Let's protect consumers and businesses from identity crime and money laundering

29%

According to the Office of the Australian Information Commissioner, compromised or stolen credentials were the source of 29% of all Notifiable Data Breaches in the first half of 2023[1].

[1] OAIC Notifiable Data Breaches Report, Jan-June 2023, 5 Sept 2023 publication

9 months is the average time it takes for data theft to be reported or known[2].

Hackers can wreak considerable damage in the lag time between the breach and its discovery.

$1.7 million was allegedly stolen from Australian and overseas victims by a single cybercrime syndicate dismantled in 2023 by the Australian Federal Police[3].

The syndicate worked with criminal associates who sourced legitimate identity documents and altered the photographs and date of birth.

80 bank accounts were set up with stolen identities to help launder money out of Australia.

[2] IBM Cost of Data Breach Report 2023

[3] AFP Media Release, 24 March 2023, Cybercrime syndicate dismantled after allegedly laundering $1.7 million

Identity takeover is a form of identity fraud where fraudsters exploit stolen data to pass through identity verification and onboarding processes and pose as real users / persons.

56%

ABS data[4] shows 56% of reported identity theft victims had money taken from their bank accounts, superannuation, investments or shares.

13HRS

Victims spend an average of 13 hours[5] dealing with identity crime.

[4] Australian Bureau of Statistics, Personal Fraud, Key Statistics for the five years prior to 2021-22

[5] The Aust Institute of Criminology (AIC), Australian cybercrime survey, Identity crime and misuse in Australia 2023

Synthetic identity theft is where personal information is used to construct a false profile or replica identity.

As there is no legitimate victim to detect irregular account activity, criminals can remain undetected while stealing or laundering substantial sums of money.

The costs for financial institutions rise with each fraudulent transaction.

Your customers often won't know their personal data has been compromised until[6]:

- Suspicious transactions appear in their bank statements, accounts or credit report
- They receive calls from debt collectors asking about unpaid bills
- They are unsuccessful in applying for credit despite a good credit history
- Their details are used to fraudulently obtain credit or open new bank accounts, mobile phones or utility accounts
- Attempts are made to obtain money from their investment or superannuation accounts fraudulently.

The type of personal information most commonly misused consists of:

- Name
- Credit or debit card information
- Mobile number
- Address
- Date of birth
- Bank account information

When pieces of personal information are combined, they become more powerful to fraudsters.

The top 5 sectors[7] to notify data breaches:

- Health service providers
- Finance (including superannuation)
- Recruitment agencies
- Legal, accounting & management services
- Insurance

[6] The Aust Institute of Criminology (AIC), Australian cybercrime survey, Identity crime and misuse in Australia 2023

[7] OAIC Notifiable Data Breaches Report, Jan-June 2023, 5 Sept 2023 publication

How are you protecting sensitive customer information against these threats?

The key to effective fraud prevention is a layered, multi-pronged approach to close the gaps exploited by fraudsters.

Equifax combines differentiated data, advanced analytics and cloud technology to help financial institutions protect against identity crime and money laundering.

Early fraud detection solutions like **Equifax ID Takeover Alert** monitor identity verification attempts within the Equifax ecosystem for fraudulent patterns. Multiple verification attempts or subtle detail changes signal potential identity fraud or money laundering risk.

When choosing an early fraud detection solution for your business, look for the following features:

1. Data quality for accurate alerts

Ensure your alert tool has a comprehensive view of identity onboarding events to detect anomalies in verifications effectively. Incomplete identity data that does not cover a broad range of institutions or industry sectors may lead to missed suspicious activity or high false-negative rates.

2. Real-time detection for swift action

Rapid response is crucial, given the speed at which identity thieves operate across multiple financial institutions. Prioritise real-time detection to flag fraudulent activities swiftly.

3. Seamless integration with existing fraud detection processes

Introducing a new tool shouldn't disrupt operations or customer experience. Opt for solutions that seamlessly integrate with existing processes to maintain efficiency.

4. Maturity of identity verification platform

In the face of technologically sophisticated fraudsters, choose a mature identity verification platform with a proven history of fraud prevention intelligence. Build trust in your customer relationships by selecting a partner with comprehensive capabilities, providing a unified view of individual risk.

Equifax's **ID Takeover Alert** monitors identity verifications performed across the entire **IDMatrix** ecosystem. IDMatrix, a leading Australian identity verification and fraud platform, verifies extensively across sectors like banking, finance, gaming, telco and remittance. Its broad customer base aids in spotting suspicious activities linked to fraudsters using stolen identity data across different financial entities.

Contact Equifax today to explore our comprehensive fraud and identity solutions, including email risk, device intelligence, document verification and biometrics.