redefining the battlefront: new tactics in the war against fraud



jack henry

contents

03 introduction – navigating the ever-changing frontlines of fraud

03 check fraud – safeguarding against an unexpected adversary

04 scams – decrypting the deception

05 machine learning and AI – a pioneering defense

06 Financial Crimes Defender – a single pane of glass

introduction – navigating the ever-changing frontlines

In the relentless battle against fraud, change remains the only constant.

Fraud is no longer confined to a single transaction or channel. Organized networks now combine stolen identity data, social engineering, generative AI, synthetic documents, account takeover, and rapid money movement. For banks and credit unions, the challenge is to recognize risk across the accountholder journey while preserving the trusted experiences legitimate users expect. Consumers may also be manipulated into authorizing payments or sharing access, making intervention both a technology and trust challenge.

How do you effectively protect yourself from the pervasive fraud threats you're facing while still putting your accountholders first?

check fraud – safeguarding against an unexpected adversary

Check use has declined over the long term, but exposure has not disappeared. A recent analysis cited by The Clearing House and PYMNTS Intelligence found check payments were 31 times more likely to be fraudulent than real-time payments.[1] (The comparison measures fraud incidence, not loss severity, but it underscores why a declining payment method can remain a disproportionate risk.)



Fraud is no longer confined to a single transaction or channel.

While check fraud has always existed, the COVID-19 pandemic allowed for fraud rings to expand their presence and recruitment operations. By turning into a widespread organized venture, check fraud was able to flourish.

Check fraud has also evolved. Altering or "washing" stolen checks remains a concern, while organized schemes may also involve mail theft, counterfeit checks, fraudulent signatures, online distribution, and recruited accounts used to deposit items and move funds. FinCEN reported that mail theft-related check fraud was the subject of increased Bank Secrecy Act reporting after its 2023 alert.[2] Institutions should look beyond the individual item to connected signals such as account age, common devices, deposit patterns, funds-availability timing, and rapid withdrawals or transfers. The best way to get ahead of emerging schemes is to use a consortium database

of information, so when one institution does identify fraud, all can benefit. Consortiums especially come in handy when it comes to transit checks, where identifying alterations can be more challenging than on-us items.

Fraudsters have continued to adapt and are now producing their own checks, complete with microprinting and thermal ink, which can easily bypass traditional defense systems. Their operations have become highly organized, utilizing social media to share methods, hire accomplices, and distribute stolen account information.

Encouraging appropriate electronic payment options can reduce reliance on checks, but no payment method is risk-free. Financial institutions should pair payment modernization with layered controls, accountholder education, channel-specific monitoring, and clear procedures for investigating suspicious activity.

Another crucial tactic is the implementation of Positive Pay, a fraud prevention tool that verifies checks presented for payment against a list of issued checks provided by your accountholder. By ensuring that only authorized checks are processed, Positive Pay serves as a robust line of defense against check fraud by keeping your consumer accounts secure, before funds can be stolen.

Outside of Positive Pay, cross-channel visibility can help institutions identify typical activity and investigate anomalies. Connecting check, deposit, identity, device, and funds-movement signals can support earlier, risk-based decisions. Real-time decisioning may also help teams intervene before suspicious funds leave the institution, subject to applicable processes and controls.

scams – decrypting the deception

Fraud losses continue to rise as criminals use investment, impersonation, romance, business email compromise, and other schemes to manipulate victims. Consumers reported losing nearly $15.9 billion to fraud in 2025, an increase of more than 27% from 2023, according to the Federal Trade Commission.[3] Because reported losses do not capture every incident, institutions should treat the figure as a documented floor rather than a complete measure of harm.



Connecting check, deposit, identity, device, and funds-movement signals can support earlier, risk-based decisions

The true scale of scam losses remains difficult to calculate because not every incident is reported. Institutions should avoid treating a single reporting system as a complete estimate and should state the geography, period, and reporting population whenever they cite a loss figure.

Reimbursement expectations, payment-authorization questions, network rules, and applicable consumer-protection requirements continue to shape how institutions handle scam claims. Fraud, operations, compliance, and legal teams should review current obligations and escalation procedures together rather than rely on assumptions about how liability will evolve.

Accountholder education remains important, but education alone cannot stop manipulation that is personalized, urgent, and AI-assisted. A layered

response combines timely warnings with behavioral signals, device and identity intelligence, cross-channel visibility, risk-based intervention, and clear escalation paths for frontline and fraud teams.

While consumer education is effective, some scams will still deceive their intended victims. Ensuring you have a real-time enabled system (coupled with transaction interdiction) is essential in the fight against scams. By monitoring activities as they occur across all channels, you're enabling immediate detection and response to suspicious transactions outside of your consumers' normal activity. Transaction interdiction allows your system to intercept and halt suspicious transactions before they are completed, granting your institution the ability to protect your accountholders from scammers and significant losses.

Using a broad set of relevant data can help institutions identify patterns that might otherwise go unnoticed. Behavioral biometrics can add context by analyzing how individuals interact with devices and accounts. These signals should inform, rather than determine, a decision and should be evaluated alongside identity, device, transaction, and network information.

machine learning and AI – a pioneering defense

Generative AI (GenAI) is a double-edged sword, capable of both innovation and misuse. Fraudsters can leverage GenAI against you and your consumers by creating realistic, convincing scams with volume and ease. From fake customer testimonials to fabricated evidence, the utilization of AI-created deepfakes amplifies the risks posed against consumers.

But not all AI serves malicious intent. AI also stands as an effective tool in the fight against fraud. As transaction volumes increase and fraud tactics evolve, institutions need systems that can grow and adapt accordingly.

Modern fraud programs increasingly combine rules, machine learning, behavioral analytics, and human review. The goal is not to replace judgment, but to improve signal quality, adapt to shifting patterns, and evaluate identity and intent across onboarding, authentication, and transactions. Model governance, explainability, monitoring, and change controls remain essential.

Rules-based systems remain useful for known patterns and policy controls, but rules alone can struggle with changing behavior and cross-channel schemes. A hybrid strategy can combine transparent rules with adaptive analytics while preserving human oversight and governance.

Financial institutions can use accountholder context to establish behavioral baselines and identify unusual activity. However, anomalies are not automatically fraud, and apparently normal activity can still be manipulated. Strong programs combine behavioral context with identity, device, transaction, and network signals, followed by proportionate review or intervention.

To capitalize on this advantage and better protect accountholders requires that traditional rules and AI work in tandem. A number of different aspects need to be considered to make this transition successful:

data analytics and fraud risk scoring

Each accountholder's banking behavior is unique. What may seem suspicious for one may be entirely normal for another. That's why conventional segmentation based on peer groups can oversimplify "normal" banking behavior and generate too many false positives.

Robust data collection and analysis can help establish a baseline of accountholder behavior and surface

suspicious anomalies. Machine learning models may consider monetary and non-monetary activity, behavioral signals, device intelligence, and other relevant data at scale. Institutions should evaluate data quality, privacy, explainability, bias, performance, and governance as part of model design and ongoing monitoring.

fraud risk strategies

As financial institutions get more comfortable with the concept and application of machine learning models, many apply a hybrid approach as an intermediate step. A hybrid of both traditional rules and a machine learning risk strategy allows for dynamic anomaly detection – improving both detection and efficiency.

As your organization's maturity in applying AI and machine learning to fraud detection evolves, agility becomes increasingly important. Updating a risk strategy often involves fraud, data, technology, operations, compliance, and model-risk stakeholders. Effective change management should support timely tuning while maintaining testing, approvals, documentation, and oversight.

Configurable interfaces can give authorized fraud analysts and data scientists more control over risk strategies while reducing avoidable implementation bottlenecks. Access controls, testing, approvals, versioning, and auditability should remain part of the operating model.

model building, testing, and governance

Many data science teams manage numerous tools for data exploration, feature engineering, and other model development tasks. As a result, they're faced with disjointed steps and must stitch together conclusions on how their rules and models are performing. As such, evaluating your overall fraud risk strategy and tuning needs can become very manual and resource-intensive.

Automation can streamline parts of model development, testing, documentation, and monitoring, but it does not eliminate governance responsibilities. Institutions need an integrated environment that helps qualified teams build, test, approve, deploy, observe, and revise models with appropriate controls.

To further strengthen this fight against fraudsters, AI/ML systems can leverage expanded threat intelligence that goes beyond the activities within a single financial institution. By accessing broader data on emerging fraud trends, your systems can prepare for, and prevent, new fraud threats before any of your accountholders are even targeted, ensuring that you remain one step ahead.

Financial Crimes Defender – a single pane of glass

Fragmented fraud and BSA/AML operations can create duplicate work, inconsistent decisions, and blind spots. Jack Henry Financial Crimes Defender™ brings fraud detection and AML capabilities into a unified platform designed to help financial institutions coordinate risk decisions and investigations.

Financial Crimes Defender is a cloud-native platform designed to support real-time fraud detection and AML monitoring. The platform uses Feedzai technology as part of its risk-detection capabilities.[4]

Financial Crimes Defender uses AI and behavioral analytics to evaluate activity and support prioritized review. The platform is designed to automate portions of data collection and investigation workflows while helping teams focus on higher-value decisions. Importantly, the dispositioning of alerts in Defender sends feedback to Feedzai and Defender's database to ensure alert quality is consistently improving and false positives are reduced.

Creating a singular true real-time platform allows your financial institution to break down the typical fraud silos based on transaction types. Analytics pull the different transaction types together to mitigate how this new generation of fraud and money-laundering actors utilize multi-channel approaches to deceive your organization and accountholders.

Datos Insights has recognized Financial Crimes Defender for providing award-winning unified case management, network-level intelligence, and integration across core banking systems and payment rails.[5] Datos also praised Defender's vendor orchestration through a single API.[6] Institutions should validate the integrations and capabilities relevant to their environment.

The FraudClassifier℠ model, introduced by the Federal Reserve after collaborating with payments industry experts, is incorporated into Defender. The model provides an intuitive and standardized approach to classifying fraud and utilizes a consistent taxonomy, which empowers financial institutions to be able to better measure and manage fraud involving payments. As Jack Henry's fraud and financial crimes expert, Rene Perez (a member of the Fraud Definitions Work Group that developed the FraudClassifier) states "The model will help you understand fraud trends that you did not know you had in your institution."

The strategic opportunity is to move from fragmented, after-the-fact review toward coordinated, risk-based decisions across identity, transactions, and investigations. A unified approach can help teams act earlier, use investigative capacity more effectively, and protect accountholder trust as threats evolve.

connect with next-generation technology

Learn more about the real-time capabilities of Jack Henry Financial Crimes Defender.

For more information about Jack Henry, visit jackhenry.com.

sources

1. PYMNTS Intelligence and The Clearing House, *Fraud Is 31x More Likely on Checks Than Real-Time Payments*, August 2025.
2. Financial Crimes Enforcement Network, *FinCEN Issues In-Depth Analysis of Check Fraud Related to Mail Theft*, September 2024.
3. Federal Trade Commission, *The Rising Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, March 2026.
4. Datos Insights, *The 2025 Impact Awards in AML*, August 2025.
5. *The 2025 Impact Awards in AML*.
6. *The 2025 Impact Awards in AML*.

© 2026 Jack Henry & Associates, Inc.® | Public – For external distribution.