

Evolving Threats Beneath The Surface

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



LEXISNEXIS® RISK SOLUTIONS CYBERCRIME REPORT

AUSTRALIA 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 Australia, 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%).



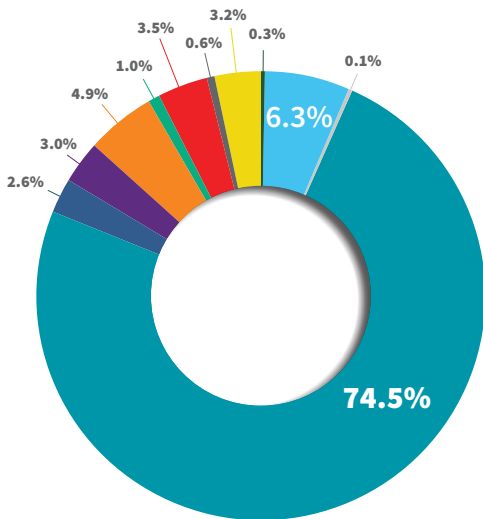
Fraud Classifications in APAC

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

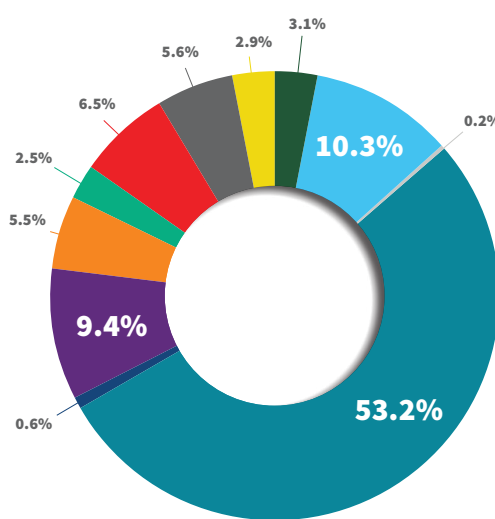
The charts on this page show how fraud attempts in our Digital Identity Network are classified by our clients. The most prevalent categories in this year's data are third party account takeover, first party fraud, and bonus abuse.

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

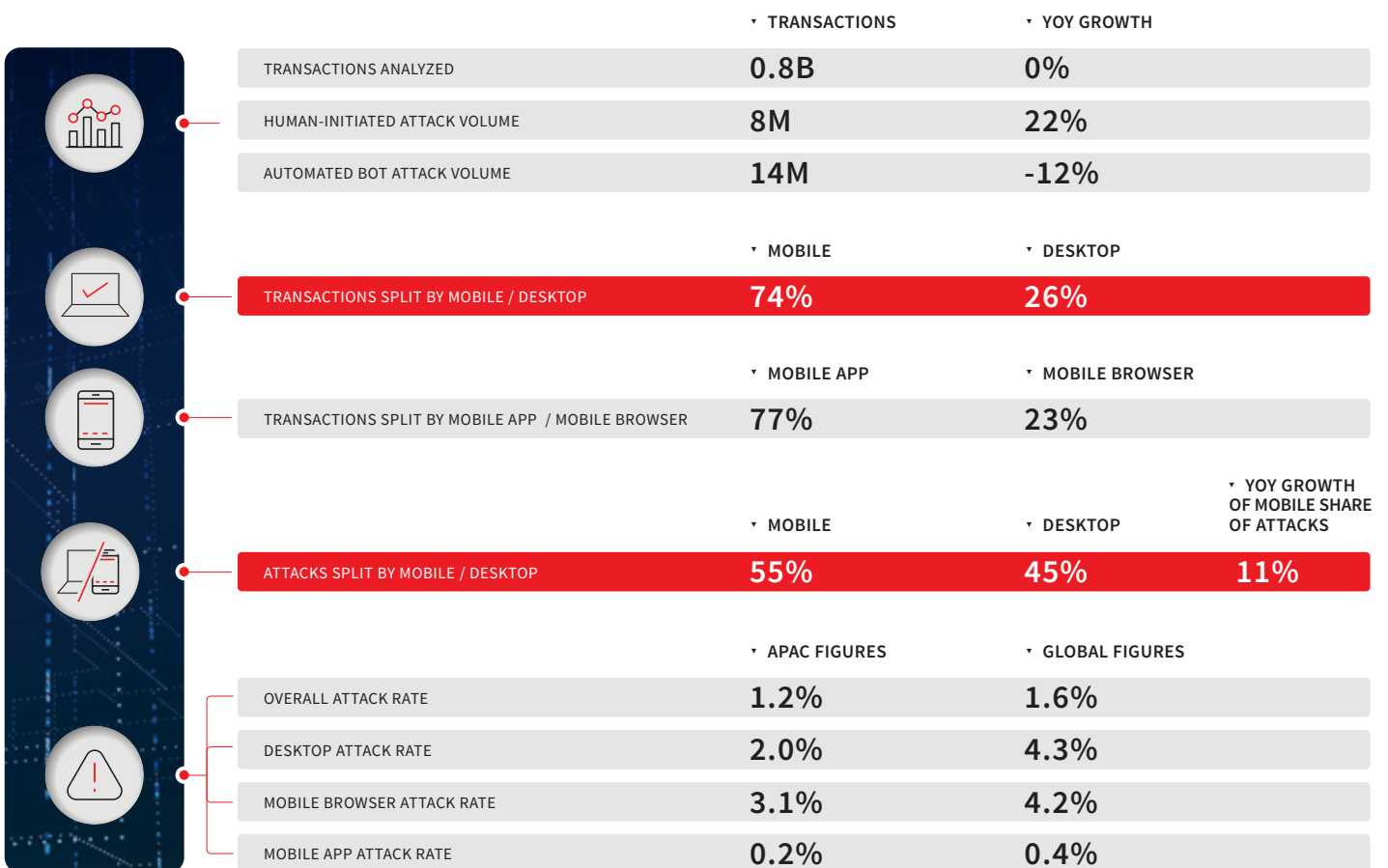
The LexisNexis® Fraud Multiplier™ value in the APAC region represents the real cost to businesses here of every dollar of fraud, once all costs are tallied.

Spotlight: Australia

>> This year, the attack rate in Australia grew substantially (up 17% YoY to 1.2%) though it remained lower than the global average of 1.6%. Well-publicized data breaches in recent years have left created plentiful opportunities for fraudsters; the Australian Bureau of Statistics has reported increasing identity theft rates in recent years. Scams and card fraud continue to be serious concerns in the country as well.

>> The attack rate here grew across all channels, with mobile attack rate growth outpacing desktop, bucking the general shift seen globally of attacks returning to the traditional desktop browser channel. In Australia the ongoing shift to mobile attacks suggests that criminals are continuing to see success with these attack methods, potentially encountering less secure defenses across mobile channels.

Bot attacks were down in Australia by 12% YOY, continuing a slow decline seen in previous years. The reduction was quite pronounced in financial services and in the communications, mobile and media industry sector.



Fraud in Australia

- » This visualization shows networked fraud (linked by digital identity) connected to organizations operating in Australia 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 an ecommerce platform in EMEA).
- » The diagram shows a strong domestic fraud network in Australia that crosses into multiple industries (finance, telecom operators and ecommerce). Cross-border network extensions tend to link to US and European organizations, with few connections to Asia or Latin America.



» 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.