FINTECH PHILIPPINES ASSOCIATION

TRUST TECH NEWSLETTER

March 2026

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 **"From Screens to Suitcases: The Investment Scam That Moved Beyond Bank Transfers."** In February 2026, Singapore authorities arrested a Malaysian national for allegedly facilitating a cross-border investment scam that blended online deception with physical asset collection. Unlike conventional scams relying solely on bank transfers, the network reportedly collected cash, gold, and valuables directly from victims before reintroducing funds into the financial system through structured deposits and cross-border remittances. The case highlights how fraud syndicates are adapting to tighter digital monitoring by spreading laundering activity across offline and international channels.

For the **AFC Community Corner**, this edition of *FinCrime Files* explores **Cross-Border Remittance-Based Money Laundering**, including fraud proceeds disguised as payroll remittances to overseas workers, fragmented transfers used to settle balances across scam operations, fictitious online marketplace sales used to justify remittance flows, and education or student support payments structured to move illicit funds across borders—showing how routine remittance patterns can be engineered to mask the movement of criminal proceeds.

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

“From Screens to Suitcases: The Investment Scam That Moved Beyond Bank Transfers”

In February 2026, Singapore authorities arrested a Malaysian national for his suspected role in facilitating a cross-border investment scam that blended online deception with physical asset collection. Unlike conventional scam cases relying solely on bank transfers, the network allegedly collected cash, gold, and valuables directly from victims before reintroducing funds into the financial system through structured deposits and cross-border remittances. The case highlights how fraud syndicates are adapting to tighter digital monitoring by fragmenting visibility across offline and international channels.

Why it matters: This arrest reflects a broader evolution in investment fraud mechanics. Criminal networks are increasingly combining digital grooming with physical collection and cross-border layering to dilute detection signals. As transaction monitoring strengthens, syndicates are redistributing risk across jurisdictions and asset types, making behavioural correlation more critical than isolated transaction analysis.

What to watch for: Sudden liquidation of savings followed by structured cash withdrawals, payroll-style remittances without verifiable employment relationships, multiple senders funding the same overseas recipient, and rapid onward transfers after receipt. When funds move predictably across borders but lack genuine economic purpose, the laundering architecture is already in motion.

👉 **Access the full blog here**: Cross-border Investment Fraud

AFC Community Corner

In this edition of **FinCrime Files**, the AFC community deep dives into key scenarios covered under **Cross-border Remittance-based Money Laundering**:

1. **Salary and Employment Cover Remittances Used to Launder Fraud and Scam Proceeds**
   Fraud proceeds are disguised as cross-border salary payments to overseas workers or contractors, often supported by shell entities to justify recurring payroll-style remittances. Recipients are mules or associates, and funds are structured monthly before being withdrawn or transferred onward.
2. **Remittance-Based Settlement of Online Scam Operations Across Multiple Jurisdictions**
   Scam syndicates fragment victim proceeds into multiple small cross-border remittances to settle balances between operational hubs. Each transfer appears legitimate in isolation but collectively launders fraud proceeds before redistribution or cash-out.
3. **Online Marketplace Sales Used as Cover for Remittance-Based Laundering**
   Criminals use fictitious or low-value online marketplace sales to justify cross-border remittances that represent illicit funds. Goods may not be shipped, and funds are quickly withdrawn, layered, or moved onward.
4. **Education and Student Support Remittances Used for Criminal Fund Transfers**
   Illicit funds are routed as tuition or student support payments, structured across multiple senders to reduce scrutiny. Recipients may not be genuine students, and funds are rapidly consolidated or transferred onward.

👉 **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