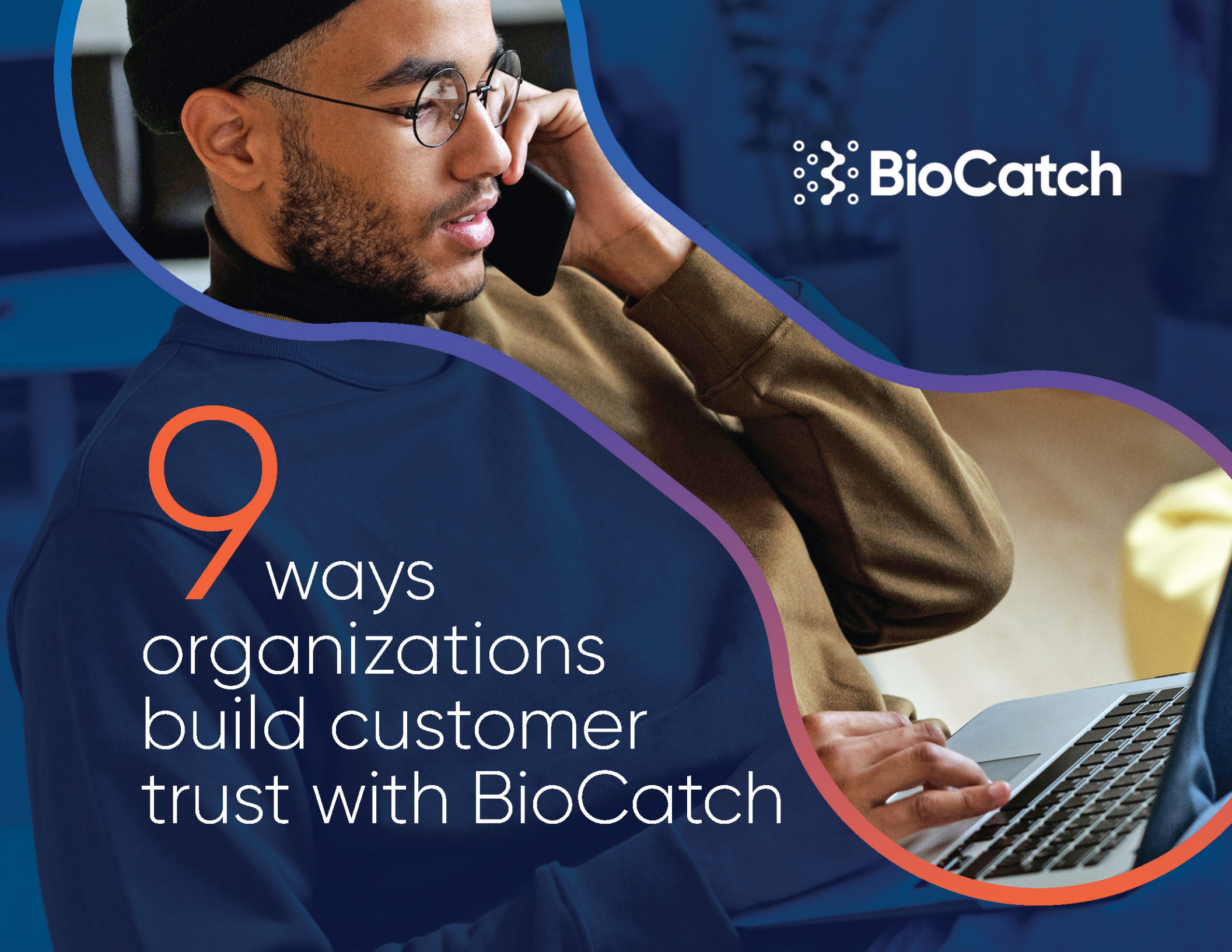


BioCatch

9 ways organizations build customer trust with BioCatch

What could be more important for financial institutions and fintechs than the trust of their customers? Today leading financial institutions strive to deliver both great financial products and customer experiences that serve to build sustained confidence and trust in their organization.

But too often, the practice of detecting and preventing fraud can undermine these goals. Fraud prevention measures may go too far and frustrate or impede customers, or they can come-up short and allow financial losses or hassles that could be prevented. Finding that balance between protection and experience is very difficult to achieve.

One thing's for sure, the traditional transaction monitoring and reporting measures used to detect and investigate fraud will probably fall short. The fraudsters have surpassed these systems, driving up fraud losses, overwhelming fraud centers, and frustrating customers.

Fortunately, Behavioral Biometrics is not only helping organizations improve fraud detection; it's also helping to drive more revenue, reduce costs, and improve customer experiences. And, the benefits of Behavioral Biometrics from BioCatch reach well-beyond the limitations of traditional technologies that have focused solely on account origination and account take-over fraud tuse-cases.

Today organizations are facing new challenges ranging from P2P fraud (such as Zelle in the U.S.) to voice scams (also known as Authorized Payment scams) and Remote Access Tool (RAT) scams that target the most vulnerable customers. As the public and regulators take notice of these challenges, organizations are seeking fraud prevention solutions that meet emerging needs, deliver returns on investments, and delight customers.

It's a tall order. BioCatch is up to the task.

Here are 9 ways BioCatch is helping organizations build customer trust.

BioCatch

9

Reduce Payment Fraud (ACH and Credit Card), and related expenses

While ACH fraud incidents are relatively low compared to other fraud channels, payment fraud using both credit cards and ACH is a growing problem, particularly with E-mail Account Compromise and Business Email Compromise scams on the rise.

Recently, one of the largest U.S. providers of financial technology for businesses and consumers was experiencing a significant drain on resources from manual reviews of suspicious transactions. In addition, transactions were being blocked, creating frustration for buyers and suppliers alike.

Upon implementing BioCatch at the online payment checkout flow, **the company realized a 70% decrease in payment fraud, with monthly savings of $3.6M from payment card fraud and $2.2M from ACH bank fraud.**

BioCatch also helps card issuers achieve Strong Customer Authentication (SCA) as prescribed by Europe's Payment Services Directive (PSD2); providing a fast, secure, and frictionless experience for online purchases.

Implementing BioCatch at the online payment flow resulted in a **70% decrease** in payment fraud.

BioCatch

8

Prevent Identity Theft Targeting the Elderly

Elderly customers are among the most vulnerable to online financial fraud and scam activity.

A recent aggregation of data from leading card issuers found that up to 40% of fraudulent credit card applications had a declared age of 60+. At the same time, it was discovered that genuine applicants in this age group were disproportionately encountering additional steps for validation, leading to a higher number of abandoned applications and lower customer satisfaction.

Following discussions with some of these issuers, BioCatch developed a cutting-edge age analysis capability to further increase fraud detection and improve customer experience. By closely assessing certain age-related factors, BioCatch can identify instances when the behavioral age of the user is not consistent with the declared age on the application.

BioCatch Age Analysis gives issuers greater visibility into application risk and increasing confidence in automatic acceptance and decline decisions. In addition to reducing fraud losses, issues are realizing operational cost savings and additional revenue. One issuer realized a $3.5M annual return on investment.

40% of credit card applications have a declared age over 60.

BioCatch

7

Detect Voice and Social Engineering Scams

(another benefit for vulnerable elderly customers!)

According to Consumer Affairs, older people in the U.S. are swindled out of more than $3 billion each year. Some banks are now reporting that scams account for 4x more fraud losses than attacks involving malware or stolen credentials.

Strictly speaking, many of these incidents aren't classic fraud, but rather coercion by extremely competent scammers. And people of all ages can be victimized by voice scammers. These scams are both difficult to detect and investigate, because the fraudster relies on both the equipment (computer, network) and emotions of the victim. After gaining the victim's trust and inciting them to log-in to their bank account, scammers frequently introduce remote access tools (RAT), giving them full access to the session. In addition to the investigative burden, in some cases the bank reimburses losses involving RAT account take over.

A top-4 Australian bank came to BioCatch after experiencing such challenges. Today this institution can identify behavior indicators of a scam in progress and session changes indicating an attacker has taken-over a session using a Remote Access Tool (RAT). **The bank can now detect 66% of these attacks.**

A top Latin American bank **reduced social engineering fraud targeting mobile users by 67%** using behavioral biometrics!

The bank can now detect **66%** of scams involving remote access attacks.

BioCatch

6

Stop Mule Activity (before it happens)

The recent rise in online money mule activity has attracted new scrutiny from global regulators directed towards a financial institution's role in detecting and handling of these accounts.

Mule accounts play a critical role in criminal money laundering and the fraud supply chain infrastructure. Money mules come in different forms, with different motivations and varying degrees of criminal intent. And, cybercriminals employ various methods to launder stolen funds. So, detecting mule activity is incredibly difficult and complex.

BioCatch has identified five persona types to look-out for when detecting mule accounts. Understanding these personas and the common behaviors associated with each one can help prevent mule accounts at account opening as well as detect mule activity within existing accounts. By zeroing-in on suspected money mule activity early, financial institutions can intervene before attempts to cash-out are made, reducing operational overhead for fraud and anti-money laundering teams.

When a large Australian bank leveraged BioCatch's behavioral insights to actively look for signs of mule activity, they quickly identified more than 2,000 mule accounts.

BioCatch was recently awarded a U.S. patent for its innovative Mule Account Detection solution, solidifying the company's unique approach to identifying mule activity.

BioCatch's behavioral insights quickly identified more than **2,000** mule accounts.

BioCatch

5 Detect Zelle and P2P payment fraud

Since its launch in 2017, the Zelle payment network has experienced rapid growth in the United States offering consumers the convenience of free and fast peer-to-peer (P2P) mobile payments. While consumers have embraced it, banks soon realized the greater risks of online fraud that P2P payments expose. Today, tens of millions of Americans fall victim to Zelle and payment app scams annually.

Today, scam victims in the U.S. have some legal rights and protections as a result of changes to the Electronic Funds Transfer Act (also known as "Reg E").

When a top U.S. credit union saw a spike in advanced cybercrime soon after launching Zelle payments for its mobile banking customers, they initially reacted by putting in additional multi-factor authentication (MF) and other controls, such as limits on Zelle transfer amounts. This helped to reduce fraud, but caused a big impact on customer experience.

After leveraging BioCatch technology to help discern between genuine and cybercriminal access, **the credit union saw a 95% reduction in residual fraud losses**, virtually eliminating all fraud associated with Zelle payments.

After leveraging BioCatch technology, the credit union saw a **95% reduction** in residual fraud losses.

BioCatch

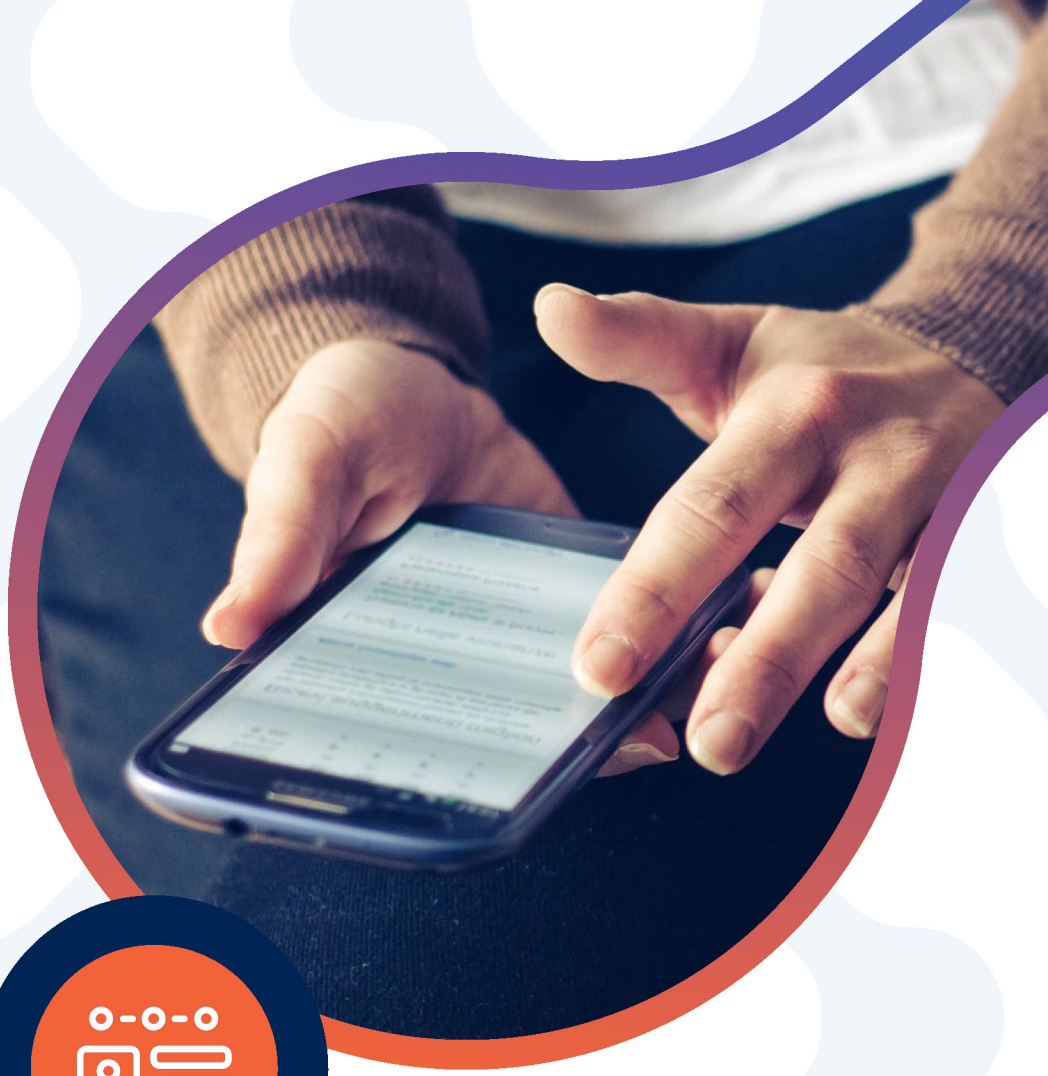
4

Approve more account applications quickly

Account opening fraud is one of the fastest-growing cyber threats today. The sheer volume of digital activity by consumers brought on by the COVID-19 pandemic has exacerbated the problem and has allowed fraudsters to hide in plain sight.

This type of fraud is especially hard to detect in cases where no prior profile of the applicant exists. And when losses resulting from fraudulent applications begin to mount, it's only natural for credit issuers to increase application scrutiny. The resulting 'declines' of genuine customers who are mistakenly caught-up in the tighter controls, can have as detrimental effects on business performance as the fraud losses.

A Top-5 U.S. credit card issuer, suffering from millions of dollars in fraud losses involving stolen personal information and synthetic ID's in applications, adopted BioCatch behavioral biometrics to add a new layer of visibility. They were quickly deciphering between legitimate applications and cybercriminals with greater confidence. A 12x ROI and $10M annually were achieved by accepting more credit card applications, decreasing operational costs, and reducing fraud losses.



Adopting BioCatch behavioral biometrics resulted in a **12x ROI** and **$10M** annually.

BioCatch

3

Reduce customer friction

Everyone has experienced declined transactions, stepped-up authentication such as SMS verification codes, phone alerts, and waiting on hold to speak with a representative.

While customers generally understand the purpose of these inconveniences, often individual circumstances can cause them to grow frustrated or lose patience.

Continuous authentication using behavioral biometrics is like an authentication express lane. Companies can make smarter decisions about when to introduce step-up authentication, leading to seamless customer experiences.

Behavioral biometrics rely partly on previous authentication to verify users in the moment, based on their established user profile. Customers don't notice it because it relies on their actions, rather than location, PINs, or passwords. Even without a user profile, behavioral biometrics can differentiate between fraudulent behavior from legitimate activity.

Continuous behavioral authentication means fewer false fraud alarms and the ability to reserve additional authentication only for truly high-risk situations. Customers can travel, shop, and bank with ease and peace of mind, while gaining confidence and trust in their retailers and financial institutions.

Continuous authentication using behavioral biometrics is like an authentication express lane.

BioCatch

2

Reduce false positives

The true costs of fraud are not limited to the financial losses of victims or institution's' reimbursement costs. Labor costs for investigating and recovering from fraud impact can mount quickly. Fraud investigators, computer security professionals, consultants and attorneys are all expensive; and none of their activities are easily scalable when fraud activity spikes, as happened in the early months of the Covid-19 pandemic.

Moreover, customer frustration due to declined transactions, long waits in call queues, and the hassles of engaging with fraud analysts is likely to drive away some valuable patrons.

When a large LATAM bank was facing significant fraud losses from account takeover attacks, their transactional monitoring system was only detecting about half of their fraud. Worse, the system was generating a high number of alerts and false positives, overburdening their fraud and security teams.

The bank brought in BioCatch to help reduce false positives and decrease the number of alerts generated. To compare, in one scenario, the transaction monitoring solution had generated over 2,300 alerts and prevented only 31% of fraud. BioCatch generated only 700 alerts and prevented 70% of fraud. Overall, by implementing BioCatch, the bank was able to reduce fraud alert volume significantly and decrease false positives by 66%. BioCatch brought much needed protection to fill the gaps that existed in the bank's fraud controls at a critical time, allowing fraud and security teams to focus on other pressing projects while keeping the bank's assets and customers safe from cybercrime.

Further, BioCatch's platform eliminates the need for discrete tools that solve discrete problems. Reducing the number of tools required to investigate fraud reduces complexity in the process, technology failures, and time spend on analysis.

By implementing BioCatch, the bank was able to decrease false positives by **66%**.

BioCatch

1

Detect more Fraud (ATO, AO)

As the problem of online fraud and scams continue to gain awareness and attention from the public and regulators alike, the need for better tools to detect fraud is greater now than ever before.

Fortunately, implementing behavioral biometrics can substantially improve detection, while reducing the need for additional friction that undermines customer experiences.

- By partnering with BioCatch, **a Top 4 Australian bank can now detect 66% of voice scams** in progress.
- **A Top 5 U.S. card issuer increased its new application fraud detection rate to over 90%**, while confirming 99.93% of applications as genuine.
- **A Top Asia bank reached over 90% accuracy rate** on new account fraud alerts, projecting over $7M annually in potential savings.
- **A Top U.S. financial technology provider prevented $5.8M of card and ACH fraud** each month.
- **A Top Latam bank boosted fraud detection rates to over 90%**, compared to the less than 50% they achieved with transaction monitoring only.

The results speak for themselves. Behavioral Biometrics help organizations detect more fraud, while reducing customer friction and burdens on institutions' fraud prevention practices.

Behavioral biometrics can substantially improve detection, while reducing the need for additional friction.

ABOUT BIOCATCH

BioCatch is the leader in Behavioral Biometrics, which analyzes an online user's physical and cognitive behavior to protect users and their assets. Our mission is to unlock the power of behavior and deliver actionable insights to create a digital world where identity, trust and ease of use seamlessly co-exist. Leading financial institutions around the globe use BioCatch to more effectively fight fraud, drive digital transformation and accelerate business growth. With over a decade of experience analyzing data, more than 60 patents and unparalleled anti-fraud expertise, BioCatch continues to innovate to solve tomorrow's problems. For more information, visit www.biocatch.com.

BioCatch