FINTECH PHILIPPINES ASSOCIATION

Dear Member,

I'm excited to present you this month's Trust Tech Committee newsletter. Each month, the committee delivers exclusive updates that are redefining financial security and strengthening customer trust.

For **Scam Watch**, this edition examines **"The App That Made Millions Overnight — Until the Money Vanished."** In April 2026, authorities in Taiwan uncovered an investment scam involving a fake trading app that displayed fabricated profits to lure victims into making repeated investments through bank transfers, cash, and even gold. One victim reportedly saw her balance surge to NT$250 million before discovering the profits never existed. The case highlights how fraud syndicates are increasingly using fabricated digital success to make fraudulent transactions appear legitimate and convincing.

For the **AFC Community Corner**, this edition of *FinCrime Files* explores **Sanctions Evasion & Illicit Fund Flows Through Complex Trade and Payment Networks**, including dual-use goods procurement hidden through split settlements, sanctions-linked payments disguised as corporate service fees, merchant settlement layering through payment aggregators, and humanitarian or NGO-related transfers used to obscure fund beneficiaries—showing how legitimate-looking trade and payment activity can conceal illicit financial flows.

I invite you to be a member of the committee and be part of a community that strives to navigate the complex landscape of anti-money laundering and fraud prevention, empowering all financial institutions in the Philippines to stay ahead of financial crimes.

Abhishek Chatterjee
Trust Tech Committee Chairperson

Member Benefits

Priority Access to Trust Tech Events

Active Participation in AFC Community Dialogues

Add Your Voice
to our Monthly Trust Tech Newsletters

Scam Watch

“The App That Made Millions Overnight — Until the Money Vanished”

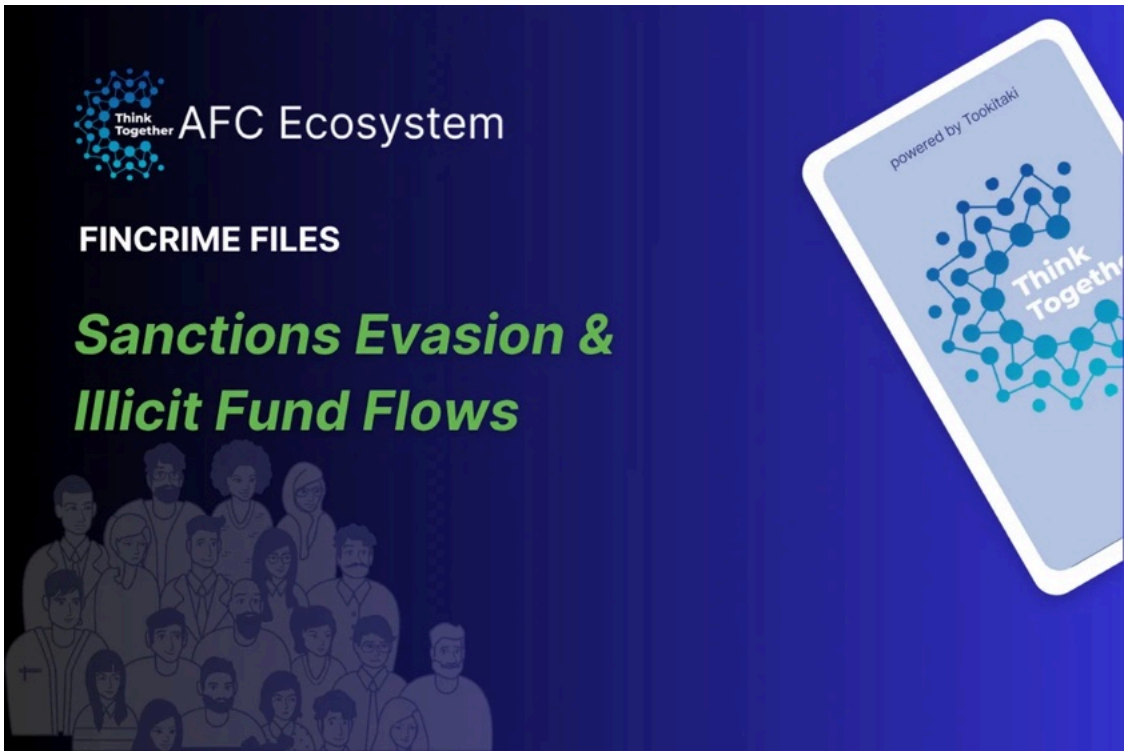
In April 2026, authorities in Taiwan uncovered a sophisticated investment scam where victims were lured through a fake trading app that displayed fabricated profits. One case involved a retired teacher in Taipei who saw her balance surge to NT$250 million, prompting repeated investments through bank transfers, cash, and even gold. The platform mimicked legitimate investment interfaces, reinforcing trust through consistent, believable gains. But when withdrawals were attempted, the illusion collapsed, because the profits never existed.

Why it matters: This scam represents a shift from promise-based fraud to proof-based manipulation. Victims are no longer convinced by opportunity alone, they are shown fabricated success. By the time transactions occur, they appear rational, even prudent. This makes detection significantly harder, as the core deception, the fake app - exists entirely outside the financial system’s visibility.

What to watch for: Gradual increase in investment amounts over short periods, repeated transfers to new or unrelated beneficiaries, and transaction behaviour inconsistent with the customer’s financial profile. Look for fragmented payment methods, including cash or asset-based transfers, and customers demonstrating strong conviction in unusually high returns without verifiable backing. When the transaction looks justified but the belief driving it is externally engineered, the risk may already be in motion.

👉 **Access the full blog here**: [The App That Made Millions Overnight]

AFC Community Corner



In this edition of **FinCrime Files**, the AFC community deep dives into key scenarios covered under **Sanctions Evasion & Illicit Fund Flows Through Complex Trade and Payment Networks**:

1. **Dual-Use Goods Procurement Through Split Cross-Border Settlements**
   Criminals use third-country distributors, procurement agents, and trading firms to conceal the true buyer and end use of restricted goods. Payments are split across invoices, freight, insurance, and refund adjustments to weaken visibility into the full trade chain.
2. **Sanctions Exposure Hidden Through Corporate Service Payments**
   Sanctions-linked actors route funds as advisory fees, retainers, consulting charges, and administrative payments. The receiving entities may appear legitimate, but their role is often unclear or disproportionate to the value transferred.
3. **Merchant Settlement and Refund Layering Through Payment Aggregators**
   Funds are embedded within merchant collections, settlement credits, refunds, reversals, and recycled payouts. This makes sanctions-linked movement appear like a routine platform or merchant processing activity.

4. **Humanitarian Relief and NGO Transfer Chain Misuse**
   Sanctions-linked payments are disguised as grants, field partner transfers, emergency support, logistics reimbursements, or programme expense reconciliations. The structure creates a plausible aid-related purpose while obscuring the true beneficiary and end use.

👉 **Access the full edition here**: FinCrime Files

Join a dynamic community of compliance leaders, innovators, and policy thinkers working together to build a safer financial ecosystem.

As a member of the Trust Tech Committee, you'll gain access to exclusive events, collaborative discussions, and opportunities to contribute to industry-wide initiatives.

👉 **Click here to join the Trust Tech Committee**

Let's build trust in fintech—together.

If you have any questions, please reach out to
Sheryll Cerezo at sheryll@fintechph.org