

2026

GLOBAL SCAMS

Using behavioral and device intelligence
to shine a light on social engineering scams

October 2026

Scams by the numbers

35% increase in scams reported
by BioCatch customers in 2026



\$6,600

average case value
for investment scams



258%

increase in victims of
employment scams



90%

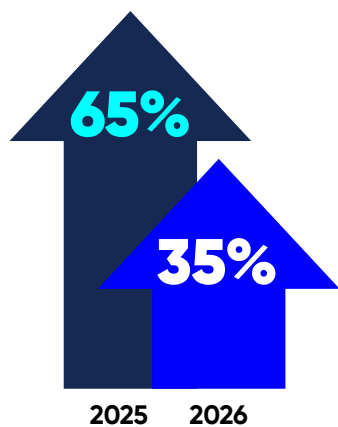
of all reported scam
attempts took place
on mobile devices



23%

increase in romance
scam attempts

Trend analysis



While a **35% increase in total scams** still represents a very significant rate of growth, it is substantially slower than the 65% figure we reported in 2025, suggesting those institutions utilizing behavioral intelligence are having greater success at combating scams than banks deploying point-in-time, rule-based defenses.

370
customers

21
different
countries

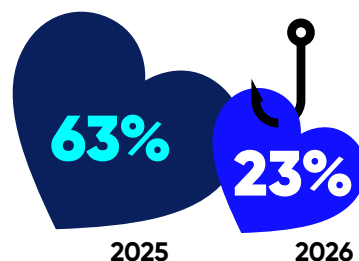
12
months



x3
increase of
reported
employment
scam victims

Among BioCatch's more than 370 customers in 21 different countries, employment scams increased more than any other scam type over the last 12 months. During that span, the number of **reported employment scam victims more than tripled**.

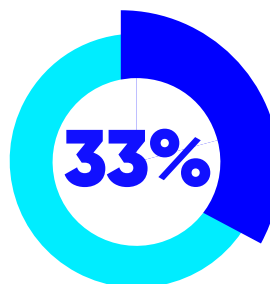
While impersonation and other voice-based social engineering scams also increased significantly in the last year, **romance scams saw the slowest rate of growth of any documented scam type, with a 23% increase in victims**. By comparison, last year's edition of this report documented a 63% uptick in romance scams.



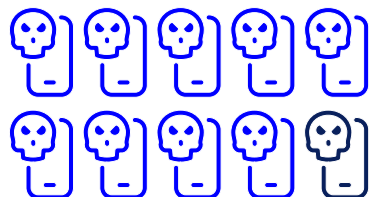
5x

greater value than
the overall average
of all scam types

Investment scams continue to account for the bulk of global scam losses, with the average investment scam case value reaching \$6,600 – nearly **five times greater** than the overall average of all scam types.



Purchase scams again retain the No. 1 ranking in terms of case volume, representing **almost one-third of all reported scams**.



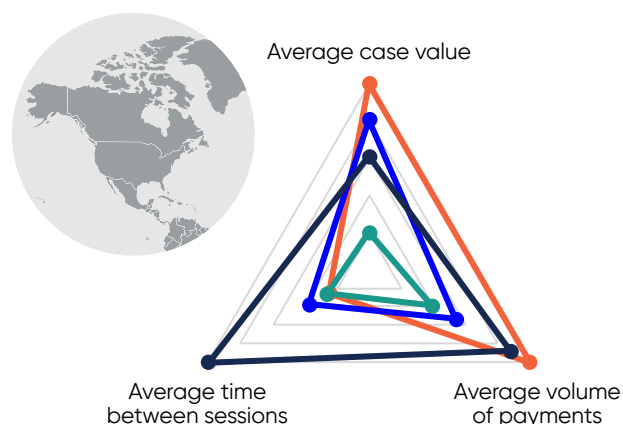
Nine out of every 10 scam sessions

now originates from a mobile device, **up by five percentage points from last year**. By comparison, traditional unauthorized fraud comes from mobile devices in just 75% of all cases.

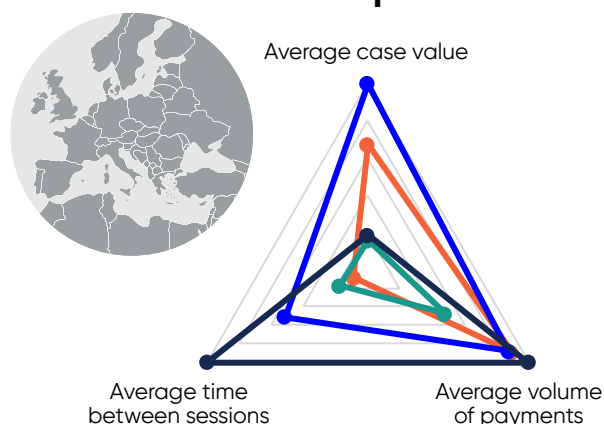
Scams: Breaking down the numbers by region

The analysis below examines four scam types (impersonation, investment, purchase, and romance) across three key areas: average case value, average time between sessions (i.e. duration of scam), and average volume of payments.

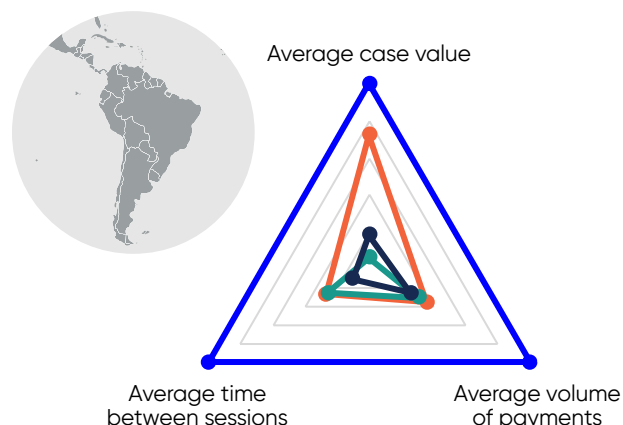
North America



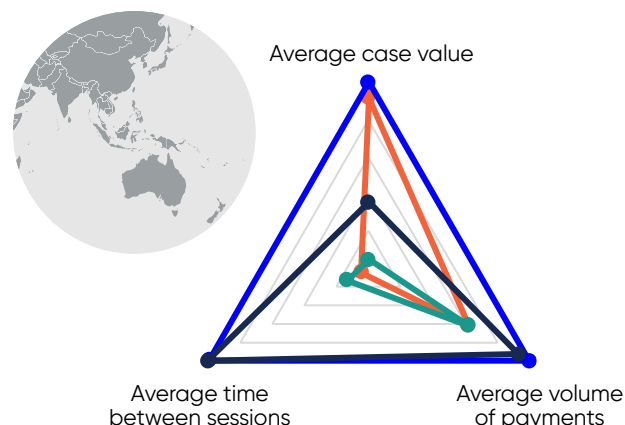
Europe



Latin America



Asia Pacific



■ Impersonation ■ Investment ■ Purchase ■ Romance

We observe a few stark differences in each of these scam types that remain mostly consistent across regions.

Purchase scams have the lowest average case value in every geography, while investment scams have the highest average case value.

In everywhere but Latin America, romance scams last longer than any other scam type, often taking place over weeks or months.

When it comes to the number of payments made, there is inconsistency across regions. The only consensus is that purchase scams often result in the fewest number of payments.



What Nigeria taught me about the global scam economy

Erin West | *Founder and executive director at Operation Shamrock*

This summer, on a rainy afternoon in Lagos, I sat in a living room with a 24-year-old man who has been scamming people for 12 years. Twelve years. He started when he was 12 years old.

The rain was coming down so hard on the tin roof that I lost some of his words, but I could tell very clearly he was completely comfortable describing his line of work the same way you would explain your job to a neighbor.

The Yahoo Boys are part of a loosely connected fraud culture that has existed in Nigeria for decades. Some work alone, others in small groups, using social engineering to target victims around the world. For some, the practice also incorporates spiritual rituals, such as charms or incantations, they believe can make victims more susceptible to manipulation.

I spent 26 years as a prosecutor. I've spent the last two years walking through scam compounds in Southeast Asia. I still was not ready for the scene I encountered in Nigeria. There was no barbed wire. No guard at the gate. Nobody locked in a room. Nothing about the setting suggested what was happening inside it. For the Yahoo Boy sitting across from me, the tools of the trade were remarkably simple: a phone, a script, a ritual, and a set of online accounts set up to receive American victims' money in half a dozen different forms before morning. The ritual might involve spices, potions, oils, or even a live chicken.

His operation is one small piece of a much larger fraud ecosystem, one our industry has paid far less attention to than the sprawling scam compounds of Southeast Asia. I flew to Nigeria in July to understand that ecosystem firsthand, meeting with prosecutors and investigators in Abuja and spending five days in Lagos with researchers, journalists, and people running the fraud themselves.

That experience challenged some of the financial industry's assumptions about how the global scam economy operates, what makes these crimes dangerous, and where financial institutions have the power to intervene. Nigeria's fraud ecosystem does not fit neatly into the model we have come to associate with industrialized scamming. It is a reminder that fraud does not have to look sophisticated to cause extraordinary harm, and that some of the opportunities to stop it may be closer than we think.

From Southeast Asia to Nigeria

One of the clearest lessons from the crackdown on Southeast Asia's scam compounds is that disrupting an operation does not necessarily dismantle the network behind it. My investigation in Nigeria offered some clues as to what can happen next.

In December 2024, Nigerian authorities uncovered a large-scale crypto-investment and romance scam operation running out of a seven-story building on Victoria Island. The Economic and Financial Crimes Commission arrested 792 people, including 148 Chinese nationals, in the raid. I learned of another Lagos scam operation that an investigator said had been seeded with money from an earlier Southeast Asian operation. Passports belonging to workers there showed travel from Cambodia.

These operations do not just resemble the scam compounds I have seen in Southeast Asia. There are signs of direct connections between the two. And they are not isolated. Weeks after the Victoria Island raid, authorities uncovered another operation in Abuja, arresting more than 100 people and seizing roughly as many workstations.

Nigeria's fraud ecosystem does not fit neatly into the model we have come to associate with industrialized scamming.

Taken together, these cases point to a larger challenge. As authorities crack down on scam compounds across the Mekong region, the criminal networks behind them do not simply disappear. They move. And when they do, they can hire locally.

Nigerian fraud never needed crypto

The arrival of the compound model is only part of the story. Nigeria already has a deeply established, decentralized fraud ecosystem.

And here is the part I really want banks to hear: This ecosystem doesn't rely on crypto.

Scammers take money however the victim can send it: gift cards whose numbers are shared over the phone, wire transfers, Venmo, Cash App, or peer-to-peer payments broken into amounts small enough to avoid detection. On the other end, that money often lands in mule accounts, including fintech wallets that take little more than a phone number to open. A scammer can use a single device to manage accounts under multiple names.

There is nothing exotic about any of this. Much of the money is moving through the same payment systems banks already monitor every day.

So, if a financial institution's fraud strategy has quietly turned into a crypto-fraud strategy, it may be looking past the channels these scammers are already using. I am not suggesting banks stop watching crypto. But they should not lose sight of the money moving through systems they can already see.

When the victim is a child

Here is the part that keeps me up at night. Some of the smallest payments moving through those systems can carry the highest stakes. The most devastating version of this crime is not aimed at the customer you are picturing. It is aimed at her son.

Financial sextortion targets boys, usually 13 to 17. A friend request comes in from what looks like a girl their age. The conversation gets flirtatious fast. Within a couple of hours, the scammer has talked the boy into sending a compromising photograph, and then the threats start: Pay or the image gets sent to his friends, family, or classmates.

The demand is deliberately small – \$100, \$200, a gift card – because that's what a 14-year-old can find at midnight. Start to finish, this can happen in a single evening while his parents are asleep down the hall.

At least 36 teenagers have died by suicide since 2021 in cases linked to financial sextortion. That is not my number. It is the number Financial Crimes Enforcement Network (FinCEN) put in front of compliance departments last September. And treat it as a floor, because it counts only U.S. reports. The National Center for Missing & Exploited Children (NCMEC) is now logging 137 reports of financial sextortion a day. Nobody has a global count of how many kids we have lost.

A Lagos professor who has been studying this for 20 years told me that all it takes to run a sextortion scam is a phone. That's it.

Boys are dying over amounts of money no monitoring system was ever built to notice. American banks cannot stop a scammer from sending that first message, but they can do something about what happens when the money starts to move.

13 to 17

age range of boys financial sextortion targets

36

teenagers have died by suicide since 2021 in cases linked to financial sextortion in the U.S.

137

reports of financial sextortion a day globally

What banks can do

So, here's what I am asking: Stop treating sophistication as the measure of risk. During my trip, I brought Nigerian investigators the case of an American victim whose deposits were followed within minutes by transfers of nearly the same amount into exchange accounts. There was little effort to disguise where the money went. It was crude, but it was fast. And that left a trail.

That trail is why the receiving side matters. Banks should watch it as closely as the sending side. Mule accounts are built to move money, not hold it. Money lands and leaves in a single sitting. And the behavior behind the account can offer clues, too. The person controlling the device often interacts with it very differently from the person whose name is on the account.

The victim's behavior can tell us just as much. A 14-year-old sending money at 1 a.m. to someone he met four hours ago or a retiree reading gift card numbers out loud while a voice on the phone coaches him: Those are the moments when a bank may still have a chance to intervene.

Reporting is not a dead end

The opportunity to act does not necessarily end once the money leaves the account. And this is where I think Americans get it wrong.

We assume that once stolen money reaches Nigeria, there is little anyone can do to recover it. That is not what I found. There are Nigerian investigators willing to work with us.

One investigator took an American police report, a pig butchering loss of about \$50,000, and followed the money through five bank accounts. He eventually traced it to two trucks purchased with the proceeds. He impounded the trucks and filed for civil forfeiture. That case is still on appeal, so I won't call it a victory yet. But think about what it means.

The money was never gone. It had become a truck. Under Nigerian law, investigators can seek to seize property purchased with the proceeds of fraud without waiting for a criminal conviction. A customer's money may still be recoverable even after the cash has changed hands or been converted into an asset.

But making that possible requires work from banks on the other side, too. Nigerian investigators need something they can act on. Banks can help by tracing where the money went and what it became, and by handing over the full picture, not a two-line referral investigators have to rebuild from scratch.

The part we can control

I keep thinking about that young man in the Lagos apartment and how little he needs to reach a family thousands of miles away. Social media. A script. A payment app. And a receiving account nobody looked at twice.

Financial institutions cannot stop that first contact. But they have visibility into much of what happens next.

So here is what I would ask the industry to consider, the same questions I ask every time: What if we looked harder at the receiving side this quarter instead of next year? What if we treated a 14-year-old's \$200 midnight payment like the emergency it can be? What if we built case files good enough that an investigator in Lagos could actually use them?

The scam compounds of Southeast Asia taught us to look for scale: rows of computers, entire buildings devoted to fraud. Nigeria taught me not to mistake scale for danger. Sometimes there is a seven-story operation with hundreds of workers. Sometimes there is a 24-year-old sitting in a living room with a phone.

Both can cause extraordinary harm. And both ultimately need somewhere for the money to land.

Banks can help by tracing where the money went and what it became, and by handing over the full picture, not a two-line referral investigators have to rebuild from scratch.

Using behavior to break the spell

When a scam is underway, the victim is rarely making decisions with a clear head. Scammers manufacture urgency, fear, or excitement with surgical precision. A fake fraud alert, a “final chance” investment, or a threatening call from “the tax office” forces the victim to make a snap judgment before they can properly consider the action they’re taking. Victims in this state aren’t being naïve. They are, in effect, temporarily not thinking like themselves. This is what fraud prevention teams increasingly refer to as being “under the spell.”

The challenge this creates for banks is counterintuitive: Telling the truth often doesn’t work. When a call center agent says “this looks like a scam,” the victim frequently disagrees, gets defensive, or repeats the scammer’s script back almost verbatim. Scammers are very good at preparing their victims for these convos: “The bank will try to stop you. Don’t listen to them. They don’t understand.”

Breaking the spell means something different from winning the argument. It means interrupting the psychological state itself, creating a pause, changing

the environment, or introducing a signal the victim’s own senses can’t dismiss the way they dismiss a stranger’s warning. Critically, the realization has to feel like it comes from the victim and not from their bank. A customer who is told they’re being scammed can double down. A customer who is shown their own behaviour – hesitation, being coached on a call, unusual navigation patterns – or prompted to notice it themselves is far more likely to break free of the spell on their own terms.

This is where behavioral intelligence becomes decisive. Rather than relying on a warning message to override the scammer’s narrative, banks can use behavioral signals – how someone types, pauses, navigates, or responds to prompts – to detect that a customer is in a coerced or induced state in real time, and to design interventions that create the conditions for the customer to break the spell themselves. The case study that follows illustrates exactly this: not a bank arguing with a victim, but a bank using behavioral evidence to help the victim see what’s happening to them.

Banks can use behavioral signals to detect that a customer is in a coerced or induced state in real time, and to design interventions that create the conditions for the customer to break the spell themselves.

Windows of opportunity

If we look at a typical scam session, there are often five main steps:

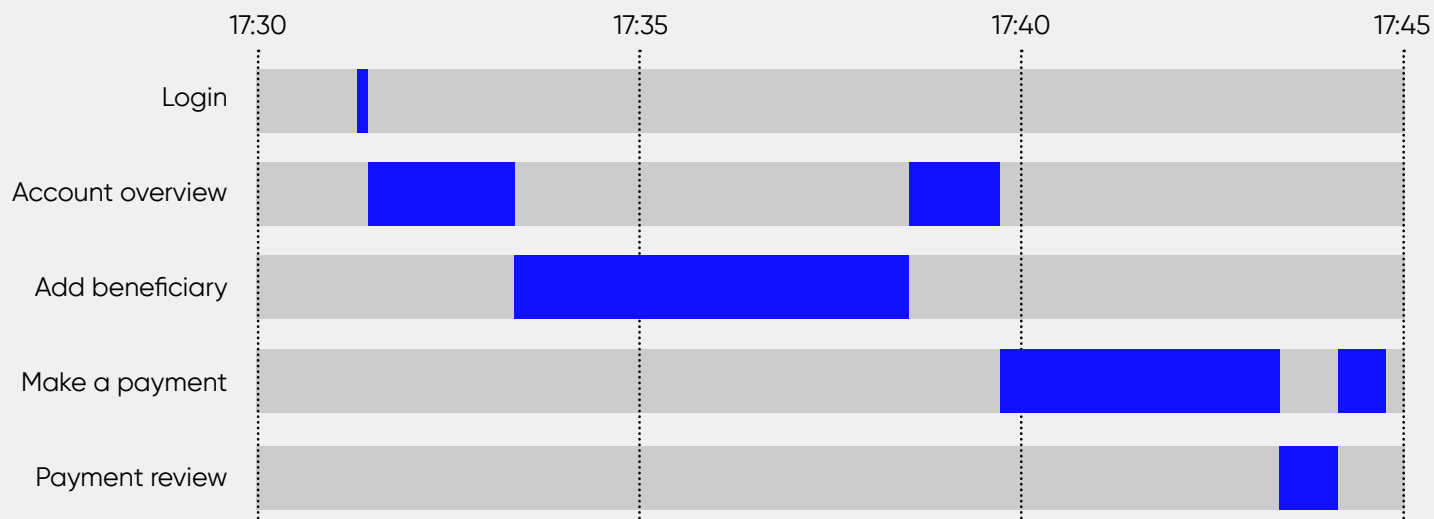


Traditional controls seek to stop the payment as the user is authorizing it.

Behavioral and device intelligence gives financial institutions opportunities to intervene well before the scam gets that far along.

In the case of the session below, we see the user navigating across five key parts of the journey. In each one, there are opportunities for the bank to engage with the victim to try and break the spell.

SESSION TIMELINE



Windows of opportunity



LOGIN



ACCOUNT
OVERVIEW



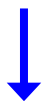
ADD
BENEFICIARY



MAKE A
PAYMENT



PAYMENT
REVIEW



At the point of login, there are several aspects that can indicate initial risk of the session that is being initiated.



Active call

The user is seen on an active call. While this alone is insufficient to determine whether it is a fraudulent session, it gives a signal that there is potential external influence.



Remote access software installed

Device analysis shows that the user has remote access applications installed on the device. The more recently this has happened, the greater the risk.



IDEAS TO BREAK THE SPELL

Reminding the user that the bank isn't on the phone with the customer may help the user question whether the call is genuine.

Windows of opportunity



LOGIN


ACCOUNT
OVERVIEW

ADD
BENEFICIARY

MAKE A
PAYMENT

PAYMENT
REVIEW


In the time after the login was successful and before the user begins to interact with payment journeys (account overview pages), we find other insights banks can leverage.

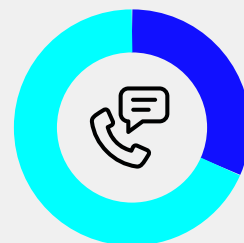


User inactivity

During the two minutes that the user is on the account overview pages, we see barely any activity. This could be a sign that the user is distracted.

DID YOU KNOW?

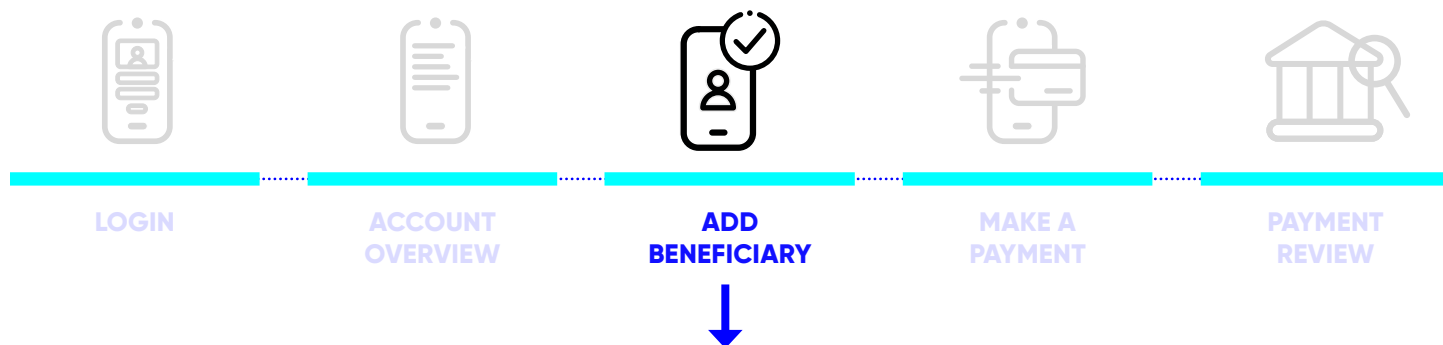
On average, 30% of activity that is reported as a social engineering voice scam has an active call during the session.



IDEAS TO BREAK THE SPELL

Messaging via pop-ups to continue planting the seed, e.g. "What are you looking to do today?" or "Do you need any assistance?"

Windows of opportunity



As the user navigates toward adding a new beneficiary, we see more signs of coercion.

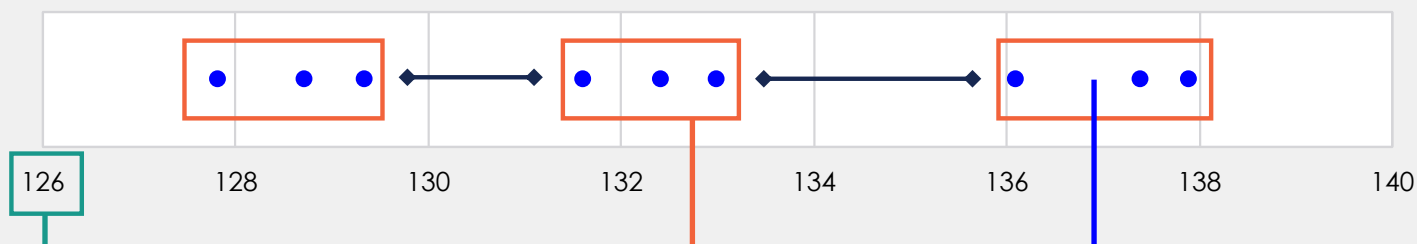


Typing dictated information

The way the user types suggests that the information they are entering is being dictated to them.

TYPING OF BENEFICIARY ACCOUNT NUMBER

Time to input (seconds)



Long delay to typing: User does not have the information readily available and is potentially waiting to receive information from someone else.

Numbers typed in groups of three: This is a common sign of dictation.

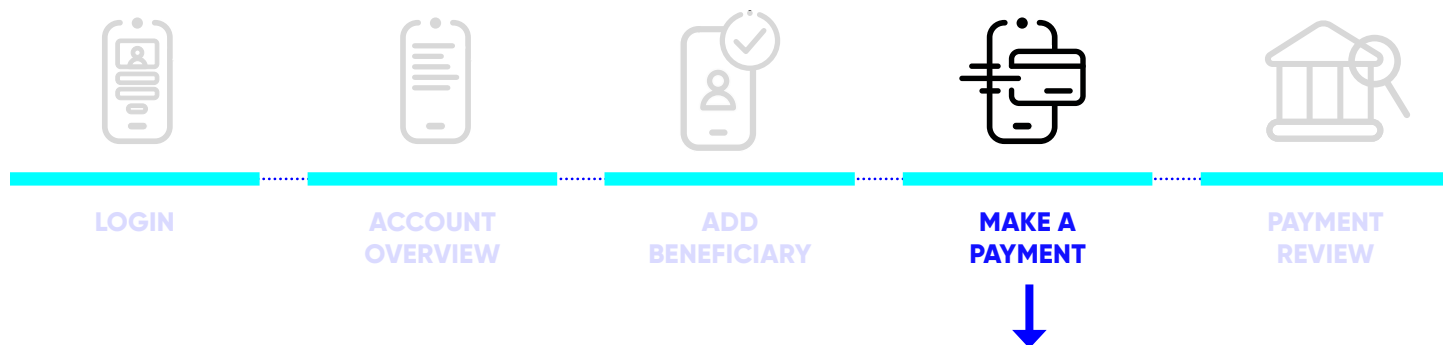
Short pauses between each group: Suggests the user awaits more information to enter.



IDEAS TO BREAK THE SPELL

Use a message to prompt the user to think about the situation. For example: "It looks like you may not be familiar with this account information. Remember that your bank will never give you instructions to make a payment. If someone is telling you to make a payment over the phone, hang up and call us."

Windows of opportunity



When processing the payment, there are further anomalies that introduce further risk.



New beneficiary

The user is paying the beneficiary for the first time. While not enough to prove on its own that the transaction is a scam, the additional context from previous flows increases the risk.



Risky amount

The transaction amount deviates significantly from the amounts historically transferred by the user.



IDEAS TO BREAK THE SPELL

A chatbot that leverages AI can enable the bank to have a conversation with the user. For example, when identifying a payment to a new beneficiary, basic questions about the relationship the user has with the beneficiary can help reinforce the need for caution. Likewise, identifying and clarifying motives behind the payment can lead the user to question if they're doing the right thing.

Windows of opportunity



LOGIN



ACCOUNT
OVERVIEW



ADD
BENEFICIARY



MAKE A
PAYMENT



PAYMENT
REVIEW



The final stage, at which point the user is reviewing the payment, provides interesting insights that confirm abnormal user behavior.



Touch event anomalies

As the user interacts with this journey, they exhibit nervousness, with excessive touch events.

The user is interacting with the screen very often, likely to keep the screen active to avoid a timeout. This is a common trait when a user is on the phone and distracted or awaiting instructions.

As the session progresses, we see the touch events become more frequent, often concentrated in the same area, suggesting the user may be feeling nervous.

Concentration of repeated touch events

Short swipes with thumb



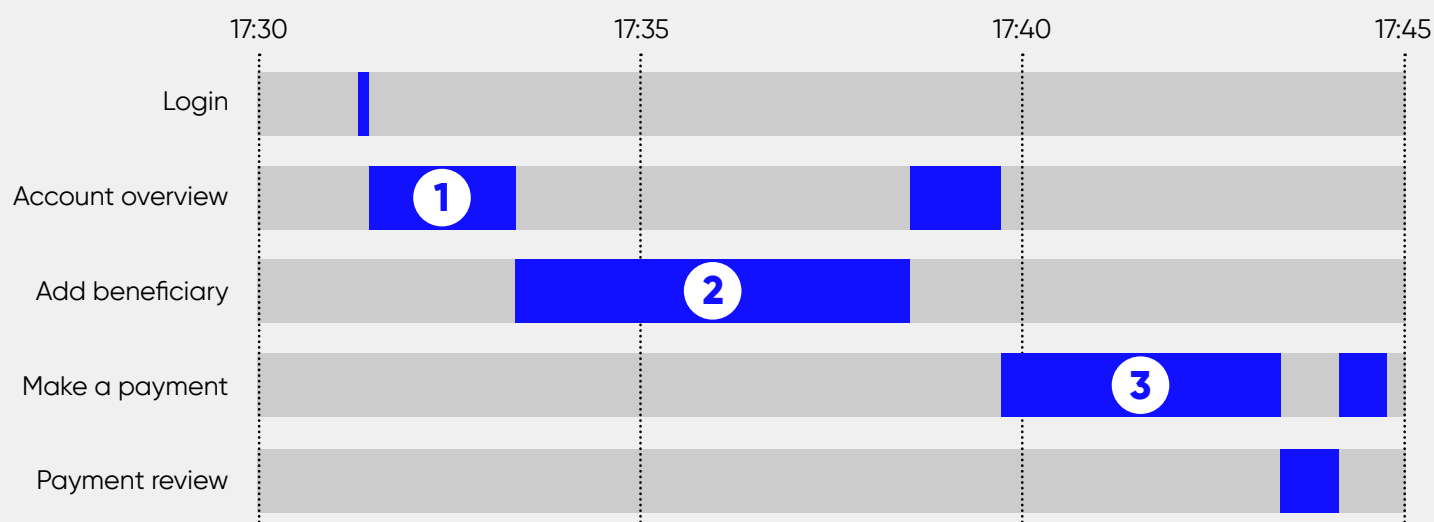
IDEAS TO BREAK THE SPELL

Ask the user further questions or send further reminders about exercising caution and the need to be aware when making payments to unknown people who reach out unexpectedly.

Proactive intervention

Returning to our case, we see that high risk was identified three times during the session, which was proactively communicated to the bank well before the payment authorization stage.

SESSION TIMELINE



- 1** High risk device information and initial contact with session shows the user is not executing the session with purpose.
- 2** Behavior observed while the user creates a new beneficiary suggests potential for a risky payment.
- 3** Final instruction of the payment confirms the risk previously detected, with additional signs of hesitation as the flow progresses.

The bank actioned this information by using dynamic messaging during the journey to provide warning signs to the customer. The nervousness that is detected as the session goes on suggests these warning signs were working. Eventually, after the final set of warnings we see the user hit a “back” button during the payment review stage and eventually abandon the payment before any score request is sent by the bank to BioCatch. Had the user continued, the session would have returned high-risk alerts and been blocked by the bank. This would have led to investigations and a likely conversation with the victim, during which time they could have insisted on the validity of the payment and sought its approval.

Instead, the bank saved the operational overhead on this case, thanks to the user realizing by themselves that the payment was not genuine.

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, AI agent usage, jailbroken devices, and more — as people interact with their digital banking platforms. With these inputs, BioCatch's AI and machine-learning models continuously assess both user intent and any signs of coercion or manipulation throughout every millisecond of every digital banking session, allowing banks to distinguish the criminal from the legitimate in real time. Insights drawn from across the entire network of BioCatch institutions further amplify the power and accuracy of that real-time risk-scoring. As of the end of H1 2026, more than 370 financial institutions deploy BioCatch solutions, analyzing 19 billion user sessions per month and protecting more than 760 million users on more than 1.8 billion devices around the world from fraud and financial crime.