The lifecycle of a scam

Some scams unfold in minutes. Others are built over days or weeks, with victims carefully targeted and manipulated long before any money moves.

For most financial institutions, a scam only becomes visible once the money is gone. But every stage leaves warning signs behind. The challenge is knowing what they look like and having the visibility to spot them before losses occur.

Stage 1: **Targeting and grooming**

What's happening in the scam

Fraudsters make first contact with potential victims through text, email, phone or social media.

How it appears for fraud teams

The scam is happening outside the financial institution's platform, but crowd-level, pre-attack indicators may appear, including spikes in cloned app or high-risk device traffic.

In 2025, U.S. scam reports hit an all-time high, with **3 million fraud reports filed, up over 15% YoY.**[1]

Stage 2: **Initiation of trust**

What's happening in the scam

Scammers build trust and urgency with follow-up messages, spoofed calls, deepfakes and cloned sites impersonating legitimate entities.

How it appears for fraud teams

The customer's behavior may start to shift, leading to hesitant or hurried login sessions and funds being moved between accounts to prepare for a transfer.

Deepfake fraud attempts increased by over 2,000% in the last three years and now account for 6.5% of fraud attempts.[2]

Stage 3: **Scam in progress**

What's happening in the scam

The victim is pushed to act, entering credentials into a fake site, granting remote access or initiating a money transfer.

How it appears for fraud teams

In-session signals indicate coercion: a call in progress, remote access tools in use, long hesitations and abnormal data entry during payment. If funds are sent, abnormal payment amounts or recipients may also appear.

Over 1 in 4 consumers reported encountering phishing emails, messages or scam calls in the past year.[3]

Stage 4: **Value transfer**

What's happening in the scam

Fraudsters capitalize by using stolen credentials to take over victims' accounts or move recently received funds off platform.

How it appears for fraud teams

Behavioral, device and network anomalies reveal account takeover attempts, while immediate transfers from high-risk recipient accounts may indicate fraudulent payments.

Stage 5: **Aftermath**

What's happening in the scam

The victim discovers the loss, or that the person behind the scam was never real. Some report it to their institution or law enforcement, while others don't for several reasons, including embarrassment.

How it appears for fraud teams

The funds are gone, and a costly investigation begins. On a larger scale, rising customer reports and notable attacks on industry peers point to campaigns already targeting your customers.

Annual consumer fraud losses rose from around **$770 million in 2015 to $15.9 billion in 2025.**[1]

Taking action

Financial institutions can't always see the manipulation behind a scam, but they can recognize the signals it leaves behind. We bring together behavioral, device, identity and fraud intelligence to help financial institutions identify risk across the scam lifecycle, enabling earlier intervention, more confident decisions and stronger protection for your customers.

Connect with one of our experts to explore how you can strengthen your scam prevention strategy, or download our white paper, for a detailed look at five common scams and the early indicators that can help fraud teams detect and stop them.

Speak with an expert

86% of consumers expect businesses to act on fraud-related concerns.[3]

View the white paper

[1] https://www.ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud
[2] https://www.signicat.com/the-battle-against-ai-driven-identity-fraud
[3] https://www.experian.com/thought-leadership/business/2026-identity-and-fraud-report