



 **BioCatch** | **Report**

2026

DIGITAL BANKING FRAUD TRENDS IN LATIN AMERICA

BioCatch report on the current
and future digital fraud
landscape in Latin America

March 2026



About this report

This report offers a comprehensive perspective on the current threat landscape and banking fraud trends in Latin America.

To create this report, BioCatch's team of experts – led by its global fraud intelligence team and supported by its local global advisory and threat analytics teams – conducted extensive research, compiling proprietary BioCatch data from 36 Latin American financial institutions serving an estimated more than 300 million customers.

In this report:

- Threat landscape in Latin America
- 2025 country-specific observations
- Manufactured trust: Voice scams and how to stop them
- The half of fraud no one is watching: A blind spot in digital transfers
- Case study: Latin America's RAT problem

Current threat landscape in Latin America

155%

increase in reported social engineering scam cases between 2024 and 2025

42%

increase in reported money mule accounts

2.7x

more account takeover attempts

5x

more incidents of fraud attempts utilizing remote access tools

Trends:

- Social engineering scam attempts against Latin American consumers increased by 155% in 2025 from the year before, with notable increases in investment, purchase, impersonation, and one-time-password-based scams.
- While Latin American banks deploying BioCatch solutions reported 42% more money mule accounts, our customers in Argentina recorded a 27% decline in mule activity. In May of 2025, three Argentinian banks announced the launch of BioCatch Trust Argentina, the hemisphere's first real-time, inter-bank, behavior-based, fraud and financial crime intelligence-sharing network.
- Account takeover attempts at Latin American financial institutions ballooned by 155%. Banks in Mexico reported the greatest spike, with a massive 324% increase in account takeover attacks, while Colombian financial institutions saw a 188% spike.
- Across the region, malware attacks increased by 225%, and stolen device cases surged by 344%.
- Latin American financial institutions documented a 409% increase in fraud attempted via remote-access tools, aligning with documented growth in voice and investment scams in the region, forming a full social-engineering-to-account-control chain.

2025 country-specific observations



Manufactured trust: Voice scams and how to stop them

By **Josue Martinez**

Voice scams continue to pose a major and growing challenge for Latin American financial institutions. Designed to create urgency, these scams often convince their victims of some immediate risk to their financial health: the detection of unauthorized charges, a compromised account, or suspicious activity.

In many cases, the fraudster poses as a bank employee and shares information that appears credible, sometimes including personal or account details the victim assumes only the bank would possess. This establishes trust between the caller and the customer. As the conversation continues, that trust deepens. The customer grows increasingly confident they're speaking with their bank and receiving legitimate assistance, too often agreeing to authorize real transactions to resolve these invented issues. Once the transfer is authorized, the money is gone – and in many geographies, the victim has no course for reimbursement.

From the bank's perspective, these transactions appear genuine. They're approved by legitimate customers, who legitimately believe they're doing the right thing.

Breaking that trust established between scammer and account holder is not easy. Even those banks that send customers real-time alerts warning them of the potential riskiness of a transaction find customers choosing to believe their scammer over their bank.

BioCatch approaches scam prevention from a different perspective, complementing traditional fraud signals with intelligence that supports real-time decision-making. The model relies on collaboration among financial institutions to identify risk indicators associated with the account receiving a transaction. Behavioral intelligence plays a central role by providing context around how a

transaction is performed, while additional signals – including device data, location, and behavioral patterns – help create a multi-layered view of risk.

This approach goes beyond analyzing transactional data alone. By combining behavioral, device, and contextual intelligence, banks can better understand the activity surrounding both the sending and receiving accounts and assess the likelihood that a transaction is linked to fraud.

In May of 2025, we launched the western hemisphere's first real-time, behavior-based, fraud and scams intelligence sharing network. **BioCatch Trust Argentina** evaluates the risk of both the sending and receiving account to gain a more complete view of a transaction. With visibility into both sides, institutions can generate clearer indicators of risk or legitimacy before funds are transferred.

Collaboration among financial institutions also enables faster responses. When risk signals are shared and acted upon in real time, banks can reduce fraud losses, limit the movement of illicit funds, and lower false positive rates. Just as importantly, these protections help preserve trust between customers and the financial system.

In many scam and credential-theft cases, the receiving account shares characteristics with mule networks used to collect and move stolen funds. These accounts – sometimes structured as baskets or smurfing networks – are controlled by third parties whose goal is to quickly disperse illicit proceeds across multiple destinations.

Even within a small portion of the broader universe of transactional and behavioral data, patterns emerge that help identify these networks. When institutions are able to recognize those signals early, they gain a powerful tool to protect customers as soon as a scam attempt begins to unfold.


Sebastian Cafaro

Santander Argentina head of fraud prevention

The half of fraud no one is watching: A blind spot in digital transfers

Over the last decade, the massive digitization of users has transformed how and where people bank. It's also opened up a new attack surface.

Digital fraud has grown exponentially in both volume and sophistication. Account takeover attacks and instant transfer scams have both grown dramatically all around the world. It's not just basic phishing anymore. Today, fraudsters operate like corporate entities: They exchange techniques in forums, sell information and access in instant messaging applications, package and list ready-to-use attacks on criminal e-commerce sites, and professionalize social engineering with artificial intelligence.

Meanwhile, banks and fintechs have invested millions into AI tools, behavioral intelligence, device intelligence, and strong authentication (such as physical biometrics and FIDO2).

And yet, digital fraud continues to grow. Why?

The blind spot: The target account

There is one variable that fraudsters cannot avoid: They need a destination account to move the funds.

Paradoxically, the receiving account is one of the least analyzed parts of any transaction. In most prevention models, the focus is on the customer who initiates the operation: their session, their behavior, their device. But when a transfer is authorized, many times only "half the risk" is being assessed.

The other half – the account that receives the money – is often analyzed with limited signals or fragmented negative lists.

The collaboration that does not arrive

Despite technological sophistication, the financial sector faces a structural barrier: the lack of open exchange and quality of information between competitors.

The reasons are multiple:

- Restrictions related to data protection
- Absence of an impartial figure to manage the exchange
- Business interests that make it difficult to share sensitive information

In Latin America, there are regulatory attempts such as the negative bases of PIX in Brazil or the CPF of COELSA in Argentina. Both share databases of accounts, devices, and users determined to have previously partaken in fraud and financial crime. These initiatives are limited to confirmed fraud data and come with some doubts about the quality of the information. They do not build dynamic intelligence or predictive scores.

The advanced collaboration scheme: BioCatch Trust

Facing these limitations, Santander Argentina partnered with two other banks in the country to address our receiving account blind spot outside of regulation.

This is how BioCatch Trust was born in Argentina: a private collaborative initiative to build real-time scores on target accounts.

The approach seeks to change the traditional logic:

- Analyze the transactionality and profile of the target account
- Combine the history of the destination account as the payer
- Generate a real-time score and risk indicators

This new approach enables us to:

- Increase fraud capture when traditional scores show medium or low risk
- Reduce friction in high-risk trades when the destination account demonstrated signs of trustworthiness

The outstanding question

The success of this real-time intelligence-sharing raises a key question: Can the financial industry fight fraud without structural collaboration?

In an ecosystem where fraudsters share information in real time, competition between banks can become our greatest weakness. In fraud prevention, our rivals are not other banks. Our rivals are the attackers.

Case study

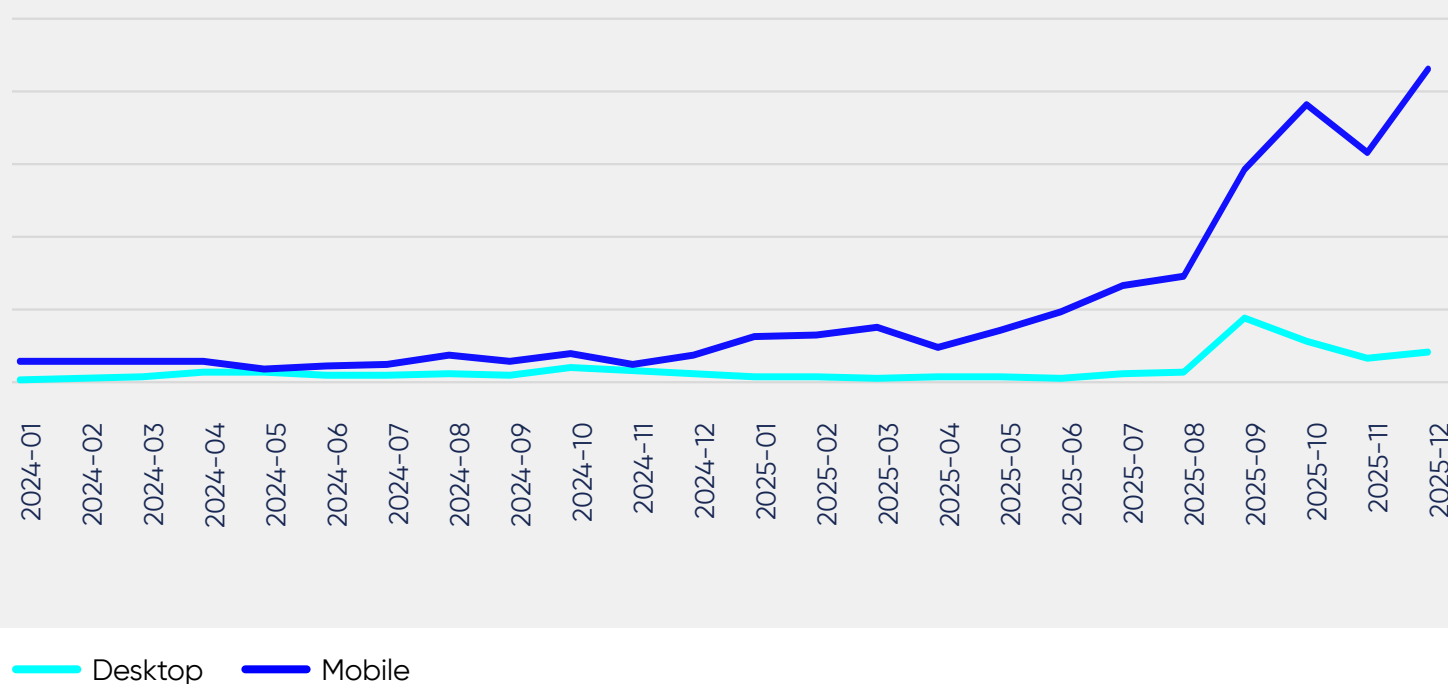
Latin America's RAT problem

Growing trend

Banks in Latin America increasingly see remote access tool (RAT) activity concentrated on mobile devices. While desktop RAT volumes remained relatively flat in 2025, mobile-based RAT activity accelerated sharply, particularly in the second half of the year. The chart above shows sustained and concentrated growth across mobile channels, indicating that mobile has become the preferred environment for executing remote access fraud.

Rather than signaling a sudden leap in sophistication, this shift likely reflects a common fraud adaptation cycle. In many regions, fraud initially relies on phishing and basic credential abuse. As authentication controls strengthen and simple account takeover becomes less reliable, attackers gradually move toward real-time social engineering and remote device control. The rise of mobile-based remote access in Latin America aligns with this broader pattern of tactical adjustment, where fraud evolves in response to defensive pressure rather than through entirely new techniques.

Total RAT sessions per month by device



Case study

Latin America's RAT problem

Why fraudsters prefer mobile sessions

The duration of remote-access sessions on desktop vs. mobile devices helps explain why we see fraudsters gravitating toward mobile apps.

Desktop RAT sessions last significantly longer, with the average session lasting 660 seconds and the median session lasting around half that long. The gap between those two figures indicates some very long remote-access sessions, extending well beyond the typical the typical RAT session length..

Longer sessions likely reflect a more cumbersome fraud journey. Perhaps the fraudster had to spend more time coordinating the handoff of control with the victim, navigating complex desktop interfaces, handling authentication challenges, or resolving technical issues inherent to remote desktop control. The more time a fraudster spends in a session, the higher the likelihood of friction, victim hesitation, technical issues, or detection controls increasing operational cost and reducing scalability.

Mobile app sessions, by contrast, are shorter and more tightly distributed. The average mobile RAT session lasts just 316 seconds, with a median of 199 seconds, suggesting faster, more consistent, and standardized execution. Mobile banking apps are generally task-oriented and streamlined, enabling faster navigation and transaction completion once control is established. Shorter sessions reduce exposure time and allow fraudsters to process more attempts within the same window, improving efficiency and output. This structural efficiency advantage provides a clear operational incentive for the observed shift toward mobile-based remote access activity.



Desktop

Average RAT session:
660 seconds

Median RAT session:
342 seconds



Mobile

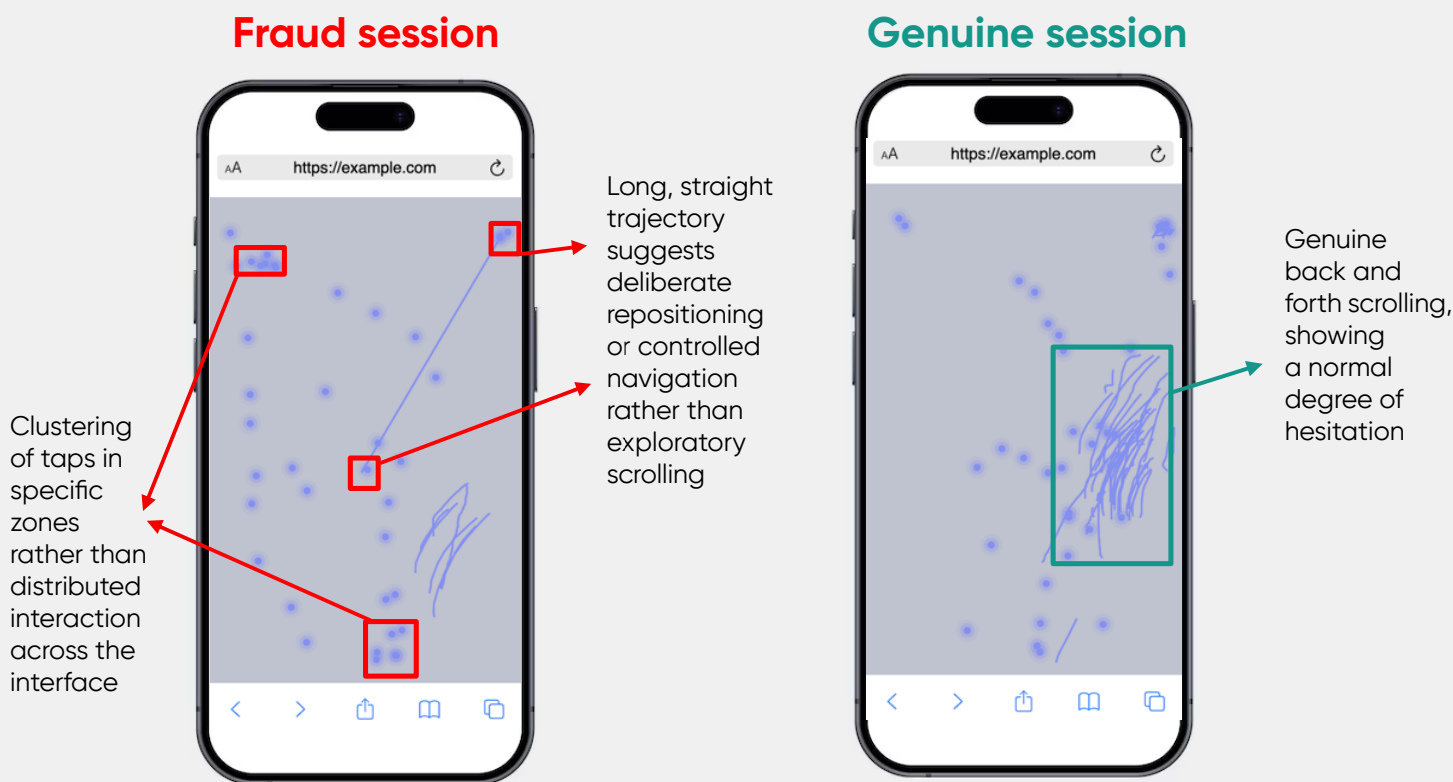
Average RAT session:
316 seconds

Median RAT session:
199 seconds

Case study

Latin America's RAT problem

How BioCatch detects mobile RATs



The images above show two different digital banking sessions accessing the same account from a mobile app.

In the fraudulent RAT session, we see linear and purposeful scrolling, which not only deviates from the user's historical behavior but is also often a tell-tale sign of remote-access fraud. The user in this session also navigates quickly from one functional step to the next with minimal deviation or hesitation. We see no exploratory gestures or corrective movements. The touch paths are direct and efficient, suggesting the operator knew exactly where to go and what to do.

In the genuine session, we see noticeably more scrolling. The customer appears to review content, adjust positioning, and navigate with small corrections and variable rhythm. The scrolling patterns are uneven and dispersed, reflecting reading and verification behavior. The genuine session shows human hesitation and interaction variability, while the fraudulent session reflects decisiveness and procedural execution with no visible uncertainty.

Case study

Latin America's RAT problem

How BioCatch detects desktop RATs

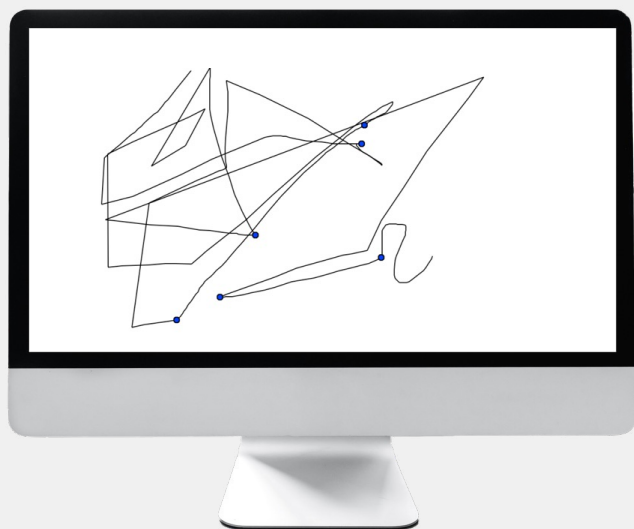
The images above show two different digital banking sessions accessing the same account from a desktop portal.

The fraudulent session shows erratic, angular cursor paths, with sharp jumps and overlapping movements – patterns common in cases of remote-control usage vs. natural, hand-driven navigation. In contrast, the genuine session displays smoother, more deliberate movements, with subtle corrections and controlled positioning before clicks.

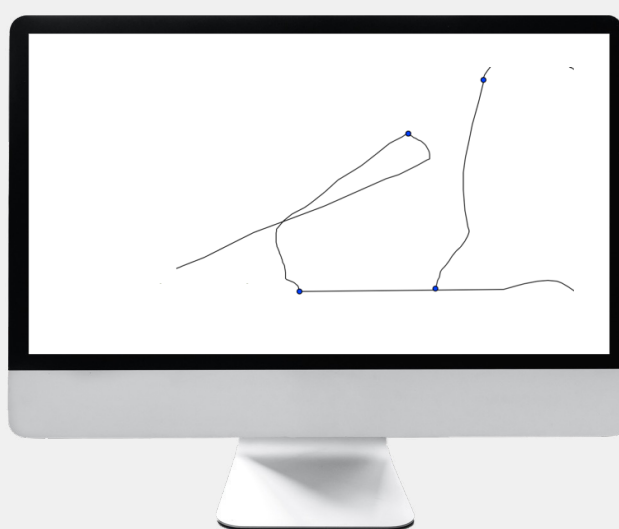
The fraud case is further supported by multiple environmental and behavioral risk indicators, including concurrent sessions, new device and IP signals, mismatching time zones, screen resolution anomalies, persistent remote access flags, and elevated device risk, all combined with risky transactional behavior.

A notable element in the fraud session is a prolonged 10-minute pause mid-flow. In desktop remote access scenarios, such inactivity often reflects operational friction, such as coordination with the victim or overcoming authentication barriers. This inefficiency contrasts with the faster, more streamlined execution commonly seen in mobile RAT cases and reinforces the narrative that desktop remote access is slower and more operationally demanding, helping explain the shift toward mobile channels.

Fraud session



Genuine session



Case study

Latin America's RAT problem

Takeaways



Remote-access fraud is increasing throughout Latin America. While desktop RAT remains present, activity is increasingly concentrated on mobile channels, reflecting tactical adaptation by fraudsters.



Desktop RAT sessions tend to be longer and more operationally taxing, often showing friction and pauses. Mobile app sessions are shorter, more structured, and more scalable, making them a preferred execution channel for fraudsters seeking efficiency and reduced exposure time.



Across both desktop and mobile cases, RAT sessions exhibit structured navigation, compressed execution timing, environmental anomalies, and interaction patterns that differ from organic user behavior. These signals expose externally guided or controlled activity even when transaction types appear legitimate.



BioCatch correlates device context, session flow, interaction dynamics, and historical behavioral baselines to identify remote-access activity in real time. By aggregating multiple risk dimensions, the platform distinguishes genuine users from externally controlled sessions with high confidence.

About BioCatch

BioCatch prevents fraud and 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](mailto:info@biocatch.com) [X @biocatch](https://twitter.com/biocatch) [in /company/biocatch](https://www.linkedin.com/company/biocatch)

© 2026 BioCatch. This content is a copyright of BioCatch. All rights reserved. Any redistribution or reproduction of part or all of the contents in any form is prohibited other than the following:

- You may print or download to a local hard disk extracts for your personal and non-commercial use only.
- You may copy the content to individual third parties for their personal use, but only if you acknowledge the document and BioCatch as the source of the material.
- You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any other website or other form of electronic retrieval system without our express written permission.