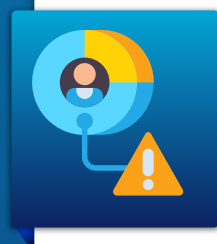


Why fraud defence now needs signals from the network

Fraud is becoming harder to detect across digital channels.¹



Synthetic identities can appear legitimate.



Enterprises need stronger ways to assess risk during customer interactions.



Real-time trust signals can help determine whether an action should proceed.¹

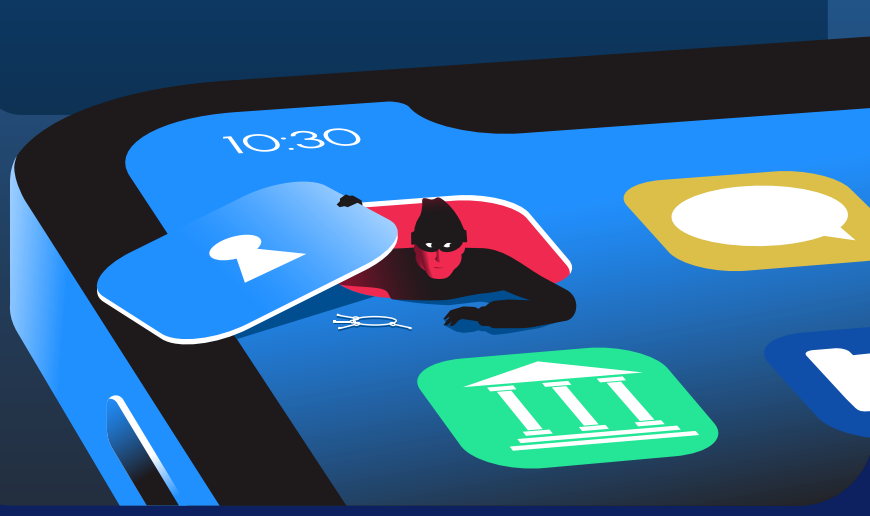
*Deepfakes can be used to support scams and impersonation.
SIM swap attacks can redirect one-time passwords to fraudsters.^{2,3,4}*

Three fraud patterns that are raising the risks

Synthetic identity fraud

Fraudsters combine real and fabricated personal information to create identities that can pass onboarding checks and build account history before being used for fraud.²

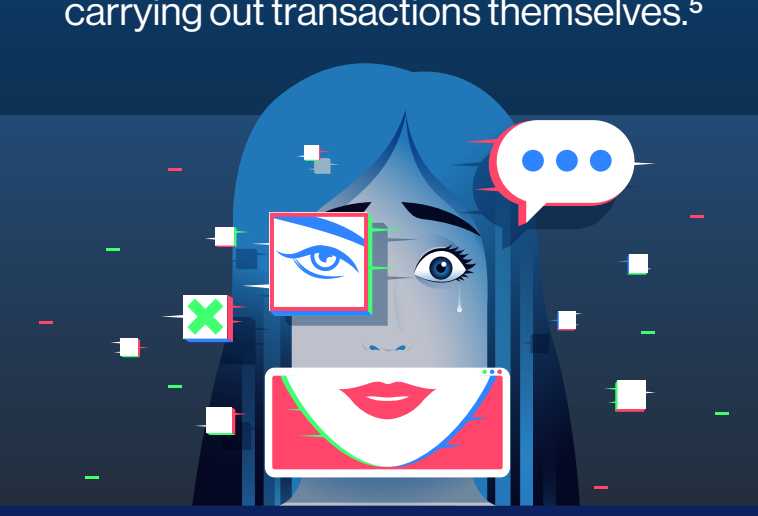
In Singapore, scam losses reached approximately **S\$1.1 billion in 2024**, with **51,501 scam cases** reported.⁵



Deepfake-assisted fraud

AI-generated voices, images, and videos can make fraudulent instructions appear to come from trusted people or legitimate processes.³

Self-effected transfers accounted for **82.4% of reported scam cases in 2024**, showing how often victims were manipulated into carrying out transactions themselves.⁵



Why traditional checks are under pressure

Passwords can be stolen through **phishing** or exposed in **data breaches**.



OTPs can be intercepted after a SIM swap.



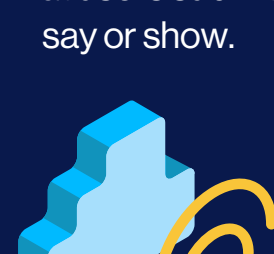
Know Your Customer (KYC) documents & profile data can be manipulated through **synthetic identities**.



Video or voice checks can be challenged by **deepfake-assisted scams**.

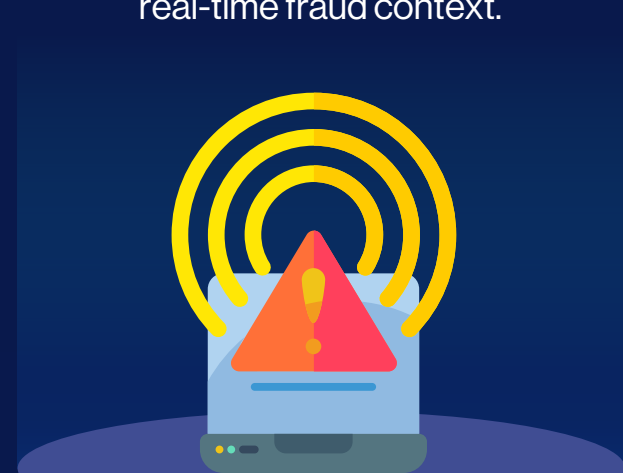


Enterprises **need risk signals** that extend beyond what users submit, say or show.

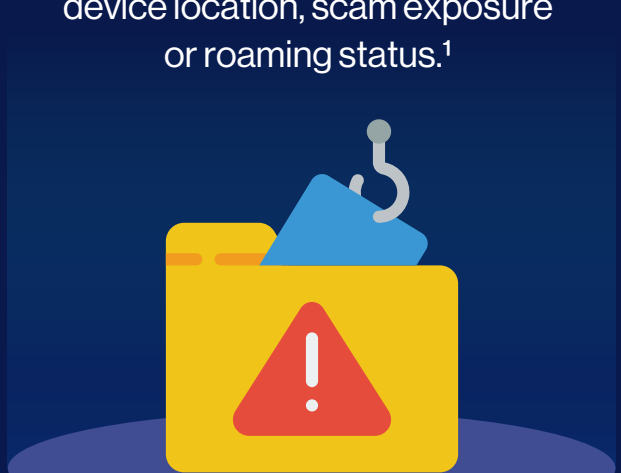


Moving beyond traditional authentication checks

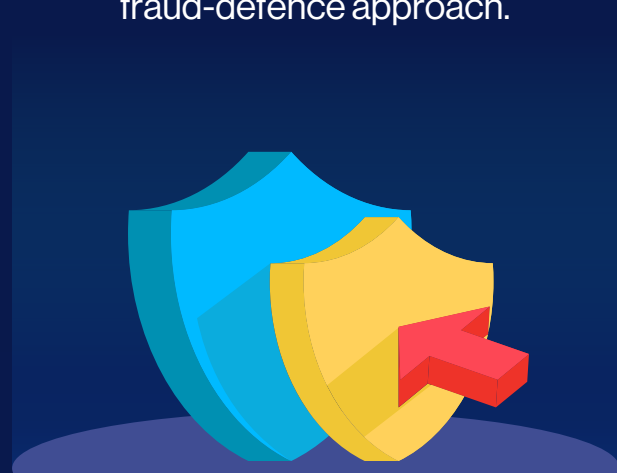
Network-derived signals provide real-time fraud context.



They can indicate SIM changes, device location, scam exposure or roaming status.¹



This supports a more layered fraud-defence approach.



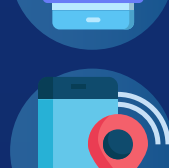
The network intelligence advantage

SingVerify is a suite of telco APIs that use real-time mobile network intelligence to support authentication and fraud-risk decision, which help enterprises add network-level context to registration, login, payments, password resets, and other high-risk actions.¹



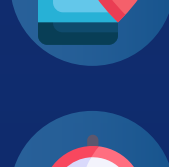
Number Verify

Is this mobile number genuinely associated with the user's device?¹



Device Location

Is the customer's device physically near the point of activity?¹

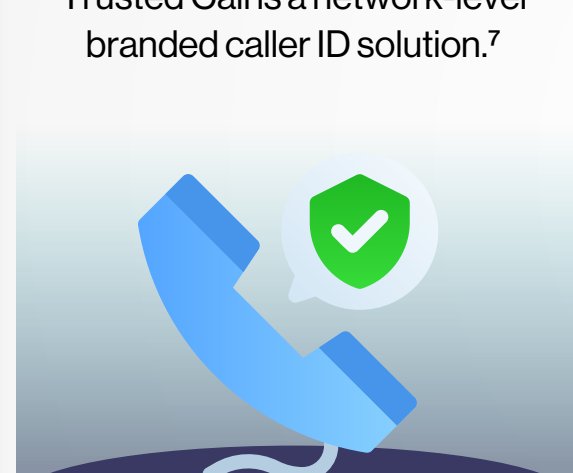


Scam Sniffer

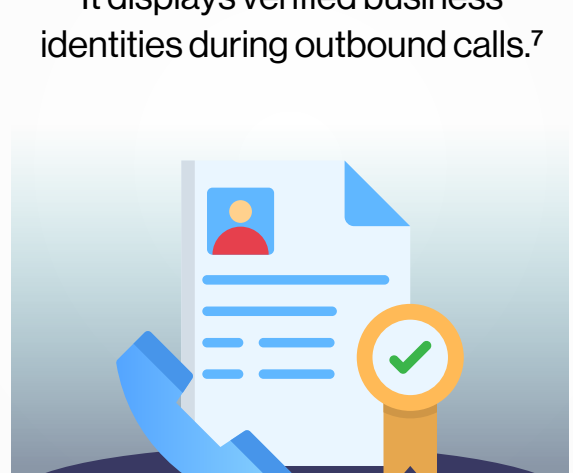
Is the user actively in contact with a suspected scammer during high-risk activity?¹

Trusted Call: Verify every business call

Trusted Call is a network-level branded caller ID solution.⁷



It displays verified business identities during outbound calls.⁷



It helps users identify genuine business calls.⁷



As fraud becomes more synthetic, more conversational and more real-time, enterprises need trust signals that are just as real-time.

Build a layered fraud defence with Singtel network intelligence.

[Discover now](#)

**Ignite the Change
Hello Possibilities**

References

- ¹ Grand View Research, Connected Car Market, 2025-2030
- ² Grand View Research, Automotive Over-The-Air Updates Market (2024 - 2030)
- ³ Onomondo, What is GSMA SGP.32? Diving into the eSIM IoT standard, 2024
- ⁴ Singtel, Singtel launches enhanced connectivity solution for enterprises pursuing international IoT expansion, 2025