THE BUSINESS TIMES

November 01, 2025

INSIGHTS FROM
CFA SOCIETY SINGAPORE

Chez Anbu

If scammers can industrialise their craft with instant money, cryptocurrency and AI voices, then regulators and industry can industrialise protection as well – without breaking convenience. PHOTO: BT FILE

Stopping the conveyor belt of crime

Today's AI-powered, crypto-enabled scam industry needs an adaptive policy response

A DECADE ago, most scams were clumsy, one-off e-mails or SMS messages. Today they are sophisticated schemes done at tremendous scale. Fraudsters run playbooks across mainstream platforms, buy ads like real businesses, and now use generative AI to clone voices and faces at near-zero cost. Add cryptocurrency transfers and instant payments, and the result is industrial-scale deception, with money moving in seconds.

In Singapore, one of the most connected places on earth, the Government has pushed some of the boldest upstream rules in the world. But losses are still huge and the scammers' playbook keeps evolving.

According to the Annual Scams and Cybercrime Brief 2024, Singapore recorded 51,501 scam cases with at least S$1.1 billion lost. Most victims weren't hacked; the money was sent by the victims themselves after being manipulated – 82.4 per cent of reported cases involved self-effected transfers.

That single statistic should change how we design our defence. If people are being coached to move money, then the system needs speed bumps, circuit breakers and shared liability – not just firewalls. It's time to update how we assign responsibility and add protection for a world that is moving rapidly towards digital assets, instant transfers and industrialised deception.

What's really changed – platforms, payment and AI

Social and marketplace platforms are now the front door. Grooming begins on apps we all use – social feeds, messaging groups, marketplace listings and creator channels. The conversation quickly moves off-platform, and within minutes you're being steered to a "broker" site, a fake merchant page, a convincing wallet download, or a QR code to a rogue payment link.

Payments are instant…and unforgiving. Real-time rails – technological infrastructure and networks that enable movement of digital assets and information – are fantastic for genuine commerce but they shrink the time to intervene. Once funds move, recovery is hard, and when victims were coached to send money themselves, traditional "unauthorised transaction" rules don't apply.

AI supercharges persuasion. The impersonation has become increasingly convincing with effective usage of AI. It also allows for instant aggregation and creation of user profiles from social media feeds and digital presence. This has huge implications from how you set your passwords (for example, don't use your pet's name as

THE BUSINESS TIMES

November 01, 2025

Creating more awareness about scams helps to educate consumers on the pitfalls to avoid.
PHOTO: BT FILE

a password) to the need to verify who is on the other end of the line.

Crypto is the new exit lane. More scams now end on digital-asset rails, luring victims with promises of "guaranteed yields" or steering them to fake exchanges and look-alike wallet apps. The hook is the same as ever – urgency and certainty – just with a modern, tech-heavy gloss and faster way to cash out. Once funds are moved across different crypto chains or mixed, the trail vanishes instantly.

What's working and where may need to improve

Singapore has shifted responsibility upstream. Telcos have come up with processes to flag suspicious SMS. ScamShield filters calls and texts and gives citizens a single place to check. Banks have added real-time surveillance, "kill-switches", lower default transfer limits, and safer defaults like link-free official messages. Platform-side duties now force quicker takedowns and reporting for scam content and seller abuses. These moves successfully tackle the most obvious vulnerabilities.

But two hard problems remain:

Authorised push-payment scams – The dominant loss area is victims being coached to send money. Traditional protections that are built for unauthorised card or account takeovers do not stop such scams. Victims technically "approved" the transfer – except they were manipulated into doing it.

Platform-payments-crypto handoff – Scams are cross-channel by design: a social ad leads to messaging, then to a fake site, then to a real bank transfer or an on-ramp to buy cryptocurrency. Current rules still assign responsibility in silos – platforms handle content, telcos handle pipes, banks handle transfers, crypto exchanges handle wallets – yet the attack is one continuous journey.

The new red flags

Be aware. Stop, if you are:

- Nudged to move off-platform to WhatsApp/Telegram and to avoid platform payments;
- Asked to install an app via a link (especially Android) or to grant accessibility permissions;
- Told to screen-share or install remote desktop tools "so we can help you invest";
- Given guaranteed returns, small "test profits" then pressured to top up in order to unlock withdrawals;
- Invited to a crypto "investment" group using jargon like "arbitrage", "liquidity mining", or "staking" with slick dashboards and "VIP mentors"; or
- Asked for credentials, transfers, or Singpass scans by a caller who claims to be a government/bank official.

If in doubt, call 1799 or use ScamShield's checker before you act. Taking just a few extra minutes can save you months of pain.

Creating a stronger regime – building on what works

There's an urgent need to evolve to an outcome-based model that mirrors the full scam journey:

- **Shared liability for authorised push-payment (APP) scams** when the system misses clear risk signals across platforms, telcos, and banks. This should include a clear, consumer reimbursement path calibrated to each choke point.
- **Create adaptive friction, not blanket holds**: Step up only on risky patterns instead of blanket delays. Use multi-factor authorisation and verified call-back for new/high/overseas payees; require short cooling-off periods or active challenges for anomalous behaviour; and block high-risk actions when screen-sharing or remote-control is detected.
- **Require stronger control for financial promotions**: Issue verified advertiser IDs and visible licence numbers, adopt stronger seller verification processes, and offer default payment protection for high-risk categories.
- **Create crypto chokepoints**: To make it harder for scammers to launder stolen funds, ensure smarter warnings when buying crypto; adopt exchange allow-lists, limits on first-time use and checks for unusual activity; offer wallet hygiene nudges and transaction simulations.
- **Require verification for high-value actions**: Ensure verification tools are able to detect deepfakes.
- **Use one-tap citizen tools**: Embed "Check with ScamShield" in bank/platform flows; keep "Likely-SCAM" labels prominent.

Here are what investors should do – today.

- **Slow the money when it matters**: Put rainy-day funds behind a Money-Lock/allow-list so a coached transfer can't drain you in one go.
- **Never install apps from links**: Requests or instructions to install a "broker" or "support" app outside official channels are a red flag.
- **Never screen-share while making bank or wallet transactions**: No legitimate institution needs to watch you log in.
- **Verify callers via official channels**: Hang up and call back using numbers you find yourself. Government officers will not ask for credentials or transfers over the phone. When in doubt, call 1799.
- **Adopt "crypto hygiene"**: Use verified or listed withdrawal addresses, start with small test transfers, and be suspicious of anything promising guaranteed yields or providing VIP statuses.

The bigger picture

Singapore has already shown it can move fast with platform duties, telco filters, safer banking defaults, and stronger police powers to disrupt scams in flight. The next step is to merge these streams into one outcomes-oriented regime that mirrors how scams actually unfold across platforms, pipes, payments and crypto.

If scammers can industrialise their craft with instant money, cryptocurrency and AI voices, then regulators and industry can industrialise protection as well – without breaking convenience. The tools exist.

The job now is to wire them together so that the safest path is the default one, and the dangerous path is slow, bright red, and expensive for the criminals who try it.

The writer, CFA, CAIA, is the founder and chief executive officer of Photis Wealth AI. He also volunteers as a member of the CFA Society Singapore Advocacy Committee.