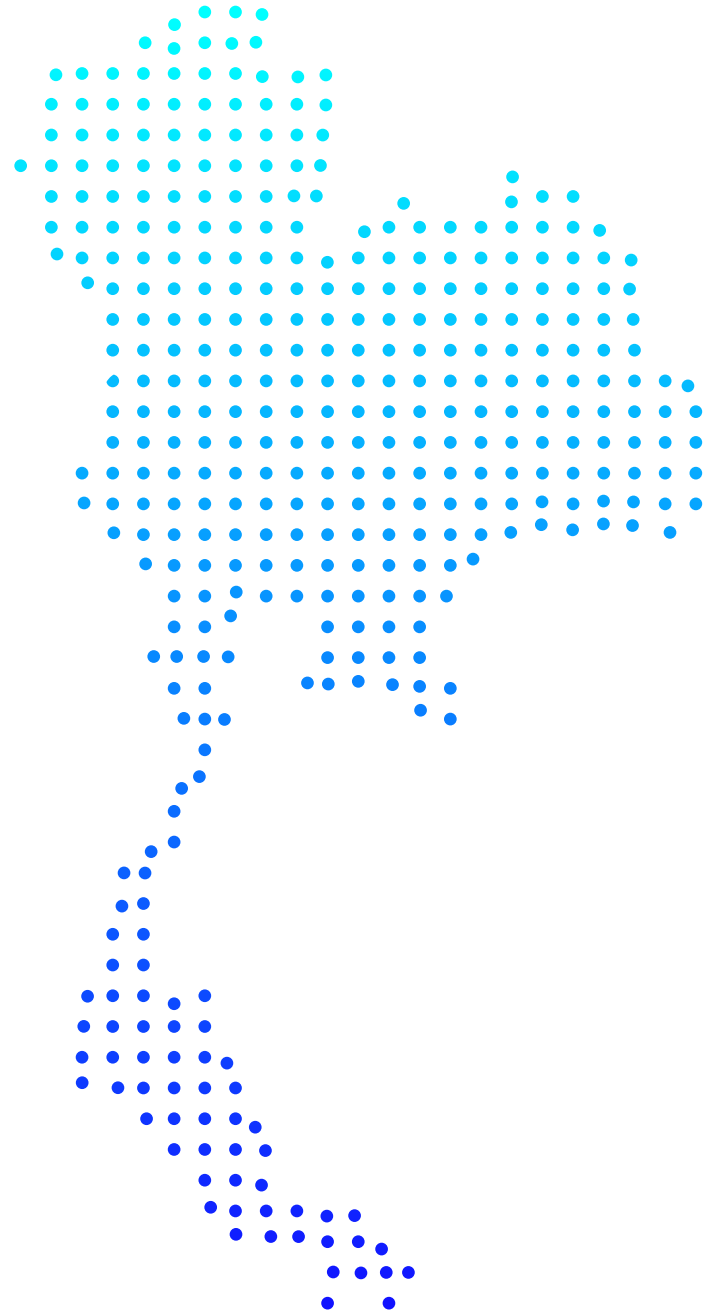


A survey of banking leaders on fraud risk

2026 THAILAND EDITION



The outlook in Thailand

Thai banks in 2026 grapple with protecting their customers from investment fraud rings and call center scams, while working to unveil sprawling networks of mule accounts across the entire Thai banking system. Criminal groups pose as bank officials, police officers, or representatives of government agencies, persuading victims to transfer funds and install malicious remote-access applications. The rapid growth of mobile banking and real-time transfers via PromptPay has accelerated digital adoption across Thailand, but it's also shrunk the window in which banks have an opportunity to detect and stop authorized push payment (APP) scams. Readily available AI tools, social media targeting, and cross-border scam compounds operating in the region have industrialized social engineering and expanded its reach.

Thai banks are also navigating a shifting regulatory and policy environment. The Bank of Thailand has introduced stricter measures to combat mule accounts, strengthen digital identity verification, and improve transaction monitoring, while collaborating with the Thai Bankers' Association and telecom providers to disrupt scam networks more quickly. Expectations around customer protection and reimbursement are rising, alongside requirements to balance frictionless digital experiences with stronger authentication and real-time fraud controls.

This survey offers a snapshot of how fraud and financial-crime leaders at Thai banks see the moment: where operational strain is intensifying, which threats pose the greatest systemic risk, and how prepared institutions feel for the technological, criminal, and regulatory shifts reshaping Thailand's financial ecosystem.

- 01** *CURRENT FRAUD
LANDSCAPE IN
THAILAND*
- 02** *FRAUD CONTROLS
AND EFFICIENCY*
- 03** *ASSESSING THE
CONSEQUENCES
OF FRAUD*
- 04** *REIMBURSEMENT*
- 05** *THE FUTURE OF
FRAUD IN THAILAND*

ABOUT THIS SURVEY

BioCatch commissioned a series of anonymous surveys of a combined 1,200 banking leaders in 12 different geographies. All respondents were of manager level or above and worked in their bank's fraud or financial crime department. One hundred individuals were surveyed in each of the Benelux region (Belgium, the Netherlands, and Luxembourg), France, Germany, Indonesia, Italy, the Nordics (Denmark, Finland, Norway, and Sweden), Saudi Arabia, Singapore, South Africa, Switzerland, Thailand, and the United Arab Emirates.

The surveys were conducted between Dec. 15, 2025 and Jan. 6, 2026.

Within the respondents from Thailand, 75% identified themselves as the primary decision maker within their departments, while 21% said they influenced decision-making. 34% of those surveyed were managers or senior managers, while 23% identified as directors or senior directors. The remaining 43% were vice president level or above. 18% were members of their bank's C-suite.



01 Current fraud landscape in Thailand

63%

**OF THOSE SURVEYED BELIEVE
FRAUD ATTEMPTS AT THEIR
ORGANIZATION ARE INCREASING**

52%

**SAY FRAUD LOSSES AT
THEIR ORGANIZATION
ARE INCREASING**

80%

**ESTIMATE THEIR INSTITUTION'S
ANNUAL FRAUD LOSSES
EXCEED \$5 MILLION**

The majority of those surveyed in Thailand report fraud attempts increasing at their institution – in line with both regional and global averages. We see concern intensify among senior leaders: Nearly three-quarters of Thai banking leaders of vice president level or above reported increases in fraud activity at their organization in the last year. Thai respondents identified social engineering scams and mule accounts as their top fraud concerns, highlighting the growing impact of organized crime and the money laundering networks through which it launders its money.

The same pattern holds for losses: While a little more than half of those surveyed in Thailand saw fraud losses rising at their bank, the C-suite once again painted a far grimmer picture, with 78% of respondents reporting growing fraud losses. The gap suggests executives may recognize the aggregate financial and reputational impact of fraud, particularly as large-scale scam operations and organized fraud networks continue to target Southeast Asian markets.

What stands out most is the scale of Thailand's financial exposure. Eight in 10 Thai banking leaders surveyed estimate their bank's annual fraud losses at greater than \$5 million – well above neighboring countries and even exceeding the global average. Among the C-suite, this was unanimous, with all C-level execs reporting annual losses of greater than \$5 million, 55% reporting annual fraud losses of greater than \$10 million, and 16% indicating their bank lost more than \$25 million to fraud every year.

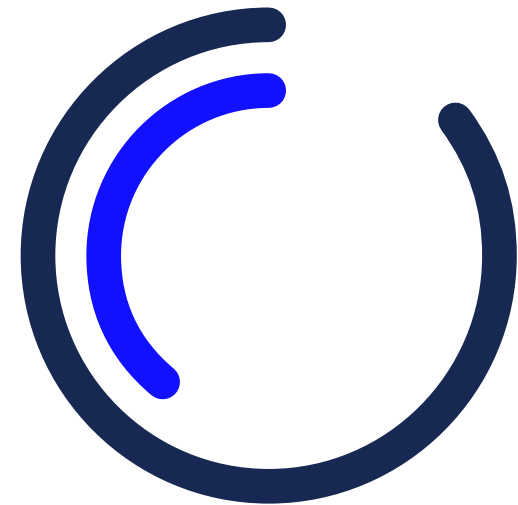
02 Fraud controls and efficiency

While, overall, Thai banking leaders expressed confidence in their existing fraud defenses, a closer examination reveals signs of operational strain. 39% do not rate their fraud controls as effective, placing Thailand behind both neighboring markets and global benchmarks on perceived control strength.

Nearly one-third of those surveyed in Thailand reported false positive rates of greater than 60%, while 71% of respondents said their existing fraud solutions came with a false positive rate above 40%. Both figures are greater than regional and global averages.

Only 24% of those surveyed said their bank fully investigates fraud cases within one day. Machine learning adoption among respondent banks stands at 42%, again trailing both neighboring markets and the global average. This combination of elevated false positives, slower case resolution, and comparatively lower advanced model usage suggests existing controls are not yet delivering optimal precision or speed.

Thai banks do appear to recognize the need for improvement. While just 10% of those surveyed indicated their organization was actively upgrading its fraud defenses, 85% said their bank was at least exploring new solutions.



39%

**BELIEVE THEIR CURRENT
FRAUD CONTROLS ARE
NOT EFFECTIVE**

85%

**SAID THEIR BANK WAS AT LEAST
EXPLORING NEW SOLUTIONS
TO DEPLOY**

03 Assessing the consequences of fraud

QUESTION: Which impact of fraud and scams is of greater concern for your organization?

73%

RANKED THE REPUTATIONAL RISK OF FRAUD AND SCAMS AS A GREATER CONCERN THAN FINANCIAL IMPACT



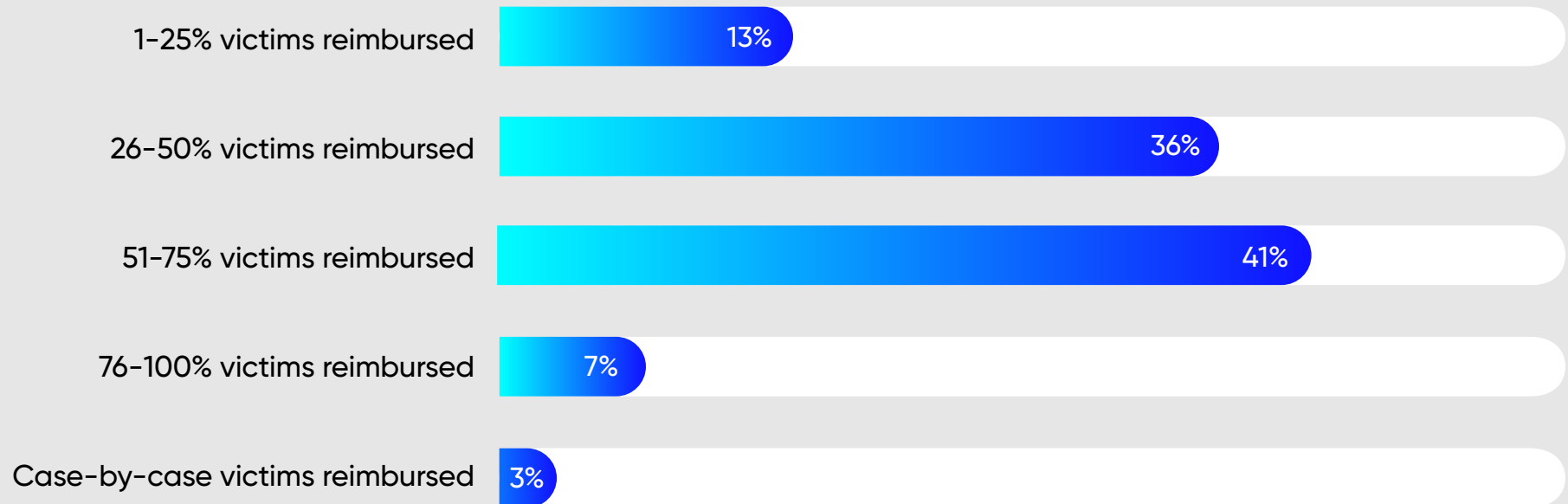
Thai banking leaders indicate the reputational damage inflicted by fraud and scams concerns them more than any economic consequences. Fraud in Thailand appears not only a financial vulnerability but also a trust and brand risk that can quickly escalate, particularly in a highly connected and socially active market where customer complaints and scam stories can spread rapidly.

Interestingly, those working on fraud teams at Thai banks report less concern about reputational damage (50%), suggesting their focus may be more operational and loss-driven. This split points to a strategic tension. Operational teams manage immediate fraud impact, while leadership weighs direct financial exposure, potentially underestimating how closely financial loss and reputational harm are intertwined in the long term.

● 56% Reputational impact ● 27% Both equally important ● 17% Financial impact

04 Reimbursement

QUESTION: What percentage of customers who fall victim to scams does your organization reimburse?



With 48% of Thai respondents indicating their bank reimburses at least half of scam victims, Thailand's reimbursement rate both aligns with those of neighboring markets and sits above the global average. The largest share falls in the 51–75% reimbursement range, indicating many organizations are willing to absorb a substantial portion of losses to preserve customer relationships and trust.

At the same time, relatively few Thai banking leaders reported reimbursing more than 75% of scam victims at their organization, while a notable portion capped reimbursement at 50% or below. This suggests a more balanced stance, protecting customers while maintaining shared responsibility. The distribution reflects an industry navigating the trade-off between customer expectations, financial impact, and the risk of creating a moral hazard, especially as scam volumes continue to rise.

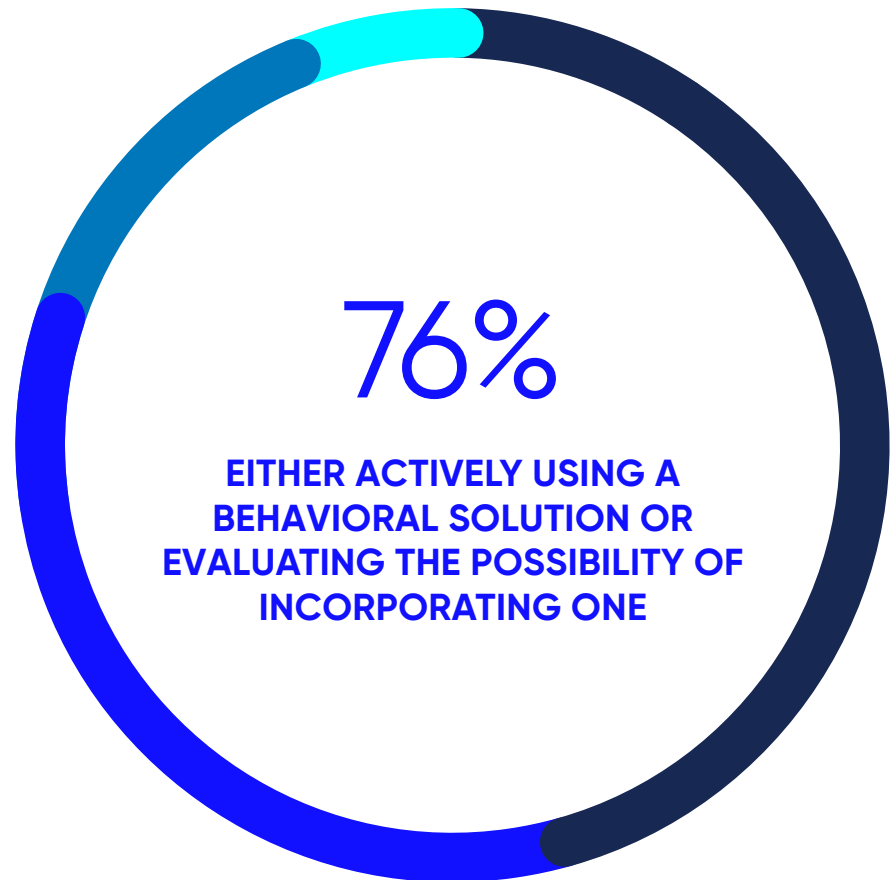
05 The future of fraud in Thailand: Human behavior

Thai respondents reported a higher adoption rate of behavioral solutions than banking leaders in any other of the 12 geographies surveyed.

While 44% of Thai banking leaders indicated current use of a behavior-based solution, an additional 32% planned to incorporate one, showing continued momentum. More than half of those surveyed in Thailand view behavioral solutions as highly valuable. This figure rises to 70% among those working on fraud teams in the country.

Thai banks clearly recognize transaction data alone is no longer enough to combat the fraud (social engineering, mule recruitment, deepfakes, AI tools, etc.) of the present or the future.

It is worth noting, however, that not all behavior-based solutions are created equal, as we see reflected in fraud attempts, fraud losses, and the perceived threat posed by mules in Thailand.



46% actively using it

34% evaluating the possibility of incorporating it

14% planning to evaluate incorporating it

6% no usage and no intention of using it

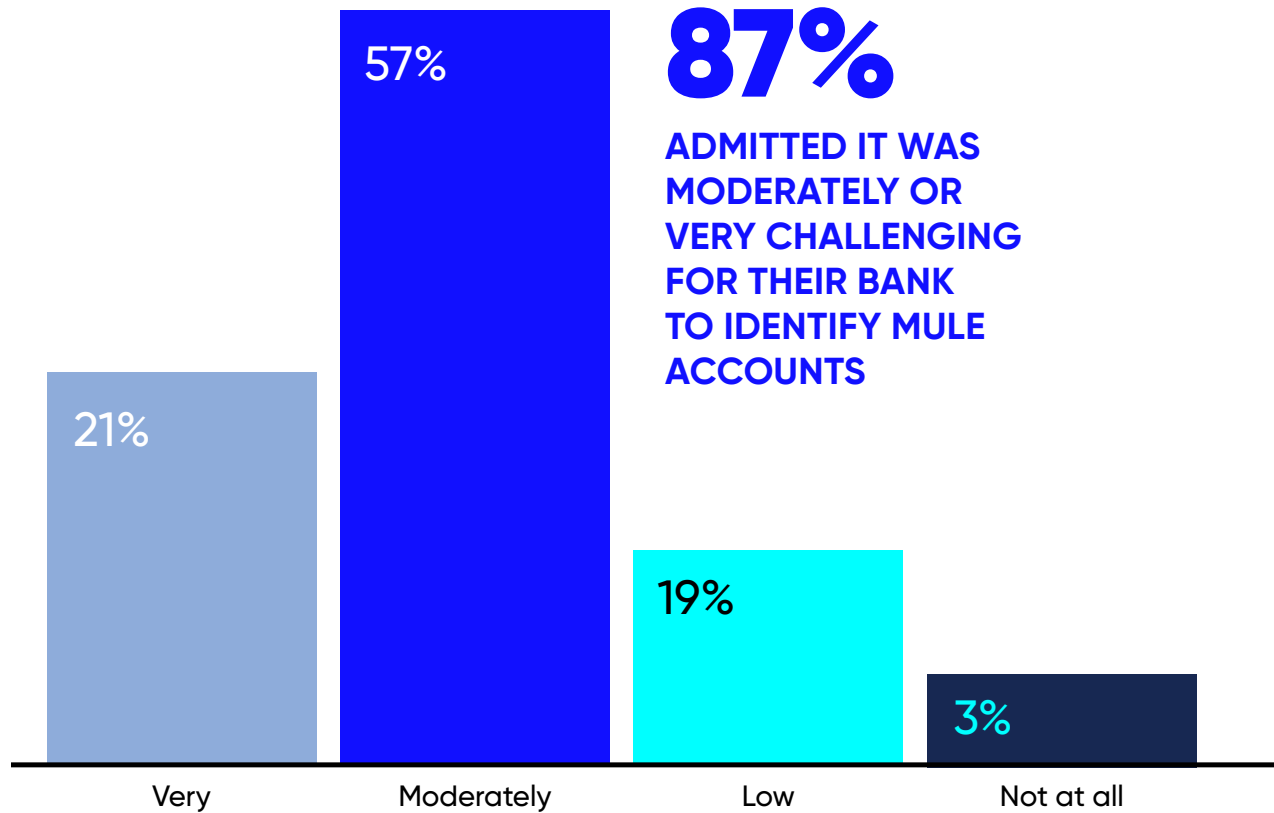
05 The future of fraud in Thailand: Mule network challenges

Thai banking leaders overwhelmingly (97%) report feeling prepared for Bank of Thailand expectations around authentication, mule prevention, and PromptPay security, indicating strong regulatory alignment and internal focus on tightening controls.

At the same time, nearly all respondents (87%) say that identifying mule accounts reused across multiple institutions remains a significant operational hurdle. This highlights the structural nature of mule activity, how accounts are not confined to a single bank, and detection becomes far more complex once funds and identities move across institutional boundaries.

While individual Thai banks may feel prepared from a policy and control standpoint, effective mule disruption will increasingly depend on cross-bank intelligence sharing, ecosystem-level monitoring, and faster collective response mechanisms rather than siloed defenses.

QUESTION: How challenging is it identify inter-bank money laundering networks?

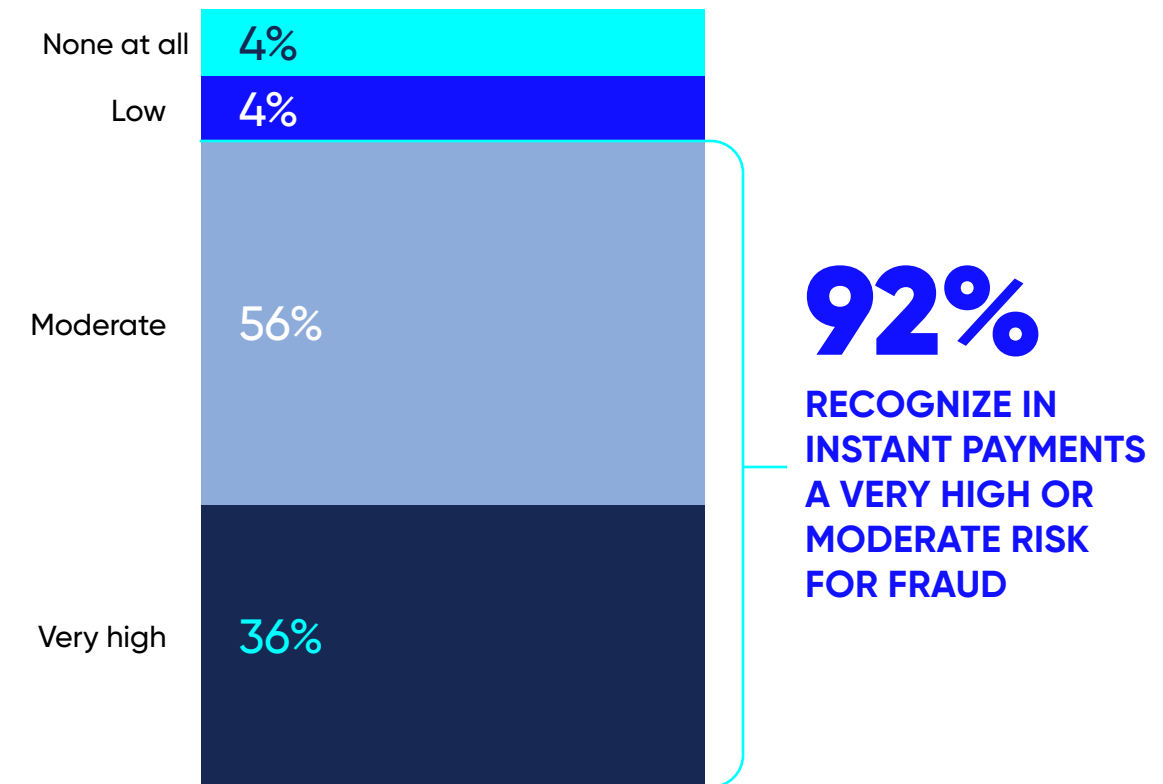


05 The future of fraud in Thailand: Real-time risk

Real-time transfers are widely viewed as a significant fraud risk in Thailand, with 92% of Thai banking leaders recognizing in instant payments a very high or moderate risk for fraud. The speed of instant payments compresses decision windows and limits recovery options, making them the preferred channel for moving funds through mule accounts once a victim has been compromised.

This directly connects to the mule challenge highlighted on the previous page. When mule accounts are reused across multiple banks, instant transfers allow fraud networks to fragment and disperse funds within seconds, reducing traceability. In that context, managing real-time risk is not only about stronger authentication at the point of payment, but also about coordinated, cross-bank visibility to detect and disrupt mule activity before funds disperse throughout the system.

QUESTION: How much fraud risk, if any, do you see within instant transfers?



ABOUT BIOCATCH

BioCatch prevents fraud financial crime by recognizing patterns in human behavior, continuously collecting more than 3,000 anonymized data points – keystroke and mouse activity, touch screen behavior, physical device attributes, and more – as people interact with their digital banking platforms. With these inputs, BioCatch's AI and machine-learning models reveal patterns in user behavior and provide device intelligence that, together, distinguish the criminal from the legitimate. The company's Customer Innovation Board – an industry-led initiative in partnership with American Express, Barclays, Citi Ventures, HSBC, Macquarie Bank, National Australia Bank, and others – collaborates to pioneer innovative ways of leveraging customer relationships for improved fraud detection. Today, more than 30 of the world's largest 100 banks and 340 total financial institutions deploy BioCatch solutions, analyzing 17 billion user sessions per month and protecting more than 660 million people on more than 1.6 billion devices around the world from fraud and financial crime.

www.biocatch.com E: info@biocatch.com [X @biocatch](https://x.com/biocatch) [in /company/biocatch](https://in.company/biocatch)

©BioCatch 2026. All Rights Reserved.

