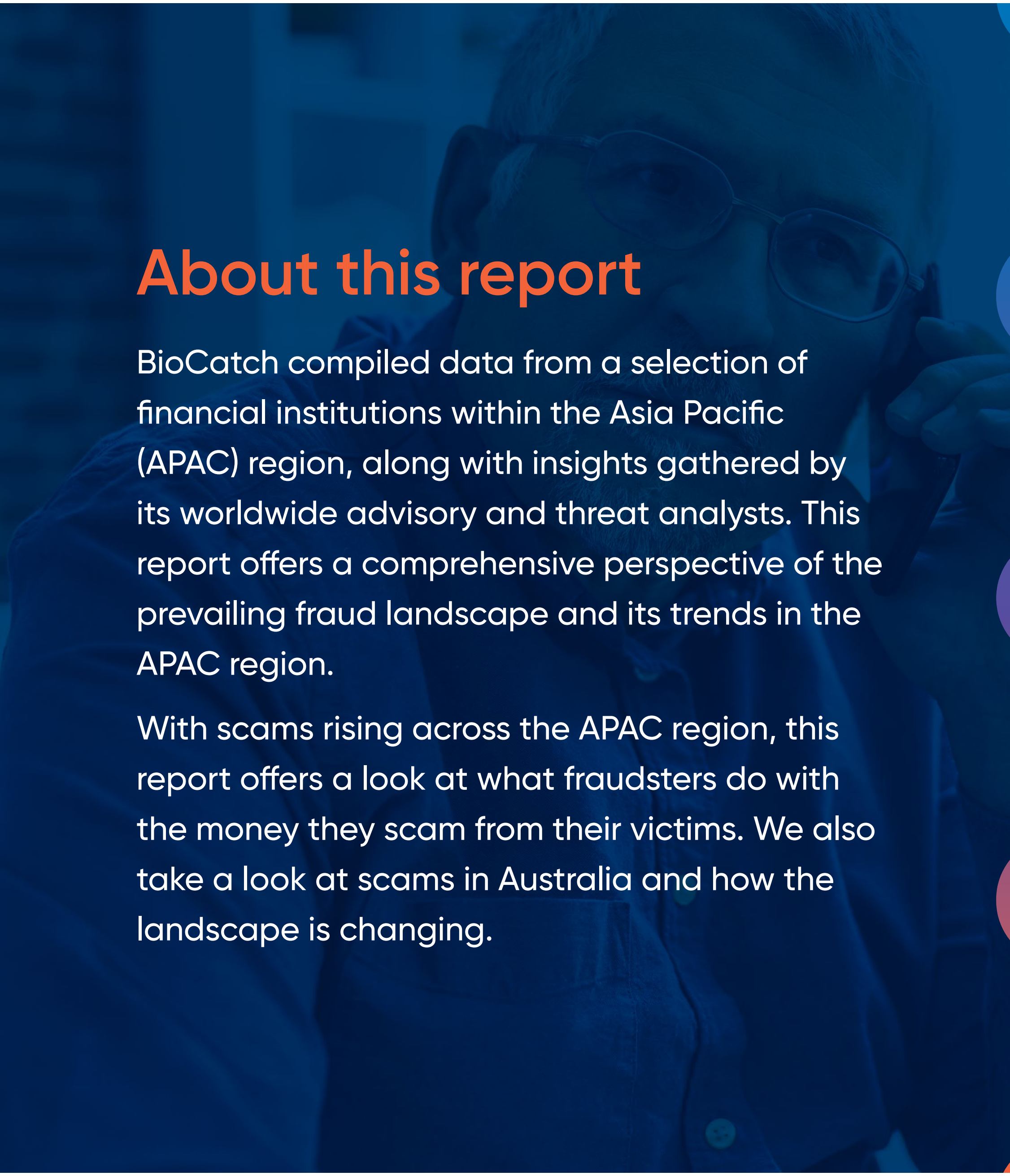
BioCatch

2024 Digital Banking Fraud Trends in APAC

BioCatch report on the current online fraud landscape in countries located throughout the Asia Pacific region, with case study and analysis.

June 2024



About this report

BioCatch compiled data from a selection of financial institutions within the Asia Pacific (APAC) region, along with insights gathered by its worldwide advisory and threat analysts. This report offers a comprehensive perspective of the prevailing fraud landscape and its trends in the APAC region.

With scams rising across the APAC region, this report offers a look at what fraudsters do with the money they scam from their victims. We also take a look at scams in Australia and how the landscape is changing.

This report is presented in the following sections:

- Key trends in APAC
- Fraud landscape in APAC
- Deep dive:
  - Money laundering syndicates funneling scam money through APAC
  - Case study: Analysis of scams in Australia
- Leverage behavioural biometric intelligence to detect social engineering scams

Key trends in APAC

BioCatch sees mobile malware as the main threat to banks in Southeast Asia, used to harvest data to execute fraud without alerting the victim, or to extort funds.

While some countries in the region saw their social-engineering scam losses decline, the volume of sessions that exhibit scam behaviours more than doubled (108% increase) in the last year. Singapore, especially, saw an explosion in its volume of scam cases, in spite of additional controls.

Australia saw 5% fewer fraud cases involving attack tools (RAT, malware, etc.) in 2023 than it did in 2022.

Detecting existing mule accounts is becoming one of the main priorities for banks, as well as establishing processes to proactively prevent them. BioCatch detected more than 150K confirmed mule accounts at banks across the region in 2023.

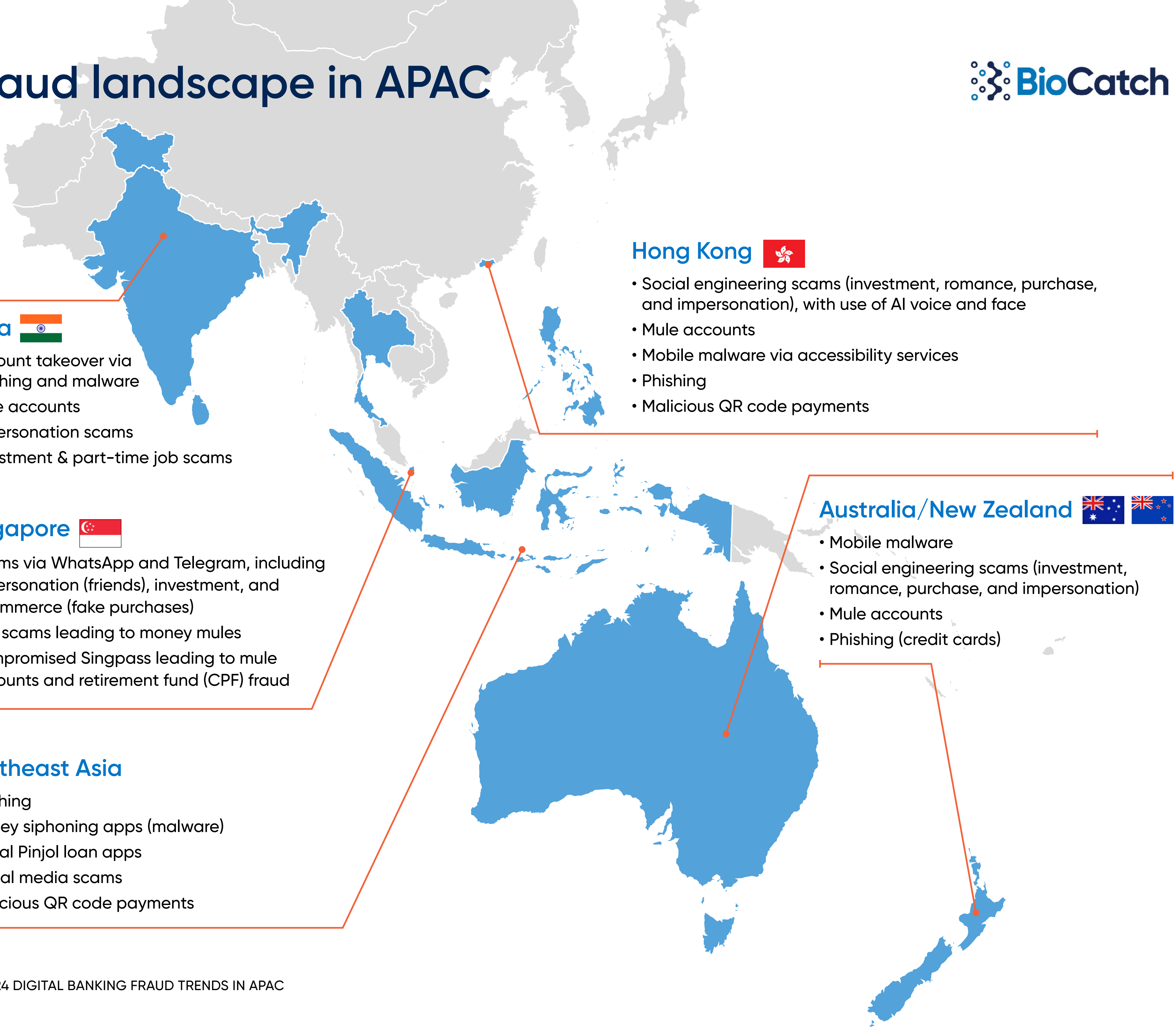
108% increase in reported voice scams cases year-over-year across the region

Fraudsters shifting to mobile is a trend we see all over the world. The APAC region is no exception, with a 17% increase in mobile fraud seen last year. It now accounts for as much as 70% of all digital fraud in the region.

70% of all reported frauds came from mobile apps, up 17% from 2022

Fraud landscape in APAC

BioCatch



India

- Account takeover via phishing and malware
- Mule accounts
- Impersonation scams
- Investment & part-time job scams

Singapore

- Scams via WhatsApp and Telegram, including impersonation (friends), investment, and eCommerce (fake purchases)
- Job scams leading to money mules
- Compromised Singpass leading to mule accounts and retirement fund (CPF) fraud

Southeast Asia

- Phishing
- Money siphoning apps (malware)
- Illegal Pinjol loan apps
- Social media scams
- Malicious QR code payments

Hong Kong

- Social engineering scams (investment, romance, purchase, and impersonation), with use of AI voice and face
- Mule accounts
- Mobile malware via accessibility services
- Phishing
- Malicious QR code payments

Australia/New Zealand

- Mobile malware
- Social engineering scams (investment, romance, purchase, and impersonation)
- Mule accounts
- Phishing (credit cards)

BioCatch

Edgar Zayas
BioCatch Director, Global Advisory

DEEP DIVE:

Money laundering syndicates funneling scam money through APAC

Criminals use mule accounts as intermediate stops between the victim's bank account and the final account from which they plan to withdraw their stolen money, often transferring the funds through a sprawling network of mule accounts at various banks in various countries to launder the money they have taken.

Historically, bad actors have sourced these mule accounts themselves, paying legitimate account-holders to receive and then transfer stolen funds to an account of the fraudster's choosing.

We are now seeing criminals in the APAC region outsourcing this laundering process to international syndicates that specialise in this activity. This both reduces overhead costs for the criminal organisation receiving the funds and adds a level of professionalism and efficiency to the scamming and laundering process.

Laundering syndicates often leverage the latest technology, employing specialised mobile apps to train, incentivise, and communicate with paid mules. These apps offer money-laundering training sessions and even provide users a leaderboard of the most active mule accounts to encourage mules to transfer more stolen money faster.

Laundering networks recruit mules through job advertisements, social media posts, and phishing emails, often targeting vulnerable or financially distressed individuals who have access to corporate bank accounts with high transaction limits.

While our internal data and external sources show these laundering networks are often based in China, we see scammed funds flow through accounts in a host of different Southeast Asian countries, getting converted into cryptocurrencies like Tether (USDT) at stops along the way to further obscure their origin.

Criminals further adopting – and, in many cases, improving upon – proven production and efficiency tactics from legitimate global businesses to commit fraud at scale only further accentuates the need for financial institutions to innovate. Banks must start sharing intelligence with other banks, as well regulators and law enforcement, and rapidly implement modern technologies if they hope to keep pace with criminal organisations capitalising on tried-and-true human resources tactics for training, gamification, and productivity to steal from the most vulnerable among us.

Android devices at risk

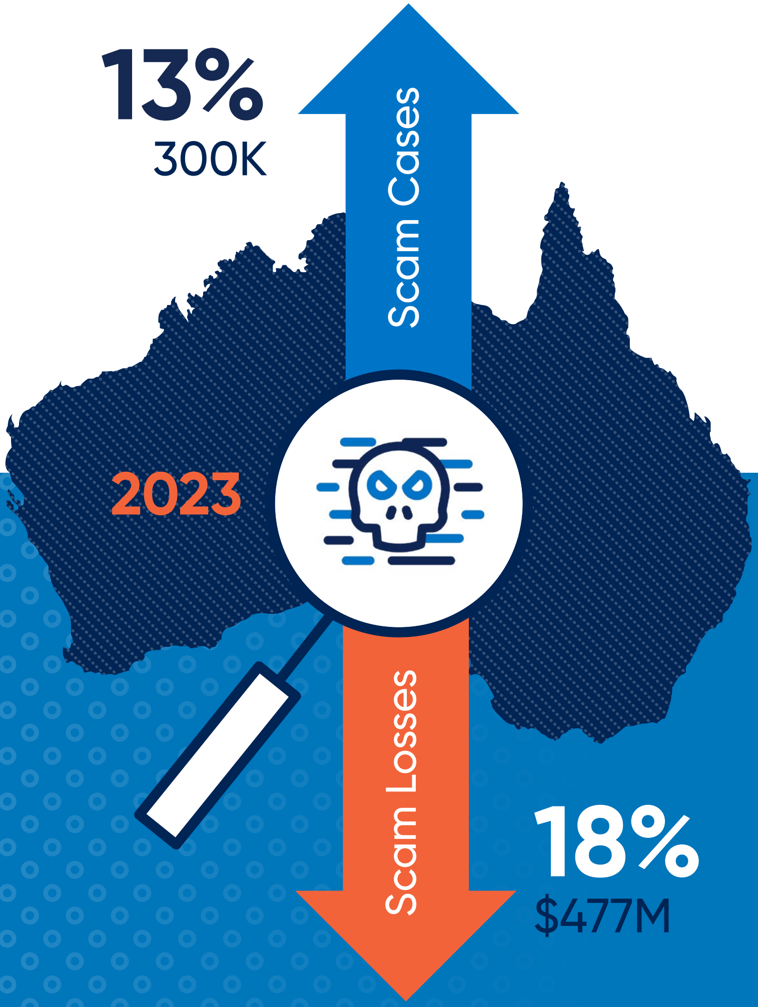
We're also seeing an explosion of Android apps leveraged for malicious purposes in the APAC region. While advanced mobile-device-mining programs like Vultur and SMSSpy are nothing new in APAC, malware developers continue to improve the capabilities of their software to circumvent bank controls.

To get around Google Play Store defenses, developers have taken to acquiring existent, legitimate applications and embedding inside of those apps backdoors through which the developers can drop their malicious software at any time. This enables keyloggers, screen-sharing, SMS-reading, and other permissions that grant scammers access to all the pertinent personal information they need to access the victim's digital banking accounts and then transfer away the victim's funds to a money mule account. In Singapore, banks now block any device that has a "side-loaded" app installed on it. Unfortunately, malware families are nimble. Developers can simply add code to their program to make it appear as though downloaded from Google Play.

Scammers are also creating "pinjol" apps. These illegal online lending apps available on Google Play lure their victims with promises of a quick and painless online loan. These apps contain malware-like features that allow a scammer to access personal data, contacts, messages, and even photos, which the scammer can then use to blackmail the borrower into paying exorbitant interest rates. Some believe the initial funds lent to the victim are also taken fraudulently and then laundered through these predatory lending companies, which are in turn run by criminal syndicates that specialise in financial crime.

BIOCATCH CASE STUDY:

Analysis of scams in Australia



Recently published data from the Australian government shows the country lost $90 million less to scams in 2023 from the year before (a decline from $567 million to $477 million), although the total number of reported scam cases rose from 240,000 to 300,000.

The first thing to note is that when defining scams, we're not talking exclusively about social engineering scams where the victim makes a payment. This also includes other fraud types such as phishing, remote access, and identity theft, which are all commonly executed by the fraudster.*

At BioCatch we believe it is important to distinguish between third-party executed fraud (account takeover), and victim-executed frauds (social-engineering scams), as there are inherent differences between the two, especially through the lens of user behaviour.

In fact, in our **Digital Fraud Trends in EMEA report**, published in March 2024, we highlighted the need for better categorisation of remote-access frauds, particularly when it comes to active RAT (where the session is controlled by the fraudster) and passive RAT (where the victim is essentially sharing their screen with the fraudster).

Also, these reported numbers exclude any losses that happen via cards, where the trend is different. Data from AusPaynet shows that card-not-present (CNP) fraud rose by 33.8% to over $608 million.*

*https://www.auspaynet.com.au/resources/fraud-statistics/July-2022-June-2023

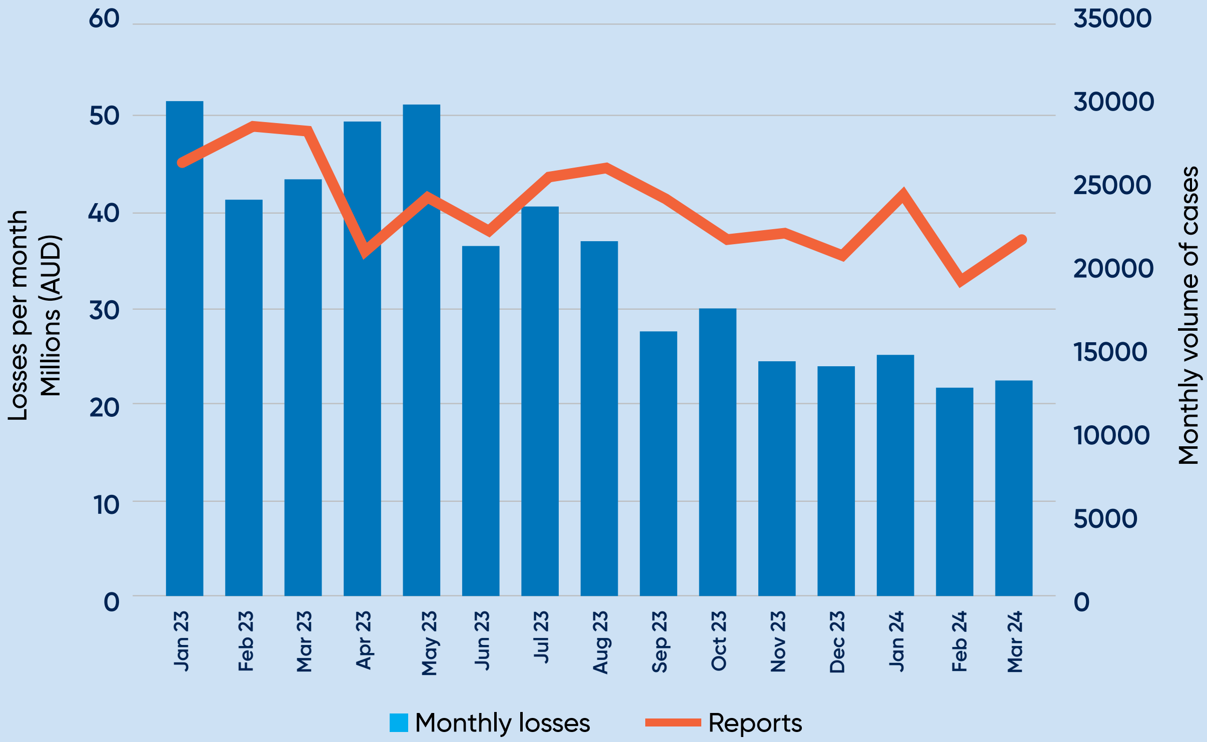
ANALYSIS OF SCAMS IN AUSTRALIA:

Loss trends

Since Q3 of 2023, there has been an undeniable trend in terms of losses, with a 48% decrease in losses seen in Q1 2024 compared to the same period in 2023. In this time, case volume has decreased around 20%. The difference in rate of change of both metrics indicates banks are reducing losses much quicker than before. In fact, data from the Scam Watch website shows exactly this: Nearly 10% of cases resulted in the victim losing money in 2023, compared to 12.1% the year before.

There is an obvious conclusion here: Banks are not only doing more to avoid customer losses but it is also their main focus.

Government scam statistics for 2023/2024

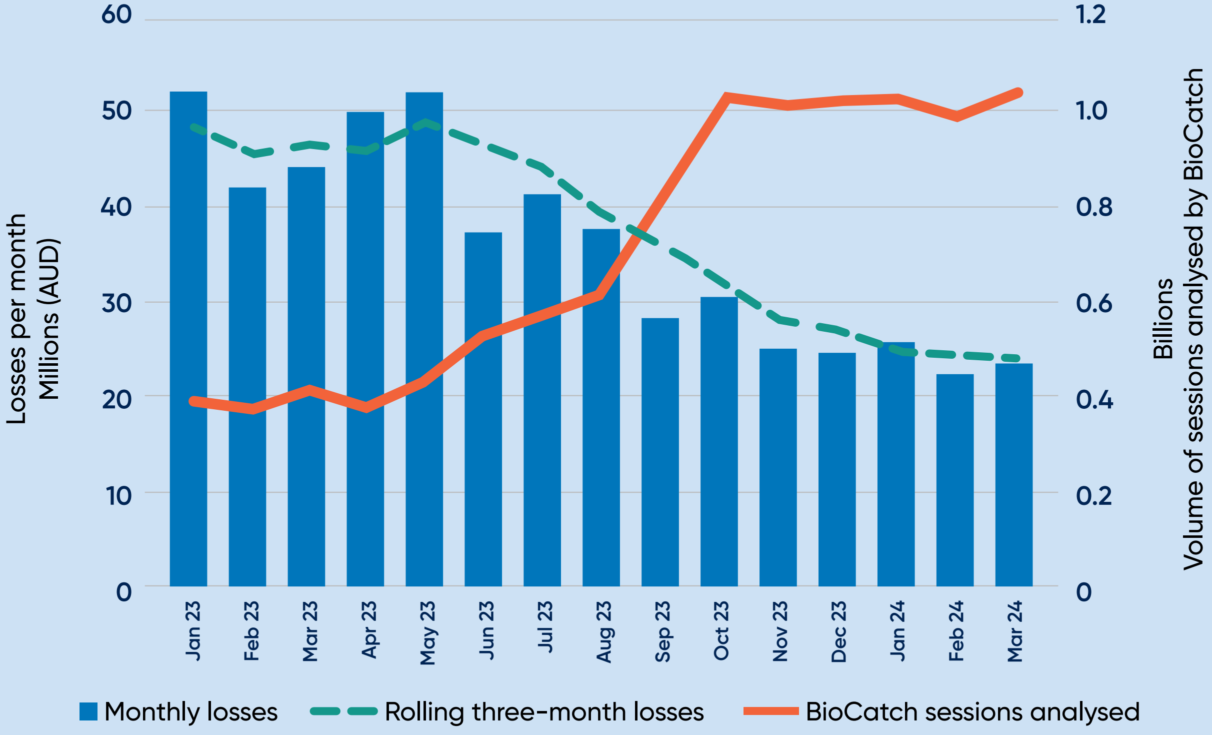


Source: https://www.scamwatch.gov.au/research-and-resources/scam-statistics?scamid=all&date=2023

ANALYSIS OF SCAMS IN AUSTRALIA:

What is BioCatch seeing?

First of all, we've noticed that the fluctuations coincide with deployments of BioCatch carried out by banks, which is empowering them with more data to tackle the fraud problem. Below we've taken the previous graph and overlaid information about BioCatch's visibility of sessions (user activity):



9 out of 10 top Australian banks employ BioCatch solutions

BioCatch increased its footprint in Australia throughout 2023, as seen by the orange line that shows the volume of sessions analysed.

As more banks deployed BioCatch's technology, scams began to decrease. This is, in part, due to the additional information offered by BioCatch, which allowed them to better combat scams.

ANALYSIS OF SCAMS IN AUSTRALIA:

Fraudsters are adapting

The behaviour we observe in fraudulent sessions is changing. Fraudsters are adapting what they do and how they operate in an attempt to circumvent these new obstacles in their path.

For example, remote access continues to change. **Our Digital Fraud Trends in APAC report from 2023** highlighted a shift from remote access fraud to social engineering scams, with remote access accounting for a shift from 35% (2021) of all frauds to just 12% in 2022. Now we see that last year (2023), this dropped further still, falling down to single-figures with just 5% of all frauds being reported as remote access.

Another change we observed relates to session duration. Typically, social-engineering scams were much longer than normal fraud sessions, given the need for fraudsters to convince their victims to execute payments. As fraudsters master the art of social engineering, however, we see the average session for an impersonation scam decrease significantly in length. While the average scam case lasted almost 12 minutes in 2022, last year this fell by 33% to eight minutes.

Finally, we see a change in behaviour before the scam happens. There has been a 230% increase in the volume of cases which see at least one failed attempt to log into the victim's account prior to the reported scam session. This suggests fraudsters are getting better at "doing their homework" on the targeted accounts, potentially to collect additional information that helps their scam appear more legitimate.

86%

percent drop in remote access fraud from 2021 to 2023

33%

percent decrease in the average impersonation scam session

230%

increase in the volume of cases in which a failed attempt to login is made

ANALYSIS OF SCAMS IN AUSTRALIA:

The changing landscape

In summary, the fraud landscape in Australia is changing, driven by banks detecting more fraud and scams. This is also leading to a further focus on identifying mule accounts, as all scams lead to mules.

As the landscape changes, it's important for banks to remain vigilant to any changes in modus operandi. It isn't enough to implement a solution. It requires constant monitoring and adaptation to keep up with ever-innovating fraudsters.

Leveraging behavioural biometric intelligence to detect social engineering scams

Although scams continue to increase in both scale and sophistication across the APAC region, financial institutions can use their customers' own behaviour to stop these scams before they can do any damage.

BioCatch collects physical and cognitive user behaviours that are turned into powerful insights. The advanced behavioural insights combine user and population-level profiling to determine user intent and emotional state in context of the activity to detect complex situations indicating high levels of risk. When a user operates in an online account under the guidance of a voice scammer signs of duress and distraction are presented.

Typing speed, swipe patterns, and every click of the mouse tell a story – one of cybercriminal activity or genuine user behaviour. Even if a criminal tricks a legitimate customer into authorising a payment, behavioral biometric intelligence can quickly spot behaviour patterns that indicate a financial scam may be in progress.

By flagging these high-risk activities in real-time, financial institutions across APAC are preventing significant losses and better protecting their customers and assets.

ABOUT BIOCATCH

BioCatch stands at the forefront of digital fraud detection, pioneering behavioral biometric intelligence grounded in advanced cognitive science and machine learning. BioCatch analyses thousands of user interactions to support a digital banking environment where identity, trust, and ease coexist. Today, more than 30 of the world's largest 100 banks and 196 total financial institutions rely on BioCatch Connect™ to combat fraud, facilitate digital transformation, and grow customer relationships. BioCatch's Client Innovation Board, an industry-led initiative featuring American Express, Barclays, Citi Ventures, HSBC, and National Australia Bank, collaborates to pioneer creative and innovative ways to leverage customer relationships for fraud prevention. With more than a decade of data analysis, 92 registered patents, and unmatched expertise, BioCatch continues to lead innovation to address future challenges. For more information, please visit www.biocatch.com.

BioCatch