BioCatch

BioCatch report

2025 DIGITAL BANKING FRAUD TRENDS IN THE UNITED STATES

BioCatch report on the current and future digital fraud landscape in the U.S.

September 2025

About this report

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

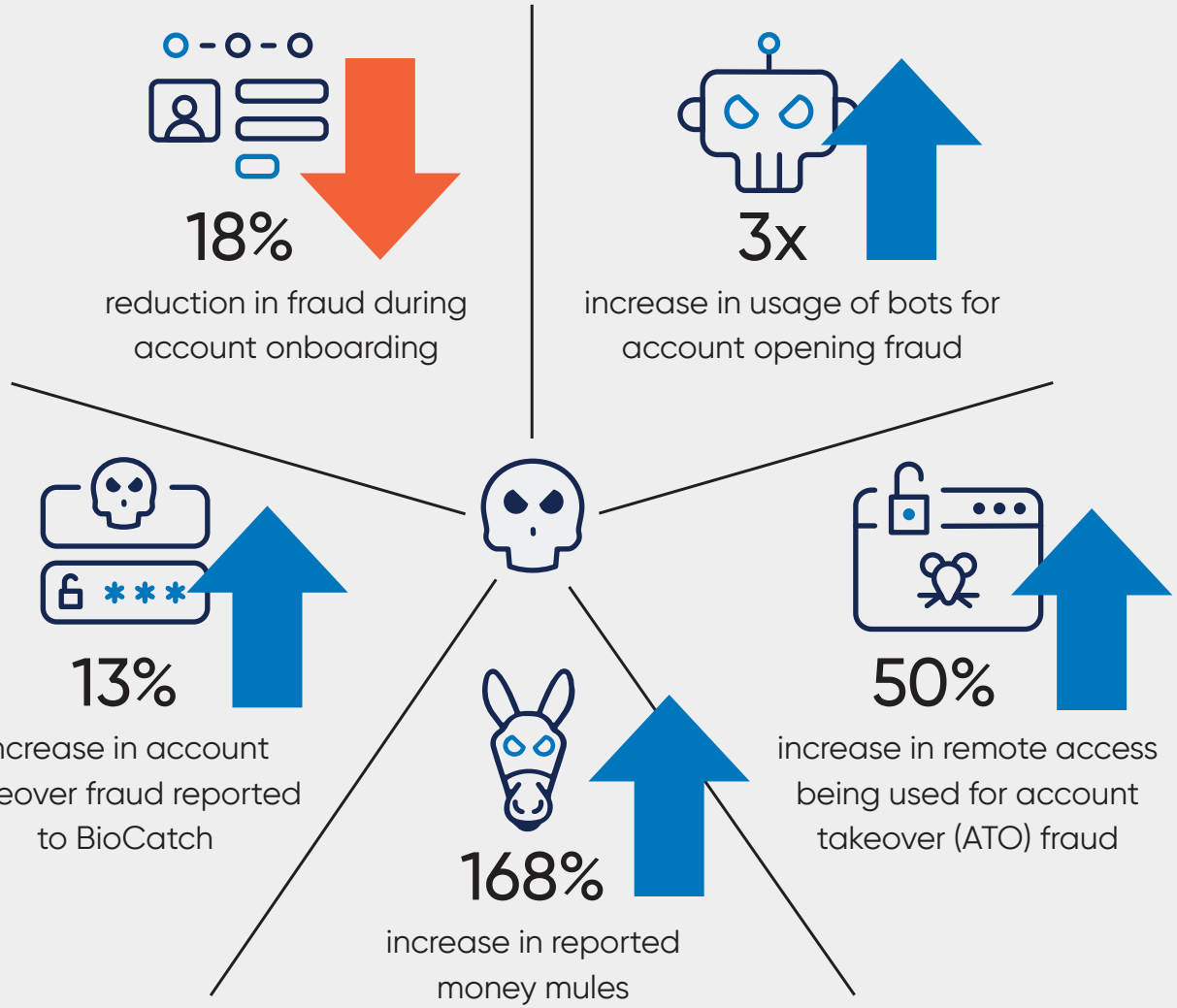
To create this report, the BioCatch team — led by its global fraud intelligence unit and supported by its local global advisory and threat analytics teams — conducted extensive research, combining proprietary BioCatch data from U.S. financial institutions with findings from third-party sources.

It offers an overview of the current threat landscape and trends seen across financial institutions in the U.S., based on our data and experience working with a variety of institutions across the country. There are two deep-dives into areas of particular concern: the threat posed by cryptocurrencies (as one of the main tools utilized by bad actors to off-ramp the illicit proceeds of fraud and scams) and the persistence of bots used to create accounts.

This report is presented in the following sections:

- Threat landscape in the U.S.
- Stablecoins: The new cashout method for fraudsters
- Case study: Using behavior to identify bots

Trends in customer data (first half of 2024 vs. first half of 2025):



$6.5 billion

Scams remain a top concern: Americans lost more than $6.5 billion to investment scams in 2024, according to FBI data.[1]

Key trends

Trends:

Social engineering scams remain the most common type of fraud in the United States, though the outlook appears more stable. Our data shows a slight drop in reported cases, mirroring Federal Trade Commission[1] data that reports more scam attempts but a 5% decline in cases where the victim lost money. The trend suggests banks and consumers are improving at spotting scams despite the rise in attempts.

Impersonation scams (in which criminals pose as trusted individuals or representatives of legitimate organizations to trick victims into sharing personal or financial information) and purchase scams (where criminals offer fake goods or services to steal payment) are the two most common scam types in the U.S. Yet, investment scams, which promise high returns on fraudulent or non-existent opportunities, account for both the greatest average loss per victim and the highest total losses of any scam type in the country. The latest annual report from the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3)[2] finds Americans lost more than $6.5 billion to investment scams in 2024.

Although it remains the most commonly reported fraud type in the U.S., deposit fraud has decreased in both account opening journeys and existing accounts.

Confirmed money mule cases have more than doubled in the first half of this year compared with the same period last year, marking a steep rise.

One emerging trend across U.S. financial institutions, while still low in total volume, is fraud executed from stolen devices. This method of operation has been detailed in BioCatch reports for other regions where it's more prominent. Criminals typically snatch devices on the street or in crowded areas, often while they are unlocked. In some cases, the criminals use shoulder surfing to obtain passcodes and unlock more functionality and access.

Something to keep an eye on: malware. While it's been a global menace for some time now, malware attacks have mostly spared those in the U.S. In recent months, however, our data shows more banks are paying attention to these threats. Banks are especially focused on web-based malware over mobile malware, which aligns with market trends.

1. https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports
2. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Thought leadership

America's scam crisis

Donna Turner
Risk Insight Solutions founder, former COO of the industry consortium behind the Zelle payments network, and PaymentSource's Most Influential Woman in Payments.

The U.S. today faces an increasingly complex and dangerous scam landscape, one that blends high-volume deception with high-severity financial harm. At the broadest level, we're seeing two scam categories dominate by volume: Impersonation scams, where fraudsters pose as trusted individuals or institutions, and purchase scams, which dangle fictitious goods and services to lure victims. These represent the majority of scam incidents and erode trust in everyday digital interactions.

When we shift from volume to severity, however, a different picture emerges. Investment scams remain the most devastating of all scam types, stripping Americans of billions of dollars and counting every year. These schemes typically lure victims with promises of outsized or guaranteed returns through opportunities in stocks, crypto, real estate, or other "can't-miss" ventures. In reality, they're sophisticated, emotionally manipulative operations, often staged over weeks or months to build trust.

I have long feared that the trifecta of fraud displacement from abroad, the rise and weaponization of advanced AI tools, and the complexity of the U.S. financial environment would combine to fuel an ever-expanding wave of successful scams against the American public. Sadly, that reality is here. More must be done to combat this growing threat to our communities, our financial health, and our national security.

Here's what I believe we must continue to advocate for in order to meaningfully reduce scam risk in the U.S.:

- Federal mandates for orchestration and accountability: Establish national oversight with the authority to align efforts, close gaps, and deliver measurable impact.
- Cross-sector safe harbors: Enable the aggregation and secure sharing of data and insights to accelerate the development and deployment of tech, tools, and processes in scam prevention and detection.
- Transparency and accountability from social media platforms: Require clear responsibility for preventing, detecting, and disrupting impersonation, purchase, and investment scams proliferating across their ecosystems.
- Centralized vetting and takedown capabilities: Proactively monitor and disable fraudulent entities posing as legitimate merchants or investment firms, supported by both technology and crowdsourced intelligence.

I do see signs of progress. Social engineering scams, which rely on psychological manipulation to trick people into sending money, clicking malicious links, or granting access to sensitive accounts, appear to be losing some ground. Reported cases may be up in terms of attempts, but the number of victims and, importantly, the financial losses are down.

Thought leadership

America's scam crisis

Donna Turner
Risk Insight Solutions founder, former COO of the industry consortium behind the Zelle payments network, and PaymentSource's Most Influential Woman in Payments.

That gives me hope. If success breeds success, we should ask: What's working?

- Tech: Microsoft deserves credit for blocking known scam sites, and Google continues to improve detection of fraudulent content while scanning messages for harmful activity.
- Financial services: Banks and institutions have stepped up technology and client education to help customers spot, prevent, and receive alerts on suspicious activity.
- Nonprofits and media: Using the passion and power of their reach, they are helping to spread the word of these hideous crimes.
- Telecom: Are we seeing signs of positive impact from STIR/SHAKEN, the U.S. framework to stop caller ID spoofing? One report indicates more than 80% of all call traffic between top carriers is signed and verified. But fraud, as always, flows to the weakest link: smaller carriers that remain outside the strongest protections.
- The war is far from over. In many ways, scammers have just opened a new — AI-powered — front. Across all sectors, we must remain vigilant. Our collective efforts are showing signs of progress, but the organized crime networks behind these attacks will not go quietly. We must continue to raise awareness, educate, and invest in the tools and technology needed to deliver sustained and meaningful success.

Threat landscape: Credit unions

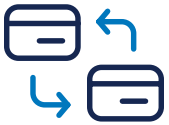
In working with around 200 credit unions in the U.S., we've found they experience fraud differently than larger banks. Customer data from the first half of 2024 compared to the first half of 2025 shows:

15%

of reported fraud has an active remote access Trojan (RAT) in the session, up 55% from last year

130%

increase in reported money mules



18%

of reported fraud relates to card activity

Trends:

- Social engineering techniques, together with standard phishing attacks, are the main methods fraudsters use to gain access to accounts. Attackers also focus on stealing one-time-passwords (OTPs) through social engineering, such as OTP vishing, to bypass the two-factor authentication controls banks use.
- Fraudsters are pivoting to multi-channel approaches to drain accounts. Through digital banking, they are able to collect card information and add it to digital wallets. They can then use these cards at ATMs, for in-store purchases, and more. In many cases, victims cannot recover any of the stolen money. This type of activity has increased significantly so far this year, rising from just 8% of all fraudulent activity reported by BioCatch's credit union customers at the beginning of 2025 to 18% in August.
- Bots are less prevalent than they are at larger retail banks, but credit unions still see some bot activity. Fraudsters often choose internet service providers (ISPs) commonly used by data aggregators, helping them blend in with other legitimate, non-human traffic and avoid detection.
- Fraudsters are increasingly using money mules to move and extract funds. That said, Zelle remains the preferred cash-out method.

Colin Parsons
head of fraud product strategy, Nasdaq Verafin

Collective intelligence for credit unions

At Nasdaq Verafin, we've supported credit unions for more than two decades. Today, nearly 1,400 credit unions across North America leverage Nasdaq Verafin's financial crime management solutions.

The first priority for credit unions has always been and will always be ensuring they're able to protect their members, who trust them implicitly. For years, we've seen criminal networks target credit union members with the types of scams and fraud that exploit that trust.

While anyone can fall victim to a scam, vulnerable populations face increased risks of exploitation. Scammers may impersonate a person in a position of trust or leverage fear tactics to extort funds. We are seeing a high volume of elder scams, including fraudsters targeting credit union members. Whether by phone, email, or elsewhere online, scammers will impersonate credit union staff to gain the trust of elderly individuals and illicitly access their online banking accounts.

Fraud will always find the path of least resistance, and with the rise of AI, fraudsters are able to leverage technology that introduces scams at a speed and scale never seen before. AI helps scammers easily customize their efforts to defraud consumers, mimicking the level of outreach and service members have come to expect from their credit unions. Criminals will also exploit information gaps between institutions, running the same playbook at credit unions across the country.

As credit unions improve their fraud-detection efforts and find ways to stop specific schemes, criminals are rapidly adapting with more sophisticated techniques to evade detection. To stay ahead of fraudsters and safeguard their members, credit unions need innovative tools that put an emphasis on prevention as soon as possible, protecting members before funds can leave their accounts.

Better tools, technology, and data can alert investigators to abnormal behaviors and stop payments in real time. The ability to draw from and inform collective intelligence across networks helps strengthen the industry's defenses against new and emerging scams.

As fraud continues to grow, it's critical that credit unions look toward the types of innovative, collaborative approaches that futureproof their fraud-prevention programs, protecting their members from the scams of tomorrow.

Thought leadership

Stablecoins: The scammer's currency of choice

Rob Autrey
director of global advisory, North America

Stablecoins and authorized push payments (APP) are now the twin engines of real-time money movement in the fraud and money laundering space.

Stablecoins themselves aren't nefarious, but they frequently serve as the getaway vehicle for scammers. In the past, bad actors primarily relied on cryptocurrencies like Bitcoin (BTC) and Ethereum (ETH) to move stolen money. They would convert illicit funds obtained through fraud or scams into crypto, often after first laundering the money through networks of mule accounts at various financial institutions.

Two flaws emerged in this previous playbook:

1. Pricing volatility meant scammers could lose thousands before cashing out.
2. Traceability made these coins easy to track, with investigators utilizing forensic tools like Chainalysis and TRM.

Enter stablecoins.

Tether (USDT) and USD Coin (USDC) are stablecoins pegged to the U.S. dollar, so one token equals about $1. That stability eliminates the price volatility and timing risk seen in other cryptocurrencies — 10,000 in is $10,000 out. Like BTC, stablecoin transfers are instant and irreversible, leaving no room for dispute or recovery. Unlike BTC, however, they can fly under the radar more easily.

Wires to Bitcoin exchanges often trigger alerts. But funding a wallet tied to USDT? Far less scrutiny, especially through platforms with weak Know Your Customer (KYC) processes or offshore compliance.

Meanwhile, consumers often perceive stablecoins as digital dollars as opposed to risky cryptocurrencies. When a bad actor manipulates a would-be-victim's emotions during an investment or romance scam, the convenience and perceived safety of stablecoins as an asset increases the likelihood of that victim agreeing to authorize the transaction. Between January of 2020 and February of 2024, 84% of romance and investment scam proceeds were laundered through USDT.[1]

Unlike Bitcoin, which is built for speculation, stablecoins are optimized for movement. This makes them attractive for a range of financial crime schemes, such as:

- **Account takeover (ATO):** Drain victim's account, buy USDT, vanish.
- **Pig butchering:** Lure victims into "investing" in fake platforms using USDT.
- **Mule payouts:** Send funds across borders without Society for Worldwide Interbank Financial Telecommunication (SWIFT) or anti-money laundering (AML) flags.

Bad actors can easily transfer stablecoins across centralized exchanges and decentralized platforms, cashing out stolen funds with minimal friction. By mid 2025, the global stablecoin market exceeded $250 billion.[2]

While traceability of these assets continues to improve, law enforcement is behind. Most fraud-detection tools still prioritize the tracing of traditional cryptocurrencies. That gives bad actors a window, and they're capitalizing on it.

1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4742235
2. https://www.theblock.co/post/356545/stablecoin-market-capitalization-surpasses-250-billion-amid-accelerating-regulatory-momentum

What banks can't see

For financial institutions, the rise of stablecoins as the scammer's currency of choice isn't just the latest crypto trend. It's a blind spot.

Most traditional anti-fraud solutions were not designed to track crypto movements, and even fewer can flag the behavioral red flags that precede these transfers.

Stablecoins pose a unique detection challenge:

- **They blend in.** When obtaining stablecoin, users often send transfers to legitimate exchanges, platforms, or protocols — many of which are often lesser-known when compared to the high-profile cryptocurrency platforms such as Coinbase or Kraken. The latter are more closely monitored and more heavily regulated than the former.
- **They appear legitimate.** Stablecoins are pegged to the U.S. dollar, giving the illusion of safety. A wire to a well-known U.S.-based exchange that ends in a USDT purchase looks clean, unless you truly understand the customer's intent.
- **Regulatory lag:** Crypto monitoring rules, internal risk models, and sanctions screening processes were largely built around Bitcoin, with stablecoins flying under the radar.
- **There are fewer legitimate use cases.** This poses a significant challenge for fraud and compliance teams. Without a deep pool of examples, it's difficult to build point-in-time alert solutions based on static data points like Social Security numbers, email and physical addresses, etc.

The threat isn't just the coin. It's the context around how and where it's moved. Banks may detect the outbound transfer, but without behavioral signals — patterns in how individual customers typically interact, transact, and behave during online banking sessions — the how, the why and what happens next are unclear. Activity blends into the noise of "normal" crypto usage. These are exactly the gaps that bad actors exploit.

Behavior sees all

How can we start to solve this issue? Behavioral analytics can spot these how's and why's.

Before a would-be-victim wires $10,000 to an exchange, for example, they often show signs of hesitation, being coached, or interacting with a (believably) impersonated loved one or official. Behavioral intelligence can identify these uncharacteristic behaviors, tracking slow typing, tabbing between windows, re-reading form fields, and 3,000 other indicators to identify signals of social engineering traditional controls miss entirely. That's why behavioral intelligence matters: It adds context around intent, enabling financial institutions to identify scams in motion, even when the payment itself looks legitimate.

Stopping the getaway car

In 2024, stablecoins accounted for 63% of all illicit on-chain transactions,[3] putting them ahead of fiat wires, cards, and traditional cross-border channels in fraud and money laundering risk, with $649 billion in fraud passing through the system last year.[4]

That's a steady climb over prior years, as bad actors have exploited stability, liquidity, and 24/7 speed to move funds before detection, making claw-back nearly impossible.

To curb this trend, financial institutions can't treat stablecoins as just another crypto risk. Instead, we must recognize stablecoins as a strategic enabler of scams, ATO, and mule networks, moving faster than traditional controls can catch and requiring equally strategic prevention.

3. https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/
4. https://cointelegraph.com/news/stablecoin-risk-crypto-transactions-bitrace-2024-report

CASE STUDY:

Using behavior to identify bots

Two years ago, we reported a year-over-year decline in bot usage, due in part to improved detection by banks. In its place, we saw a rise in mobile emulator use — software that mimics a real device, such as a smartphone. These have legitimate uses, such as allowing developers to test code and applications without needing multiple physical devices. However, fraudsters use these in an attempt to evade banking controls.

Bot use started rising again toward the end of 2024 and has yet to slow down. While we are still far from the bot numbers seen back in 2022 — in the first half of 2025, just 4% of 2022's total has been identified — bot-driven fraud increased 233% in the first half of this year, compared with the same period last year.

With this in mind, we've taken a fresh look at how behavior helps banks identify bots.

One obvious sign of a bot is how quickly it completes applications and what fields it fills out.

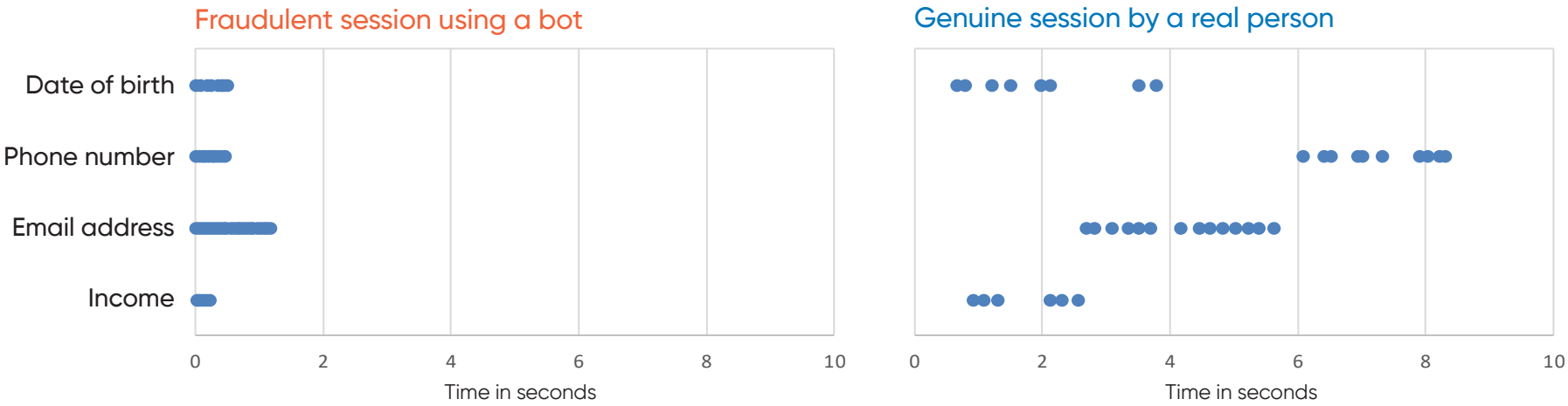
	Time to input personal information	Field interaction
BOT	20 seconds	Completes minimum requirement: date of birth, email, phone, address, etc.
Genuine user	2 minutes, 44 seconds	Interacts and completes more than the required minimum, including information of an additional card holder

CASE STUDY:

Using behavior to identify bots

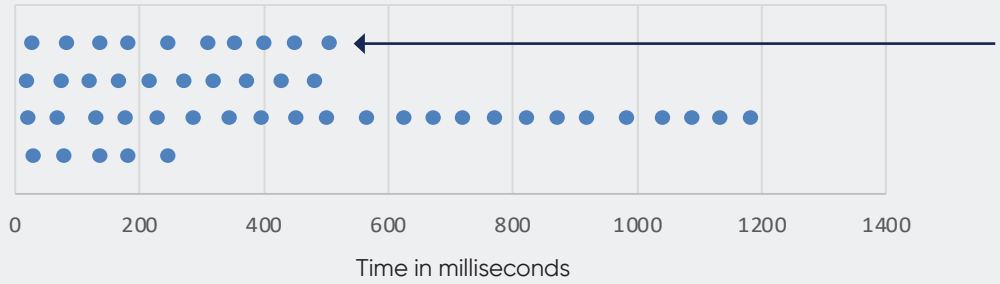
Much of bot detection comes from analyzing how information is typed into an application form.

Below, we compare the typing cadence for four mandatory fields across two applications — one completed fraudulently and one completed by a genuine person. Each dot represents a keystroke, recorded whenever a new character is typed.



As shown above, the bot inputs information very quickly, typically within one second per field. Only the email address, which contained 23 characters, took longer than one second to complete. In contrast, the genuine user took several seconds to type their information into each field.

On the fraudulent session, the typing pattern was consistent, as shown in the zoomed-in view of the graph below. Meanwhile, the genuine user had a broken pattern, consistent with human interaction.



Notable insight:

For the date-of-birth field, the bot typed a total of 10 characters, compared to the common eight typed by most users filling out a date-of-birth field. This is because the bot typed not only the numbers but also the day/month/year separators with forward slashes.

This step isn't necessary, as the application form automatically prepopulates these characters. Genuine users notice this in real time, whereas bots are programmed to input information, and cannot spontaneously interpret the application form.

CASE STUDY:

Using behavior to identify bots

A closer look at this case study reveals clear differences in the way information is entered by a bot versus a genuine user.

First, the genuine user paused for a couple of seconds after clicking into each field before starting to type, a standard human reaction. The bot, however, began typing almost instantly, with virtually no delay.

Second, the time between keystrokes is highly revealing. While human cadence varies based on age, agility, and experience, bots type at a notably different pace. In this case, the bot's intervals were extremely short, producing an almost impossibly fast typing speed.

Average time to start typing

BOT

22 milliseconds

Genuine user

2.6 seconds

Average time between keystrokes

BOT

52 milliseconds

Genuine user

291 milliseconds

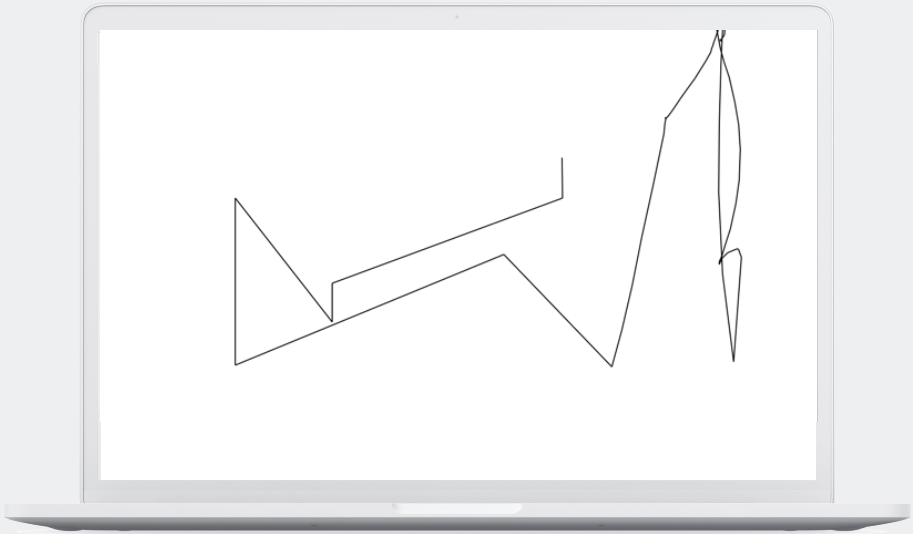
CASE STUDY:

Using behavior to identify bots

Mouse interaction is another way to identify non-human interaction indicative of bots.

The examples below show mouse movement patterns while completing an application, highlighting the differences between a bot and a genuine user.

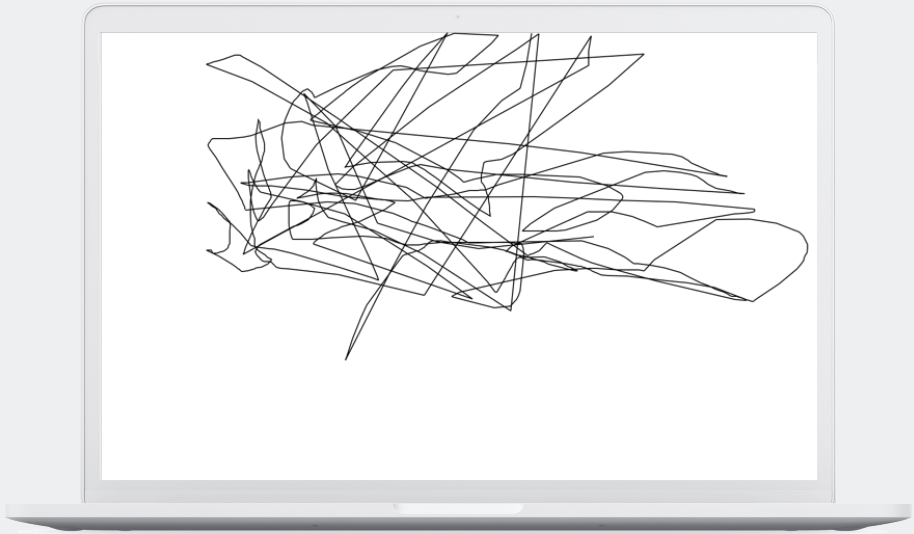
Fraudulent session using a bot



Key findings:

- Perfectly straight lines between mouse clicks
- Minimal movement on screen

Genuine session by a real person



Key findings:

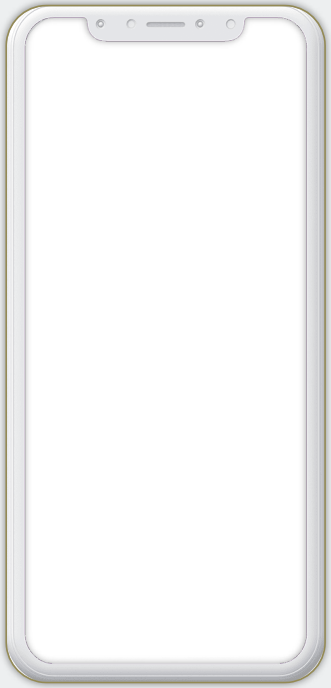
- Significant movement on pages
- Areas of higher concentration of mouse movement, aligned with fields on the page
- Loops seen around mouse clicks

CASE STUDY:

Using behavior to identify bots

On mobile devices, mouse movement and clicks are replaced by touch events and swiping. These are harder for bots to execute, so fraudsters turn to mobile emulators in an attempt to simulate the human interaction on the mobile channel. Just as it can with bots, behavioral intelligence can also identify the presence of an emulator, recognizing there still isn't a real human in control of the session.

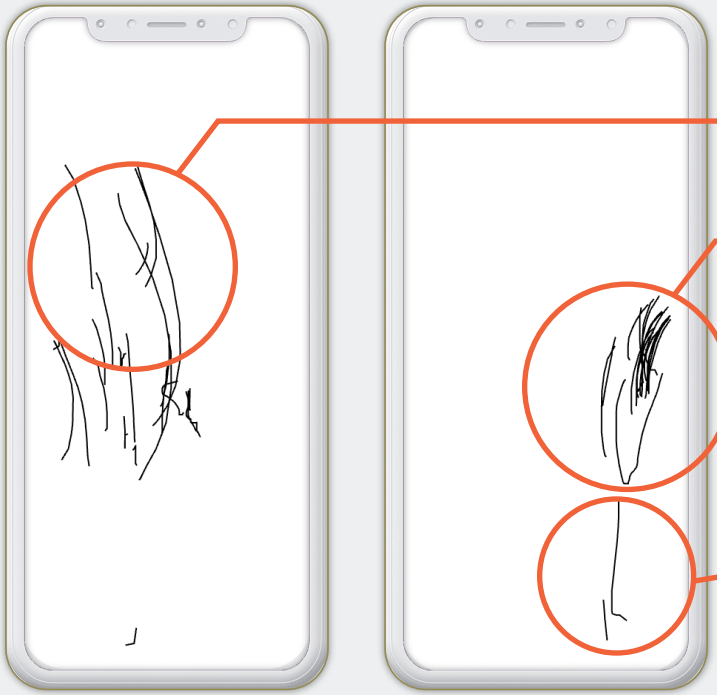
Fraudulent session executed by an emulator



Key findings:

- No swipes identified
- Touch events are very precise (the size of one pixel)

Genuine sessions executed by real users



Key findings:

- Normal swipes, each with a natural curvature caused by using a thumb
- Lots of interaction concentrated on specific areas of the screen
- Touch events tend to have small swipes around them

These examples illustrate just a few behavioral insights that can help distinguish fraud-enabling tools from genuine users. While device telemetry can assist in detecting some of these tools, fraudsters can often obfuscate the data or mimic legitimate scenarios relatively easily. Behavior, however, tells a different story, allowing institutions deploying behavioral solutions to identify criminal bot activity that device telemetry alone cannot.

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 Customer 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 287 total financial institutions deploy BioCatch solutions, analyzing 16 billion user sessions per month and protecting more than 532 million people on more than 1.6 billion devices around the world from fraud and financial crime.

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

www.biocatch.com E: info@biocatch.com @biocatch in /company/biocatch