experian

White paper

Scam detection:
a guide for financial institutions

A closer look at five of today's most common scams, how fraud teams identify them and the warning signs you can spot sooner.

Table of contents

The evolving U.S. scam landscape

In 2025, U.S. scam reports hit an all-time high: 3 million fraud reports were filed, up over 15% from 2024. It was the 10th consecutive year in which consumers lost more money to fraud than they did the year prior. During that period, annual losses rose from around $770 million in 2015 to $15.9 billion in 2025.[1]

It's no coincidence: As consumers increasingly manage their lives and finances online, fraudsters have evolved their tactics to exploit digital channels. They're using real-time payment methods, social media and artificial intelligence (AI) to execute increasingly sophisticated authorized push payment (APP) scams.

Shifts in scam tactics

Unburdened by organizational processes or limitations, fraudsters have moved quickly to integrate AI into their scam schemes. And they're already reaping the benefits.

AI is the single most impactful driver behind the evolving scam landscape. Generic, mass-sent scam messages, which used to be a necessity for resource-constrained fraudsters, are being phased out in favor of hypertargeted, personalized schemes. Globally, these AI-driven scams are over four times more profitable than traditional tactics.[2]

Tactics being phased out:

Generic spam emails:

Consumer awareness and stronger spam filtering have reduced the effectiveness of mass scam emails, pushing fraudsters toward more targeted approaches.

Gift card payments:

While still present, gift cards are becoming less common as scammers increasingly favor real-time payment methods and digital transfer platforms.

Robocalls:

Improved call-blocking technology and growing consumer skepticism have made mass robocalling less effective than personalized voice and deepfake-based tactics. Scam robocalls have fallen nearly 20% in recent years.[3]

Tactics on the rise:

6.5%
of fraud attempts are comprised of deepfakes

Deepfakes:

AI has made realistic audio, image and video impersonation fast and inexpensive to create. As a result, deepfakes are increasingly being used in scams that rely on trust, including imposter, romance and employment schemes. Deepfake fraud attempts increased by over 2,000% in the last three years and now account for 6.5% of fraud attempts.[4]

$8.6B
in losses to crypto-related scams in 2025

Crypto scams:

Accounting for over 7 in 10 investment scams, crypto scams (where victims use cryptocurrency as a payment method) draw fraudsters' attention due to their lucrative potential. Crypto scams often require additional coaching and effort from fraudsters, but the return is immense: crypto-related scams incurred over $8.6 billion in losses in 2025.[5]

30%
of all scams now originate on social media

Social media:

Social platforms give fraudsters access to personal information that can be used to craft highly targeted scams. Combined with AI, this makes personalized social engineering attacks easier to execute at scale. As a result, 30% of all scams now originate on social media.[6]

How consumers and businesses are responding

As scams grow more powerful, consumers are under constant pressure to protect themselves. In a 2026 Experian survey of U.S. consumers, over 1 in 4 reported encountering phishing emails, messages or scam calls in the past year, and 18% said they had suffered a financial loss due to online fraud.

That exposure is shaping how consumers act online. Over half of consumers said they're at least somewhat concerned about engaging in online activities, with scams ranking among their top fears. And they aren't just worried about scammers directly; they're also worried that legitimate businesses may fail to protect their data once it's collected.

64%

of consumers want more control over how their data is used.

Consumers' growing caution is eroding trust with businesses. Only 17% said they are very willing to share personal data with online businesses, and 64% say they want more control over how that data is used. Most notably, 86% expect businesses to act on fraud-related concerns. Increasing protectiveness over data signals that this expectation isn't being met.

86%

of consumers expect businesses to act on fraud-related concerns

For businesses, that creates a difficult balancing act. If anything, consumers' concerns make fraud detection harder, as even legitimate account security notifications are met with skepticism. Businesses are increasing fraud prevention budgets in response — 64% of businesses plan to spend more on account takeover prevention in 2026, 60% on APP fraud prevention and 59% on AI models that improve customer decisions — but increased spending, even if it reflects well on internal fraud numbers, hasn't proven to increase consumer trust. If those investments don't result in solutions that are effective, secure and frictionless, without relying on excessive data collection, they'll ultimately fail to rebuild trust.

The anatomy of a scam

As you'll see throughout this guide, scams take many forms, but almost all follow the same basic pattern: they methodically manufacture trust and manipulate victims.

Typical scam lifecycle:

01 — 02 — 03 — 04 — 05

Targeting and grooming:

Fraudsters make initial contact with potential victims.

Building trust:

Victims are routed to a seemingly legitimate channel: a spoofed phone call, deepfake or cloned website.

Scam in motion:

Victims act on the fraudster's prompt — sharing credentials, sending money.

Value transfer:

Fraudsters cash in: account takeover or funds moved off-platform.

Aftermath:

The victim discovers the loss — compromised accounts, missing funds and a broken promise.

Most organizations don't know if a scam has occurred until the final stage, if they find out at all. The goal for businesses, and the purpose of this guide, is to achieve detection earlier in the lifecycle and stop scams before losses occur.

Inside today's most common scams

Consumers are often the point of entry in scams, but they're rarely the final point of control. Fraudsters' messages and manipulations usually happen away from the institution that will ultimately be used to steal funds. A fraud team can't see the convincing text message, spoofed support call or deepfake voice note that persuaded the victim to act.

What fraud teams can see are the signals that manipulation leaves behind: unusual behavioral shifts, high-risk payment patterns, logins from unrecognized devices and more that indicate a scam in progress. To stop scams before they turn into losses, fraud teams need to be able to recognize the red flags of today's most prevalent scams and craft controls around them.

While not exhaustive, the following list highlights five of the most impactful tactics currently targeting financial institutions.

Phishing scams

These are low-touch scams where fraudsters trick consumers into disclosing credentials, account details, one-time passcodes or other sensitive information, often through cloned websites and apps.

Lifecycle of a phishing scam

Lifecycle stage	What's happening to the consumer	What it looks like for the financial institution
Targeting/ grooming	The consumer receives a message appearing to be from a trusted source, such as their bank, a government agency or a mortgage provider. The message prompts urgency: suspicious account activity, a password reset request or a payment issue that needs immediate action.	The scam is happening entirely off-platform, but crowd-level indicators may begin to emerge. Fraud teams may see a surge in high-risk devices, particularly devices associated with cloned apps.
Initiation of trust	The consumer is directed to follow a link to a cloned site or contact a "representative" from the organization being impersonated.	The scam is still occurring off platform, but a coordinated scheme may cause reports of phishing attempts on other customers to start rolling in.
Scam in progress	The consumer enters their credentials into the fake site or provides information to the fraudster. In more advanced schemes, the phishing flow may also capture device and network information that can be used to mimic the legitimate user later.	There are still no account-level scam indicators, but warning signs can grow more apparent. Fraud teams may see spikes in automated activity as fraudsters test and verify stolen credentials in batches.
Execution and value transfer	Using the now-stolen credentials, the fraudster logs in to the victim's account and begins trying to move money or change account details.	As the fraudster accesses the compromised account, behavior deviates from the victim's norms. Warning signs include login attempts from unfamiliar devices or locations, abnormal session behavior or transaction amounts that differ from the account's normal activity.
Aftermath and recovery	The consumer receives notice of the fraudulent activity on their account — except this time, it's real.	The institution receives a fraud complaint and begins a resource-intensive investigation.

How AI is impacting phishing:

In the past, phishing messages carried obvious warning signs like poor grammar, awkward formatting or strange URLs and email addresses. AI is removing those, generating polished phishing lures that are increasingly difficult for consumers to identify.

Red flags to monitor:

- **Logins from new devices, networks or locations** that don't align with the customer's historical behavior
- **Behavioral deviations** from account norms during login or session activity, even when the credentials are correct
- **Rapid movement** from abnormal logins to high-risk actions such as credential changes, multifactor authentication (MFA) resets, payee additions or outbound transfers
- **Devices accessing multiple accounts** with repetitive, high-risk actions, signaling coordinated phishing-driven account takeover activity

Tools to stop phishing scams in progress:

- **Device and network signals** to identify spikes in cloned apps, emulators or suspicious devices in use
- **Behavioral analytics** to distinguish the legitimate account owners from someone using compromised credentials
- **Link analyses** based on device and network data to connect compromised accounts and coordinated attack patterns that may look benign in isolation
- **Multifactor authentication step-ups** triggered by abnormal account activity

Imposter scams

Imposter scams involve fraudsters pretending to be trusted family members, friends, colleagues or employers. The goal is to manipulate victims into sending money, sharing sensitive information or taking account actions that benefit the scammer. Unlike phishing scams, where information is stolen quickly with little interaction between the scammer and the victim, imposter scams rely more heavily on social engineering.

Lifecycle of an imposter scam

Lifecycle stage	What's happening to the consumer	What it looks like for the financial institution
Targeting/ grooming	The consumer is contacted, often via phone call or text, by someone claiming to be a person they know or trust, like a family member, friend or coworker. The scammer's story creates urgency and emotional pressure.	At this stage, the interaction is off the financial institution's platform, instead of going through phone, text, email, social media, video calls or messaging apps.
Initiation of trust	The scammer works to make the request feel authentic. They may reference personal details gathered from social media, breached data or prior conversations. Increasingly, AI-generated audio and video are used to replicate the likeness of someone the victim knows.	The customer — using their own, legitimate account — may begin behaving differently. They might log in during or immediately after the conversation or contact support with vague urgency. Because the customer is authenticated, traditional login defenses may not flag the activity on their own.
Scam in progress	The fraudster directs the consumer toward the payment rail or other platform that will be used to steal funds. The victim is instructed to act quickly (and often told not to tell anyone about the request).	The abnormal user behavior carries over into a transaction session. Possible indicators include hesitation during payment flows, repeated navigation between screens, copy-and-paste behaviors that are unusual for the customer. Though the transaction is initiated by a genuine user, the user behavior suggests coercion or external coaching.
Execution and value transfer	The consumer sends funds through wire transfer, peer-to-peer (P2P) payment or another method that's fast and difficult to reverse. The scammer may keep the victim emotionally engaged to push for additional transfers.	The transaction is submitted and likely deviates from the customer's normal payment activity: Funds are sent to new recipients, transfer amounts increase sharply or transactions are structured just below review thresholds.
Aftermath and recovery	The consumer realizes the person they thought they were helping was not actually in trouble — or that the voice, video, message or caller was fake.	The institution receives a scam report. Fraud teams must determine not only whether the customer initiated the transaction, but whether there's enough evidence to confirm that the customer was manipulated.

How AI is impacting imposter scams:

With AI-powered voice cloning and deepfakes, fraudsters can imitate the sound, speech patterns or appearance of someone the victim knows. Those deepfakes can be paired with highly specific details pulled from public profiles, social media or compromised data.

Red flags to monitor:

- **First-time or unusually high-value payments** to new recipients
- **Multiple transfer attempts** in a short period, particularly when amounts are adjusted after declines or warnings
- **Activity suggesting urgency or coaching**, such as long hesitations, repeated corrections and frequent navigation between pages and windows
- **Payment attempts to accounts or wallets** associated with prior scam reports

Tools to stop imposter scams in progress:

- **Behavioral analytics** to reveal sudden changes from users' normal digital behavioral profiles that indicate coercion
- **Transaction risk modeling** that evaluates recipient history, payment rail, amount, timing, velocity and deviation from customer norms
- **Call-in-progress signals** to detect signs of in-session coaching
- **Contextual warnings** displayed when a transfer involves a suspicious recipient tailored to common imposter narratives

Investment scams

Investment scams occur when fraudsters convince consumers to invest in fraudulent opportunities. Victims believe they are making legitimate investments, while the fraudster is keeping funds for themselves. These scams often look less like a single fraudulent event and more like a legitimate customer gradually adopting a risky new financial behavior.

Lifecycle of an investment scam

Lifecycle stage	What's happening to the consumer	What it looks like for the financial institution
Targeting/ grooming	The consumer encounters an investment opportunity through social media, online ads or direct outreach. The offer may appear to come from a successful investor or a professional-looking trading platform.	As usual, grooming happens off-platform, often over days or weeks.
Initiation of trust	The fraudster builds confidence by showing fake dashboards, fabricated returns or testimonials. The victim may be encouraged to start small and may even be allowed to withdraw a small "profit" early on, reinforcing the belief that the investment is real.	Activity may look legitimate. The customer is authenticated and appears to be voluntarily funding an investment. Early red flags may include new external payment recipients or unusual movement from savings into checking before outbound transfers.
Scam in progress	The victim is persuaded to invest more. The fraudster claims the opportunity is growing and that additional funds are needed to unlock larger returns.	The victim's initial payment may show visible signs of risk, particularly large transaction amounts and unusual recipients. Initial transactions may feature behavioral abnormalities and active calls during sessions — signs that the victim is being coached through the process.
Execution and value transfer	Funds are moved to the scammer-controlled destination. Because the fake platform shows fabricated, growing returns, the victim may continue sending money.	High-risk payment behavior escalates through repeated payments. As the victim looks to funnel more money into the scam, they may also show unusual funding behavior, drawing from credit, moving retirement funds or transferring from multiple accounts.
Aftermath and recovery	The consumer discovers the investment was fake when withdrawals are denied, the platform disappears or the fraudster stops responding. By this point, the victim may have sent several payments over time, resulting in significant losses.	The institution receives a scam report involving authorized payments that may have occurred over an extended period.

How AI is impacting investment scams:

With AI, fraudsters can generate polished investment websites and fake trading dashboards while maintaining consistent messaging across chats and platform notifications, making the investment feel more legitimate over time.

Red flags to monitor:

- **First-time payments** to cryptocurrency exchanges, trading platforms, fintech wallets or unfamiliar external accounts
- **Repeated, increasing outbound transfers** to the same new recipient, platform or wallet
- **Rapid movement of funds** from savings, deposits or incoming transfers into outbound payment channels
- **Unusual funding behavior**, such as liquidating savings, requesting higher limits or moving money from multiple accounts before outbound transfers

Tools to stop investment scams in progress:

- **Transaction risk modeling** that evaluates payment amount, velocity, recipient history, payment rail and deviation from the customer's normal activity
- **Behavioral analytics** to detect when an authenticated customer's session behavior changes during high-risk transfer activity
- **Call-in-progress signals** to detect signs of coercion in initial transactions
- **Device-based link analysis** to connect seemingly unrelated payments that flow to the same beneficiary, wallet, device, account cluster or mule network

Tech support scams

Tech support scams occur when fraudsters impersonate support members from legitimate organizations. They offer to help fix fake security or technical issues by remotely accessing victims' devices. Once connected, the scammer can directly control an already-authenticated session, commit fraudulent transactions or steal sensitive data.

Lifecycle of a tech support scam

Lifecycle stage	What's happening to the consumer	What it looks like for the financial institution
Targeting/ grooming	The consumer sees a fake alert claiming their device or account has been compromised. The warning may say their computer is infected, or an unauthorized transaction has been submitted with the consumer's bank account.	The interaction is happening outside the financial institution's platform, but these schemes rarely happen in isolation. Once fraudsters identify a vulnerable platform, repeated attacks may result in a stream of customer support reports.
Initiation of trust	The consumer connects with a fake support representative. The scammer asks the victim to download remote access software, promising to fix the issue for the consumer.	The initial contact prompts a legitimate login from a known device and familiar network. Prior to contacting the fake support representative, the consumer may explore account security options or check balances of their own accord.
Scam in progress	The victim is prompted to log in to their account. With remote access established, the scammer takes control of the session.	Once the fraudster takes control, behavioral abnormalities emerge in full. Uneven or delayed cursor movement and keystrokes are common signs of a remote access tool in use.
Execution and value transfer	With control over the authorized session, the scammer initiates transfers from the victim's account.	While remote access is active, a rapid sequence of risky actions occurs within one session. Fraudsters may review balances, add payment recipients, check transfer limits and initiate transactions in a matter of minutes.
Aftermath and recovery	The victim realizes the support representative was fake after funds leave the account and never return.	Customer support receives a complaint from a consumer, often referencing remote access tools or refund policies that don't exist within the real company.

How AI is impacting tech support scams:

Fraudsters can generate realistic system warnings, polished troubleshooting scripts and convincing chat interactions that mirror the language of legitimate institutions. While the scam is in progress, fraudsters can use AI to respond fluidly to questions and adapt instructions based on what the customer sees onscreen.

Red flags to monitor:

- **Indicators of remote-access software**, screen sharing or remote-control tools active during an authenticated session
- **Familiar device and credential use** paired with unfamiliar session behavior
- **Rapid movement from login to sensitive actions**, such as MFA changes, profile updates, payee creation or outbound transfers
- **Frequent mentions of viruses**, refunds, pop-ups, device compromise and remote support in support conversations

Tools to stop tech support scams in progress:

- **Remote access detection signals** to identify signs of remote access tools in use to stop remotely controlled transactions in real time
- **Behavioral analytics** to detect when a known customer on a known device begins acting unlike themselves
- **Cross-channel monitoring**, including call center or chat interactions where customers mention pop-ups, support agents, refunds, viruses or device access

Romance scams

Often targeting victims on dating apps or social media platforms, fraudsters pose as potential romantic partners. They manipulate victims into sending money, sharing sensitive information or taking financial actions on the fraudster's behalf. They function similarly to imposter scams, but romance scams add a deeper layer. Fraudsters exploit victims' desire for companionship; that emotional investment can make victims less willing to accept that the person they're speaking with is not real.

Lifecycle of a romance scam

Lifecycle stage	What's happening to the consumer	What it looks like for the financial institution
Targeting/ grooming	The consumer is contacted by a potential romantic partner on a dating app, social media platform, messaging app or online community.	The relationship is developing entirely off platform, often through private messages, calls or video chats.
Initiation of trust	The fraudster messages the victim, building a connection over time. They may claim to live far away, work overseas, travel frequently or have another reason they can't meet in person.	As trust is built with the victim, the fraudster waits to introduce a financial request. Because the scam begins as a personal relationship, there may be no early indicators.
Scam in progress	Once trust is established, the fraudster introduces a financial need, like a medical emergency, travel issue or investment opportunity. The first request may be relatively small. If the victim pays, the fraudster escalates the requests.	A modest, first-time payment is made to a new recipient account. The transaction is carried out by the authorized account owner, and due to the trust built between the fraudster and the victim, clear signs of coercion might not be present.
Execution and value transfer	The victim continues to send money, believing they are helping someone they care about. Losses can snowball over weeks, months or even years.	Repeated payments to the same recipient, often increasing in value, appear over time. Payments may escalate to larger wires, real-time payments or crypto wallet transfers. These patterns may emerge in quick succession — or over the course of multiple months.
Aftermath and recovery	The victim realizes the relationship was fake, often after the fraudster disappears, promised visits never happen, or family members and friends intervene. The victim's emotional investment may make them reluctant to report the scam.	If reported, the institution receives a dispute or intervention request. Fraud teams may need to reconstruct a long-running pattern of transactions and determine whether earlier warning signs could have indicated an ongoing romance scam.

How AI is impacting romance scams:

Fraudsters use AI to create realistic photos, tailored messages, engaging conversations and deepfake video/audio with far less effort than before. If victims grow suspicious, these convincing images and messages can reinforce trust.

Red flags to monitor:

- **Repeated, increasing payments** to the same new recipient, wallet or external account
- **Continued payment attempts** after fraud warnings, declines or step-up challenges
- **Customers moving funds** from savings, retirement, credit or multiple accounts to fund outbound transfers
- **Customers showing resistance** to warnings or insisting the recipient is trustworthy despite limited verification

Tools to stop romance scams in progress:

- **Transaction pattern analysis** to detect repeated payments to the same new recipient, especially when amounts escalate over time
- **Persistent device recognition** to flag recipient accounts connected to devices with high-risk traits or previous history of fraud
- **Cross-channel analysis** connecting digital behavior, payment history, support interactions, warnings and prior risk events into a unified scam-risk view
- **Customer prompts focused on verification** whether the customer has met the recipient in person, independently verified their identity or been asked to keep the relationship or payments secret

Building a smarter scam defense

Scam tactics all follow a similar process, but the signals they leave behind can look very different. That's why there's no silver bullet for scam prevention. Holistic prevention requires multiple, unique data types to ensure comprehensive coverage.

Does that mean it's time to overhaul your fraud stack and implement every tool available to stop scams? Not necessarily. If you're looking to reduce scam losses and hasten detection, the most significant gains can be made by targeting your greatest vulnerabilities. The challenge is identifying those vulnerabilities.

First steps to stronger scam prevention

Retroactively searching for red flags, or tracking them through future investigations, can provide a solid idea of what tactics fraudsters are targeting your customers with. If you don't have visibility into your own scam data, though, targeting your industry's greatest challenges first can yield the fastest upgrades.

Industry	Greatest areas of exposure	Immediate scam prevention opportunities
Banks	Serve as the primary destination for payment initiation and fund movement, making them a common, high-loss-potential target.	Combine transaction risk modeling, device intelligence and behavioral analytics to identify unusual logins and high-risk payment activity.
Fintechs	Fast onboarding, low-friction experiences and rapid transactions make it easier for scammers to move money before suspicious activity is detected.	Use device intelligence and link analysis to identify suspicious account relationships, coordinated fraud activity and high-risk transfers.
Credit unions	Strong member relationships and a service-oriented approach make it more difficult to identify when trusted customers are acting under manipulation.	Deploy real-time intervention workflows and behavioral analytics to passively detect signs of coercion.

Stopping fraud across the customer lifecycle

Regardless of the tactic in play, every scam leaves behind signals along the way. The challenge for fraud teams isn't understanding that scams exist. Rather, it's identifying those signals early enough to intervene before a customer becomes a victim.

The most effective strategies combine multiple defenses to detect high-risk activity wherever it occurs: during account creation, login, payment or other account activity. The list of signals that can reveal scams is seemingly endless, but leveraging behavioral analytics, device data and network intelligence across the customer journey gives organizations a strong foundation to spot scams earlier and reduce losses.

Ready to learn how to detect high-risk activity across the entire user lifecycle?
Click here to speak with an expert

[1] https://www.ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud

[2] https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat

[3] https://www.cloudcommunications.com/news/october-2025-youmail-robocall-index

[4] https://www.signicat.com/the-battle-against-ai-driven-identity-fraud

[5] https://www.forbes.com/sites/steveweisman/2026/04/12/ic3-report-reveals-surge-in-cryptocurrency-investment-scams/

[6] https://www.ftc.gov/news-events/news/press-releases/2026/04/new-ftc-data-show-people-have-lost-billions-social-media-scams