LexisNexis®
RISK SOLUTIONS

Evolving Threats Beneath The Surface

How Criminal Networks In APAC Are Changing Tactics to Stay Ahead of Developing Defenses

LEXISNEXIS® RISK SOLUTIONS CYBERCRIME REPORT

SINGAPORE IN FOCUS

2025 saw steady digital growth in transactions across the LexisNexis® Digital Identity Network® globally, including a 20% rise in the Asia Pacific region. This growth has been driven in part by mature digital markets such as Singapore, where high levels of online engagement continue to expand the transaction landscape. Unfortunately, global fraud is rising even faster. In APAC, the overall attack rate has risen 12% YOY and now sits at 1.7%, higher than the global average of 1.6%.

Transactions in APAC are up 20% YOY, but human attacks and bot volume are rising faster (up 36% and 39%).

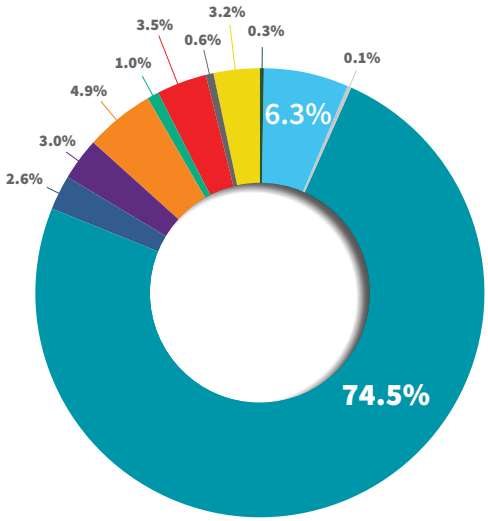
Fraud Classifications in APAC

Third party takeover remains the most prevalent fraud, but has lost ground to a range of other kinds of attacks

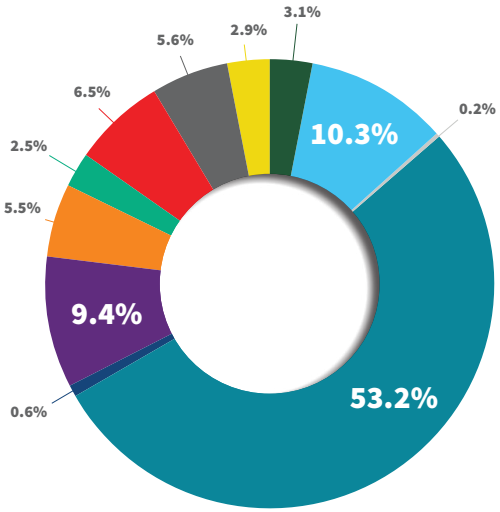
The charts on this page show how fraud attempts in our Digital Identity Network are classified by our clients. The most prevalent categories in this year's data are third party account takeover, first party fraud, and bonus abuse.

Last year, around three out of four attacks in the APAC region were due to third party account takeover, by far the highest ratio across the four global regions. This year, third party fraud still accounts for more than half of all attacks, but a wide array of other attacks have gained significant ground, including first party fraud (up from 6.3% to 10.3%), bonus abuse (up from 3.0% to 9.4%), scams (up from 3.5% to 6.5%) and synthetic identity fraud (up from .6% to 5.6%).

PREVIOUS YEAR



THIS YEAR



FRAUD GROUP

- 1st Party Chargeback Fraud
- 1st Party Fraud
- 2nd Party Fraud Collusion
- 3rd Party Account Takeover
- 3rd Party Chargeback Fraud
- Bonus Abuse
- Buyer Fraud
- Other
- Scam
- Subscription Fraud
- Synthetic Identity Theft
- True Identity Theft

$7.14 The LexisNexis® Fraud Multiplier™ value in the APAC region represents the real cost to businesses here of every dollar of fraud, once all costs are tallied.

Spotlight: Singapore

Bot attacks more than doubled in Singapore in 2025 (up 116%) as both the ecommerce industry and financial sector were targeted with increased automation.

Strong ecommerce transaction growth (up 59%) this year was offset by reduced financial sector transactions, resulting in an overall 23% decrease in transactions. Human attacks, driven primarily by ecommerce attacks, rose 2% YOY, but bot attacks more than doubled, driving the overall attack rate up 35% YOY to 1%—still well below the global average of 1.6%.

Singapore, an important financial and fintech hub, has been a leader in implementing antiscam measures. Their Shared Responsibility Framework, introduced in late 2024, came into full force in 2025, including additional measures like account drainage guidelines designed to keep scammers from rapidly draining victim accounts within a 24-hour period.

As in Hong Kong, mobile app transactions heavily dominate the Singapore dataset, with a high mobile app vs. mobile browser transaction ratio. However, in Singapore the share of mobile attacks relative to desktop attacks grew 15% this year, bucking the trend we see in Hong Kong and globally.

	TRANSACTIONS	YOY GROWTH
TRANSACTIONS ANALYZED	0.9B	-23%
HUMAN-INITIATED ATTACK VOLUME	9M	2%
AUTOMATED BOT ATTACK VOLUME	44M	116%

	MOBILE	DESKTOP
TRANSACTIONS SPLIT BY MOBILE / DESKTOP	91%	9%

	MOBILE APP	MOBILE BROWSER
TRANSACTIONS SPLIT BY MOBILE APP / MOBILE BROWSER	93%	7%

	MOBILE	DESKTOP	YOY GROWTH OF MOBILE SHARE OF ATTACKS
ATTACKS SPLIT BY MOBILE / DESKTOP	43%	57%	15%

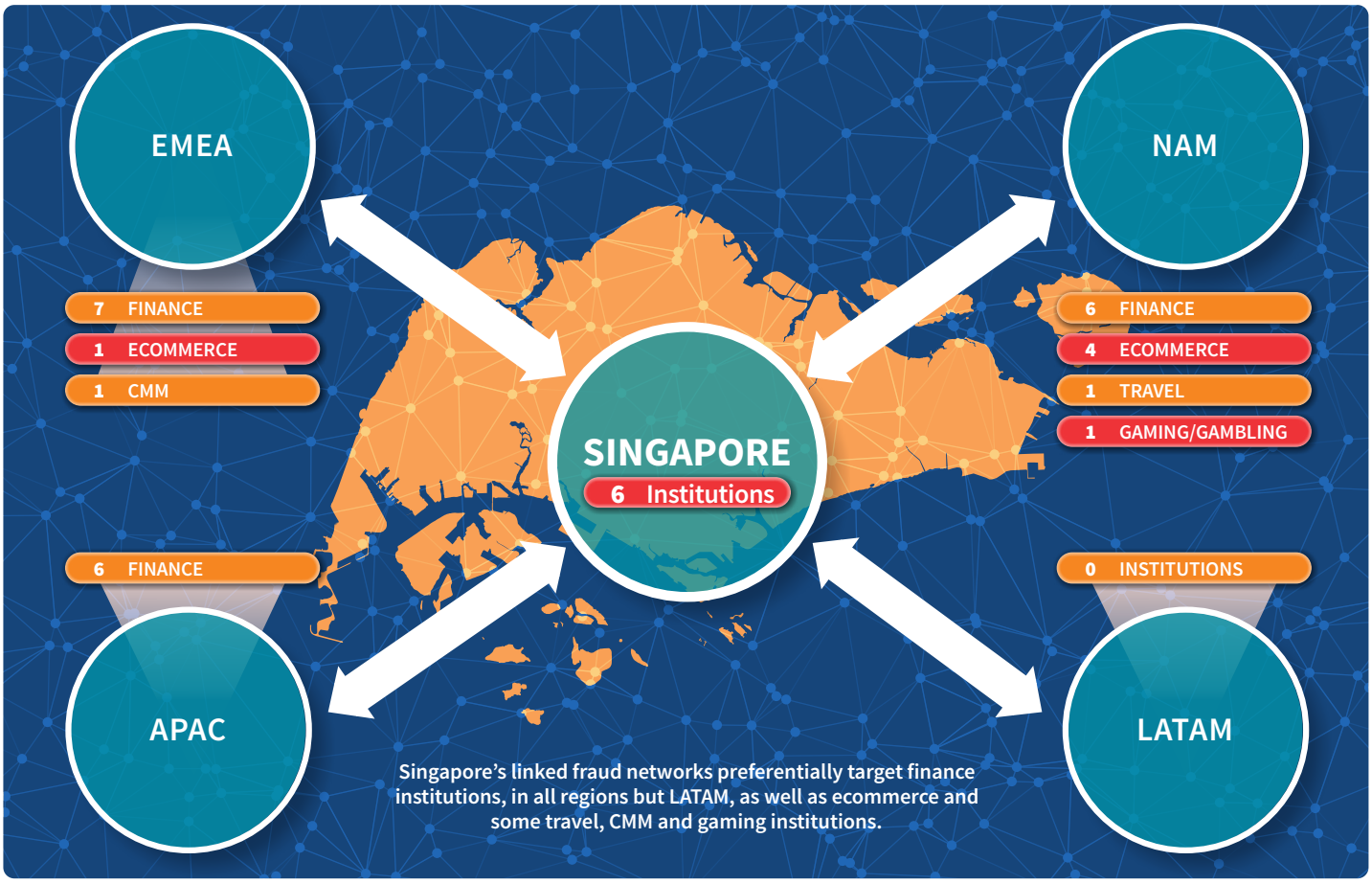
	APAC FIGURES	GLOBAL FIGURES
OVERALL ATTACK RATE	1.0%	1.6%
DESKTOP ATTACK RATE	6.1%	4.3%
MOBILE BROWSER ATTACK RATE	4.8%	4.2%
MOBILE APP ATTACK RATE	0.2%	0.4%

Fraud in Singapore

This visualization shows networked fraud (linked by digital identity) connected to organizations operating in Singapore during the third quarter of 2025.

The arrows illustrate digital identities associated with confirmed fraud attempts at one organization within the LexisNexis Digital Identity Network that then cross over to another organization (for example, to a finance platform in EMEA).

Fraud networks target accounts across multiple banks in Singapore, and this diagram reveals significant links across borders to other financial institutions in EMEA and North America in addition to more locally in southeast Asia. The same fraudulent digital identities additionally target ecommerce and travel related digital services, as well as telco operators and gaming sites.



How Can We Help?

Successful risk intelligence comes from domestic organisations as well as from across the globe. Detect and prevent more complex forms of fraud with a more comprehensive range of solutions that better protect you, and your customers, at every touchpoint.

Our AI-powered modelling of industry-leading data and vast networks of digital, email and behavioural intelligence come together to help uncover hidden risk, increase customer conversions, and stop fraud across all channels with greater confidence.

Contact us for more information.