BioCatch | Solution Brief

Scams360

Combine behavioral, device, and transaction intelligence to stop major scam types with ONE single solution.

STOP scam payments in real-time, cut operational costs and protect your reputation.

Scams never stop evolving. From romance and investment scams to business email compromise and purchase fraud, today's threat landscape extends far beyond just impersonation scams. To stay ahead of this endless evolution, financial institutions must adopt fraud defenses able to combat the full spectrum of authorized push payment (APP) scams across all channels.

Impersonation scams
Purchase scams
Business email compromise
Romance scams
Investment scams

Where legacy scam solutions fall short

Traditional fraud defenses – often based on device or network intelligence, or rule-based solutions – now find themselves unable to address the full spectrum of Authorized Push Payment (APP) fraud. These legacy solutions fail to detect the subtle, human-driven manipulation that defines modern scams, resulting in large quantities of false positives. Because APP fraud involves the deceived customer willingly authorizing the payment, traditional systems are fundamentally limited in their ability to intervene.

Without behavioral intelligence, financial institutions lack the contextual understanding needed to distinguish genuine user intent from signs of manipulation across the wide array of scams occurring globally. This behavioral blind spot leaves both the customer and the institution dangerously exposed, undermining scam-detection efforts and putting brand reputation and trust at risk.

An ongoing and escalating threat

$1.03T

stolen by scammers in 2024, according to the Global Anti-Scams Alliance (GASA).

1 in 2

were exposed to more scams in the last 12 months than they were in the previous 12.

70%

did not report the scam to law enforcement.

Source: GASA Global Scam Report 2024

Introducing Scams360 from BioCatch

Scams360 is a breakthrough behavioral intelligence solution that builds on our proven success in stopping impersonation scams and extends protection across major APP scam typologies. By analyzing user behavior in real time across a variety of digital channels, Scams360 detects multiple different cognitive behaviors pertaining to scams.

Cognitive behaviors pertaining to scams

Pressured?

Are there signs of faster navigation and data entry? E.g., are the session times longer with signs of dictation and coercion?

Confused?

Does there seem to be unusual mouse behaviour? E.g., excessive movement, scattered clicks and repeated interactions.

Hesitant?

Are there signs of hesitation with mouse activity? E.g., pauses before clicks, smaller movements, and slower cursor speed.

Frustrated?

Is the user input erratic? E.g., rapid mouse movements, forceful clicking, and typing mistakes.

Distracted?

Are there periods of inactivity with no keyboard interaction? E.g., doodling with mouse, and highlighting page contents.

How Scams360 differentiates itself

50%

Increase in detection of investment, romance, purchase and BEC scams

1%

Alert Rate

Scams360 helps financial institutions detect and prevent a variety of scam types with one solution. Unlike legacy tools, it monitors the entire digital session and not just isolated events, giving teams real-time visibility into risky behaviors before a payment is authorized. It works seamlessly across both web and mobile channels, ensuring consistent protection regardless of how customers choose to bank. With the risk assessment Scams360 provides, banks can choose the kind of user treatment they prefer to deter users from making payments to scammers.

Our approach to scam detection

To effectively detect scams where the user is coerced into sending money to a scammer unwittingly, we analyze a combination of subtle behavioral signals to help accurately detect scam risk. Key indicators may include whether the user is on an active call during a transaction, as well as increased "dead time," which can indicate hesitation or distraction. Additional red flags include signs of screen sharing or remote access (often used by fraudsters to guide victims through the payment process), and unusually long payment completion times. These data points, when assessed together, help surface high-risk activity that may otherwise appear legitimate to historical fraud solutions.

Case study

Here are key some observations and metrics observed from an investment scam in 2025.

90%
of reported fraud payments happened while the **user was on an active call.**

70%
of all payment activity received a **high social engineering scam score** at the point of payment.

42%
of **dead time** seen in some of the fraud sessions, suggesting the user is distracted.

80%
of payments took place on a device with **screen broadcasting,** suggesting potential passive RAT.

3 vs 9
Time taken to execute a payment in minutes (fraud vs genuine) is three times longer for genuine payments.

To learn more about how we detect investment scams, along with other forms of social engineering such as romance scams, business email compromise, purchase scams, please request an Intelligence Briefing.

Want to know more?

Request an intelligence briefing at **info@biocatch.com**

The most effective way to tackle all forms of APP fraud is by embedding behavioral intelligence into your fraud prevention strategy. Join us for a 30-minute introduction to BioCatch, where we'll explore your fraud challenges and discuss how we can help address them directly.

About BioCatch

BioCatch prevents 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 machine-learning models reveal patterns in user behavior and provide device intelligence that, together, distinguish the criminal from the legitimate. The company's Client Innovation Board – an industry-led initiative in partnership with American Express, Barclays, Citi Ventures, HSBC, 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 267 total financial institutions deploy BioCatch solutions, analyzing 14.9 billion user sessions per month and protecting 511 million people around the world from fraud and financial crime. For more information, please visit **www.biocatch.com**.