BioCatch

2024 AI, Fraud, and Financial Crime Survey

AI's Role in Perpetrating and Fighting Financial Crime

KEY TAKEAWAYS

STATE OF FRAUD AND FINANCIAL CRIME

- **56%** of fraud-management decision makers, AML professionals, and risk and compliance leaders at banks and financial institutions say financial-crime activity increased in the last year.
- **46%** expect financial-crime activity to increase in 2024.
- **58%** of decision makers say their organizations spent between $5 million and $25 million in operational costs associated with investigating, combatting, or rectifying financial crime or consequences of financial crime in 2023.
- **48%** expect the total value of the losses due to fraud to increase in 2024.
- **43%** expect fraud-activity volume to increase in 2024.

MAJOR THREATS

- **69%** say that criminals are more advanced at using AI for financial crime than banks are at using AI to fight financial crime.
- **51%** of organizations lost between $5 million and $25 million in total to AI-based or AI-driven threats in 2023.
- **72%** of respondents said their organization faced cases of synthetic identities when onboarding new clients.
- **91%** of financial services or banking organizations are re-thinking the use of voice verification for big customers given the risks of voice cloning with AI.

Executive Summary

Financial crime poses an existential threat to financial institutions, their customers, and our society as a whole. From money laundering and terrorist financing to bribery and human trafficking, financial crime undermines the very foundation on which we've built our financial systems. Current investments in AI and biometrics already prove inadequate in deterring financial crime. Anti-money laundering (AML) and fraud-fighting executives report a concerning increase in financial crime in just the last year. BioCatch expects that trend to continue into 2024 and beyond.

Consumers and, increasingly, governments look to financial institutions to combat fraud and prevent financial crime. Consumers spend more and more of their lives online, posting personal updates to social media, shopping on e-commerce sites, and paying bills, transferring funds, and checking balances from their phones. It is no longer possible to operate without a digital identity, leaving every one of us vulnerable to bad actors, who find in this vast digital world ample opportunities to scam us.

To better understand the current state and future landscape of financial crime and how and where it intersects with AI, BioCatch commissioned a global survey of fraud-management decision makers, AML professionals, and risk and compliance leaders at financial institutions around the world.

What we found is that banks are facing a variety of emerging threats, many of which are powered and/or enabled by AI. At the same time, banks are investing in AI and integrating solutions that leverage this technology. But it isn't enough. Further investment is needed. While most financial institutions are already using AI for financial-crime detection (74%) and fraud detection (73%), all respondents expect both financial crime and fraud activity to increase in 2024.

KEY TAKEAWAYS

PUTTING AI TO WORK

- **74%** of organizations are currently using AI for financial-crime detection.
- **73%** of organizations are currently using AI for fraud detection.
- **94%** say their organization is using AI/ML techniques to detect risk from user behavior.
- **87%** say AI has increased[1] the speed with which their organization responds to potential threats.
- **69%** believe AI will lead to more revenue (i.e., improved customer interactions, less time spent investigating false positives, etc.) than loss (i.e., fraud, breaches, etc.).

88%

of fraud decision makers say more[2] information should be shared between banks, financial institutions, and government or regulatory authorities in the next one to two years to combat financial crime and fraud

This suggests – despite continued investment in technologies and resources to combat financial crime and fraud – threat actors are finding ways to circumvent these prevention measures. Thanks in part to AI, criminals are innovating faster than banks can keep up.

Bad actors share intelligence with other fraudsters, helping to improve attack methods and avoid detection. To combat fraud and financial crime in 2024, banks must also share with their competitors. Rules and regulations make this process difficult, generating information silos that make collaboration difficult even within individual banks. This allows threat actors to stay a step ahead. Financial institutions must assess how they can take more thoughtful, forward-thinking action to share intelligence and account information to be more agile and rectify this problem.

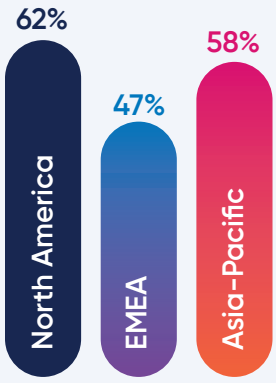
Sharing information, collaborating with regulatory authorities, and implementing emerging technologies will be vital in combatting fraud and financial crime in 2024 and beyond. Employing behavioral biometric intelligence will allow financial institutions to leverage the only element of digital identity that is truly human and almost impossible to replicate, thus providing better protection for their customers. Continued evolution will ensure financial institutions are ready for whatever the future may bring.

1 Significantly increased / increased speed
2 Much more information / more information

Financial Crime

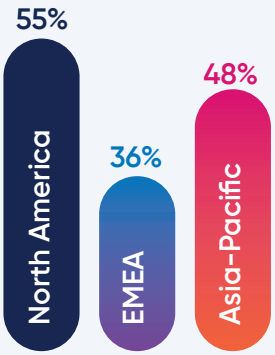
Financial transactions and activities increasingly occur online. The pandemic sped up this digitalization of the banking world. Further enhancements via peer-to-peer payment services offering immediate transfers have led to more and more consumers relying on digital banking for their financial needs. While the move toward online banking and financial services has increased convenience for consumers, it's also created additional risks for banks and their customers and opportunities for threat actors. More than half (56%) of respondents globally report that financial-crime activity has increased in the past year.

Financial institutions in North America report the largest increase in financial-crime activity over the last 12 months. Likewise, more respondents from North America expect financial-crime activity to increase in 2024 than their counterparts in other regions. This finding is not surprising considering a 2022 report which found the United States was the top destination for stashing money illegally, ranking ahead of traditional tax shelters like Singapore, Switzerland, Luxembourg, and the Cayman Islands. In fact, in 2021 former Treasury Secretary Janet Yellen said: "In the popular imagination, the money laundering capitals of the world are small countries with histories of loose and secretive financial laws. But there's a good argument that, right now, the best place to hide and launder ill-gotten gains is actually the United States."



Based on your experience in your role, has financial-crime activity increased in the past year?

All respondents report an **increase** in financial-crime activity in the past year.



Do you expect financial-crime activity to increase in 2024 compared to last year?

74%
of organizations globally are currently using AI for financial-crime detection

Although the possibility of increased financial crime in 2024 is concerning, technologies like AI can assist in combatting evolving threats. BioCatch found financial institutions in Europe, Middle East, and Africa (EMEA; 86%) most likely to already use AI for financial-crime detection, followed by North America (71%) and Asia-Pacific (APAC; 67%).

While not all banking and financial services organizations currently use AI for financial-crime detection, decision makers indicate their organizations plan to change this. More than one in five (22%) respondents globally say their organization is not currently using AI for financial-crime detection but plans to start in the next six months.

Globally, banks use AI to detect financial crime through advanced machine learning (83%), natural language processing (72%), and deep learning (67%). Financial institutions can use AI technology to further understand user behavior and identify suspect activity.

94%
say their organization is using AI/ML techniques to detect risk from user behavior

Organizations worldwide face a multitude of problems regarding the ability to combat financial crime, including data security and privacy (36%), cybersecurity (31%), and integration issues in technological systems (23%). AI also poses an additional problem, as nearly seven in 10 (69%) say criminals are better at using AI to enact financial crime than banks are at using it to detect the crimes.

Financial crime is costing organizations significant time and money. From the costs associated with investigating and uncovering financial crime to the costs of remediation, the monetary impact of financial crime is huge. Only one in four (28%) globally say their company spent less than $5 million in operational costs associated with investigating, combatting, or rectifying financial crime or consequences of financial crime in 2023. On the other hand, 16% report their company spent $25 million or more.

Furthermore, the cost of financial crime extends beyond measurable monetary losses. Financial crime can also cost organizations through damage to their reputation, causing negative perception among existing clients, potential customers, and investors, leading to further losses. Penalties for failed compliance with AML can be devastating to financial institutions. In 2023, the Federal Reserve fined Deutsche Bank and its U.S. affiliates **$186 million** for failing to address AML shortcomings. Binance, the world's largest cryptocurrency exchange, was fined **$4.3 billion** in relation to AML violations. Investing in tools to fight financial crime is imperative to business success in 2024.

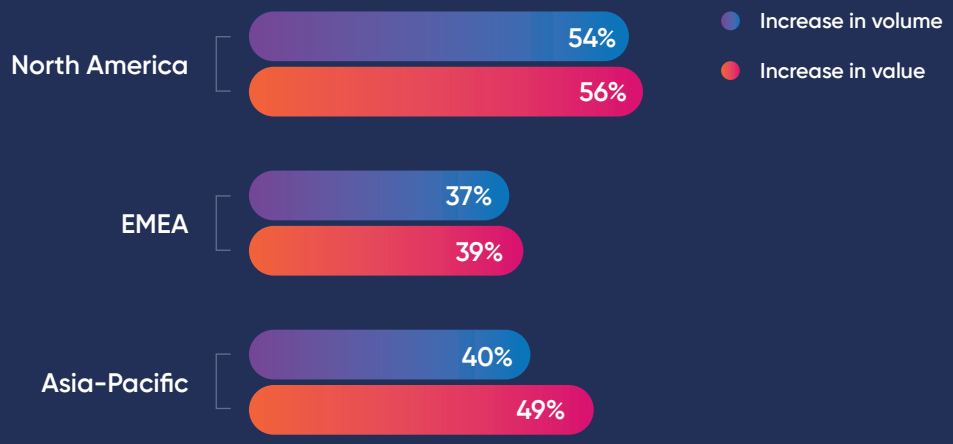
58%
of decision makers say their organizations spent between $5 million and $25 million in operational costs associated with investigating, combatting, or rectifying financial crime or consequences of financial crime in 2023

Fraud

Fraud increased globally in 2023 and should continue increase in 2024. Survey respondents agree that all types of fraud – from payment fraud to credit card fraud to identity theft – either stayed the same or increased in the past year.

Approximately three-quarters of global fraud-management decision makers expect fraud activity to stay the same or increase in 2024 in both the total value of financial losses (76%) and volume (74%). Decision makers in North America are most likely to be pessimistic about fraud activity in 2024 compared to other regions.

How do you expect fraud activity to change in 2024 compared to the last year?



Despite the importance of combatting financial crime and fraud, many organizations are still using siloed operations. Concerningly, two in five (41%) anti-fraud decision makers say fraud and financial crime are handled in separate units (i.e., different teams, divisions, etc.) with no cross-collaboration. Three in 10 (31%) say fraud and financial crime are handled in separate units with cross-collaboration. Only 28% report that fraud and financial crime are handled by the same unit at their organization. Siloed operations with a lack of communication pose a major issue to an organization's ability to accurately track and successfully combat both financial crime and fraud.

41%

say fraud and financial crime are handled in separate units with no cross-collaboration

As fraud continues to evolve online, often powered by technologies like AI, many organizations are turning to the same technologies to drive improved detection and response. Many organizations are already using technologies like AI to improve their ability to detect fraud, while others indicate plans to adopt AI for fraud detection in the near future. Nearly three-quarters (73%) of organizations are currently using AI for fraud-detection.

Approximately one in four (23%) fraud decision makers globally say that while their organization does not currently use AI for fraud detection, there are plans to start using AI for this purpose in the next six months. More than three in five financial organizations are currently using the following AI-enabled technologies to detect fraud: advanced machine learning (79%), natural language processing (NLP) (71%), and deep learning (65%). While AI can be useful for financial institutions in fraud-detection and -response, AI is being used by bad actors to power increasingly advanced threats. AI allows these threat actors to automate tactics and scale attacks beyond traditional limitations. AI and large language models (LLMs) are also being used to create believable messages for social-engineering attacks, power voice scams, and fuel deepfake videos.

The use of AI in social-engineering attacks will make events like the hack of MGM—which resulted in the exposure of personally identifiable customer information and cost the company $100 million—much more prevalent in the future. This is especially concerning given that more than 90% of all cyber-attacks begin with phishing. Furthermore, a 2022 IBM report found that targeted phishing attacks that included phone calls were three times more effective than those that did not.

51%

of organizations lost between $5 million and $25 million in total to AI-based or AI-driven threats in 2023, and only 3% said their organization did not lose anything

These AI-driven threats pose a major challenge for financial organizations in 2024, and fraud-management decision makers expect these threats to result in major losses at their organizations. Globally, respondents expect automating scam tactics to scale attacks (45%), AI scanning for leaked PII (42%), and LLMs drafting believable messages for social engineering (36%) to have the highest related dollar losses for their organization.

AI-based threats also proved to be damaging for organizations in 2023. Only 3% of respondents reported that their organization did not lose anything to AI-based or AI-driven threats in 2023.

Global organizational losses varied in 2023 – with some organizations experiencing fewer losses while other companies were faced with recovering from significant damages. One in three (33%) lost less than $5 million, while 12% lost $25 million or more to AI-based threats in 2023.

DEEP DIVE ON SYNTHETIC IDENTITIES

Another threat financial institutions faced in 2023 was synthetic identities, which fraudsters can use to apply for credit cards and open new accounts to borrow or launder money. Identified as the fastest-growing type of financial crime in the United States in 2019 by the Federal Reserve, synthetic identities have largely escaped detection, with an estimated 85-95% of applicants identified as potential synthetic identities not flagged by traditional fraud models. Synthetic-identity fraud costs companies billions and is also a contributing factor to the increase in new-account fraud.

72%

of respondents said their organization faced cases of synthetic identities when onboarding new clients

These organizations were largely able to uncover these synthetic identities within three months, with more than one-third (35%) discovering the fraud within 30 days and one-quarter (26%) within 90 days. Only 16% were able to uncover the synthetic identities within 24 hours.

Organizations uncovered these synthetic identities several ways, most notably through information from other financial institutions or law enforcement/regulatory authorities (49%). As synthetic identities become increasingly difficult to identify due to the evolution and use of AI among bad actors, organizations will need to allocate appropriate resources and processes to uncovering this type of fraud. Moving forward, it will be critical for financial institutions, law enforcement agencies, and regulatory authorities to share information to better combat this synthetic-identity fraud.

Organizations also use AI technology (48%) to uncover these synthetic identities, proving that while the use of AI by bad actors still poses a threat to financial institutions, it can also be greatly beneficial in proactive detection of fraud, such as synthetic identities.

Nearly half of organizations have also used anomalies in identity elements (48%) and behavioral analysis (41%) to uncover synthetic identities. The evolution of behavioral analysis to incorporate both expertise in online user behavior and the psychology of cybercrime and social engineering has resulted in behavioral biometric intelligence, an integral tool in identifying fraud. Behavioral biometric intelligence leverages elements of user behavior like application fluency, data familiarity, and expert behavior to uncover fraud in the new-account opening process. It will be integral for financial institutions to apply behavioral biometric intelligence to gain insights that traditional fraud-prevention tools do not offer and successfully distinguish between legitimate users and cybercriminals.

PREVENTING FRAUD THAT FUNDS GLOBAL CRIMINAL ACTIVITIES

According to the U.S. Treasury's 2024 National Money Laundering Risk Assessment, fraud is the largest driver of money laundering activity, generating billions of dollars every year. Collaboration across entities and nations will be critical to fighting fraud effectively in 2024. Nearly all (97%) fraud management experts agree that nations should strengthen international cooperation to share intelligence and coordinate efforts in enforcing sanctions surrounding fraud or financial scams.

Virtual assets also pose a significant threat to the integrity of financial systems and combatting financial crime. The U.S. Treasury 2024 report noted: "While the use of virtual assets for money laundering continues to remain far below that of fiat currency and more conventional methods that do not involve virtual assets, U.S. law enforcement agencies have observed virtual assets being misused for ransomware, scams, drug trafficking, human trafficking, and other illicit activities." Indeed, two in five (42%) global respondents think that international collaboration will be key to combatting the use of cryptocurrencies to fund criminal activities.

Other critical approaches are:

- User-identity verification (**49%**)
- Stricter oversight (**45%**)
- Stricter penalties (**43%**)
- More transparency (**42%**)
- Self-regulation by platforms (**40%**)

Protection and Prevention

As threats evolve and grow increasingly advanced, financial institutions must also improve their protection and prevention strategies to keep up. Organizations can do this by implementing evolving technologies like AI in addition to tactics like behavioral biometric intelligence. Financial institutions can also collaborate with other banks, industry bodies, and law enforcement agencies to share information and ensure greater protection and prevention across the industry.

While organizations look to AI to improve protection and fraud-prevention capabilities, the technology continues to be a double-edged sword, with bad actors employing AI to develop increasingly advanced attacks. AI can be used to create deepfake videos, craft more realistic messages to be used in social-engineering attacks, clone voices to take advantage of voice verification systems, and more.

94%

of respondents say they anticipate leveraging AI to promote information-sharing across different banks about high-risk individuals in the next 12 months

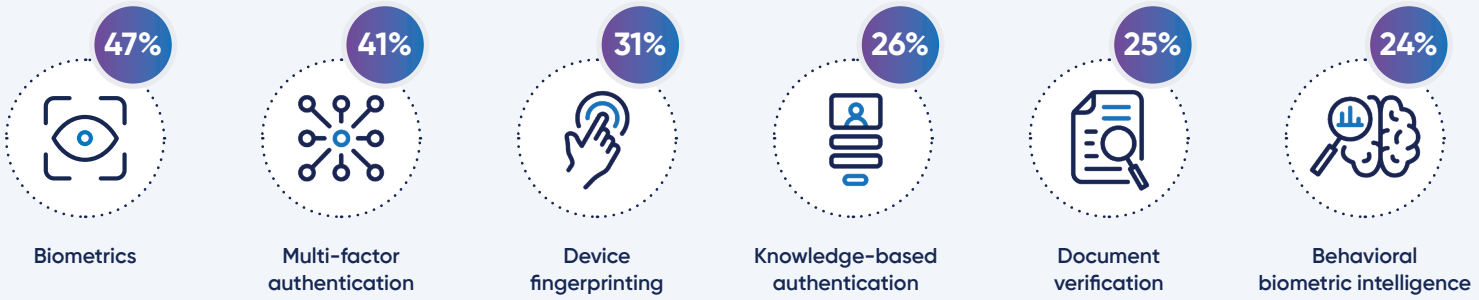
Financial institutions must implement broader information-sharing to bring attention to recent trends in financial crime and fraud. Nearly nine in 10 (88%) fraud decision makers say more[3] information should be shared between banks, financial institutions, and government or regulatory authorities in the next one to two years to combat financial crime and fraud.

While once considered cutting-edge and a promising answer to complex threats, voice verification will no longer be adequate for financial institutions to protect their customers. As such, financial institutions will need to use a strategic combination of authentication methods to minimize user frustration while maximizing protection. Notably, of the top authentication methods listed below, only behavioral biometric intelligence reduces friction for the end user.

3 Much more information / more information

The question must be asked: Why will biometrics remain the most widely adopted method of banking customer authentication for 2024 given its historical ineffectiveness against fraud and financial crime? Organizations must evolve protocols and utilize the vast trove of historical data collected around customer behavior through behavioral biometric intelligence. Failing to embrace behavioral biometric intelligence, coupled with a lack of information-sharing across the industry, will allow financial criminals to continue to win.

What methods of authentication for customers will be most prominent in your organization in 2024?



From customer idiosyncrasies to their digital habits, behavior is the only element of digital identities that is uniquely human. Paying close attention to customer behavior and intent behind the biometrics, device, geo-location, and other machine-created signals can ensure financial institutions truly know their customers. By applying methods like fraud telemetry, continuous behavioral sequencing, and predictive intelligence, leading financial institutions and banks can keep customers safe from digital fraud and build long-lasting trust. For financial institutions and banks to adapt and appropriately tackle the obstacles presented by modern financial crime and fraud, they must use and share behavioral biometric intelligence if they hope to leap-frog criminal innovation and protect customers.

In addition to expanding authentication methods, financial institutions should focus on educating customers around the risks of AI. Many organizations are already taking steps to support customers that fall victim to AI scams like Elon Musk's crypto investment YouTube deepfake, including:

- Providing educational resources on identifying scams, including AI scams (**45%**)
- Offering additional customer support for scam-related inquiries (**41%**)
- Running awareness campaigns on AI-related risks (**41%**)
- Collaborating with law enforcement for investigations (**40%**)
- Using AI scam detection tools or filters (**38%**)
- Providing guidelines for safe online practices (**38%**)
- Refunding or returning stolen funds (**27%**)

By employing behavioral biometric intelligence and educating customers on AI-driven scams or risks, financial institutions can ensure their organization and customers are better protected in the future.

Future of AI

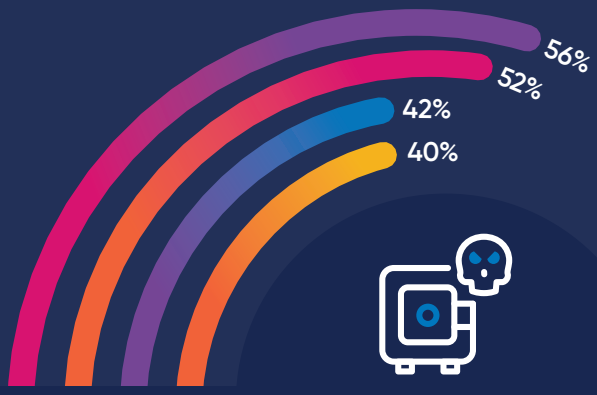
Despite the concerns surrounding AI, experts in fraud management, AML, and risk and compliance are confident that AI will lead to more positive outcomes than negative results.

69%

believe AI will lead to more revenue (i.e., improved customer interactions, less time spent investigating false positives, etc.) than loss (i.e., fraud, breaches, etc.)

Those in APAC are most confident that AI will lead to more revenue (73%), followed by North America decision makers (64%). According to respondents, AI is also expected to impact several areas of financial-crime prevention, from detection to compliance.

Respondents in EMEA also believe that regulatory compliance will be affected by AI, with half (50%) reporting that regulatory compliance will be most impacted by AI in 2024 in comparison to decision makers in North America (37%) and APAC (35%).



Areas of financial crime that will be most impacted by AI in 2024

- Fraud detection
- Cybersecurity
- Money laundering prevention
- Regulatory compliance

As to whether AI will positively impact their organization's ability to comply with regulatory requirements, the jury is still out. While 43% think the use of AI has made it more difficult[4] for their organization to comply with regulatory requirements, approximately an equal percentage (46%) believe it has made it easier[5] to comply.

AI will also prove useful in combatting various activities, attacks, and threats, from social-engineering attacks to identity theft and even check fraud. Organizations who are not investing in AI in 2024 are at risk of missing out on the additional protections and benefits the technology can provide.

Types of activities, attacks, or threats AI will be most useful in combatting

40% Payment fraud

35% Identity theft

34% Ransomware attacks

31% Social-engineering attacks

4 Much more difficult / somewhat more difficult
5 Much easier / somewhat easier

ABOUT THE STUDY

The findings detailed in this report are based on data collected by TEAM LEWIS through an online survey of 600 professionals within fraud management, anti-money laundering, and risk and compliance. All respondents were of manager-level or above at banking or financial services companies in the United States, Canada, France, Germany, Spain, the United Kingdom, the United Arab Emirates, Netherlands, Sweden, Australia, and India. There were 200 responses per region (North America, EMEA, and APAC). Data was collected from January 19 to February 2, 2024 with a margin of error of +/- 3.9 percentage points.

ABOUT BIOCATCH

BioCatch stands at the forefront of digital fraud detection, pioneering behavioral biometric intelligence grounded in advanced cognitive science and machine learning. BioCatch analyzes 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 more than 180 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.

Conclusion

Financial institutions and banks are facing numerous threats in 2024 and beyond. From combatting global financial crime to protecting their organization and their customers from fraud, banks will need to do even more in the future.

Threat actors are sharing intelligence among themselves. Shared intelligence allows attackers to evolve and succeed, even though banks are investing more in technology to detect and prevent fraud and financial crime. This is of great importance, especially as the consequences of fraud and financial crime grow in impact and monetary value. Banks, financial institutions, and regulatory authorities must share more information to stand a chance against combatting and preventing financial crime and fraud in 2024.

Despite financial institutions increasingly investing and employing technologies like AI and behavioral biometric intelligence, experts and practitioners in the industry largely expect financial-crime and fraud activity to continue to increase in the next year. This finding shows that the current level of investment is simply not enough. Banks will need to adopt a new approach to successfully combat fraud and financial crime. Banks who are not investing in innovative approaches to detect financial crime and fraud will put themselves and their customers at great risk.

Global fines for AML and other financial crimes grew by **50%** in 2022 to almost $5 billion

Financial institutions must evolve and transform to survive this unprecedented era of rapidly increasing fraud and financial crime. By understanding what makes their customers uniquely human, financial institutions can protect customers from even the most advanced types of fraud while providing the simple, personalized customer experience that drives brand loyalty.

With more than a decade of data analysis, 90 registered patents, and unmatched expertise, BioCatch continues to lead innovation to address future challenges.

For more information, please visit www.biocatch.com.