FINTECH PHILIPPINES ASSOCIATION

TRUST TECH NEWSLETTER

July 2025

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**, it showcases a deep dive on how a $1.2 million investment scam based in Thailand defrauded Australians through fake investment apps, social media manipulation, and remote-controlled accounts — revealing how international scam networks exploit digital platforms and weak AML oversight to carry out cross-border financial crimes.

For the **AFC Community Corner**, the Fincrime Files explores how social engineering scams — from romance and tech support to job and inheritance fraud — are evolving into complex laundering operations. Victims are manipulated through digital platforms, while illicit funds are funneled via shell companies, gift cards, fintech channels, and layered e-wallet transfers across Southeast Asia, exposing the growing convergence of online deception and financial crime.

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

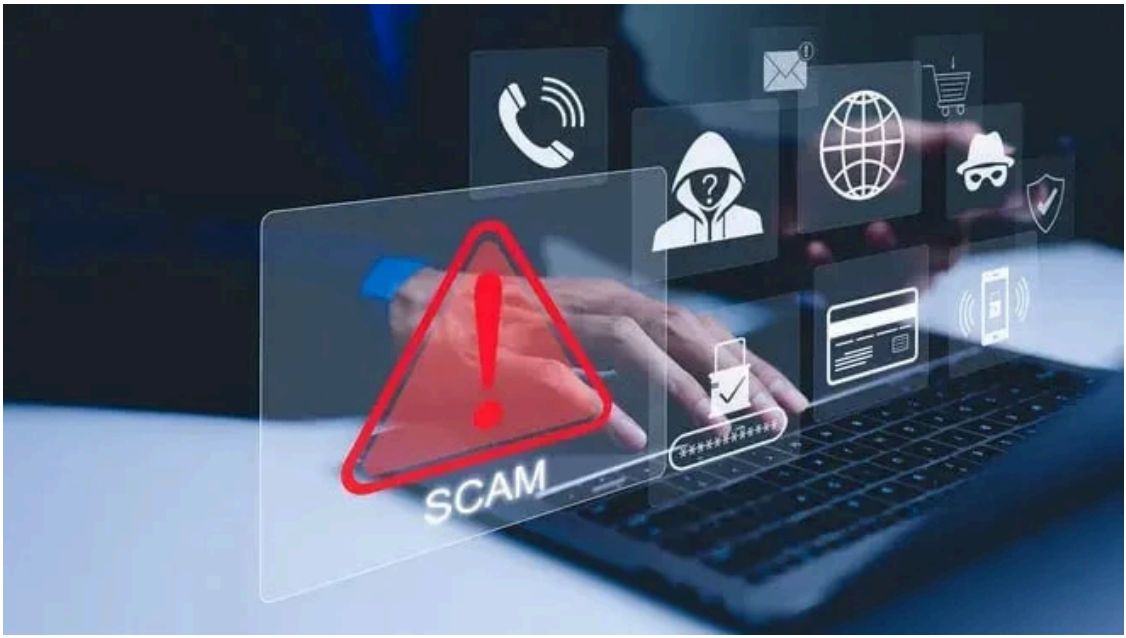
Member Benefits

Priority Access to Trust Tech Events

Active Participation in AFC Community Dialogues

Add Your Voice
to our Monthly Trust Tech Newsletters

Scam Watch



“Lured, Logged In, and Left Broke”: Unmasking Thailand’s $1.2M Investment Scam on Australians

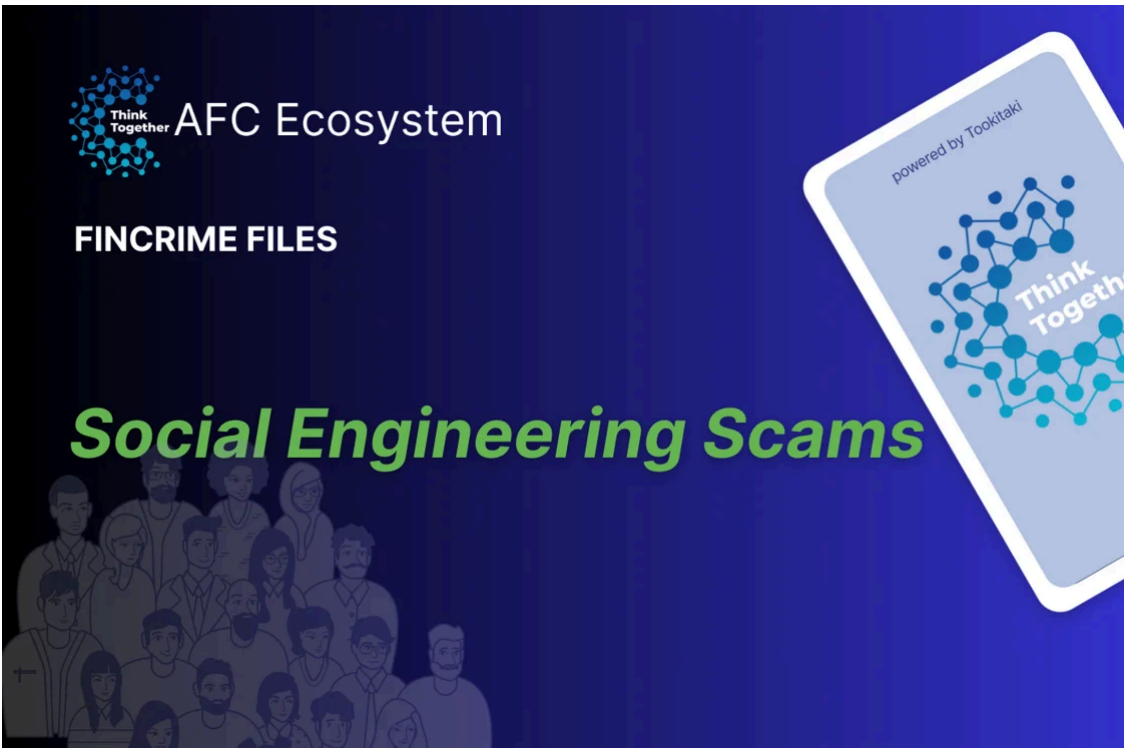
In a cross-border crackdown, Thai police arrested 13 foreigners behind a sophisticated investment scam that defrauded Australians out of $1.2 million. Fake investment apps, social media lures, and remote-controlled accounts were all part of the playbook.

Why it matters: The case exposes how international scam rings are exploiting digital platforms and weak AML oversight to target victims across borders — with Australian investors squarely in the crosshairs.

What to watch for: Remote access tools tied to high-volume transfers, layered transactions through Southeast Asian banks, and offshore app platforms offering unrealistic returns.

👉 **Access the full blog here**: Thai Investment Scam

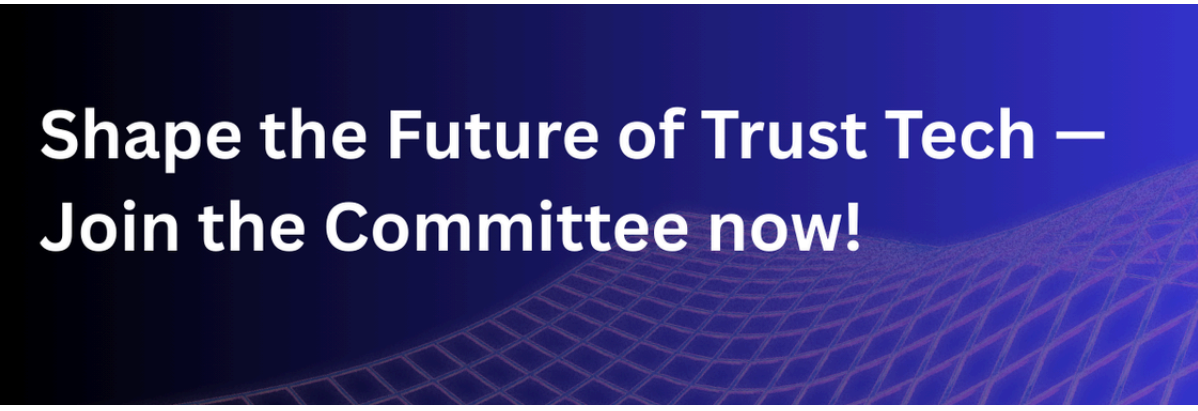
AFC Community Corner



In this edition of Fincrime Files, the AFC community dives deep into key scenarios covered under Social Engineering Scams:

1. **Romance Scam Funds Laundered via Shell Firms and Instant Payments**
   Victims were manipulated on dating apps, with over USD 3.5M funnelled through shell companies and fintech channels.
2. **Tech Support Scam Moves Suspected Terror Funds via Retirees and E-Wallets**
   Illicit funds were layered using smurfing, fintech remittances, and microfinance loans.
3. **Job Scam Launders BEC Funds via Gift Cards and Fake Invoicing**
   Graduates were duped into acting as 'payment admins' to clean corporate funds through digital banks and shell entities.
4. **Inheritance Scam Launders Funds via Trade and Shell Firms**
   Victims were tricked into paying fake legal fees, with proceeds laundered through import-export trade, luxury purchases, and fragmented e-wallet transfers across Southeast Asia.

👉 **Access the full edition here**: [FinCrime Files - June 2025]



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