redefining the battlefront: new tactics in the war against fraud

jack henry™

contents

introduction

navigating the ever-changing frontlines of fraud

In the relentless battle against fraud, change remains the only constant. Fraud has always been a shifting adversary, but recent technological advancements are being manipulated for criminal purposes.

As fraudsters are leveraging modern technology to enhance their sophistication, efficiency, and success rates of their attacks, banks and credit unions are left on the front lines to find solutions and answers. To add to the problem, the line between ally and enemy is beginning to blur – as consumers become unwitting accomplices in the fight against fraud.

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

Once deemed an archaic method of payment, checks were expected to fade into obscurity as their numbers in circulation have declined by approximately 82% in the past 25 years.[1] Yet check fraud was listed as the primary top fraud concern for 75% of financial institutions in Jack Henry's 2024 Strategy Benchmark.[2]

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 gone through its own evolution. Traditionally it was primarily perpetuated by altering or "washing" stolen checks. With their newly organized operations, fraudsters have begun robbing United States Postal Service staff in efforts to obtain universal mail keys, also known as "arrow keys."[3]

After procuring these arrow keys, fraudsters were able to gain easy access to thousands of mailboxes in densely populated areas. Despite recent USPS changes implemented to increase the security of mailboxes and other vulnerabilities that are contributing to the surge in check fraud, the damage is done. Altered and counterfeit checks are on the rise.

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.

The most effective strategy to combat check fraud is to encourage accountholders to switch to secure electronic payment methods. Although changing consumer payment habits is challenging, this transition significantly reduces exposure to check fraud. Financial institutions must advocate for, and facilitate, this change to safeguard both themselves and their accountholders.

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.

Having **full transparency powered by real-time decisioning systems** is pivotal in detecting fraud attempts.

Outside of Positive Pay, maintaining a 360-degree view of all transaction channels is essential for identifying typical account activity and spotting anomalies. This comprehensive surveillance allows you to follow cashflow activity and to understand usual or unusual account patterns. Having full transparency powered by real-time decisioning systems is pivotal in detecting fraud attempts. By implementing real-time decision-making, you can close this vulnerability and act swiftly to intercept fraudulent transactions.

scams – decrypting the deception

While fraudulent checks dominate as the top fraud threat for financial institutions, romance and investment scams rank as the second-greatest threat[4] The 2024 Global Financial Crime Report by NASDAQ revealed North and South American consumers lost $13.8 billion to scams alone in 2024.[5]

At the same time, it is paramount to acknowledge that the true value of scam losses is difficult to calculate, as many scams continue to go unreported due to absence of mandatory reporting within the United States, as well as victims unwillingness to come forward from feelings of shame and embarrassment. Despite the absence of concrete figures, the U.S. regulatory landscape is aware of the extent scams are having on consumers, and changes are expected to regulations pertaining to liability in these incidents.

To compound the difficulty institutions are facing, according to Feedzai, 77% of consumers will leave their institution if they do not receive a refund for a scam.[6] Poised with such a risk, and with the Electronic Funds Transfer Act, also known as Reg E, expected to fall in favor of consumers, many institutions have proactively adapted their fraud case processes but still aim to mitigate the scams targeting their consumers as a whole.

Consumer education remains paramount in combating scams. Financial institutions must invest in comprehensive educational campaigns to inform consumers about the sophisticated nature of scams and how to recognize them. By empowering consumers with knowledge, institutions can significantly reduce the success rate of these fraudulent schemes and lower their losses.

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, in turn granting you the ability to protect your accountholders from scammers and significant losses.

Behavioral biometrics can provide an additional layer of data points and security by analyzing the unique ways individuals interact with their devices and accounts.

Leveraging full data points is crucial for seeing through obscurity and identifying patterns that might otherwise go unnoticed. Behavioral biometrics can provide an additional layer of data points and security by analyzing the unique ways individuals interact with their devices and accounts. This technology can detect unusual behavior indicative of fraud or scams, allowing you to take preemptive action against these threats, ensuring that no suspicious activity slips through the cracks.

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 detection systems enabled with AI/ML models are agile and responsive to emerging trends as they develop, rather than depending on inefficient static data points and rigid logic as legacy systems often do.

Banks and credit unions can no longer rely on traditional rules-based systems alone. Fraudsters quickly learn a bank's rules and thresholds – allowing them to circumvent these barriers to commit fraud. Typically, banks and credit unions respond by creating new rules once fraudsters outsmart the old ones. This can accumulate to hundreds or thousands of rules to manage, which is not manageable.

Through AI, financial institutions can discern what is normal for each and every accountholder. Knowing what's normal makes it easy to spot the abnormal - **and fraud is always abnormal.**

Financial institutions have one major advantage over the criminals, though, in being able to better understand their accountholders. institutions can discern what is normal for each and every accountholder. Knowing what's normal makes it easy to spot the abnormal – and fraud is always abnormal.

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.

You need robust data collection and analysis capabilities to build an accurate baseline of each accountholder's banking behavior to spot suspicious anomalies. Machine learning models can take into account hundreds of data points (monetary, non-monetary data, behavioral biometrics, device intelligence, and more) for each individual – at scale. This enables hyper-targeted detection of subtle changes in behavior for each individual's unique banking patterns. This robust analysis allows legitimate users to login, make account changes, and transact without friction while also ensuring fraudsters are stopped.

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 with applying AI and machine learning techniques for fraud detection evolve, an important factor to keep in mind is agility. Typically, updates in risk strategy involves a lot of personnel – from data analytics, fraud managers, IT, and more. To be effective against fraudsters and reduce fraud losses, your system needs to be flexible and fast when fine-tuning risk strategies.

Employing a no-code interface can improve autonomy. This self-service capability allows fraud analysts and data scientists to create, manage, and deploy models in real time without needing extensive IT support. Having a platform with intuitive design and built-in data science tools can make it easy to configure, based on your fraud risk appetite.

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.

By utilizing a variety of machine learning techniques, such as AutoML, OpenML, and more, you can automate time-consuming tasks for model development and governance. You need a platform with an accelerated environment for data scientists and analysts to efficiently build, test, and deploy models to adapt to evolving threats – within days, not weeks – in one integrated runtime environment.

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

In the complex realm of fraud prevention, fragmented operations can hinder effectiveness. That's why Jack Henry Financial Crimes Defender™ is a comprehensive solution that integrates fraud and BSA/AML under one platform, offering an all-encompassing view of financial crimes. This integration breaks down silos, creating faster and smarter fraud prevention, allowing for Defender to be your premier asset.

Financial Crimes Defender provides a next-generation, cloud-native platform to manage/automate fraud processes in true real time. The Defender platform's analytics engine integrates Feedzai, the world's largest RiskOps engine for financial risk management.

Utilizing AI and behavioral analytics, Financial Crimes Defender learns accountholder behavior, proactively uncovering new fraud and BSA trends – providing you only the alerts you need to review. Repetitive tasks are also automated, reducing manual work in investigations.

Proven analytics then make anomaly detection proactive, instead of the traditionally reactive approach used by most systems today. 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.

The platform uses one of the top AI/ML learning engines and works with digital systems to offer some of the best alerting technology on the market. The solution not only detects the activities in question, but helps you act on the intel to mitigate losses or recover funds immediately. With its open API, you can also integrate the data you want to monitor into a single, real-time platform.

The FraudClassifier℠ model, introduced by the Federal Reserve after collaborating with payments industry experts, is incorporated into Defender. The model provides an intuitive 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."

With Defender, financial institutions are empowered to be proactive rather than reactive in the fight against fraud, ensuring robust protection for today's accountholders and your assets.

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. Federal Reserve System, Commercial Checks Collected through the Federal Reserve--Annual Data, accessed September 2024.
2. Jack Henry 2024 Strategy Benchmark.
3. United States Postal Inspection Service, 2022 Annual Report, accessed September 2024.
4. Jack Henry 2024 Strategy Benchmark.
5. NASDAQ, 2024 Global Financial Crime Report, accessed September 2024.
6. Feedzai, The Human Impact of Fraud and Financial Crime on Customer Trust in Banks, accessed September 2024.