialized fraud operations like "pig butchering" and AI-driven deception.

Call to Action: A Framework for Engagement

[3] https://www.thestandard.com.hk/hong-kong-news/article/315461/HK-police-upgrade-Scameter-app-with-AI-engine-scam-rankings-to-combat-fraud

To transition from reactive investigation to proactive prevention, the Forum proposes the following **four pillars of engagement** for further exploration across the SAR:

I. **Legislative Expansion of Information Sharing**

- **Formal Channels:** Provide for a legal or administrative framework enabling banks and VASPs to share real-time intelligence regarding suspicious wallets without fear of "tipping off" violations.

- **Shared Technical Protocols:** Develop a digitized protocol where a fraud alert sent by one party reaches all involved intermediaries (Bank, VASP, OTC desk) simultaneously.

II. **Unified Industry Code of Conduct**

The Forum proposes the establishment of a formal Code of Conduct that standardizes how banks, VASPs, and other financial intermediaries interact during a live fraud event. This framework aims to replace current manual processes with a streamlined, professionalized channel for the whole industry.

- **Standardized Information Sharing Channels**: Establish a dedicated, secure channel for the holistic financial ecosystem. This platform will provide a single point of entry for notifying all involved parties—including VASPs, who are currently outside traditional bank-to-bank safe harbors—of illicit flows in real-time.

- **Provisional Permission to Act (PPA):** Under the Code of Conduct, participating members would adopt a "provisional permission" model, drawing on precedents from fast-moving industries like property management. Such a protocol would allow institutions to ring-fence suspicious assets immediately upon receiving a high-confidence alert via the formal channel, providing a critical window for Law Enforcement to intervene before assets are moved to unhosted wallets.

- **Reciprocal Disclosure Obligations:** The Code would mandate a "two-way street" for intelligence. While banks require safe harbors for disclosure, the Code establishes a standardized set of Minimum Essential Data that all participants (including VASPs) agree to share when a nexus to fraud is identified, ensuring consistent information across all parties.

- **Operational "Stop-Action" Standards**: To combat the current T+3 day delay in bank actions, the Code could define specific triggers that allow for immediate "Stop Payment" or "Stop Wallet" actions without increasing the recovery risk for the individual institution.

III. Unified Public-Private Taskforce

Hong Kong has a world-class legacy of successful pubic-private collaboration through the Anti-Deception Coordination Centre (ADCC) and the Fraud and Money Laundering Intelligence Taskforce (FMLIT). These institutions have proven that the SAR is at its strongest when the public and private sectors act as a single unit. However, as fraud evolves into a cross-sector, high-velocity threat, we must expand this success to combat current and future threats. We propose the creation of a holistic Financial Integrity Taskforce. This next-generation public-private partnership will integrate the entire ecosystem—TradFi, crypto-native firms, and digital forensic experts—into a unified effort that matches the speed of the digital age.

- **Real-Time Collaborative Analysis:** Move away from LE acting as the sole intermediary, leverage available data (such as blockchain, travel rule and other payment data) and break information silos. Create a environment where private sector analysts (e.g., blockchain analytics providers, bank investigators) can facilitate the investigation and fund tracing work of LE in real-time on complex cross-sector cases.

- **Periodic Horizon Scanning:** Regular typology workshop and knowledge sharing between public and private sectors to stay abreast of the trends and plan for timely preventive and risk-mitigating measures.

IV. Consumer Defense & Education

- **Targeted Prevention:** Launch a joint campaign to educate the public on the latest fraud typologies and resources available in preventing and fighting frauds, aiming to reduce the "average loss per victim" and total value of annual losses by increasing scepticism of unverified digital solicitations.

C. Conclusion and Next Steps

The Q1 Digital Asset Integrity Forum has transitioned the conversation from identifying threats to designing the structural architecture required to defeat them. The consensus among the participants—spanning the BIS, global systemic banks, and leading virtual asset platforms—is that Hong Kong possesses the unique regulatory agility to lead the world in cross-sector fraud prevention.

However, the "velocity gap" remains the greatest ally of the fraudster. Closing this gap requires a fundamental shift from sequential, siloed investigations to a parallel, synchronized response model.

The FTAHK remains committed to spearheading this public-private partnership over the coming months, refining these four pillars into a standardized operational framework that secures Hong Kong’s position as a high-integrity leader in the global digital asset ecosystem.