3 IDENTITY HACKS

HOW THEY GOT IN & HOW TO STOP THEM

Identity fraud cost Americans $43B in 2023. Of that sum, $20B could be traced directly to modern identity fraud scams preventable by strong identity security.

Javelin Strategy & Research, 2023

Introduction

Snowflake, Experian, and Westpac—three industry giants, each hit by major data breaches that exposed sensitive information and shattered trust.

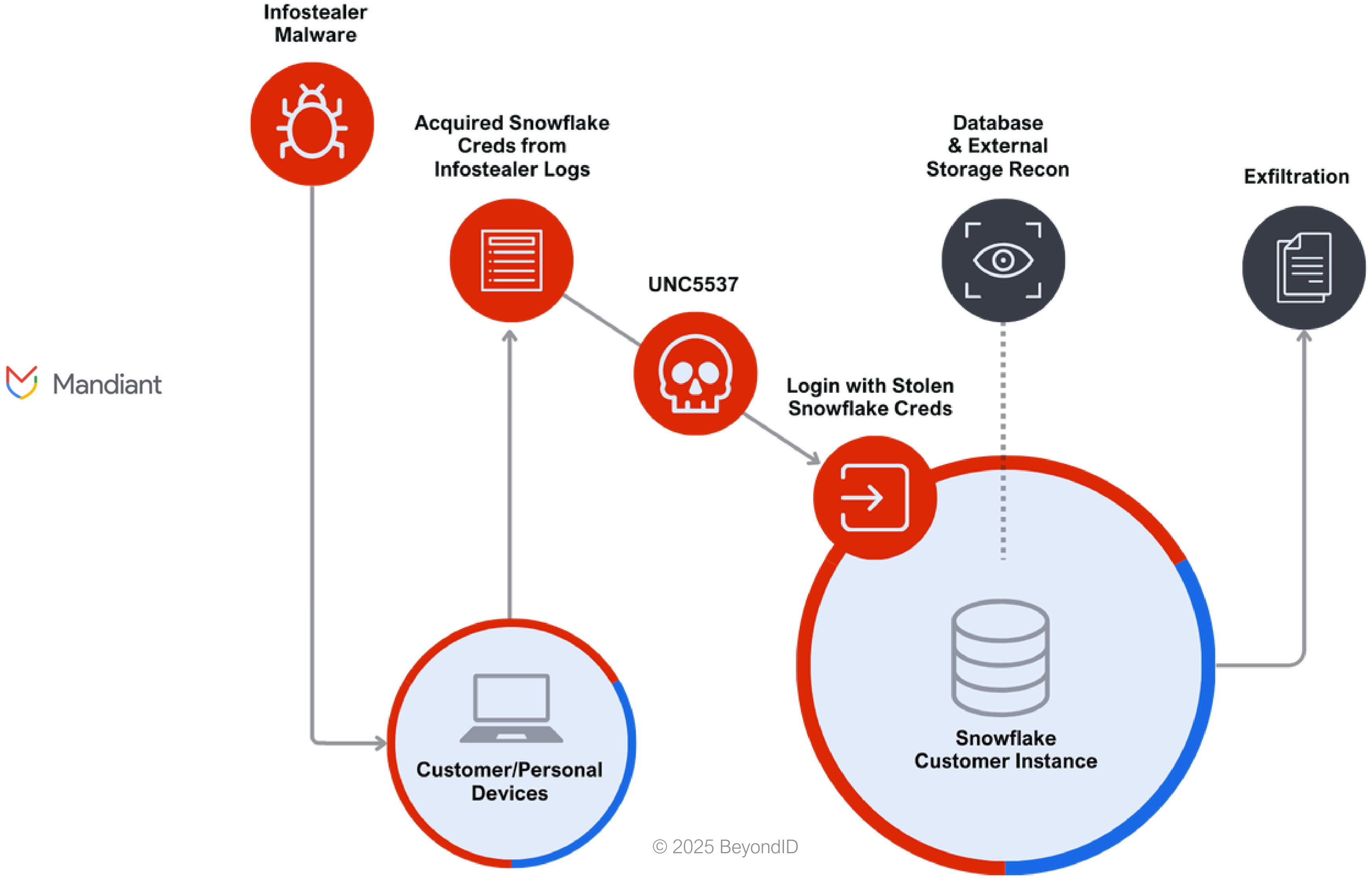
The worst part? **These breaches were entirely preventable.** What went wrong, and how can you make sure it doesn't happen to you? Read on to find out.

WHAT HAPPENED?

Snowflake Breach

Attack Path Diagram

snowflake DATA CLOUD


Infostealer Malware
Acquired Snowflake Creds from Infostealer Logs
UNC5537
Database & External Storage Recon
Exfiltration
Login with Stolen Snowflake Creds
Mandiant
Customer/Personal Devices
Snowflake Customer Instance

How one person managed to help hackers breach not one, not two, but dozens of well-known brands by reusing their password.

Snowflake employee Jeremy (not their real name) didn’t feel like creating a new password during their onboarding process with dozens of well-known customers.

In several Snowflake-related investigations, Mandiant observed that the initial compromise of infostealer malware occurred on contractor systems that were also used for personal activities like gaming and downloading pirated software. Attackers exploited compromised credentials to access individual customer accounts on Snowflake's platform.

Impacted accounts were not configured with MFA, which allowed hackers to enter with only a username and password. Credentials were valid years after they had been stolen.

snowflake
DATA CLOUD

Experian Breach

Social Engineering Attack

A social engineering attack on credit reporting giant Experian exposed the data of **>24 Million** customers and nearly **800,000** businesses.

In August 2020, a bad actor posing as a POC at one of Experian's client organizations called the company's South Africa office and successfully solicited internal customer data.

An investigation into the incident revealed that hackers planned to sell the data as marketing leads.

Experian claims that data provided was commonly exchanged with clients, and not extraordinarily confidential.

Data Obtained

- Residential addresses
- Work addresses, job titles, & start dates
- Home, mobile, & work phone numbers
- Email addresses

Westpac PayID

Third Party Attack

In 2018, hackers exploited a weakness in mobile-pay partner PayID's security posture that would allow them to obtain the personally identifiable information (PII) of ~98,000 Westpac customers across Australia.

Unbeknownst to many Australians, PayID functions like a telephone book, allowing users to enter mobile numbers or email addresses to verify the names of account holders.

Using 7 compromised Westpac logins, bad actors carried out an enumeration attack that used 600,000 random searches to hit on almost 100,000 matches.

Full names, email addresses, phone numbers, and unspecified account information made up the data leaked during this attack.

07

Westpac Live accounts compromised

600k

PayID lookups made from those seven accounts

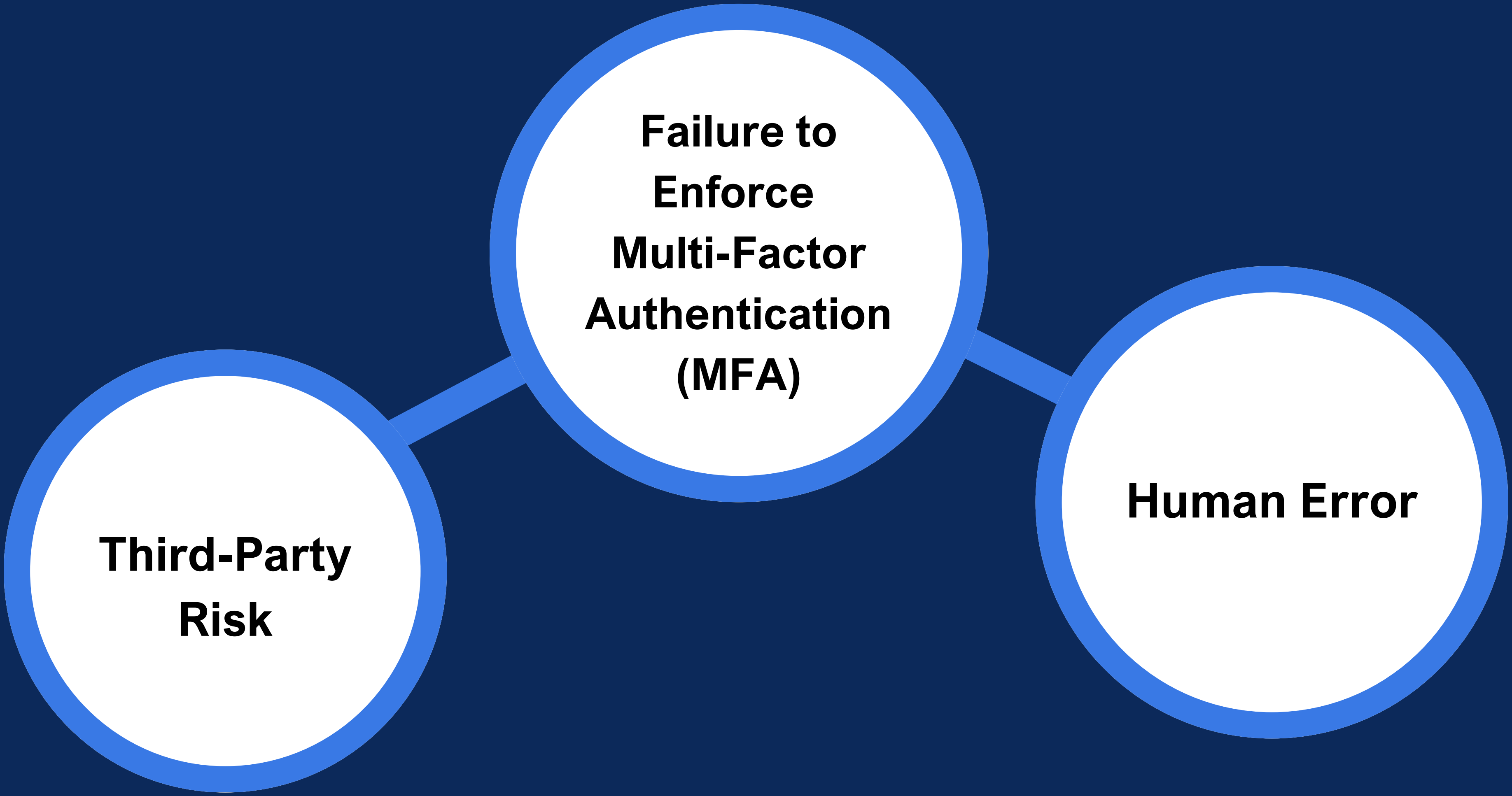
98k

Of 600,000 lookups exposed PII to hackers

WHY DID IT HAPPEN?

Common Vulnerabilities

Snowflake | Experian | Westpac



Failure to Enforce Multi-Factor Authentication (MFA)

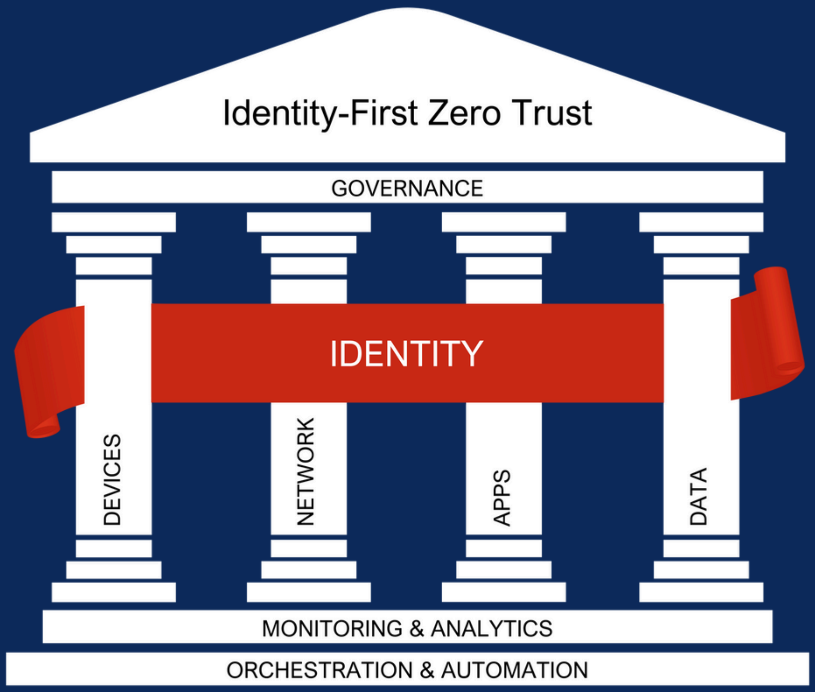
Third-Party Risk

Human Error

HOW TO STOP IT FROM HAPPENING TO YOU

Identity-First Zero Trust

Architecture



With a robust, identity-centric zero trust strategy things could have gone much differently for Snowflake, Experian, and Westpac.

Identity-first zero trust architecture brings identity into focus as the throughline of zero trust function, ensuring:

- **Contextual and continuous authentication** is in place before any data, application, network, or service is accessed.
- **Strengthened Incident response** processes through enhanced visibility into user behavior and rapid detection of anomalies.
- **Seamless user experience** that minimizes friction by adapting authentication requirements based on risk signals, allowing users to work securely without unnecessary disruptions.

Case Study: Texas Dow Employees Credit Union

Fraud Prevention Strategy

TDECU

YOUR CREDIT UNION

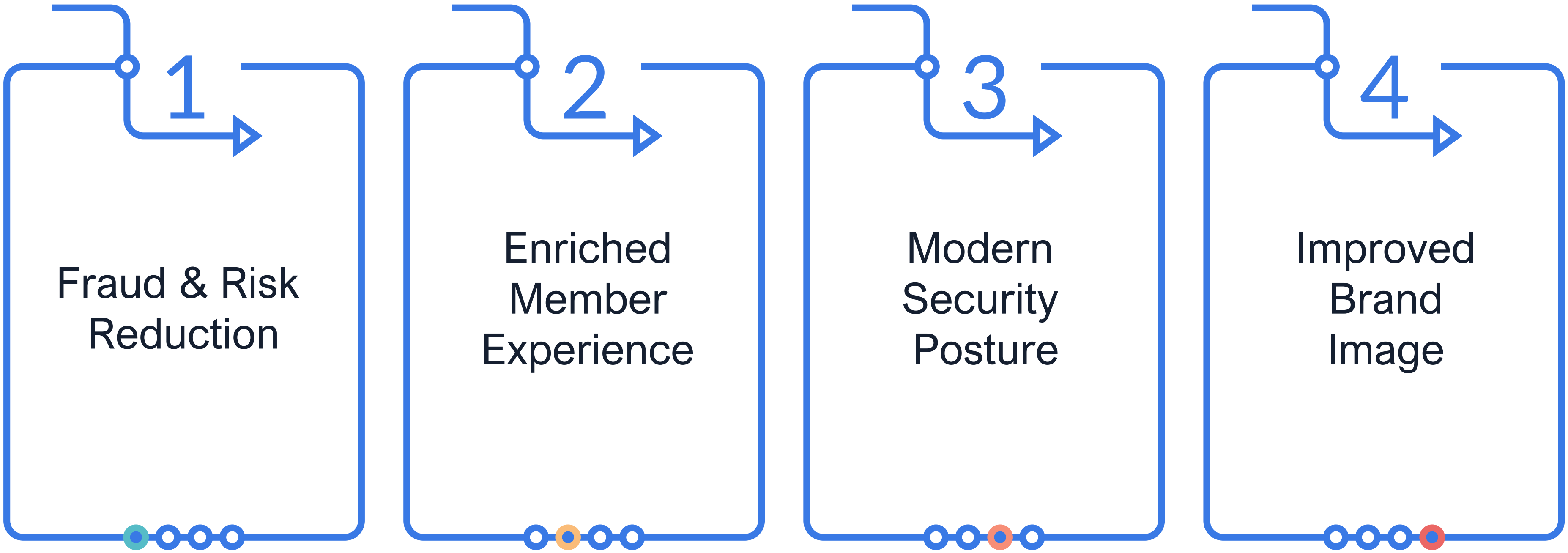
- HQ: Lake Jackson, TX
- 40+ branch offices in Texas
- 366,000+ members
- Assets of $4.5B
- Full range of banking & financial services

Implementation Strategy:

- Modernize banking experience
- Enhance security
- Continuous release cycles
- Automate identity proofing
- Optimize mobile application

TDECU
YOUR CREDIT UNION

Expected Outcomes



1 Fraud & Risk Reduction

2 Enriched Member Experience

3 Modern Security Posture

4 Improved Brand Image

Case Study: Commerce Bank

Balancing Security & User Experience

Commerce Bank®
Member FDIC

- HQ: Kansas City, MO
- 275+ branches across Missouri, Kansas, Illinois, Oklahoma, and Colorado
- Assets of $31B
- Full range of banking & financial services

Commerce Bank aimed to modernize their customer experience by developing new web and mobile applications. It was important these changes would not undermine, but enhance, their security posture and support their fraud prevention strategy.

They selected the Okta Platform with BeyondID managed services to integrate Commerce Bank's *legacy platform* and enhance *IAM* capabilities for a seamless migration.

Outcomes

With a fully-integrated customer identity solution, Commerce Bank securely onboarded all existing customers without requiring re-registration, ensuring widespread adoption of a more modern customer experience.

With identity at the center of their CX strategy, Commerce Bank was able to strike a balance between security and experience. A central view of activity within their Okta environment will help them maintain that balance.

Commerce Bank®
Member FDIC

Lessons Learned

Security and experience must be balanced to prevent breaches

Data-driven security is essential for early fraud detection and risk reduction

Adopting an Identity-First Zero Trust approach is crucial to mitigating risk

BeyondID & Okta
Better Together

BeyondID

Okta Apex Partner
3x Partner of the Year

BeyondID is a leading, AI-powered managed identity solutions provider (MISP). Since its inception, BeyondID has partnered with Okta to deliver comprehensive identity solutions, including fraud prevention for financial services organizations. BeyondID employs more Okta certified professionals than any other partner.

okta

Leading Independent Identity Provider

BeyondID is a managed identity solutions provider. Since its inception, BeyondID has partnered with Okta to deliver comprehensive identity solutions, including fraud prevention for financial services organizations. BeyondID employs more Okta certified professionals than any other partner.

GET STARTED TODAY

Let’s talk about your fraud prevention plan.

info@beyondid.com

Sources

Buzzard, J. (2023). *The Butterfly Effect*. Javelin Research & Strategy.

Identity Theft Resource Center. (2024). *Q1 2024 Data Breach Analysis.*

Mandiant. (2024). *M-Trends: 2024 Special Report*.

Mandiant attack path diagram