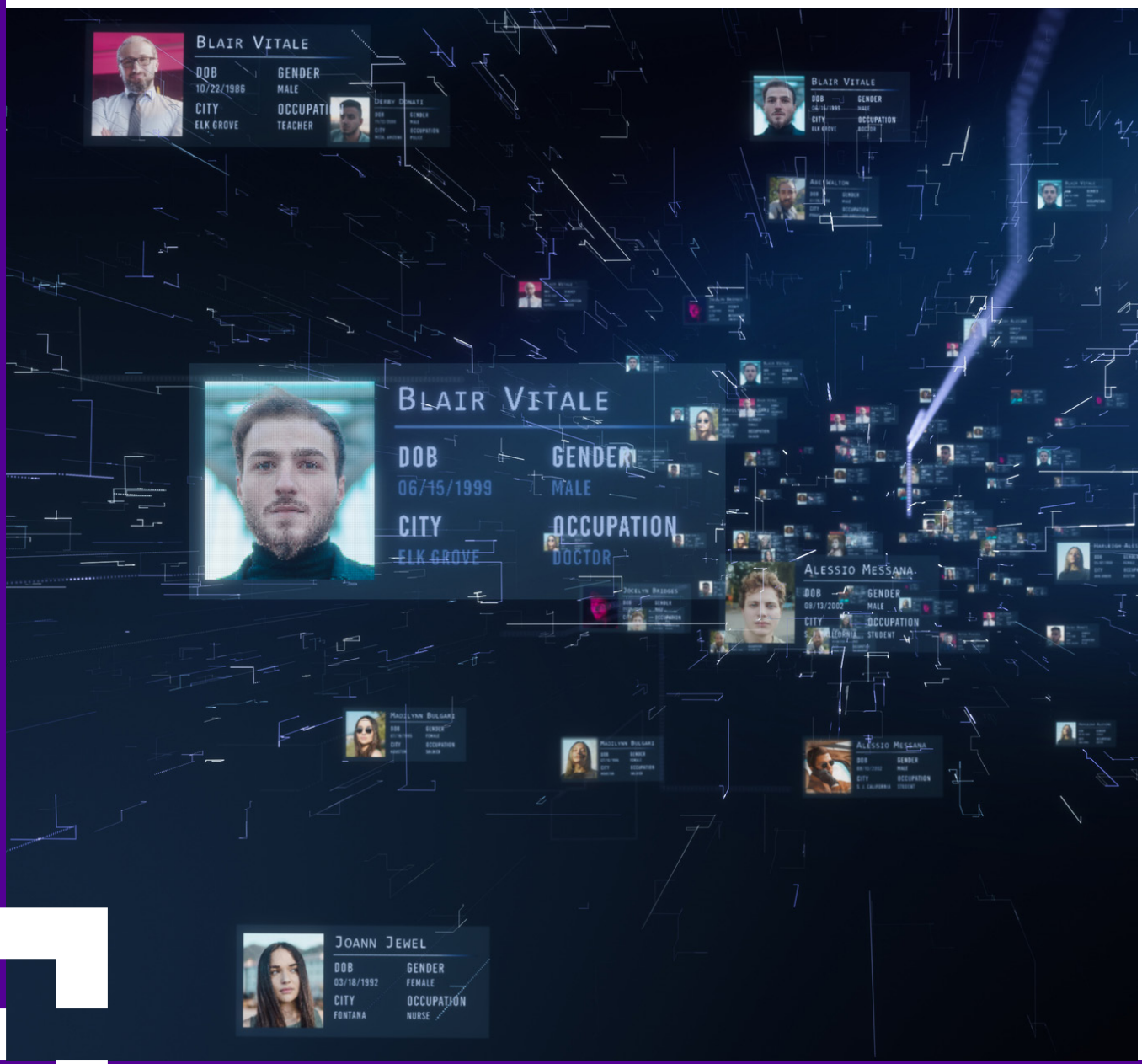
javelin | PLAID

# From Data to Decision:

## Detecting Fraud Risk Earlier




WHITEPAPER | JUNE 2026

# Table of Contents



# Table of Figures





javelin

# Meet the Author

**Jennifer Pitt**
Senior Analyst,
Fraud & Security

Jennifer is a senior analyst in Javelin's Fraud & Security practice. She analyzes data and trends and provides recommendations to financial professionals regarding best practices for fraud prevention and cybersecurity.

# Foreword

This report, sponsored by Plaid, explores why fraud risk often develops before organizations have enough information to detect it. As fraudsters gather, reuse, and scale identity and account data earlier in the customer lifecycle, many detection processes still rely on signals that appear later, after alerts, transactions, or disputes. This report examines how earlier, more connected data and signals from identity, document, biometrics and liveness, device, behavior, accounts and payments, cross-network intelligence, and customer response can help organizations improve detection, support better risk decisions, reduce losses, and strengthen customer trust.

This report was adapted from the *2026 Identity Fraud Study: The Illusion of Progress*, published by Javelin Strategy & Research in April 2026. Javelin Strategy & Research maintains complete independence in its data collection, findings, and analysis.

# Overview

Fraud risk often begins before an account is opened, a login is attempted, a profile is changed, or a transaction is initiated. Fraudsters gather and reuse identity and account data early and at scale. For organizations that rely on isolated data, the risk may not become visible until later (after alerts, transactions, or disputes), allowing new-account fraud, account takeover, scams, and first-party fraud to continue longer. Earlier, more complete data and signals—including those from identity, document, biometrics and liveness, device, behavior, accounts and payments, cross-network intelligence, and customer response—can help organizations detect risk earlier, reduce losses, limit unnecessary friction, and maintain customer trust.



javelin

# Executive Summary

**Organizations need data earlier in the customer lifecycle.** Fraud risk often appears before onboarding, login, payment activity, disputes, or investigations. Earlier identity, device, behavior, account, payment, and network data can help organizations identify risk before it becomes a loss, customer harm, or operational escalation.

**New-account fraud was the only fraud typology in which both dollar loss and victim count increased.** In 2025, the number of victims increased by 31%, and consumer dollar losses increased by 13%. Fraudsters can now quickly open and test accounts en masse. New accounts have less comparative historical information available, making it harder to spot stolen identity data, synthetic identities, manipulated documents, clean devices, bots, or automated application tactics before the account is used for fraud.

**Fraud damages customer trust.** Not only does fraud result in dollar loss, it can also create operational strain, customer service volume, reimbursement pressure, regulatory scrutiny, reputational harm, loss of customer trust, and customer attrition. In 2025, 18% of scam victims reported reduced trust and growing suspicion after the scam, and 31% of fraud victims closed the account where the fraud occurred.

# Recommendations

**Partner with vendors that use cross-network fraud signals.** Organizations should work with vendors that help connect identity, device, behavior, account, payment, and network signals across the customer life cycle. Fraudsters move across accounts, organizations, and payment channels. Detection has to do the same. Cross-network signals can help organizations see fraud patterns they may not catch from their own data alone.

**Implement identity verification controls that address modern fraud tactics.** Identity verification tools that worked several years ago may not be enough against AI-driven document manipulation, synthetic identities, deepfake injections, and spoofed liveness checks. Organizations should evaluate whether their controls can detect tampered images, virtual camera use, reused identity elements, and other signs of scaled fraud.

**Layer fraud controls across the customer lifecycle.** Fraud detection should not depend on a single checkpoint at onboarding, login, or transaction review. Organizations should use a defense-in-depth approach that applies risk assessment throughout the lifecycle, including account opening, early account activity, profile changes, login behavior, payment initiation, and post-transaction review.

**Strengthen customer trust through smarter risk decisions.** Fraud controls should protect customers without creating unnecessary friction. Organizations should use earlier and more complete data to make risk-based decisions, apply step-up verification when needed, reduce false positives, and help customers trust legitimate fraud alerts, warnings, and security processes.

# The Fraud Landscape Continues to Evolve

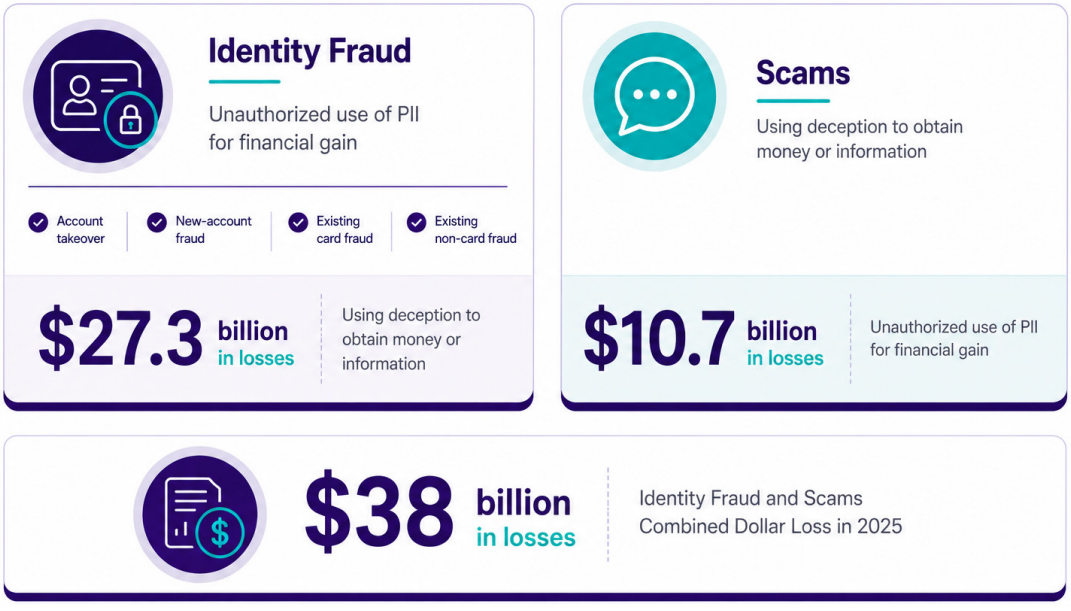
Fraud tactics continue to evolve, and fraud attempts and successful attacks are outpacing detection. This cat-and-mouse game of fraud detection has quickly turned into a tortoise and the hare race, and fraud professionals are falling further behind.

Fraudsters now understand flagging and reporting thresholds, as well as detection limitations created by existing silos, legacy technology, data-sharing restrictions, and limited collaboration among fraud prevention professionals. They continue to skirt detection by transacting below flagged thresholds, spreading activity across accounts and organizations, and bypassing weak onboarding, login, and account controls. And with the rapid advancement of AI, fraud-as-a-service tools, and automation, fraudsters can scale attacks with less effort. What once required specialized skills, expensive tools, manual effort, or more time is now easier to access and easier to execute. AI can help fraudsters test credentials, generate application variations, create synthetic identity elements, and make scams more convincing.

Even consumers are keenly aware of how AI continues to impact fraud. Nearly 90% of consumers said they are concerned fraudsters will use AI along with their personal information to commit identity fraud. Among those concerned, 33% said they were worried AI would be used to create deepfakes that would be used to bypass authentication or identity verification at their bank, credit union, or credit card company. Another 23% said they were concerned fraudsters would use AI to impersonate them when contacting their bank or credit union. That concern creates a second problem for organizations. AI not only helps fraudsters create more convincing attacks, it also makes legitimate customer communication harder to trust. If consumers believe a call, message, warning, or alert could be fake, they may ignore the very interaction meant to protect them (see Javelin's *2026 Identity Fraud Study: The Illusion of Progress*).

**Combined Identity Fraud and Scam Losses Are Significant**

Figure 1. Identity Fraud and Scam Dollar Losses, 2025




Source: Javelin Strategy & Research



javelin

Scams—defined as the use of deception to obtain money or information—cost consumers nearly $11 billion in 2025. And identity fraud—defined as the unauthorized use of personally identifiable information (PII) for financial gain—cost consumers over $27 billion in 2025. Identity fraud includes existing card fraud, existing non-card fraud, account takeover, and new-account fraud.[1]

These losses are only part of the cost. Weak, redundant, or time-consuming detection workflows can add operational strain, extend investigations, increase customer service volume, and create more reimbursement pressure. Organizations can also face regulatory scrutiny, reputational harm, loss of consumer trust, and customer attrition. In fact, 18% of scam victims reported reduced trust and growing suspicion as a result of their scam victimization. And 31% of fraud victims closed their accounts (financial and non-financial) where the fraud occurred.[2]

# Current Detection Exposes Vulnerabilities

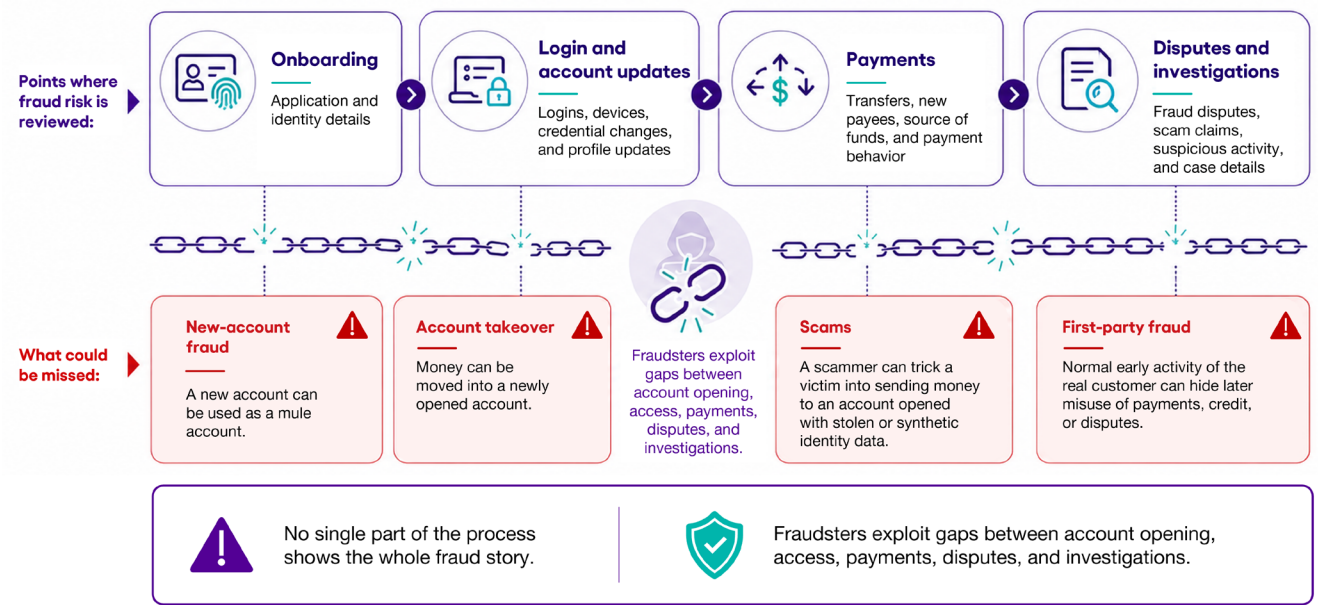
Most fraud programs are organized around decision points: onboarding, login, account changes, payment initiation, disputes, claims, and investigations. Teams use those moments to approve, block, review, reimburse, or investigate activity. Complaints, fraud claims, disputes, alerts, and suspicious activity reviews may each be handled separately.

Fraudsters don't stay within those same boundaries. They move across accounts, products, channels, and organizations, testing controls, reusing data, and exploiting gaps between systems. By the time one organization detects fraud, related activity may already exist elsewhere. The same device may have been used to open several accounts. An email address or phone number may be tied to suspicious applications or failed account-opening attempts. And a linked account may already be associated with risky payment activity.

New-account fraud, account takeover, scams, and first-party fraud become harder to detect early when teams see only their part of the activity, especially when these typologies intersect. A new account can become a mule account. A fraudster who takes over an existing account can move money into a newly opened account. A scam victim can be instructed to send money to an account opened with synthetic or stolen identity data. A first-party fraudster can exploit gaps in onboarding, payment rules, and dispute processes. Fraudsters often choose the path of least resistance. Without connected data, organizations see the customer narrowly instead of viewing the activity holistically.

**No Single Review Point Shows the Entire Fraud Picture**

Figure 2. Points in the Customer Lifecycle Where Fraud Risk is Reviewed and What Isolated Data May Miss, by Fraud Typology




Source: Javelin Strategy & Research



javelin

The problem isn't always a lack of data. Often, the data exists but is split across teams and systems. Onboarding teams may see identity data, authentication teams may see device activity, payment teams may see the transaction, customer service may receive the scam claim, anti-money laundering (AML) may see suspicious movement, and disputes may be handled somewhere else entirely. Fraud findings may not feed back into models, rules, warnings, or future investigations. That missing context affects decisions. For example, a fraud team reviewing a payment may not know that the destination account has appeared in other suspicious activity. An onboarding team may not know that the same device was tied to rejected applications. An AML team may not know that incoming money was tied to a scam claim at another organization.

One outdated assumption is that identity is limited to static personal information. Name, address, date of birth, government ID, and selfies still matter, but they don't fully represent identity in a digital financial environment. A person's identity also includes patterns of access, devices, account relationships, payment behavior, funding sources, counterparties, and other signals that show whether the activity is consistent with the customer. Fraudsters often exploit organizations that separate these signals instead of using them together.

This does not mean every digital signal is proof of fraud. A new device may be legitimate. A customer may travel. A person may change phone numbers. A transaction may be unusual but genuine. Device and behavioral data should not be used as blunt instruments. Their value comes from context. A new device matters more if it follows credential changes and comes before a high-risk transfer. A new beneficiary matters more if the customer is moving money in a pattern associated with scams. A shared device matters more if it appears across several applications with inconsistent identity details.

Signal timing also matters. Information that is not available at onboarding may become important after the first login, account change, payment, claim, or investigation. Risk changes as new information becomes available, but many organizations still make decisions too statically. For example, an account that looked legitimate at onboarding may need a different decision if the same device later appears in rejected applications or if the account starts sending money in a pattern associated with scams.

The larger issue is that many organizations are still relying on controls designed for an earlier fraud environment. A document verification process that worked several years ago may not be strong enough against better forged documents, edited images, screen spoofs, synthetic camera feeds, or virtual camera software. Basic selfie-to-ID matching may not be enough if the fraudster can manipulate the image, use a high-quality fake, or exploit weak liveness checks. Static rules may miss coordinated activity that changes quickly. Manual review alone cannot keep up with high-volume testing, especially when each event looks only slightly unusual.

# Early Data and Connected Signals Mean Early Detection

Earlier data is valuable when it helps an organization make a better decision before money is lost or the case becomes harder to resolve. The purpose is not to collect every possible signal or build a surveillance-heavy customer experience. The purpose is to use the right data early, so organizations can make better risk decisions without adding unnecessary friction for legitimate customers.

At onboarding, earlier data can help organizations assess whether an applicant appears legitimate or whether the application needs more review before the account is opened. Early in the account lifecycle, the focus shifts to whether the account starts behaving as expected. At login, the goal is to determine whether access still appears consistent with the customer and the account. At payment initiation, earlier detection gives organizations a chance to intervene before funds leave. During investigation, connected data helps teams understand what happened and feed confirmed outcomes back into prevention. Different teams may handle different parts of the lifecycle, but the information should not stay separated. What one team learns should help the next team recognize risk sooner and reduce losses.

Consider an account that looks normal at first glance. The identity information appears valid, the login looks normal, and no single action is enough to confirm fraud. But the pattern changes when the organization connects the data. The device has appeared in other risky activity, contact information was recently changed, the user quickly adds a new recipient, and the payment activity does not fit the customer's normal behavior. The customer also rushes through an alert or gives an explanation that matches a known scam script. Viewed separately, each issue may look explainable. Viewed together, they give the organization a stronger reason to step up verification, delay the payment, contact the customer, or send the activity for review before money leaves the account.

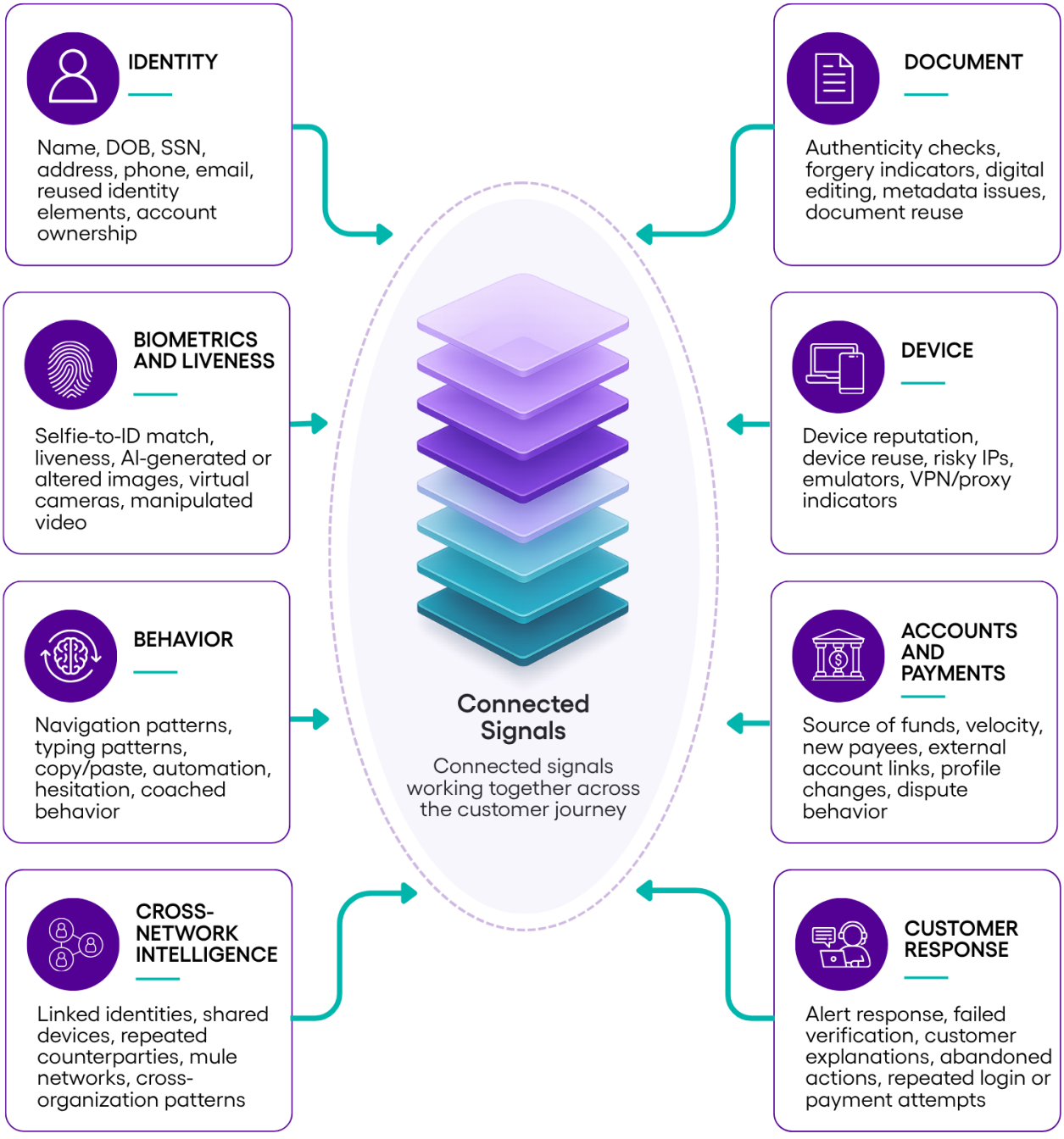
**No single control will stop new-account fraud, account takeover, scams, and first-party fraud.**

**The goal is to turn breadcrumbs into decisions.**

This is where a layered approach of connected signals comes into play. This approach relies on eight core independent but connected signals: **identity, document, biometrics and liveness, device, behavior, accounts and payments, cross-network intelligence, and customer response.**

**Earlier Detection Requires Connected Signals**

Figure 3. Signals Used to Detect Fraud Earlier




Source: Javelin Strategy & Research



javelin

Here is a look at each core signal:

**Identity** signals help organizations determine whether the person or business appears legitimate and whether the identity elements make sense together. A name, Social Security number, address, phone number, email, or account ownership detail may look fine on its own, but reused or inconsistent identity elements can point to stolen identities, synthetic identities, or repeated application abuse.

**Document** signals help determine whether the submitted identity document appears authentic or has been reused, altered, or manipulated. Strong document checks are important because fraudsters can use edited images, forged IDs, or reused documents to pass basic onboarding controls that were not built for today's fraud tactics.
Biometric and liveness help show whether the person presenting the identity is live and matches the document being used. These checks matter because a selfie can look believable while still involving an AI-generated or altered image, a virtual camera, or manipulated video.

**Device** signals help show whether the device being used fits the customer, account, or application activity. A new device is not automatically suspicious, but a device tied to repeated applications, risky IPs, emulators, VPNs, proxies, or other suspicious activity can help connect behavior that would otherwise look unrelated. Consumers appear more open to this type of data use when the purpose is fraud prevention: 70% said they were comfortable with companies collecting location or device information to prevent fraudulent activities.

**Behavior** signals help show whether the user's activity during onboarding, login, or payment activity matches normal customer behavior. Navigation patterns, typing behavior, copy-and-paste activity, automation, hesitation, or coached behavior can indicate that the person is not acting normally, is being guided by someone else, or is using a scripted process.

**Accounts and payment** signals help show whether account activity and money movement make sense. Funding sources, payment velocity, new payees, beneficiary risk, external account links, profile changes, and dispute behavior can help identify account takeover, scams, new-account fraud, or first-party fraud before the loss becomes harder to stop.

**Cross-network fraud** signals help connect activity that may look unrelated when viewed in isolation. Linked identities, shared devices, repeated counterparties, mule networks, and cross-organization patterns can show when accounts, applications, or payment activity are part of a broader fraud pattern. Unlike static attributes or surface-level behaviors, these signals are rooted in activity over time, which makes them harder to fabricate.

Customer response signals show how the customer or fraudster reacts when the organization interrupts, questions, verifies, warns, blocks, or delays an action. These signals may include alert response, failed verification, customer explanations, abandoned actions, or repeated login or payment attempts. They should not be treated as proof of fraud on their own, but they can help organizations decide when to add friction, delay a payment, escalate for review, or contact the customer.

Unfortunately, some victims don't respond to fraud alerts from their bank. Of those who didn't respond to a fraud alert, 55% said it was because they thought the alert was a scam.[3] If consumers ignore legitimate alerts, it can cause a significant ripple effect. They won't be alerted to potential fraud, which makes them more susceptible to victimization.

If they become fraud victims, they may wonder why their bank didn't stop the fraud. The customer loses trust in the organization's ability to help them. This could lead to the customer closing their account. They might even tell their friends or family not to bank with that organization because of the perceived lack of fraud controls.

If customers can't trust the alerts that legitimately come from their bank, that's one less method available for detection. Real-time alerts (particularly those regarding scams) can often help break the brain's automatic response and allow someone to react out of logic instead of fear. Ignoring those real-time alerts can often mean repeated scam victimization.

## SIGNALS TIED TO SPECIFIC FRAUD TYPOLOGIES

The need for earlier detection is easier to see when looking at specific fraud types. Fraud teams often first see the problem at account opening, login, credential reset, profile change, payment initiation, customer report, or dispute. But that is rarely where the fraud started. In account takeover, scams, new-account fraud, and first-party fraud, earlier activity often points to the risk before the organization sees the actual loss.

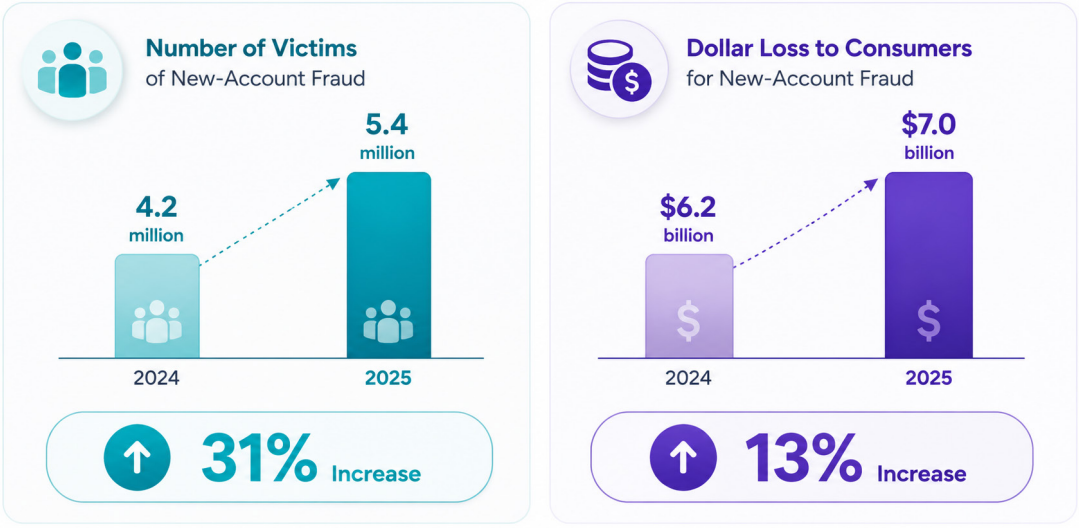
### New-Account Fraud

New-account fraud occurs when fraudsters open a new account using stolen, synthetic, manipulated, or misused identity information, or when someone opens an account with the intent to use it fraudulently.

New-account fraud was the only identity fraud typology to increase in both loss and number of victims in 2025. The number of victims of new-account fraud increased by 31% and consumer dollar losses increased by 13%. Fraudsters can now quickly open and test accounts en masse.[4] New accounts have less comparative historical information available, making it harder to spot stolen identity data, synthetic identities, manipulated documents, clean devices, bots, or automated application tactics before the account is used for fraud.

**New-Account Fraud Is the Only Fraud Typology That Increased in Victim Count and Dollar Loss in 2025**

Figure 4. Percentage of Increase in Number of Victims and Consumer Dollar Loss for New-Account Fraud




Source: Javelin Strategy & Research



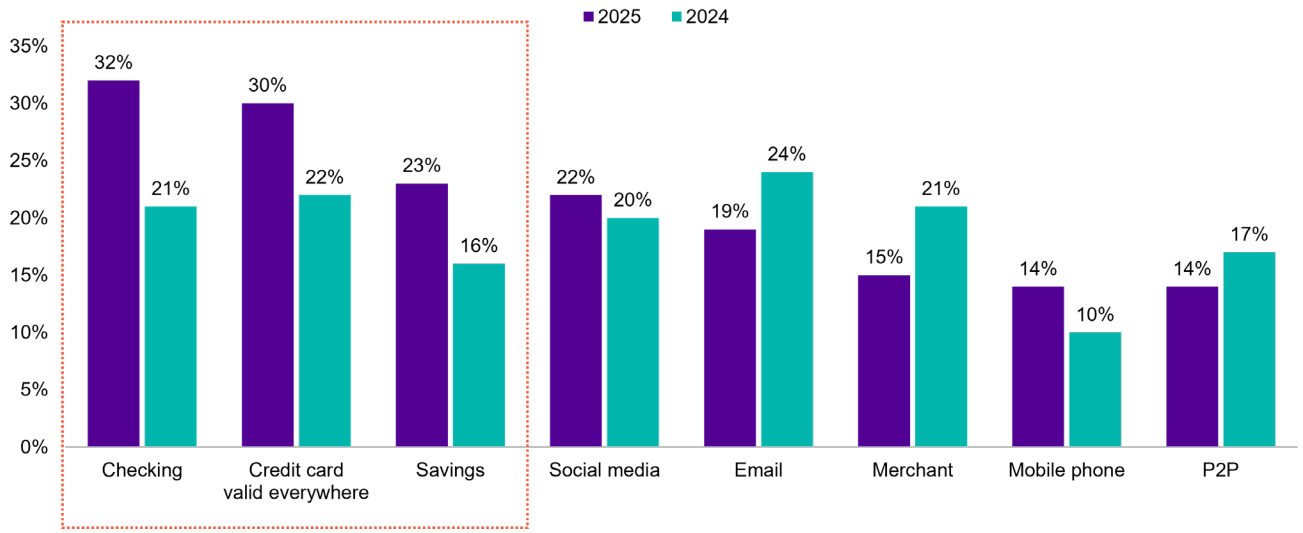
javelin

The account may be opened to access credit or funds directly, receive scam proceeds, move money, build credibility, test identity data, launder funds, or enable fraud across other platforms. Some accounts may seem dormant at first, only to be used later for payments, transfers, mule activity, or other fraud. Because the account is new, organizations may have limited customer history to rely on. An applicant's identity information may appear valid. An ID document may pass review. A selfie may match the ID. That makes early identity, document, device, behavior, and network signals especially important.

New-account fraud can involve deposit accounts, credit cards, loans, fintech accounts, payment apps, cryptocurrency accounts, social media accounts, merchant accounts, or other digital accounts. But the most common targets are still traditional financial accounts. In 2025, 32% of new-account fraud victims said a checking account was fraudulently created using their information. Major credit card accounts (30%) and savings accounts (23%) also ranked among the top reported fraudulent new accounts, and all three rose sharply from the prior year.[5] Checking accounts receive deposits, send payments, connect to external accounts, and often serve as funding sources for other digital services. Major credit card accounts give fraudsters access to a revolving credit line that can be used quickly for purchases or cash advances. Savings accounts can give them additional funds to draw from or move.

**New Fraudulent Traditional Financial Accounts Rose Sharply in 2025**

Figure 5. Percentage of Consumers Who Reported That an Account Was Fraudulently Created Using Their Information, by Account Type




Source: Javelin Strategy & Research

Earlier data can help organizations identify new-account fraud before the account is used to move money, access credit, or link to external accounts. It can also help catch patterns that onboarding checks may miss, such as risky devices, repeated identity elements, suspicious funding sources, unusual early account behavior, or links to accounts with similar activity.

## Account Takeover

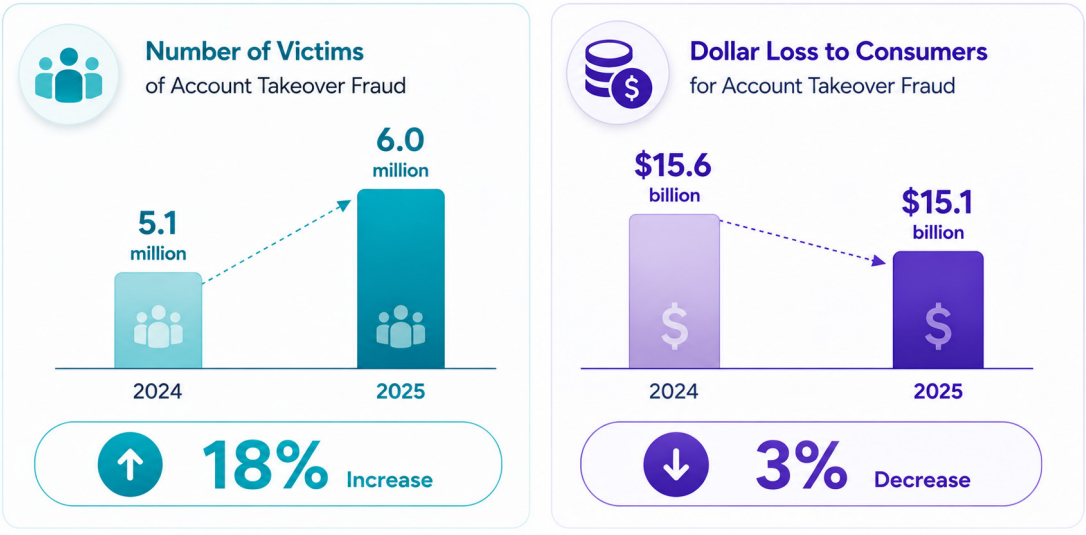
Account takeover occurs when fraudsters gain unauthorized access to an existing account.

To gain access, they may have bought stolen credentials, tricked the customer into entering login information on a fake site, intercepted a one-time password, attempted a SIM swap, used malware, or gathered enough personal information to impersonate the customer. Once a fraudster gains access to an account, they may change account settings, intercept authentication codes, lock the accountholder out, add new devices or beneficiaries, or initiate unauthorized payments. They also change information, such as name, phone number, physical address, email address, password, card PIN, or user ID. Passwords and email addresses remain the top pieces of information modified during account takeover.[6]

And though account takeover losses decreased, it's still the top identity fraud typology for consumer dollar loss at $15.1 billion in 2025.[7] Existing accounts have already gone through know your customer (KYC) and onboarding checks, and existing accounts often provide additional usable personal information the attacker did not have before (including the account profile information).

**Account Takeover Fraud Is Still a Pricey Problem**

Figure 6. Percentage Increase or Decrease in Number of Victims and Consumer Dollar Loss for Account Takeover



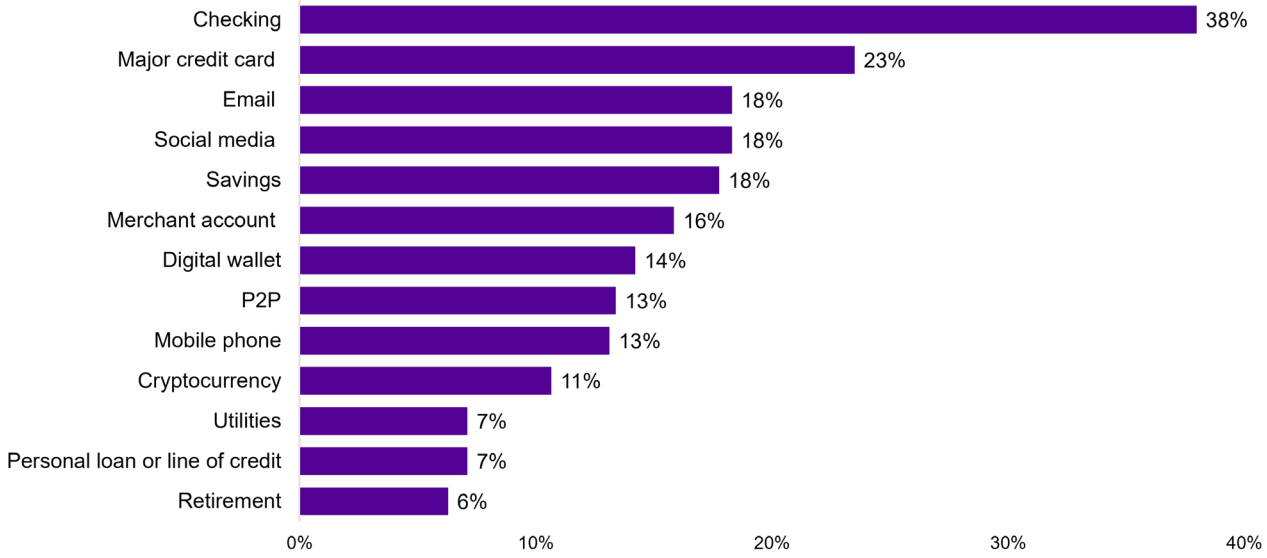

Source: Javelin Strategy & Research

Among consumers whose bank account was taken over, 60% said the incident occurred at a giant bank (the largest U.S. banks, each with more than $1.5 trillion in assets). This mirrors what Javelin has found during field research with banks. Larger banks report a higher problem with account takeover, while smaller banks report a bigger problem with first-party fraud.

The accounts most commonly taken over are checking accounts, as reported by 38% of account takeover victims.[8] Checking accounts often provide a high return on investment to fraudsters. Because of the economy, most people keep easily liquidated money in checking accounts. And although checking accounts and major credit card accounts topped the list of accounts taken over, non-financial accounts (including email, social media, or utility accounts) are still valuable, as they can often provide fraudsters with an easier gateway to financial accounts.

**Checking Accounts Are Most Common Target for Account Takeover**

Figure 7. Type of Accounts Taken Over by Criminals




Source: Javelin Strategy & Research

Account changes and activity tied to account takeover can look legitimate when reviewed in isolation.

The concern becomes clearer when organizations consider the timing and velocity of account access changes, device changes, behavioral shifts, payment activity, and external account additions. For example, a new device may be a phone upgrade. A password reset may be routine. An email change may be valid. A large transfer may be expected. A failed login may simply be customer error. But failed logins followed by an email change, phone number update, new device enrollment, password reset, external account addition, or high-risk transfer may justify a different response.

Earlier connected data can help organizations make a more timely and proportionate decision. A single login event may not be enough to block, but the larger pattern may support step-up authentication, out-of-band confirmation, delayed payment approval, customer contact, temporary limits, or manual review.

## Scams

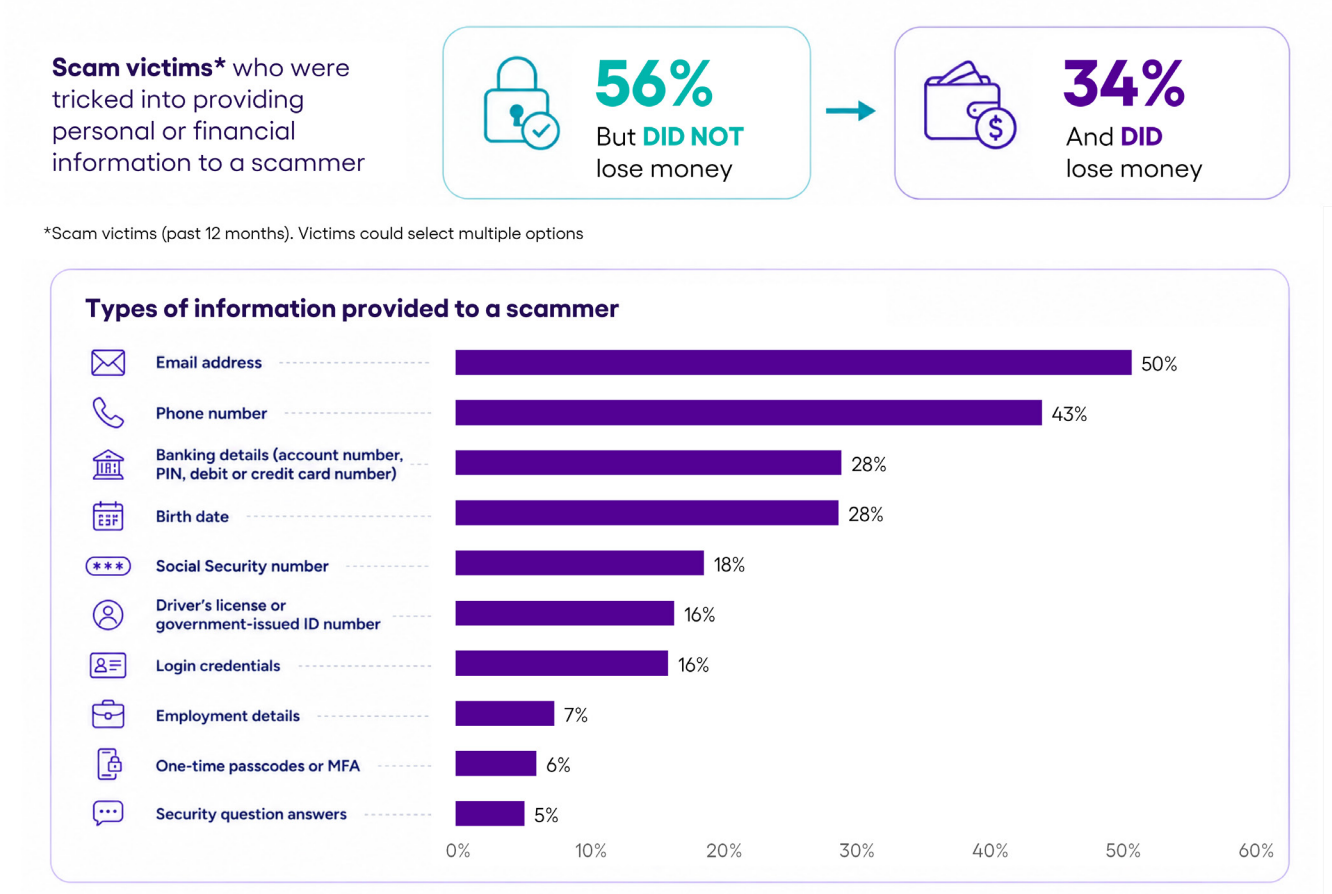
With scams, the legitimate, verified customer is involved. Scams involve manipulating consumers into providing financial or personal information to the scammer or even authorizing a payment themselves.

Scam dollar losses to consumers decreased by $8.8 billion in 2025, but the losses were still substantial at $10.7 billion. The decline should be interpreted carefully. Scam losses are difficult to measure because many victims do not report what happened, and consumers do not always distinguish between scams and identity fraud when describing their experiences (see *Javelin's 2026 Identity Fraud Study: The Illusion of Progress*).

Modern scams aren't limited to money loss. Scammers are increasingly more interested in obtaining personal information from the victim.

### PII Is a Hot Commodity for Scammers

Figure 8. Percentage of Scam Victims Who Were Tricked Into Providing PII to a Scammer in 2025




Source: Javelin Strategy & Research



javelin

**While many consumers lost money to scams in 2025, frighteningly, 56% of scam victims said they were tricked into giving personal or financial information but did not lose money as a result.[9]**

**So the question becomes:**
**What will those scammers do with the information? And when will they use it?**

Of scam victims tricked into providing personal or financial information, 50% said they provided email addresses, 43% said phone numbers, and 28% said banking details. Many of these victims were tricked into providing multiple pieces of information. Though email addresses and phone numbers may seem like rather benign information, they can be the missing puzzle piece fraudsters need to commit identity fraud or additional scams. And with access to banking details, the fraudster could easily bypass weak authentication and move money or even take over an existing financial account. The theft of personal information could even lead to the creation of synthetic identities or new-account fraud, and the victim might never know unless the information hits their credit report or they receive a collections notice.

Verifying the customer's identity does not always mean the transaction is legitimate. In a scam, the real customer may be using the real device from the usual location, completing step-up authentication, and initiating the payment themselves because the scammer coached them through it. The payment may look legitimate on its own, but the behavior around it may not. A new beneficiary, a transfer from savings, higher transfer amounts, or an ignored fraud warning may each have a legitimate explanation. But together, these signs can show that the customer is being coached into sending money or providing information to the scammer.

Earlier connected data can help organizations see when a verified customer's activity no longer fits the customer's normal behavior or starts to match known scam patterns. That context can support stronger warnings, payment delays, customer contact, or escalation before the scammer gets the money or information.

## First-Party Fraud

First-party fraud occurs when a legitimate customer disputes or abuses a transaction they authorized.

First-party fraud accounted for 36% of all reported fraud across multiple industries in 2024.[10] This type of fraud can be difficult to classify. Identical behavior may be treated as a dispute, credit abuse, refund abuse, account misuse, or fraud, depending on the organization, product, or team reviewing it.

Because the accountholder completed the transaction, distinguishing fraud from a valid dispute can be difficult. A customer can use their own identity and still intend to defraud. That intent may not be visible when the account is opened, which means identity proofing alone may not show the problem. The issue may appear later through rapid credit utilization, unusual repayment patterns, inconsistent income claims, disputes that do not match account activity, linked accounts with similar behavior, or sudden activity after a period of normal use.

Earlier data can help organizations separate normal account activity from behavior that suggests planned misuse. The goal is not to treat every dispute, missed payment, or repayment issue as fraud. It is to identify when the customer's activity, claims, and repayment behavior point to intentional misuse.

## ANALYTICS FOR MORE EFFECTIVE FRAUD DECISIONS

Detecting fraud early depends on more than collecting additional data. Organizations also need the ability to analyze that data quickly enough to identify fraud and scams as risk emerges. AI and machine learning can help, especially when fraud patterns are too complex for static rules alone. But they cannot fix bad inputs. Bad data, missing signals, late fraud outcomes, and weak monitoring all limit how much these tools can improve fraud decisions, especially as fraudsters change tactics. Consumers see a role for AI in that process. In fact, 61% of consumers think the best way their bank can use AI to protect their identity and account is through real-time fraud and scam detection, while 21% think AI should be used for predictive actions to protect their account from risky transactions.

Risk scores can also help fraud teams make decisions earlier, but a score alone is not enough. Teams need enough context to understand why a customer was stepped up, a payment was delayed, an account was restricted, or an alert was escalated. Without that context, decisions are harder to explain, complaints are harder to resolve, and investigations are weaker.

Controls should be applied differently to different situations. A returning customer making a normal payment isn't the same as a newly opened account rapidly transferring money. But risk still needs context, especially when activity looks unusual but may be legitimate. Consumers aren't necessarily opposed to added friction when it protects them from fraud. In fact, half of consumers say security of their account information during account opening matters more than the speed of the account opening.[11]

# Final Thoughts

Fraud breadcrumbs often start outside an organization's four walls, before the first login, payment, dispute, or claim that brings the risk to the organization's attention. Fraudsters may have already tested controls, reused identity data, manipulated the customer, built a synthetic identity, or spread the activity across multiple accounts and organizations.

Traditional controls fall short when they rely on one point in the customer lifecycle. Onboarding, authentication, payment monitoring, disputes, claims, investigations, and feedback loops may be handled in different systems or reviewed by different teams, but the information should not stay separated. These decisions work better when connected signals are used together across identity, document, biometrics and liveness, device, behavior, accounts and payments, cross-network, and customer response because the full pattern is harder for fraudsters to fake, spoof, or explain away.

Earlier detection also depends on what organizations do with what they learn. Confirmed fraud, scam reports, dispute findings, customer responses, and investigation outcomes should improve future onboarding decisions, authentication challenges, payment reviews, warnings, model updates, and investigations. Earlier, more connected data helps organizations make better fraud decisions before losses occur, trust erodes, or the case becomes harder to resolve.

# Methodology

The Javelin Identity Fraud Study provides businesses, financial institutions, government agencies, and other organizations with an in-depth and comprehensive examination of identity fraud and the success rates of methods used for prevention, detection, and resolution. This ID fraud survey was conducted online among 5,010 U.S. adults over the age of 18; this sample is representative of the U.S. Census demographics distribution. Data collection took place Nov. 10-Dec. 3, 2025. Data is obtained using 18-plus U.S. population benchmarks on age, gender, race/ethnicity, household income, and region from the most current CPS targets with a variance of +-2% points. Due to rounding errors, the percentages on graphs may add up to 100% plus or minus 1%. To preserve the independence and objectivity of this annual report, the sponsors of this project were not involved in the tabulation, analysis, or reporting of final results. The ID Fraud Study estimates key fraud metrics for the current year using a base of consumers who have experienced identity fraud in the past six years. Other behaviors are reported based on data from all identity fraud victims in the survey (i.e., fraud victims experiencing fraud up to six years ago) as well as total respondents, where applicable. For questions answered by all 5,010 respondents, the maximum margin of sampling error is +/-1.4 percentage points at the 95% confidence level. For questions answered by all identity fraud victims, the margin of sampling error is +/-3.0 percentage points at the 95% confidence level.

Additional consumer data for this report was sourced from Javelin Strategy & Research's Privacy Survey, conducted Feb. 5-24, 2026. The 2026 survey includes responses from 2,006 U.S. consumers. For all Privacy surveys, data is gathered from a sample of the adult U.S. population and is weighted to match the latest U.S. Census Bureau data. The margin of sampling error is +/-2.2% at the 95% confidence level. The margin of sampling error is higher for questions answered by subsegments.

# Endnotes


1 Javelin Strategy & Research, "2026 Identity Fraud Study: The Illusion of Progress." Published April 21, 2026; accessed May 1, 2026.
2 Ibid.
3 Ibid.
4 Ibid.
5 Ibid.
6 Ibid.
7 Ibid.
8 Ibid.
9 Ibid.
10 LexisNexis Risk Solutions, "First-Party Fraud Surpasses Scams to Become the Leading Form of Global Attacks." Published May 13, 2025; accessed May 21, 2026.
11 Javelin Strategy & Research, "2026 Identity Fraud Study: The Illusion of Progress." Published April 21, 2026; accessed May 1, 2026.




javelin

# About Plaid

Plaid is a global data network that powers the tools millions of people rely on to manage their financial lives. Plaid's network spans over 12,000 financial institutions across North America and Europe, giving organizations permissioned access to the real-time account, payment, and identity data needed to detect risk earlier and make better decisions across the customer life cycle. Plaid works with thousands of companies—including leading fintechs, Fortune 500s, and the largest banks—to connect the signals that help organizations identify fraud before losses occur, reduce unnecessary friction for legitimate customers, and maintain the trust that keeps financial relationships intact.

# About Javelin

Javelin Strategy & Research, part of Escalent group, helps its clients make informed decisions in a digital financial world. It provides strategic insights to financial institutions including banks, credit unions, brokerages and insurers, as well as payments companies, technology providers, fintechs and government agencies. Javelin's independent insights result from a rigorous research process that assesses consumers, businesses, providers, and the transactions ecosystem. It conducts in-depth primary research studies to pinpoint dynamic risks and opportunities in digital banking, payments, fraud & security, and lending. For more information, visit www.javelinstrategy.com.

Follow us on LinkedIn



javelin