

# Trust and Collaboration as Foundations to Fight Fraud in Australia

January to December 2022

The LexisNexis® Risk Solutions Cybercrime Report

## Transaction and Attack Patterns<sup>1</sup>

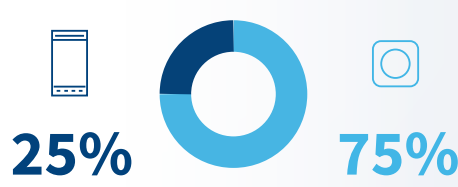


## Transactions by Channel

Desktop / Mobile

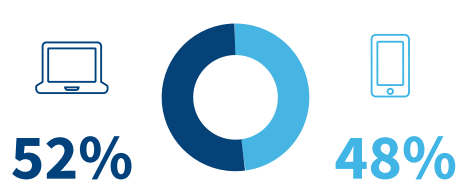



Mobile Browser / Mobile App



## Attacks by Channel

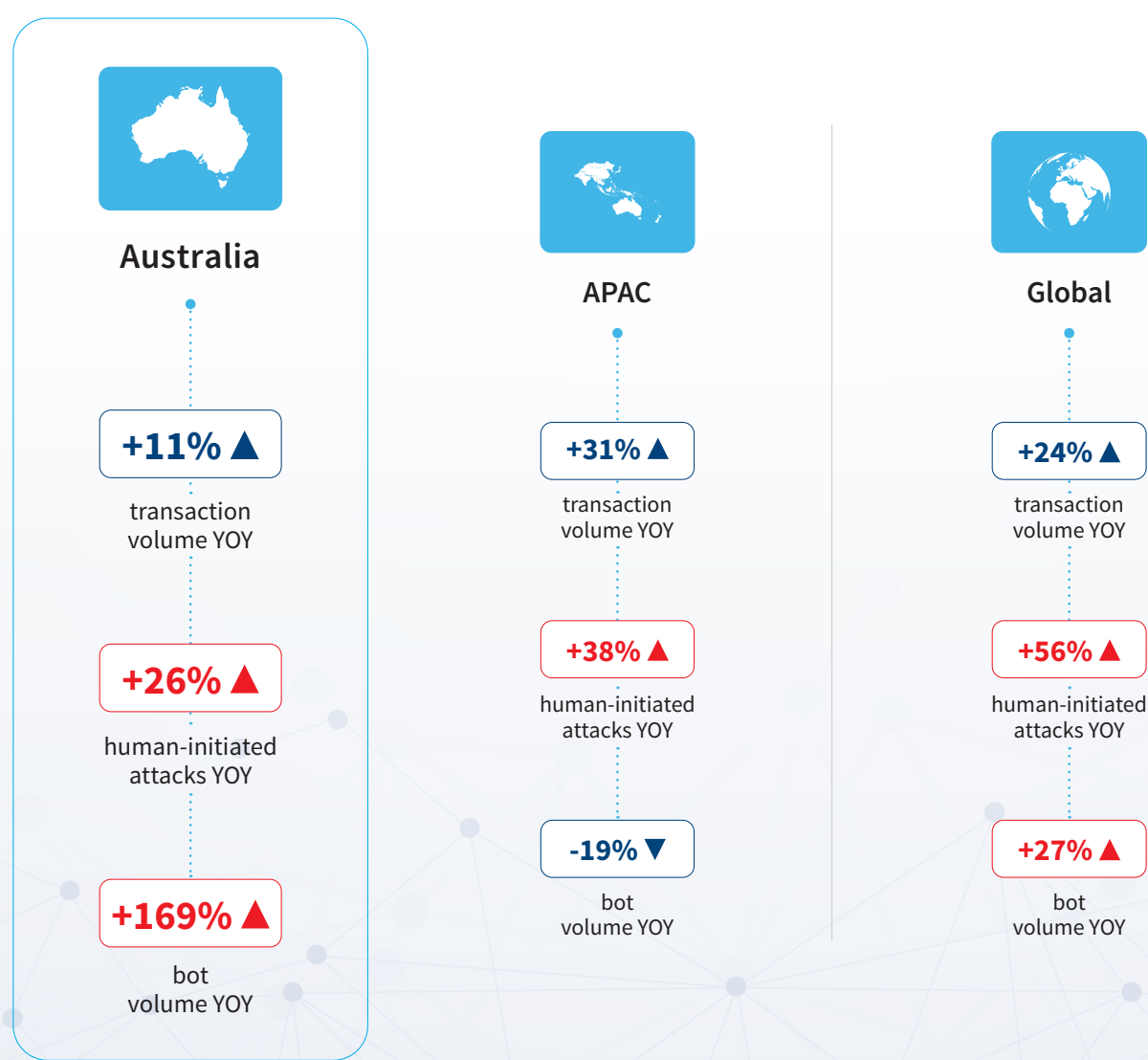
Desktop / Mobile



 **12% decrease in percentage of attacks coming from mobile devices YOY (2022 vs. 2021).**

## Spotlight: Australia vs. APAC vs. Global

The amount of bot attacks originating from Australia is traditionally low compared to some other parts of APAC. The growth in the volume of bot attacks in Australia in 2022 suggests that bot networks are diversifying — possibly originating from places not previously associated with bots, to try to bypass some basic bot mitigation methods.

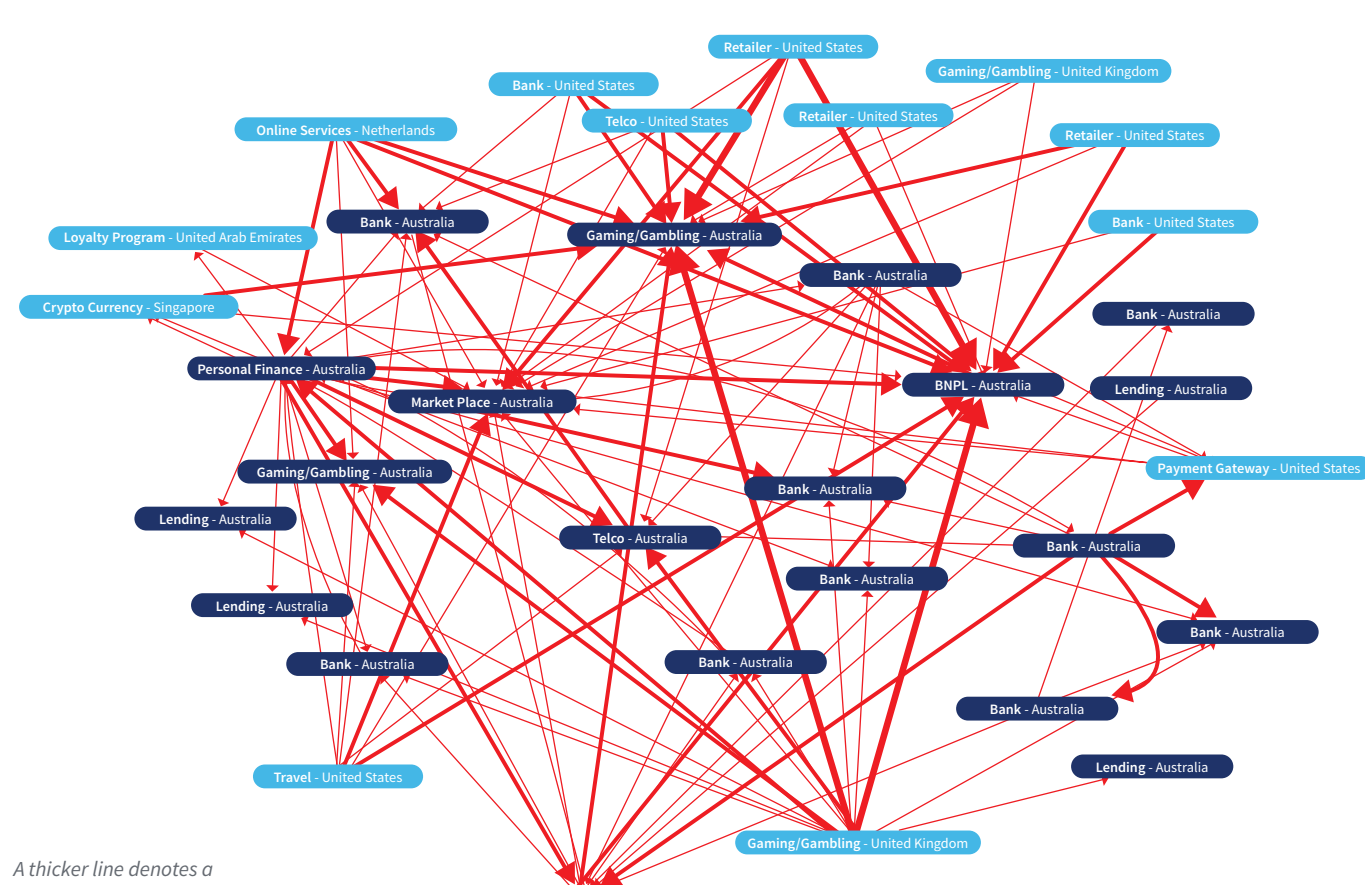


## Networked Fraud Threats

This visualisation shows networked fraud (linked by digital identity) connected to organisations operating in Australia during the first quarter of 2023. This network highlights that whilst much of the fraud seen in Australia may be domestic in origin, there are clear links to fraud rings operating internationally.

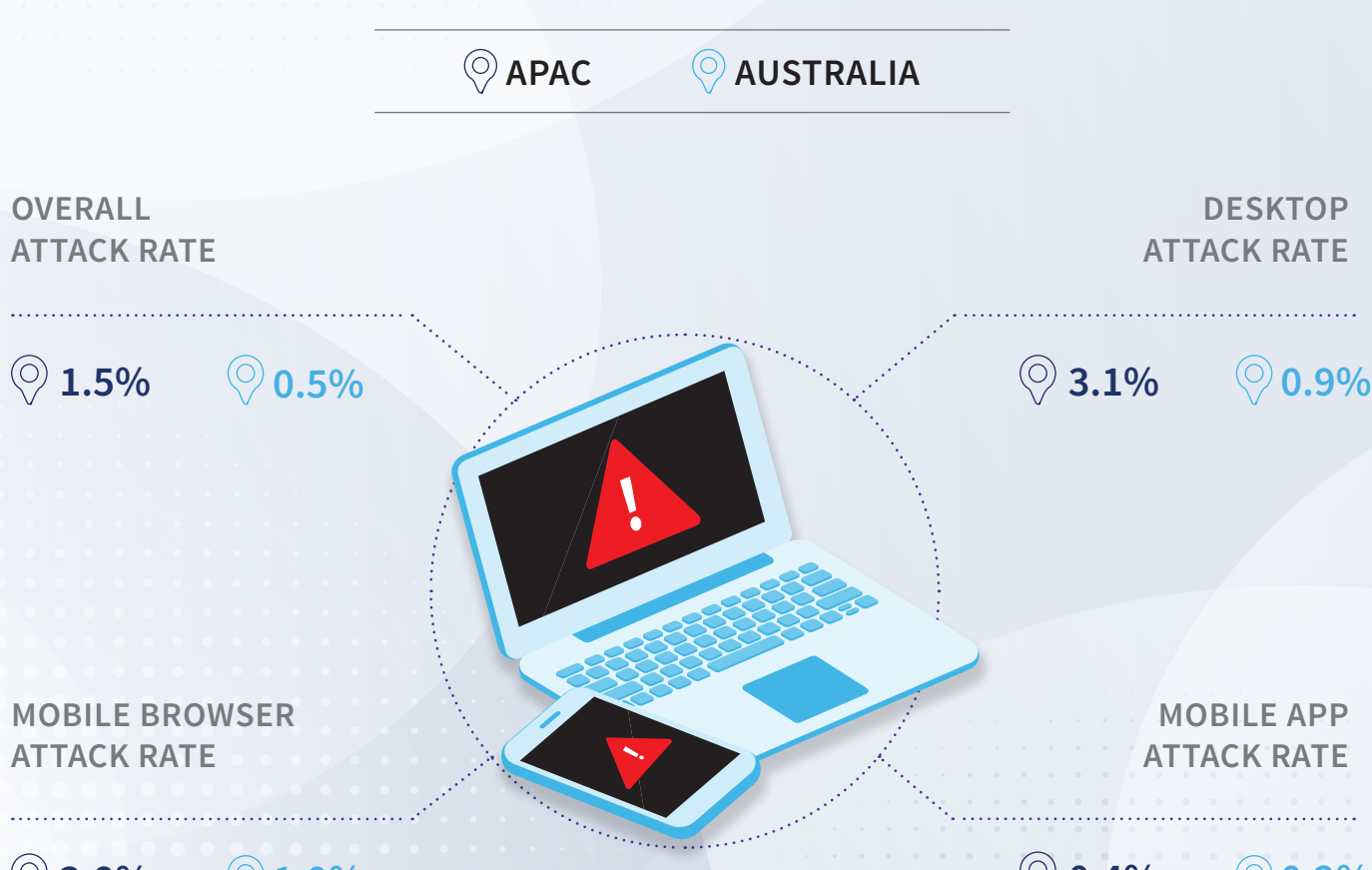
Each 'blue box' represents an individual organisation.

Each arrow illustrates digital identities associated with confirmed fraud attempts at one organisation, crossing over to another organisation in LexisNexis® Digital Identity Network®.



## Australia's Fraud Patterns Compared to APAC

Whilst the overall attack rate in Australia is low compared to the APAC average, it is growing more rapidly than the regional average<sup>1</sup>, likely due to the availability of significant volumes of breached data in 2022.



For further insights, download the LexisNexis Risk Solutions Cybercrime Report at [risk.lexisnexis.com/cybercrime-report](https://risk.lexisnexis.com/cybercrime-report)