# Fraud Detection Ecosystems

## How Behavioral Biometrics Intelligence is Elevating Customer Safety in Digital Banking

BioCatch

WHITE PAPER

# Foreword

Fraud detection and prevention in digital banking is a community effort – from collaboration between the internal teams that fight it to the numerous public-private partnerships that seek to extend information sharing beyond the bank's perimeter.

Technology vendors play a crucial role within the ecosystem. Safeguarding the digital landscape necessitates collective action, and vendors must be open to collaboration and prepared to complement the capabilities of other solutions within existing technology stacks.

Financial institutions are feeling the pressure to consolidate technology and reduce the number of vendors they work with. This is evidenced by the growing number of financial institutions investing in cyber fraud fusion centers to create a centralized environment that aligns the data, technology, and operational capabilities of traditionally siloed teams. According to Gartner, by 2028, 20% of large enterprises will shift to cyber fraud fusion teams to combat internal and external adversaries targeting the organization, up from less than 5% today.

Fraud detection vendors are addressing the needs of the clients they serve by combining best-of-breed capabilities within their offerings to expand the number of fraud use cases they solve. For example, the combination of device and behavioral biometrics intelligence has emerged in recent years to improve detection of mule account networks and enable better collaboration and efficiencies across fraud and AML teams.

In addition, fraud detection vendors are working to simplify deployments to better serve smaller financial institutions and credit unions, affording them the same access to advanced fraud protection as their larger enterprise peers.

This white paper will present examples of how behavioral biometrics intelligence is being used by both large and small institutions to increase the effectiveness of existing solutions within their fraud detection ecosystem, provide a shared technology framework to improve operational capabilities, and elevate customer safety in digital banking.

> By 2028, **20% of large enterprises will shift to cyber fraud fusion teams** to combat internal and external adversaries targeting the organization, up from less than 5% today.
>
> Source: Gartner

# Adopting a Digital Banking Platform from a Third Party

A growing trend in North America is the increasing use of cloud-based digital banking platforms. These platforms empower credit unions, regional banks, and challenger banks to provide modern, user-friendly digital banking experiences to valued customers and members. The offerings of these platforms encompass a wide array of features, including online and mobile banking, account management, bill payments, and other essential digital banking services.

BioCatch partners with several leading cloud-based digital banking platform providers in the U.S. allowing them to extend fraud prevention technology and managed services to their SMB clients. This enables credit unions and smaller financial institutions the benefit of providing their customers and members enhanced protection against various fraud threats including account takeover, payment scams, and mule accounts.

## Before BioCatch: Leading Credit Union Targeted with Zelle Impostor Scams

A top 100 credit union in the U.S. saw its members being targeted by impostor scams through voice and SMS phishing. Fraudsters were attempting to trick members into divulging the one-time passcode required to set up a Zelle account and transfer money out. With no solution in place, the credit union estimated $4 million in annual fraud losses based on the highest impact months.

## After BioCatch: 95% Reduction in P2P Payment Fraud

Working with their digital banking provider, Lumin Digital, the credit union was able to deploy BioCatch technology to combat the rapid rise in P2P payment fraud. BioCatch provided full visibility across the digital journey, combining device intelligence augmented with behavioral biometrics as an additional passive fraud prevention layer.

With BioCatch deployed, several patterns quickly emerged that indicated account takeover. Using BioCatch device intelligence capabilities, the credit union identified multiple users coming from the same device and same location. Using BioCatch behavioral intelligence capabilities, the credit union was able to detect behavior patterns not typical of genuine users. For example, fraudsters often demonstrate a high level of familiarity with the targeted payment channel's enrollment process indicated by the way they navigate through the banking application. On the other hand, they display behaviors consistent with someone who lacks familiarity with personal data such as segmented typing (indicating working off a list of stolen credentials), pasting certain elements and multiple deletions.

The credit union saw immediate results upon deploying BioCatch and are on pace to have less than $10K a month in losses which is a 95% reduction from what they experienced during the highest impact months of the attack.

# Layering Behavioral Intelligence into the Existing Fraud Stack

## Integration Description

For many years, one of Canada's top banks has relied on two enterprise-grade fraud management systems and a dedicated Anti-Money Laundering (AML) system to oversee its fraud and AML operations. These systems have played a pivotal role in safeguarding customer onboarding and existing accounts across the bank's digital channels comprising the website and mobile app.

The three core systems within the bank's fraud technology stack include:

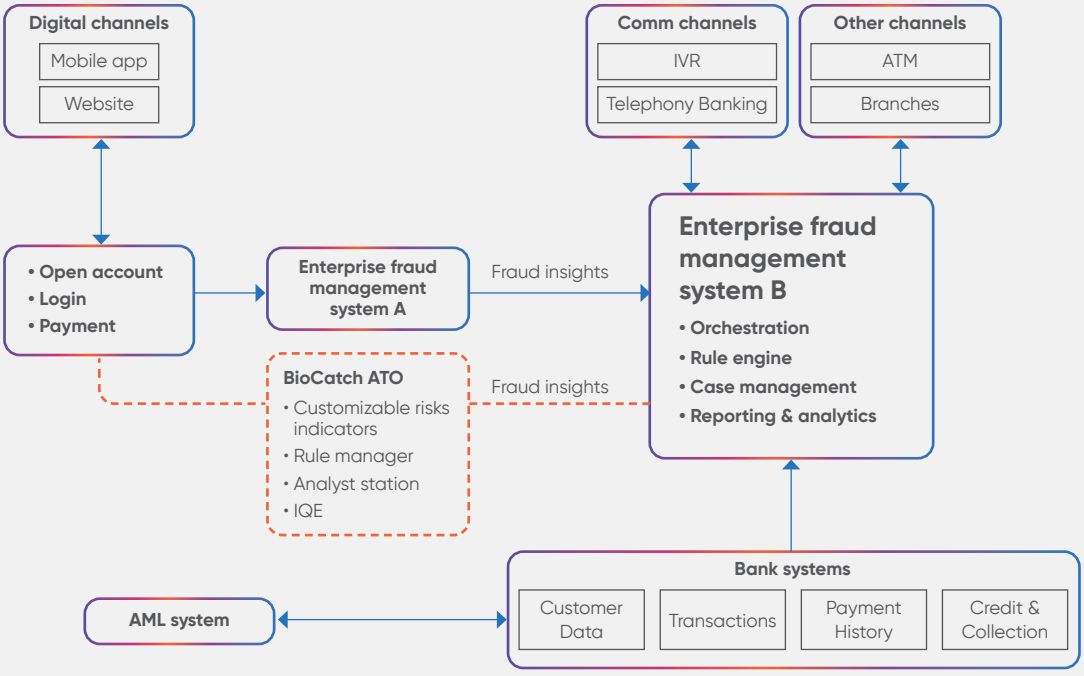
- An enterprise fraud management system that serves as the central orchestrator, the primary risk engine, the case manager, and analytics tool
- A customer onboarding fraud protection and account takeover fraud defense, enriching the fraud management system with additional insights
- An Anti-Money Laundering platform

## Before BioCatch: Account Takeover Fraud Surges

While offering substantial fraud protection, the bank experienced a surge in account takeover attacks after fraudsters were able to circumvent existing controls. In addition, their existing fraud detection controls introduced high friction into the customer journey, characterized by frequent step-up authentication requests, even when such measures were unnecessary.

## After BioCatch: Improved Fraud Detection by 56%

In response to an escalation in account takeover fraud, the bank made a strategic decision to fortify its fraud defense by integrating the BioCatch Account Takeover Protection solution to provide additional risk assessment capabilities on top of the bank's existing enterprise fraud management system. The following diagram shows how BioCatch is implemented within the bank's fraud technology stack.



Since integrating BioCatch, the bank has used customizable risk indicators to realize a 56% uplift in account takeover fraud detection. A second unexpected benefit for the bank was the substantial reduction in step-up authentication challenges presented to customers, marking a noteworthy reduction in customer friction and improvement in the overall online banking experience.

The bank also leverages BioCatch's advanced applications and tools in its daily operations, including:

- Rule Manager applies logic to fraud indicators, facilitating the refinement of insights before they are fed to the enterprise fraud management system.
- BioCatch Analyst Station is used for conducting thorough investigations of specific events.
- Insights Query Engine (IQE) is empowering the fraud team to freely analyze data, uncovering additional fraud patterns and trends.

## Adding a New Tool to Solve a Specific Problem while Expanding Fraud Protection Across the Ecosystem

### Integration Description

A U.S. regional bank operates with a centralized enterprise fraud management system that integrates and orchestrates various underlying fraud solutions in the areas of authentication, device intelligence, onboarding, and more.

### Before BioCatch: Remote Access Trojans Cause Significant Losses

Between 2021 and 2022, the bank was incurring significant fraud losses, mostly attributed to account takeover. During this time, dispute rates stood at 0.6%, with fraud losses comprising 0.3% of all payments. Remote Access Trojans (RATs) were prevalent in most of these cases and greatly impacting the bank's micro-payment online services.

### After BioCatch: Fraud Losses Decrease Over 80%

In response to the increase in account takeover fraud, the bank made the strategic decision to incorporate BioCatch into their fraud defense strategy. During mid-2022, BioCatch Account Takeover Protection was integrated to add an extra layer of defense across the bank's website and mobile applications. This integration effectively complemented the existing fraud technology stack, which had shown limitations in flexibility and features, rendering it less effective in detecting RATs which were at the center of the explosion of account takeover cases. BioCatch's advanced behavioral biometrics capabilities and robust RAT detection features played a pivotal role in the bank's decision.

BioCatch Rule Manager stands as an invaluable asset in the bank's toolkit, empowering the fraud operations team with enhanced flexibility in applying diverse logic to the model's output before transmitting the data to the enterprise fraud management system.

BioCatch played a key role in driving accelerated growth in the online micro-payment service, fostering increased visibility and trust. In two years, the bank doubled the volume of online micro-payments, surpassing $1.5 trillion in total transactions. Notably, despite this surge in activity, disputes and fraud rates consistently declined. Disputes decreased from approximately 0.6% to just 0.13%, while fraud losses dropped from around 0.3% of all payments in 2021 to approximately 0.05% in 2023. These reductions not only resulted in substantial monetary savings but also contributed to considerable operational cost savings in dispute handling.

# Prioritizing Behavioral Intelligence in the Fraud Stack

## Integration Description

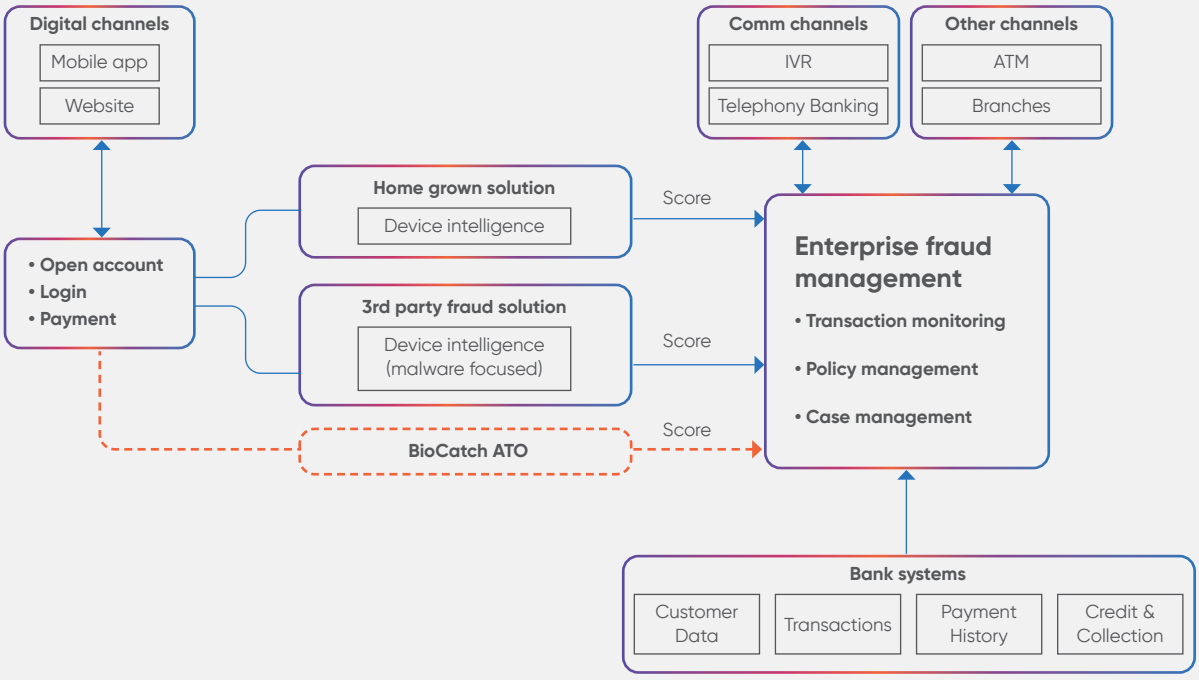
A leading European bank employs a comprehensive fraud technology stack that operates in synergy and includes:

- A transaction monitoring system for fraud detection, equipped with policy rule writing and case management capabilities
- Coverage of all banking channels, including online and mobile banking, telephony banking, and branch and ATM usage
- In-house capabilities for device intelligence, specifically device ID profiling
- Utilization of a third-party provider for additional device intelligence, with a focus on malware detection

## Before BioCatch: Limited Ability to Detect Voice Scams

While the bank's existing fraud management framework displayed resilience and excelled in many aspects, it faced a growing challenge — the rise in false positives and the inadequacy of in-session visibility, especially concerning voice scams and sophisticated account takeover attempts.

The existing systems were unable to effectively detect and analyze nuanced user behavior during banking sessions, including key indicators of potential fraud. Recognizing the pressing need for a solution that would complement their existing defenses, the bank decided to incorporate the BioCatch Account Takeover Protection solution as an additional layer of defense into its fraud technology stack. The diagram below shows where BioCatch fits within the bank's enterprise fraud management system.



### After BioCatch: Fraud Attempts Decreased by 85%

BioCatch Account Takeover Protection addressed the critical gap, providing increased accuracy and unparalleled visibility into user behavior during each session. BioCatch's technology seamlessly integrated with existing third-party solutions helping the bank to realize the following results after deployment:

- Achieved an average of 70% detection rate
- Provided an outstanding 10x return on investment
- Led to an 85% decline in fraud attempts over three years

## Adding a New Fraud Model to Address Sophisticated Fraud (Social Engineering Scams)

### Integration Description

A top 10 bank in Latin America has been a BioCatch customer for several years, successfully leveraging behavioral biometrics technology to combat account takeover fraud. Over the years, the bank equipped itself with a diverse array of technologies and tools sourced from various solution providers to form a best-of-breed fraud protection strategy.

The fraud technology stack includes:

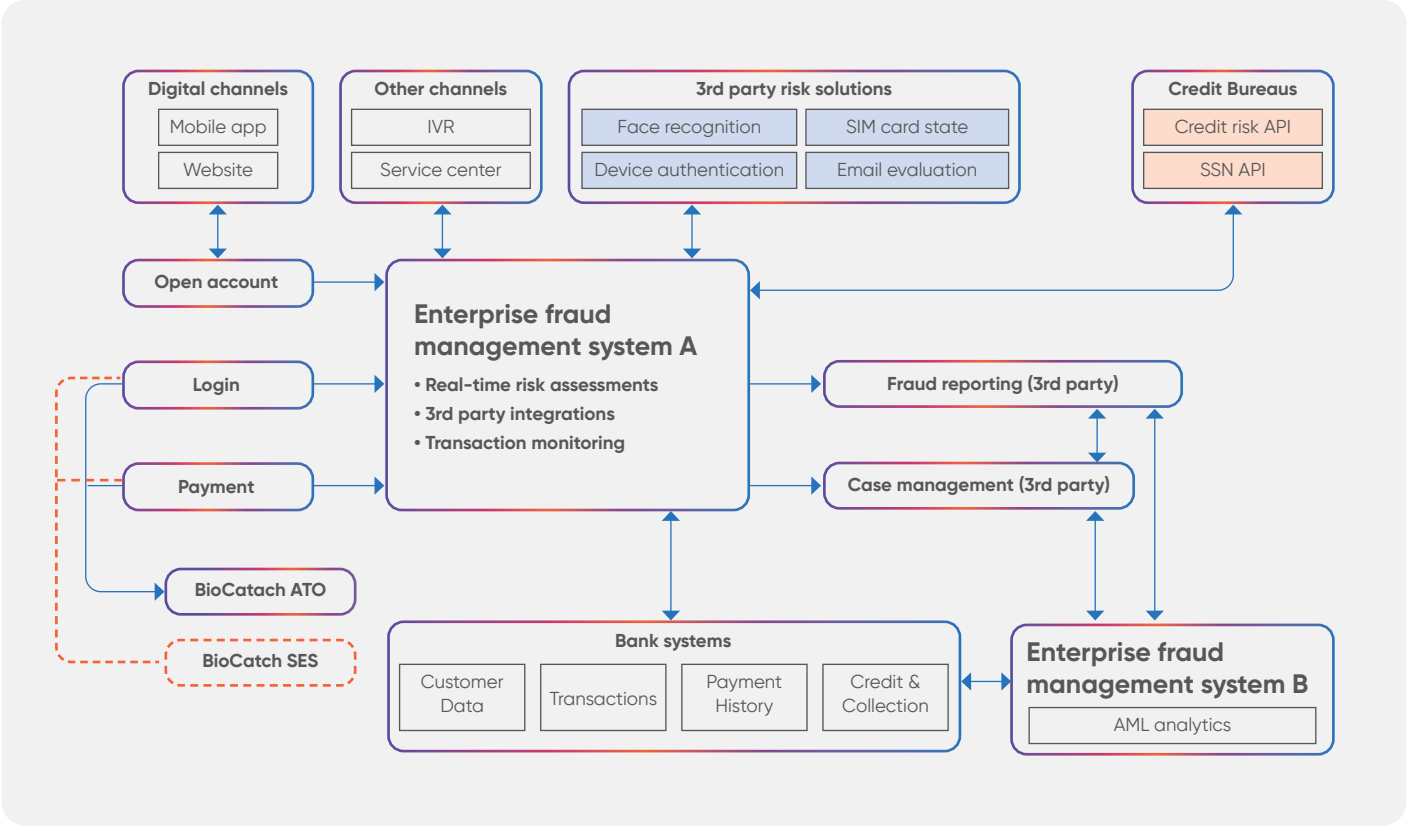
- Two Enterprise-Grade Tier-1 Fraud Management Systems: Serves as the foundation for fraud management strategy.
- AML Analytics: Monitor and scrutinize financial transactions for signs of money laundering
- Fraud Reporting Tools: Ensure rapid responses to potential threats while identifying abnormal patterns
- Case Manager Application: For tracking and resolution of fraud cases.
- Email Risk Evaluation: Assess the risk of customer email addresses.
- SIM Card State Monitoring: Monitor the state of customer SIM cards.
- Facial Recognition: Employ biometric authentication through facial recognition technology
- Device Authentication: Verifying device authenticity to prevent unauthorized access.
- External APIs:
  - Credit Risk API: Assessing customer creditworthiness to pinpoint potential risk factors.
  - Social Security API: Validating customer identities and assessing the authenticity of provided information.

### Before BioCatch: Fraudsters Defy Existing Defenses

While the bank's existing security framework exhibited resilience against traditional account takeover attacks, the rapidly evolving threat landscape revealed a critical vulnerability in their defenses when the bank experienced a surge in voice scams. Existing systems lacked the essential visibility to detect and analyze user activity, or lack of activity, taking place during the banking session, including indicators of a voice scam in progress such as user hesitation, distraction, stress, and other emotional cues.

## After BioCatch: 70% Reduction in Losses from Voice Scams

In response to this pressing challenge, the bank adopted the BioCatch Social Engineering Scam Detection solution to enhance the effectiveness of their existing technology stack. BioCatch served as the missing piece, providing unparalleled visibility into behavioral signals throughout the banking session that indicate a user is acting under the guidance of a fraudster. The following diagram demonstrates how BioCatch is layered into the bank's fraud technology stack.




Within just six months of implementing BioCatch Social Engineering Scam Detection, the bank achieved the following results:

- A 70% reduction in fraud losses, totaling over $4 million, attributed to voice scams
- An 8X return on investment
- A significant decrease in the frequency of attempted voice scam incidents

# Unifying Fraud Detection with an Effective Consortium

## Integration Description

In response to the growth of financial fraud, most of the top banks in Australia have taken proactive measures to reinforce their defense against sophisticated and emerging digital threats by integrating behavioral biometrics to complement existing enterprise fraud management systems.

A typical fraud tech stack in the region includes:

- An enterprise fraud management system serves as the foundation of their fraud strategy
- Robust transaction monitoring capabilities
- Device/network/geo intelligence, either through in-house solutions or via the enterprise fraud management system
- Integration with external APIs, including government services for customer details validation
- Utilization of two-factor authentication, primarily through SMS one-time passwords (OTP), for high-risk transactions

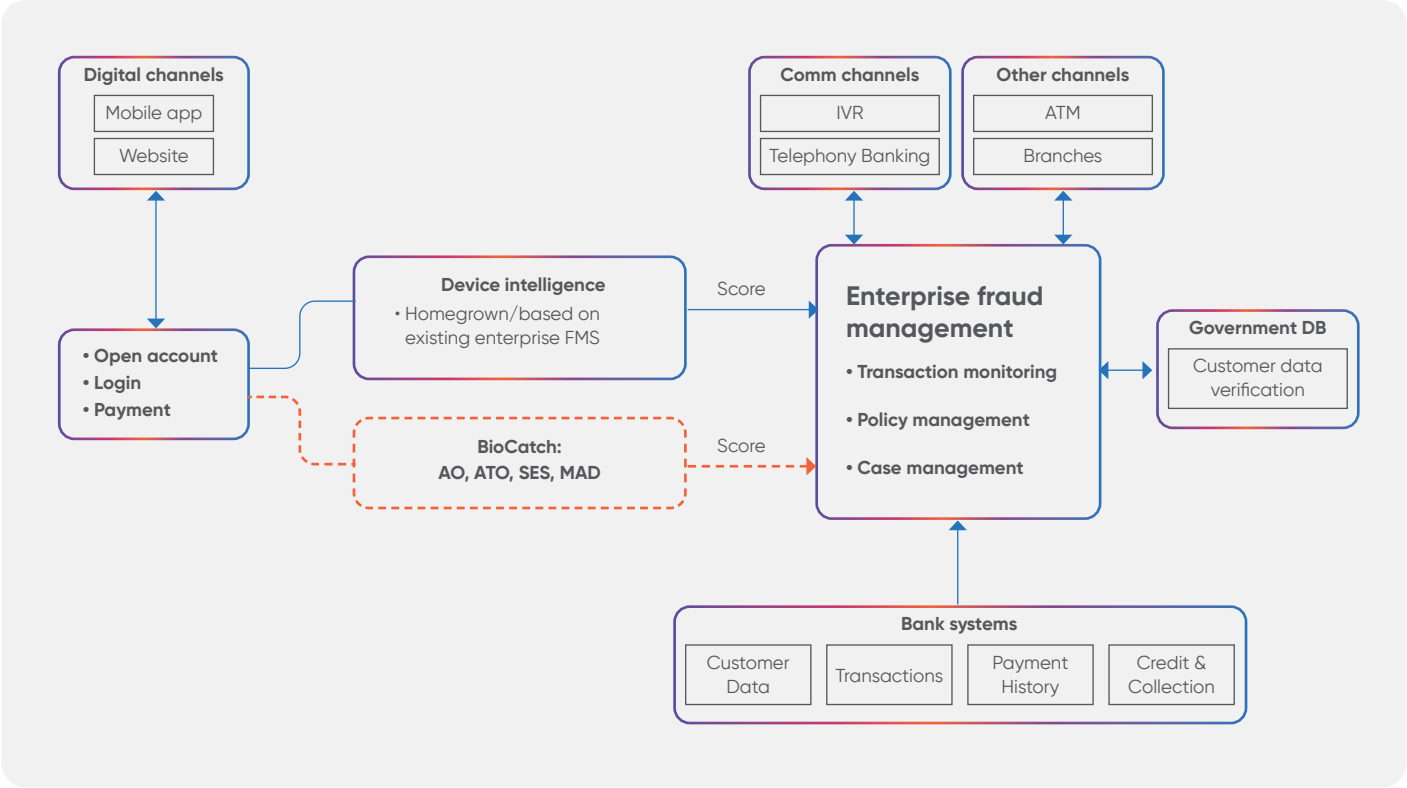
## Before BioCatch: Emerging Fraud Types Challenge Existing Defenses

While historically effective, Australian banks encountered growing challenges stemming from emerging fraud types such as remote access attacks, mobile malware, social engineering scams, and a surge in mule accounts. Acknowledging the need to adapt and innovate, these banks sought to enhance their fraud detection capabilities by embracing behavioral biometrics technology and integrating it into their fraud protection stack.

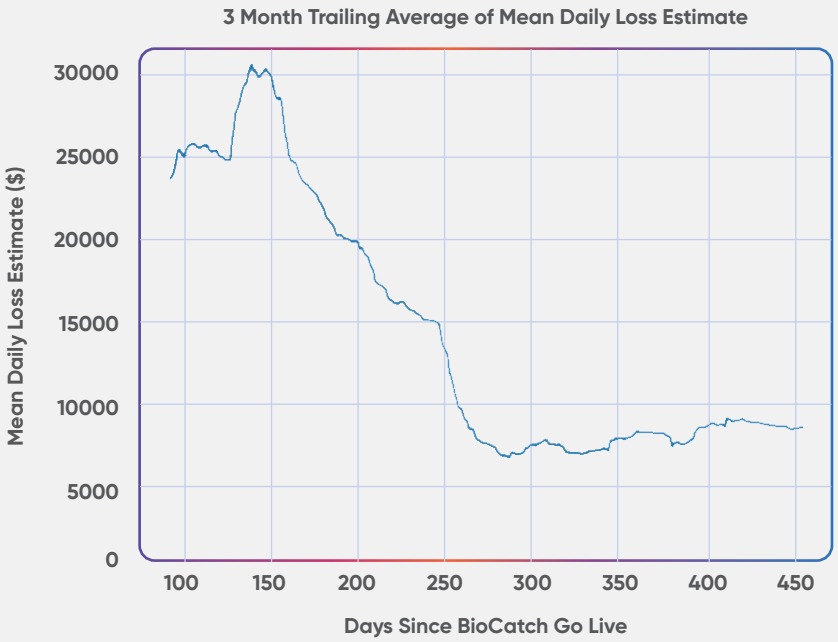
The integration journey commenced in 2020, and over time, most of the major Australian banks adopted BioCatch's suite of products to address new account fraud, account takeover, social engineering scams, and mule accounts. This has transformed BioCatch into an integral and mission-critical component of the technology stack for banks across Australia, protecting over 90% of the adult banking population in the country.

## After BioCatch: 70% Reduction in Fraud Losses

BioCatch solutions are deployed as an additional protective layer and fed into the enterprise fraud management system, providing scores, risk and genuine factors, and other data points to improve fraud risk assessments. The diagram below illustrates where BioCatch fits within a typical enterprise fraud management technology stack in Australian banks.



The tangible benefits of behavioral biometrics are demonstrated by the remarkable success of one Australian bank which experienced a substantial 70% reduction in fraud losses within the first year. This equates to savings of approximately $30 million AUD annually.




**70%**
**reduction in digital banking fraud losses**

## Conclusion

Fraud detection has become a community and an ecosystem requiring a layered technology approach to eliminate risk throughout the customer journey. Point solutions no longer fare well in an environment that requires cooperation, even among historically competing technologies. Behavioral biometric intelligence is proven to enhance the legacy fraud detection ecosystem to improve fraud capture rates, reduce operational costs, and elevate customer safety.

## Additional Resources

Datos Insights Matrix: Behavioral Biometrics and Device Fingerprinting Solutions

CBA Says Scam Losses Slashed by a Third

ANZ Banking Group Stops Fraudulent Digital Accounts From Being Opened

How Banorte Uses BioCatch to Enhance Customer Experience and Reduce Fraud

How Suncorp Bank Uses BioCatch to Support its Fraud and Scams Response

## About BioCatch

BioCatch is the leader in Behavioral Biometrics, a technology that leverages machine learning to analyze an online user's physical and cognitive digital behavior to protect individuals online. BioCatch's mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease seamlessly co-exist.

Today, BioCatch counts over 25 of the top 100 global banks as customers who use BioCatch solutions to fight fraud, drive digital transformation and accelerate business growth. BioCatch's Client Innovation Board, an industry-led initiative including American Express, Barclays, Citi Ventures, and National Australia Bank, helps enable BioCatch to identify creative and cutting-edge ways to leverage the unique attributes of behavior for fraud prevention. With over a decade of analyzing data, more than 70 registered patents, and unparalleled experience, BioCatch continues to innovate to solve tomorrow's problems.

For more information, please visit www.biocatch.com

BioCatch

www.biocatch.com
E: info@biocatch.com
@biocatch
/company/biocatch