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

HONG KONG 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 Hong Kong, 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%).**

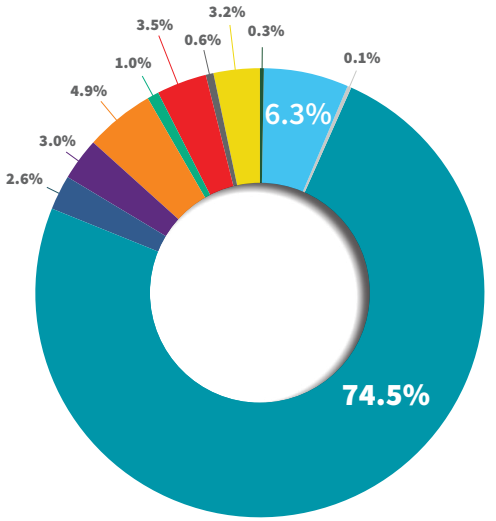
# Fraud Classifications in APAC

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

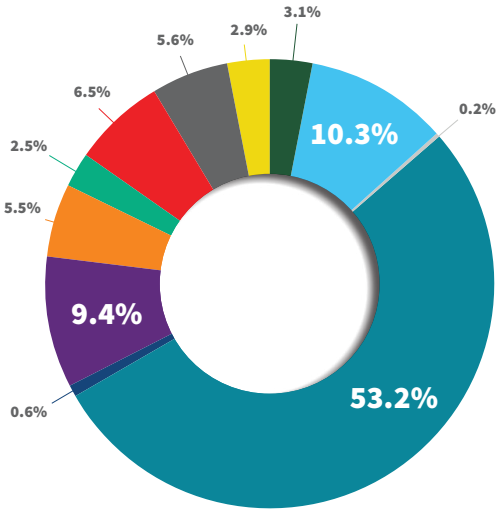
The charts on this page show how fraud attempts in our Digital Identity Network are classified by our clients. The most prevalent categories in this year's data are third party account takeover, first party fraud, and bonus abuse.

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: Hong Kong

**In the Digital Identity Network, Hong Kong transactions grew a robust 9% this year, but the fraud attack volume grew much faster. As a result, the attack rate for Hong Kong more than doubled (up 118% YoY). While the overall 1% attack rate here is still significantly lower than the 1.6% global average this reflects a significant increase in fraudster activity in Hong Kong: seen across most industries, but especially ecommerce and gaming & gambling.**

The Hong Kong Monetary Authority, Hong Kong Police Force and Hong Kong Association of Banks, in April of 2025, jointly announced new measures to detect, prevent and disrupt financial crime including fraud and associated mule networks.

Mobile app-based transactions in Hong Kong dominate the data set, with a much higher mobile app vs. mobile browser transaction split than the global average. This is also true of the general mobile vs. desktop split. From an attack perspective, attacks here are moving back to desktop and away from mobile. This mirrors the general global trend, but with an even faster return to desktop: Hong Kong saw a 40% decline in the mobile share of attacks this year.

| | ▾ TRANSACTIONS | ▾ YOY GROWTH |
|---|---|---|
| TRANSACTIONS ANALYZED | 1.3B | 9% |
| HUMAN-INITIATED ATTACK VOLUME | 12M | 130% |
| AUTOMATED BOT ATTACK VOLUME | 44M | 172% |

| | ▾ MOBILE | ▾ DESKTOP |
|---|---|---|
| TRANSACTIONS SPLIT BY MOBILE / DESKTOP | 90% | 10% |

| | ▾ MOBILE APP | ▾ MOBILE BROWSER |
|---|---|---|
| TRANSACTIONS SPLIT BY MOBILE APP / MOBILE BROWSER | 97% | 3% |

| | ▾ MOBILE | ▾ DESKTOP | ▾ YOY GROWTH OF MOBILE SHARE OF ATTACKS |
|---|---|---|---|
| ATTACKS SPLIT BY MOBILE / DESKTOP | 26% | 74% | -40% |

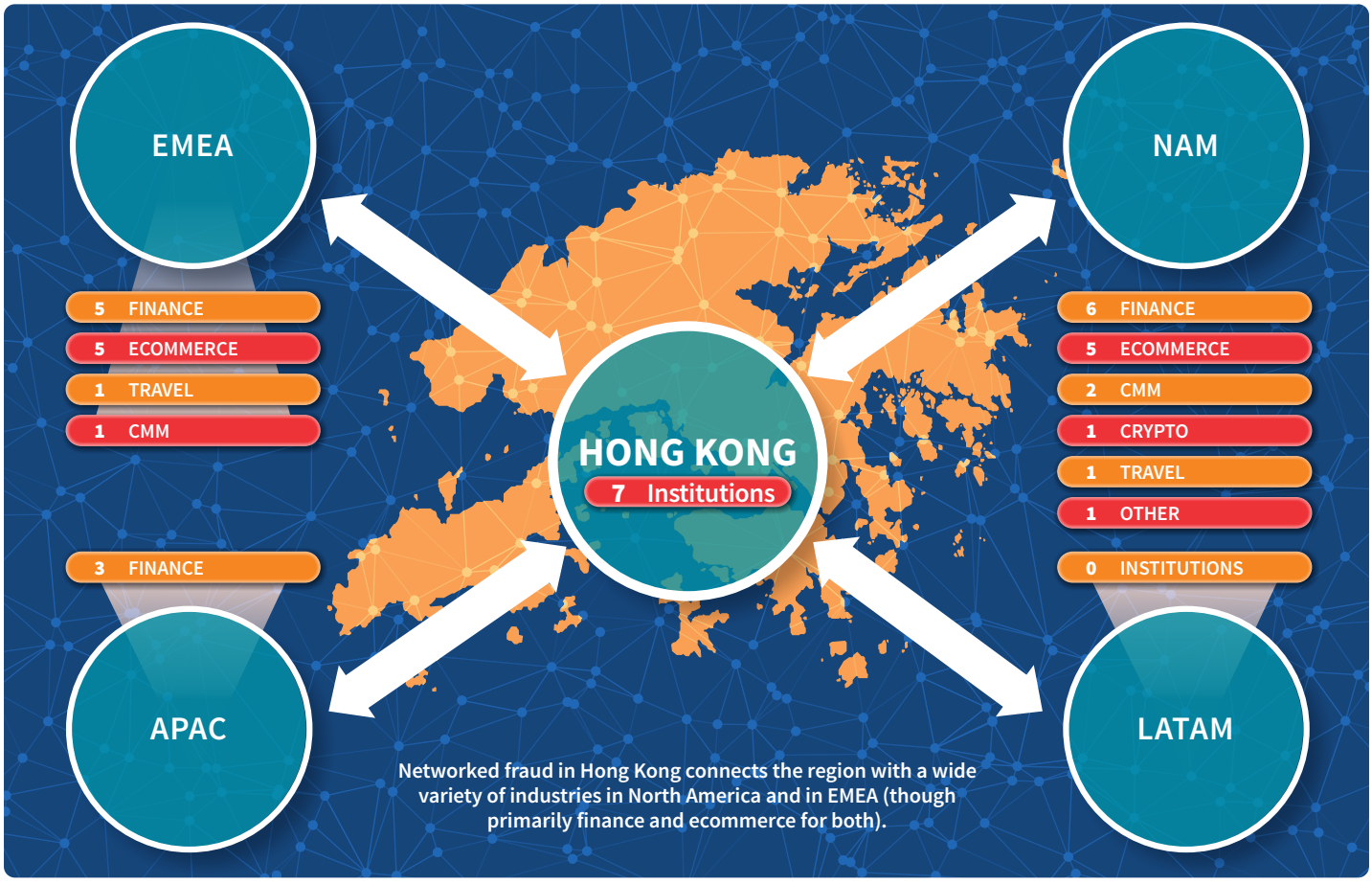
| | ▾ APAC FIGURES | ▾ GLOBAL FIGURES |
|---|---|---|
| OVERALL ATTACK RATE | 1.0% | 1.6% |
| DESKTOP ATTACK RATE | 7.2% | 4.3% |
| MOBILE BROWSER ATTACK RATE | 5.5% | 4.2% |
| MOBILE APP ATTACK RATE | 0.1% | 0.4% |

# Fraud in Hong Kong

This visualization shows networked fraud (linked by digital identity) connected to organizations operating in Hong Kong 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 operating in Hong Kong have significant links beyond its borders, to financial institutions but also ecommerce, travel, telecom operators and crypto exchanges. These tend to be based in the U.S. or Europe, although links to regional banks in Asia can also be seen.




## 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.**