REPORT

Fraud & SAR Filings in Fintech: How to Combat ACH Fraud Cases

A data-driven look at the surge in SARs, evolving fraud typologies, & how to fight back

Unit21

TABLE OF CONTENTS

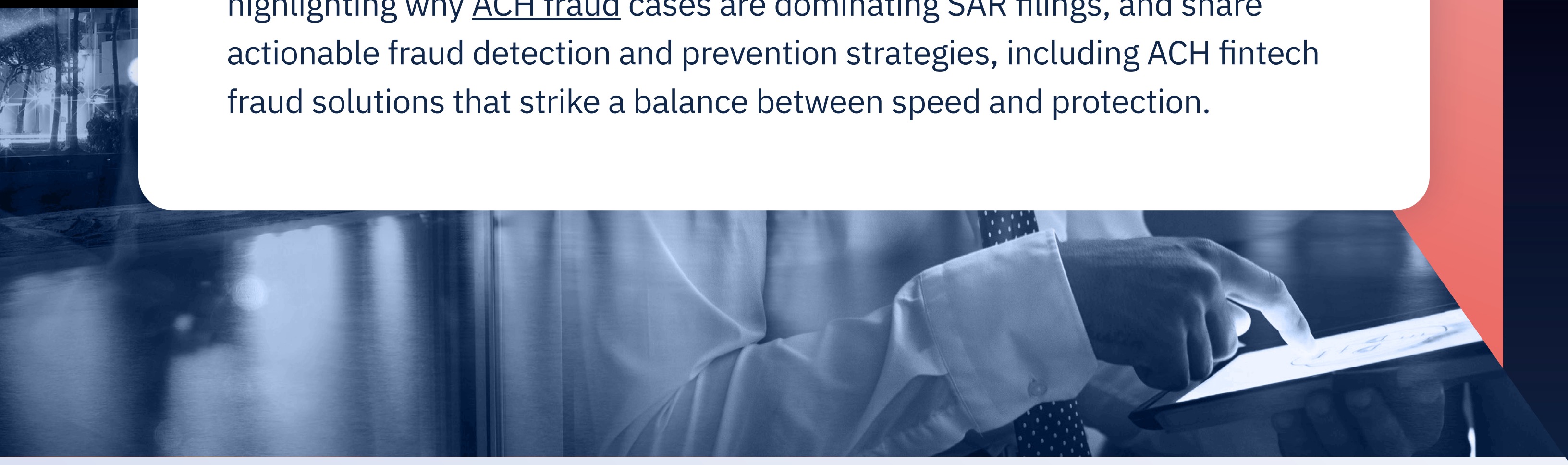
What's Inside

Introduction

Fintech platforms have revolutionized the payment space, but with it has come friction.

Although these players can move quickly with technological advances, they are also becoming more regulated and attracting fraudsters, much akin to traditional banking.

In this report, we delve into the data behind fraud trends in fintech, highlighting why ACH fraud cases are dominating SAR filings, and share actionable fraud detection and prevention strategies, including ACH fintech fraud solutions that strike a balance between speed and protection.



The Role of SAR Filings in Understanding Fintech Fraud

As the use of fintech increases, so does the risk of fraud and the importance of fraud detection and prevention, including Suspicious Activity Report (SAR) filing. Financial institutions, fintech, and other regulated entities are required by FinCEN to report any suspicious behavior that could allude to fraud, money laundering, terrorist financing, and other illicit crimes.

The SAR is an important piece of the puzzle used by FinCEN and law enforcement to facilitate collaboration, identify patterns, and create actionable intelligence.SAR filing is not simply an act of banks “checking the box” to be compliant. It’s a window into activity seen at individual institutions and companies.

SARs also give insight into the overall fraud landscape fintechs encountering various fraud typologies depending on their product offerings, and customer base.

The SAR Filings Surge Across Fintech

The volume of SAR filings is on the rise, particularly among fintech. Unit21's annual State of Fraud and AML Survey found that 48% of fintech companies reported an increase in SAR filings year-over-year, with 13% experiencing a significant increase. This upward trend adds to the workload of AML teams, requiring them to navigate complex reporting requirements while maintaining compliance with evolving regulations.

SARS Growth Across Fintechs

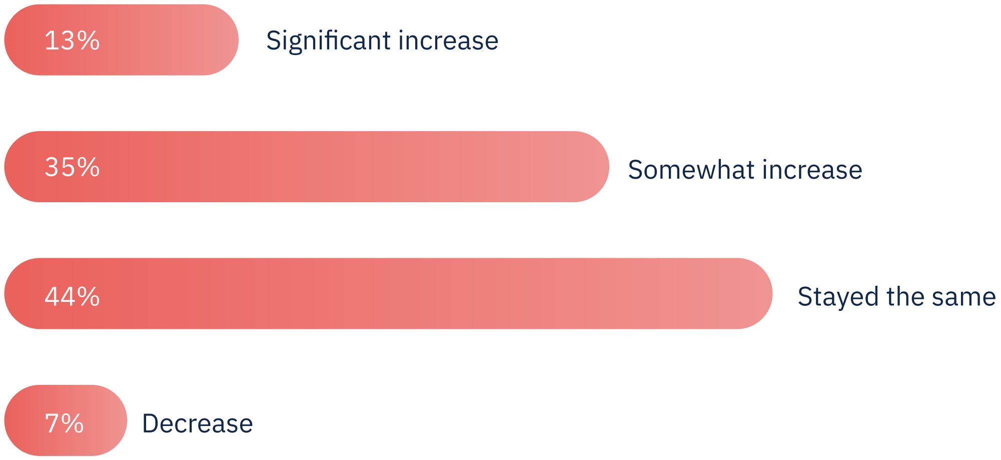
48%
of fintechs saw SAR increases YoY; 13% saw significant growth

40%
face an increased burden due to consent orders

23%
are actively dealing with regulatory actions

Source: Research from State of Fraud & AML: Fintechs

Growth in SARs Filings This Past Year



Regulatory actions, such as consent orders—legal agreements imposed by regulators to address compliance deficiencies without formal litigation—further compound the challenges faced by AML teams. A concerning 40% of respondents indicated that these consent orders require a significant amount of time and resources, diverting attention from core AML activities.

Within the fintech industry, approximately a quarter (23%) of companies are actively facing regulatory actions. This highlights the ongoing compliance pressures prevalent in the sector.

The Growing Distraction for Fintechs

40%
indicated that consent orders demand a significant amount of additional time and resources

23%
And nearly a quarter (23%) of fintechs are actively facing regulatory actions

Source: Research from State of Fraud & AML: Fintechs

4 of the Most Common Types of Fraud Across Fintechs

As with traditional banking, fintechs are not immune to fraud. Unit21 analyzed the SAR reporting from fintech customers over a one-year period to understand which types of fraud were driving SAR filings. Let's take a look at them below:

1 ACH Fraud

ACH took the cake when it came to the highest dollar amounts of potential fraud in the fintech landscape at $2.1 billion, and was the highest reported, with 9,972 SAR submissions.

There was a 100% growth in the dollar amounts associated with ACH SARs from Q1 2024 compared to Q1 2025. Submissions saw a steady increase as well, growing from 1,582 in Q1 2024 to 1,891 in Q1 2025, a 19.5% increase.

Although submissions also grew, the dollar amounts associated with these SARs grew exponentially higher.

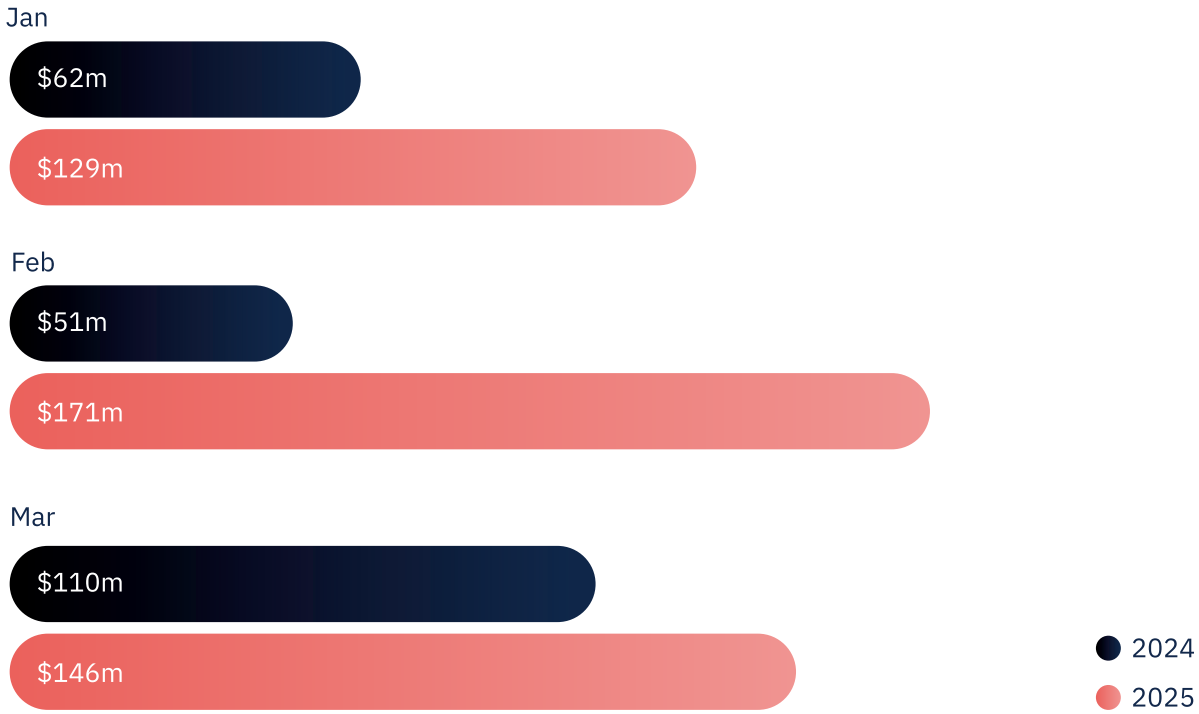
ACH Fraud: Fintechs' Most Concerning Fraud Vector

$2.1b
Amounting to $2.1 billion of potential fraud filed within Unit21

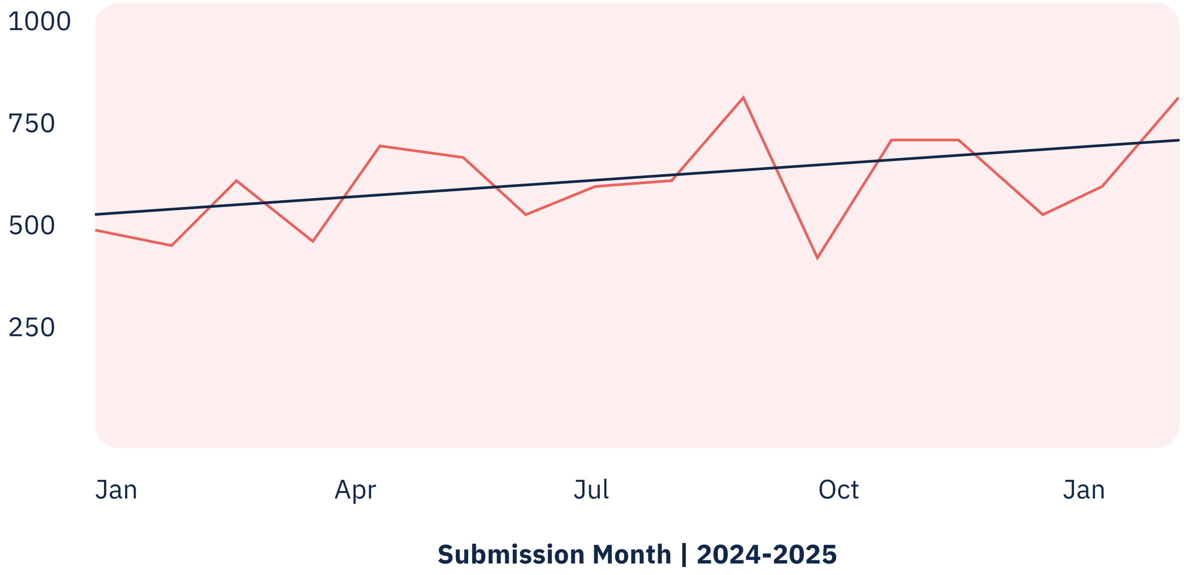
10k
Across nearly 10,000 SAR filings

SAR Filings: Growth in Quantity and Amount Filed

Q1 2024 vs Q1 2025 dollar amounts associated with ACH SARs saw 100% growth



Total Count Per Month



2 Credit and Debit Card Fraud

Credit and debit card fraud was the second most reported type of fraud, with 7,448 SAR submissions and a total dollar amount of approximately $1.76 million. While the volume is high, the average amount per SAR is relatively low compared to other types of fraud, indicating that these incidents are frequent but typically involve smaller dollar amounts.

This pattern highlights the widespread nature of card fraud and the operational burden it places on fintechs and AML teams. And, while each incident may involve relatively small dollar amounts, the high frequency means the cumulative operational and reputational impact is significant.

Fintechs should expect continued growth in card fraud attempts, particularly through mobile and e-commerce channels, as consumers increase their digital spending.

3 Identity Theft

Identity theft accounted for approximately 14.9% of total SAR submissions, making it the third most common type of fraud. However, it only ranked fourth in terms of total dollar value. This suggests that although identity theft occurs frequently, it often involves lower monetary losses per incident.

The data reflect the persistent challenge of identity theft in fintech, where a high volume doesn't necessarily equate to high-dollar losses, but still demands significant resources for fraud detection and prevention.

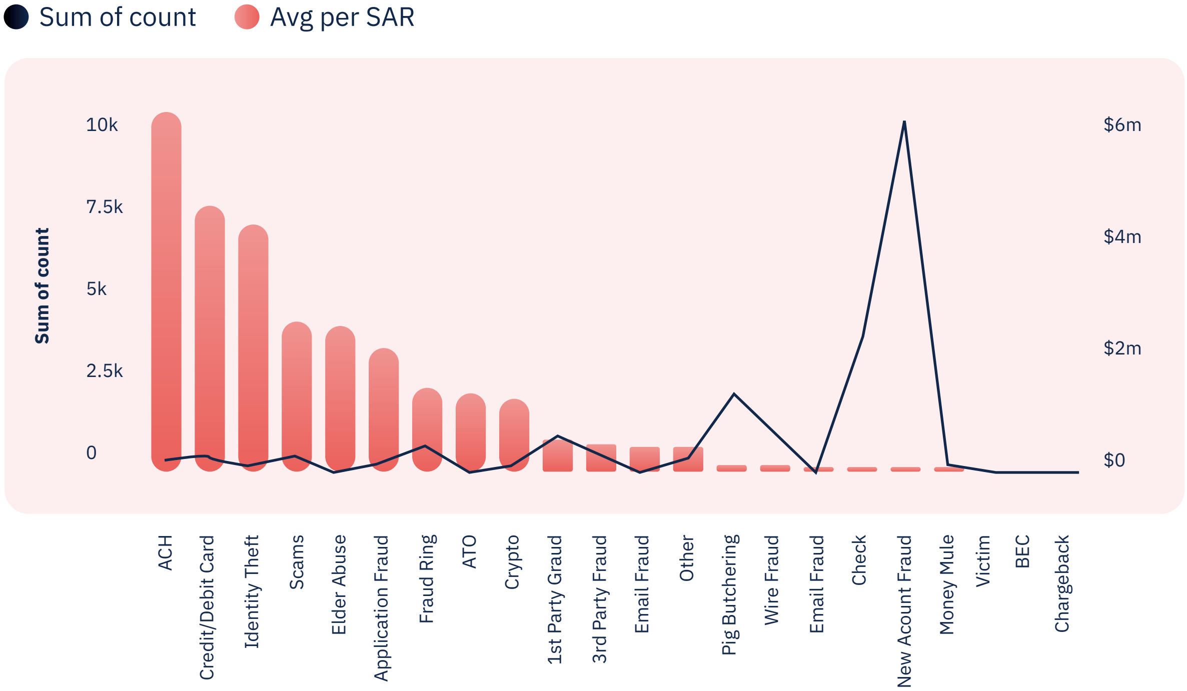
One of the most pressing forms of identity-related fraud affecting fintechs today is synthetic identity fraud. In these cases, fraudsters combine real and fabricated information to create new identities, enabling them to open accounts and initiate fraudulent transactions.

Without robust ACH fintech fraud solutions and identity verification controls, these cases frequently go undetected until substantial losses have occurred.

4 New Account Fraud

New account fraud stood out due to its disproportionate financial impact. Despite having relatively few SAR submissions, the average dollar amount per filing reached $5.7 million, which is by far the highest across all fraud types. This suggests that it doesn't occur often, but when it does, the amount involved is substantial.

Fraud Type and Number of Submissions



Why ACH Fraud Cases are Fintech's Primary Concern

So why are ACH fraud cases the most prevalent amongst fintech? It's largely because ACH is most commonly used in the fintech space because it is a low-cost alternative to card payments and wire transfers.

Unlike card transactions, ACH settles directly between financial institutions, cutting out the middleman. While some methods take days to process, ACH typically settles in two days or less, making it a preferred option as customers increasingly expect faster payments.

Additionally, fintechs rely on ACH for a variety of use cases, including direct deposit payroll, payment to vendors and supplies, and peer-to-peer transactions. It also plays a key role in driving customer acquisition, and engagement, as consumers now expect fast account funding and direct deposit capabilities.

Moreover, ACH supports embedded finance and modern user experiences, making instant account opening and funding via ACH a core feature for neobanks and their sponsor banks.

However, the same qualities that make ACH attractive also introduce risks. The industry not only expects faster payments, but it demands the least amount of friction possible. ACH helps fintechs deliver that expectation.

Unfortunately, as fintech prioritizes user experience and speed, the more it opens the door to an increase in ACH fraud cases. The faster the payments, the fewer opportunities there are to perform thorough Know Your Customer (KYC) checks and less time for risk evaluation.

How ACH Fraud Cases Happen

ACH fraud cases can occur in various ways. For new account funding, a fraudster could fund the account with an ACH to an unauthorized account and withdraw the funds before the debit comes back.

Fraudsters could also obtain compromised credentials and initiate ACH transactions. Or, using trickery and scams, convince someone to send a push payment via ACH. The use of push payment fraud amongst criminals is a growing trend in ACH fraud cases.

In fact, according to the 2025 AFP Payments Fraud and Control Survey Report, ACH credits were the target of more Business Email Compromise (BEC) scam activity in 2024 than in the previous year, rising to 50% from 47%.

This trend prompted the National Automated Clearing House (NACHA) to announce in March 2024 that its members had approved a set of rules intended to reduce the incidence of fraud that utilizes credit-push payments. The new rules don’t shift liability, but receiving financial institutions (RDFIs) will have a defined role in monitoring the ACH payments they receive.

Unless fintech companies take a more proactive approach to identifying new customers and performing due diligence, we can expect this trend to continue.

How to Identify Fraud Typologies and File Smarter SARs

To optimize the SAR filing process, fintechs should consider the various fraud typologies, their common characteristics, and the necessary information for the SAR.

Each fraud typology typically includes distinct elements, such as:

- **The target**
  This refers to the individual, account, or system that the fraudster aims to exploit or manipulate.
- **The instrument used**
  This is the financial tool or channel involved in the fraudulent activity, such as ACH transfers, wire payments, or debit and credit cards.
- **The method employed**
  This describes the specific tactic or approach used to carry out the fraud, including techniques like phishing, spoofing, or social engineering.
- **Associated red flags**
  These are the warning signs or unusual patterns that may indicate suspicious or anomalous activity related to a particular type of fraud.

When filing a SAR, the narrative is key in helping the fraud detection team understand what was suspicious and includes the specific typology involved. To streamline this process, fraud teams can match observed red flags with known typologies. This helps both in identifying suspicious behavior and crafting stronger SARs. Let's take a look at the examples below.

Enhancing SAR Narratives with Typology Mapping

If You Observe	Then the Typology Might Be	Associated Red Flags Include
Unverified funding sources tied to recurring payments	ACH Fraud	Returns, mismatched sender info, and micro-deposit abuse
Large, irregular transactions or layering of funds	Money Laundering	Unusual wire activity, structuring, and attempts to evade thresholds
Multiple failed logins or device/ location mismatches	Account Takeover	Unrecognized transactions, password resets, and unfamiliar IPs
Use of stolen identities or mismatched personal details	Identity Theft	Discrepancies in KYC info and unusual onboarding behavior
Rapid withdrawals or transfers from newly opened accounts	New Account Fraud	High-velocity transactions and synthetic identity indicators

Tip

Having templates for the different typologies can make it faster and more efficient when writing the SAR, as it allows you to know what to look for and what red flags are associated with the various fraud types.

How to Detect and Prevent ACH Fraud Cases in Fintech

Fraudsters are leveraging faster payments, new technologies, and regulatory gaps to exploit vulnerabilities across platforms. Without robust fraud detection and prevention strategies in place, fintechs will continue to face rising losses and regulatory scrutiny. Below are key strategies fintechs can implement to stay ahead of emerging threats and reduce exposure to ACH fraud cases, synthetic identity fraud, account takeovers, and other types of fraud.

AI & Machine Learning

Advanced technologies, such as AI and machine learning, are becoming increasingly essential in fraud detection and prevention. These tools enable fintechs to analyze massive datasets in real-time, flagging unusual activity that may signal a threat.

For example, ACH fintech fraud solutions using machine learning can detect anomalies in payment timing, device behavior, or location data that deviate from established user norms.

When paired with behavioral analytics, these systems build a baseline for each user's activity. If a transaction is attempted at an unusual time, from an unknown device, or in a foreign location, it triggers further scrutiny, often before the payment is finalized.

Real-Time Monitoring Making Impact

96% of those who have real-time monitoring implemented for more than a year testify to improvements, with **58%** noting a significant positive impact.

Real-Time Monitoring

Fraud moves fast, and so should detection. According to Unit21, 96% of fintechs that adopted real-time monitoring (RTM) for over a year reported improvements in their fraud prevention efforts. Over half (58%) saw a significant positive impact.

RTM is particularly effective for monitoring ACH fraud cases, as fraudulent transactions often happen within minutes of account compromise. With RTM in place, fintechs gain the ability to flag, delay, or block suspicious activity before funds are moved, preventing loss before it happens.

Fintechs can also integrate AI and machine learning into their fraud detection systems. These technologies enable the processing of large volumes of transactional data, the identification of behavioral anomalies, and the prediction of potentially fraudulent activity in real-time.

The key is finding the right balance: protecting customers and maintaining the integrity of payment flows without adding unnecessary friction to the user experience.

Automated SAR Filings and Case Prioritization

The ability to quickly file accurate SAR filings is a core component of compliance and investigation. AI-powered automation tools can help by collating alert data, grouping related activity, and drafting preliminary narratives, freeing up investigators to focus on high-priority cases.

Automation not only improves the speed and accuracy of filings but also maintains consistency in how types of fraud are documented and reported. The result is stronger compliance, faster response times, and a reduced operational burden.

Dynamic Risk Scoring

Fraud risk evolves over time; that's why fintechs need dynamic risk scoring models that adjust in response to changes in customer behavior. Instead of performing a one-time risk assessment at account opening, continuously updating the risk score enables smarter interventions and faster responses to emerging threats.

This approach is particularly valuable when monitoring types of fraud that emerge after onboarding, such as friendly fraud or synthetic identity misuse.

Consortium Data Sharing and Third-Party Integration

Fraud doesn't exist in a vacuum. Sharing data across fintech platforms through consortium models enables the detection of broader trends in fraudulent behavior. Integrating third-party sources, such as credit bureaus, sanctions lists, and adverse media databases, enhances real-time customer screening and risk profiling.

This collaborative intelligence is especially valuable for fintechs that operate across borders or serve underbanked populations, where traditional fraud signals may be less effective.

Multi-Factor and Biometric Authentication

Security at the login and transaction level is fundamental. Fraud detection and prevention start with requiring multi-factor authentication (MFA) for every login or high-risk transaction. While some view MFA as friction, it adds a critical layer of protection beyond just usernames and passwords.

To take it a step further, fintechs can implement biometric verification, such as fingerprint or facial recognition, to verify the user's identity before authorizing high-value ACH transfers or account changes.

Rule Automation and Rapid Deployment

The pace of fraud innovation demands fast response times. Fintech teams should be equipped with tools that allow them to quickly write, test, and deploy custom rules, often within hours, rather than days.

Additionally, automated rule deployment systems identify anomalous behavior early, enabling analysts to take action before fraud escalates. For example, a fintech might flag first-time ACH transactions that exceed a certain dollar threshold or hold transactions when there's a mismatch between the device fingerprint and the customer's usual behavior.

This agility is significant when dealing with new or evolving ACH fintech fraud solutions, as fraudsters constantly test for weaknesses in rules-based systems.

Device Intelligence and Velocity Checks

Device intelligence is a powerful layer in any fraud detection and prevention strategy, particularly when addressing ACH fraud cases. By incorporating device fingerprinting, fintechs can identify and block known fraud tools, emulators, or repeat devices linked to suspicious activity.

Velocity checks add another dimension, enabling platforms to monitor rapid ACH activity, such as multiple ACH credits across several accounts in a short period, which can be a red flag for fraud rings or mule account networks.

Fintechs should also monitor for anomalies such as unusual IP addresses, VPN masking, or inconsistent geolocation data. These indicators, when combined with behavioral and transaction data, provide deeper visibility into emerging types of fraud and help refine ACH fintech fraud solutions in real-time.

Tiered and Intelligent KYC Processes

Traditional Know Your Customer (KYC) methods often fall short in today's fintech landscape, either by creating unnecessary friction for low-risk users or by failing to catch high-risk individuals early. Instead of a one-size-fits-all approach, fintechs should adopt tiered KYC frameworks that scale based on user risk.

For instance, low-risk customers can benefit from a streamlined onboarding process, while high-risk users are subjected to more rigorous checks. The goal would be to minimize friction for legitimate users while requiring more stringent requirements for those who don't pass the initial checks.

To support this strategy, fintechs can implement tools such as document authentication, facial recognition, and real-time ID verification. Additionally, live detection technology can enhance online enrollment by confirming that the person behind the screen is genuine and present. Cross-referencing names and Social Security numbers with consumer reports and trusted databases can also help identify synthetic identities and other high-risk profiles.

The Future of ACH Fraud

Evolving Threats, Emerging Opportunities

Fintech has come a long way since its early days as a disruptive force in the financial services industry. What began as an agile, innovative alternative to traditional banking has now matured into a critical component of the global payments ecosystem, which is increasingly targeted by sophisticated fraud tactics.

As this landscape continues to evolve, so too must the strategies fintechs use to defend it. Unit21's latest findings make it clear: fintechs that invest in real-time monitoring and automation are seeing measurable gains in their fraud detection and prevention efforts.

With 96% of fintechs reporting improvements, and over half citing significant impact, it's evident that proactive, tech-enabled solutions are no longer optional; they are essential. The regulatory environment will also continue to tighten, especially around ACH fraud cases and other emerging types of fraud.

Fintechs must remain vigilant by not only staying on top of shifting guidance but also by building adaptive, intelligent systems capable of detecting and preventing fraud in real-time.

By combining advanced tools such as AI-driven behavioral analytics, dynamic risk scoring, automated SAR filings, and flexible rule deployment engines, fintechs have the opportunity not only to defend against fraud but also to lead the way in modernizing financial crime prevention.

Fight ACH Fraud with Smart Tools from Unit21!

In this fight against fraud, speed, strategy, and smart technology will be fintechs' greatest assets. Unit21 offers fintechs a comprehensive platform designed to adapt to today's most urgent threats.

Our ACH fraud solution helps fintechs and financial institutions prevent potentially fraudulent ACH transactions from entering the network, greatly lowering the risk of fraud and financial loss. It also flags suspicious ACH transactions through real-time analysis and automates ACH fraud case management to improve detection and response.

With Unit21, you gain the ability to detect risks early, prevent fraud effectively, and handle investigations confidently.

Get a demo today to learn how Unit21 can streamline your fraud investigations, increase detection accuracy, and reduce fraud losses.

Unit21