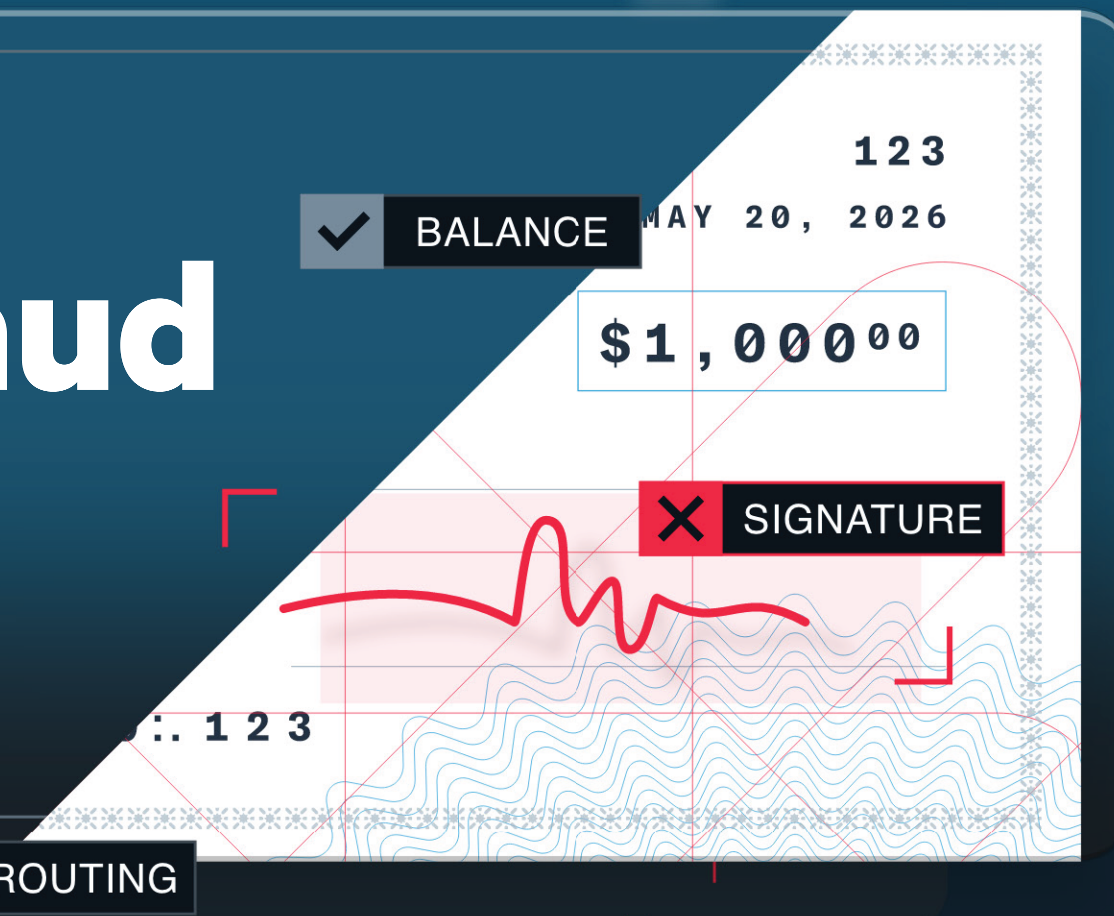
Mitek

e-Book:

Check Fraud Defender

ADDRESS



ACCOUNT

The resurgence of check fraud

Check fraud accounts for 31% of all bank fraud[1]

Check fraud is no longer a legacy payments issue — it has become one of the most persistent and financially damaging fraud threats facing financial institutions today.

According to the 2026 AFP Payments Fraud and Control Survey, checks remain the payment method most impacted by fraud, with 63% of organizations reporting attempted or actual check fraud activity. Fraudsters continue to target business checks due to their high transaction values, predictable payment patterns, and continued reliance across commercial payment workflows.

At the same time, check fraud activity has surged in recent years, fueled by mail theft, counterfeit and altered checks, and increasingly sophisticated fraud operations. Despite the continued growth of digital payments, billions of checks are still processed annually, creating a significant attack surface for financial institutions.

This combination of volume, value, and vulnerability has fundamentally changed the fraud landscape — forcing financial institutions to modernize traditional fraud controls and move detection earlier in the deposit lifecycle.

Check fraud remains high due to a variety of factors:

- **Low-tech, high impact**: The low-tech nature of paper checks offers a path of less resistance for would-be fraudsters. Using Generative AI, “casual fraudsters” are able to make alterations relatively easily, making paper checks a favored target in a world brimming with far more complex scams.
- **Enormous volume, enormous risk**: Despite the shift to digital payments, nearly 3 billion checks were still processed by the Federal Reserve in 2024, underscoring the continued reliance on paper-based payments and the significant opportunity this volume creates for fraud.
- **Easy access**: A significant number of checks are pilfered from seemingly secure routes, such as residential mailboxes and the familiar blue mail drop-off boxes. Criminals can easily leverage uncomplicated tools and techniques to alter these checks and make unauthorized transactions.
- **Rising sophistication of crime**: No longer are criminals merely altering checks; they’re counterfeiting them, creating multiple layers of deception that range from double presentment fraud to synthetic identity fraud—a hybrid of authentic and invented details to create new identities.

1 www.frbservices.org

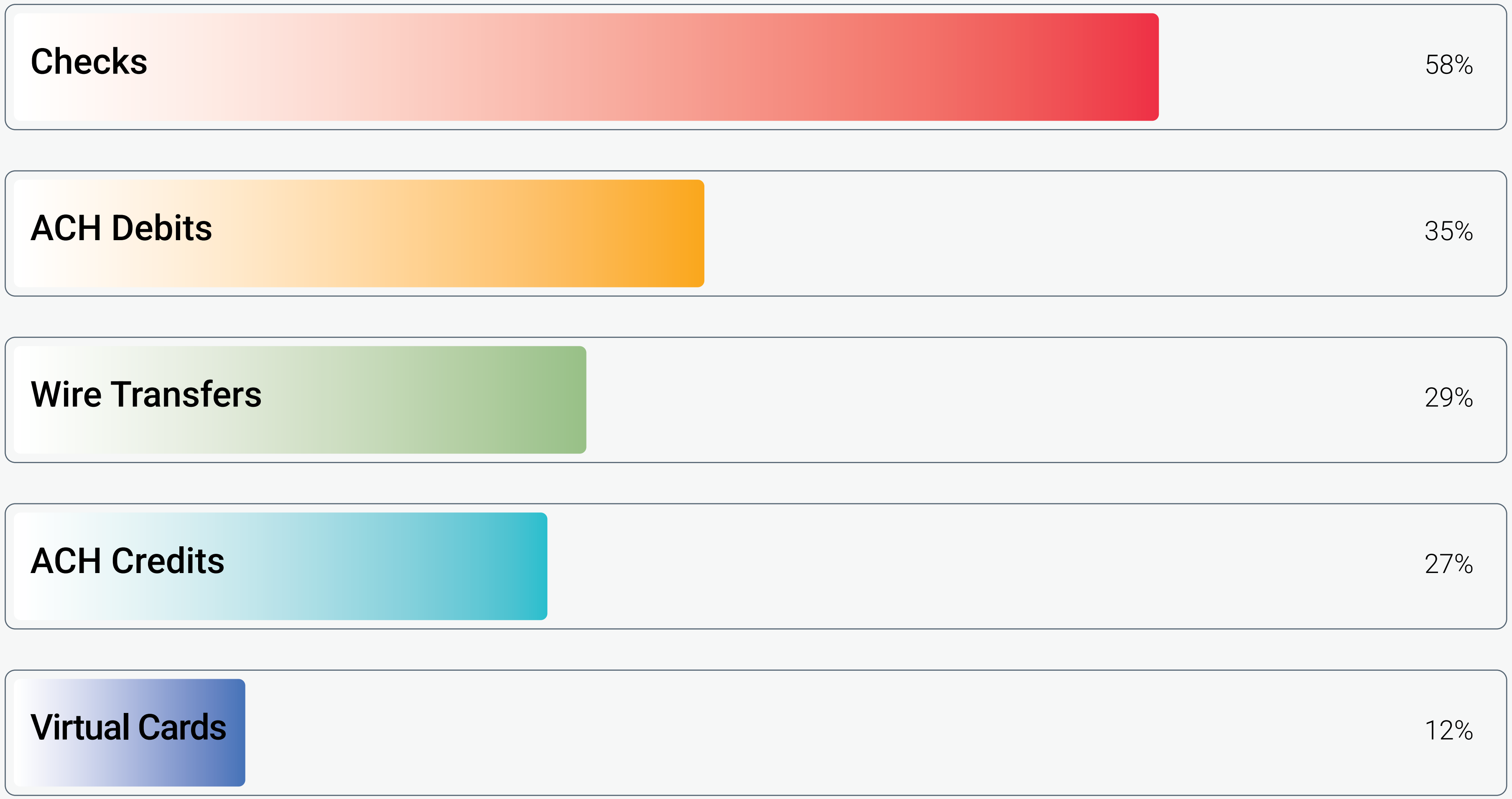
Check fraud is a game of opportunity. It's a low-tech and relatively easy crime to pull off, and there is still a sizeable pool of potential victims.

- **Check fraud-related suspicious activity exceeded $688 million** in a six-month period following FinCEN's nationwide alert on mail theft-related check fraud, highlighting the growing scale and sophistication of organized fraud activity[1]
- **According to the 2026 AFP Payments Fraud and Control Survey, 63% of organizations experienced attempted or actual check fraud in 2025**, with checks remaining the payment method most frequently targeted by fraudsters[2]
- **Business check fraud losses continue to rise, with the average incident now exceeding $150,000**, reflecting the increasing financial impact of counterfeit, altered, and stolen check schemes targeting commercial accounts[2]

1 Financial Crimes Enforcement Network (FinCEN) – Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Association for Financial Professionals

2 Association for Financial Professionals (AFP), 2026 Payments Fraud and Control Survey Report

Fraud loss expense by payment type



The significant rise of check fraud over the past several years continues to be costly for financial institutions and their customers. Now, more than ever, institutions need a better way to quickly and accurately detect check fraud to reduce operational expenses and overall losses.

Operational costs to your institution

Fraudsters are working together across criminal social networks to gain insights into the inner workings of financial institutions. They are collaborating to ultimately be more successful in their check fraud tactics and strategies. They are also capitalizing on financial institutions' outdated processes for detecting fraudulent checks and taking advantage of holes in their systems that allow for false positives and false negatives.

The large number of false negatives and false positives identified in existing fraud solutions force financial institutions to manually review numerous checks that are "flagged" as potentially fraudulent and to set review thresholds relatively high to bypass the investigation of fraud involving smaller amounts.

Both actions result in greater costs. Either from actual losses incurred or by increased operating costs for fraud and risk mitigation departments.

Ultimately, the nature of an institution's fraud costs means that improving the quality, and accuracy, of fraud detection translates into reduced exposure and lower overall operational costs.

Areas contributing to operational costs include:

- Ownership of one or more fraud detection solutions
- Staffing salaries and other operational overhead for fraud analysts
- Prosecution and legal fees

Your reputation and the customer experience

Even as the number, and types, of fraud prevention solutions proliferate, financial institutions of all sizes continue to experience substantial losses from check fraud. FIs must also contend with added expenses when the solutions lack automation, and often see negative impacts to their customer experience and overall brand reputation which can affect the bottom line.

Banks should consider the added exposure associated with:

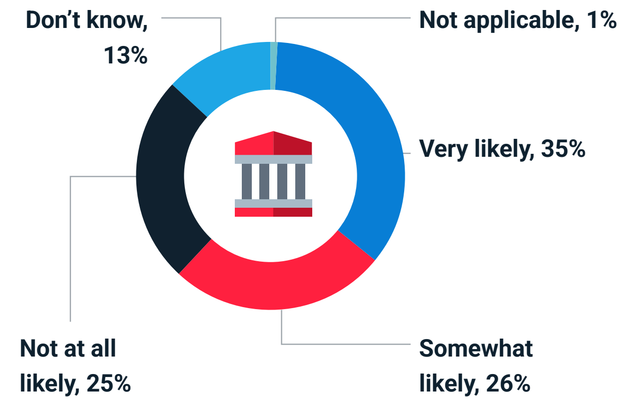
- Employees reviewing alerts, handling disputes, and interacting with customers
- Slower transaction processing and greater financial risks
- Poor customer experience and negative brand perception

Depending on your institution's policies, the number of customers that can be affected by poor check fraud mitigation, whether due to delayed transaction confirmation, having transactions blocked, or even money loss, can be a major concern.

In fact, according to a Datos Insights' fraud and authentication survey, 61% of consumers indicate that they would be likely, or somewhat likely, to leave their institution if unauthorized or fraudulent transactions occurred on their checking account.

Q. How likely would you be to leave your bank or financial institution if unauthorized or fraudulent transaction occurred on your checking account?

(Base: U.S. Banked consumers)



Source: Datos Insights fraud and authentication survey of 1,026 U.S. consumers, Q2 2024

Detecting check fraud

Financial institutions have historically implemented rules-based fraud detection systems and considered them as the standard in “on-us” and deposit fraud operations. In turn, institutions end up executing several rules and “tune” them, using experience to learn and improve, resulting in suspect fraud ratios between 250:1 to 300:1.

Thankfully, advanced image data analytics has provided the answer to reducing the cost of fraud:

A direct correlation exists between fraud losses, operational fraud management costs, and the quality and number of alerts generated by a fraud management system. By improving the accuracy of fraud detection, a financial institution will experience significant cost savings.

Effective fraud detection utilizes information curated from a variety of criminal channels to recognize known fraud patterns as well as incorporate images from new and emerging fraud schemes.

Ultimately, the number of fraudulent transactions compared to the total number of transactions represents a very small amount, making it difficult to find all fraudulent items while at the same time, not generating too many false positives. To select the correct items, a solution must consider many attributes, including the transaction, the customer, and the merchant.

Experts cannot develop or maintain business rules with escalating levels of complexity. Computer vision and AI detection provide the right balance between fraudulent and authentic items across a large number of attribute dimensions.

The power of a consortium

For many financial institutions the idea of a consortium is new. Sharing information and the risks and challenges involved can seem daunting. Consortiums, such as credit bureaus, telecommunications, and transportation consortiums are commonplace and those businesses that are part of the ecosystem benefit from the sharing of certain information, and by working together to achieve a common goal – in the case of a fraud consortium, institutions are working together to reduce fraud in their institutions.

When thinking about a fraud consortium, it's best to start with known best practices, such as enabling the latest security technology to prevent data breaches. Examples of these type of practices include:

- Securing data, through encryption, while it's at rest
- Mandating controlled access management
- Implementing industry standards and compliance requirements
- Creating a user group to discuss and collaborate on consortium priorities

A true consortium can accelerate both detection and reaction. Just as fraudsters get more sophisticated and collaborate to enhance their schemes, financial institutions must begin to work together to share fraud information and insights, ultimately banding together to deter and defeat fraud attempts before they gain traction or move from one institution to another.

> "If you have an apple and I have an apple and we exchange these apples, then you and I will still each have one apple. But if you have an idea and I have an idea and we exchange these ideas, then each of us will have two ideas."
>
> — George Bernard Shaw

The Check Fraud Defender advantage

Check Fraud Defender is a secure, cloudbased solution that strengthens your existing fraud prevention and management solutions by leveraging advanced AI for real-time check comparison and analysis across all channels. Our solution is bolstered by a cloud-hosted consortium that expands fraud intelligence and decisioning beyond the “four walls” of a single bank and allows for fraud detection in real-time. It reduces the number of checks routed for manual review and can help reduce risks associated with synthetic and account fraud, forged checks, and identity theft.

Check Fraud Defender also uses proprietary image analysis to extract data from stolen checks, account screens, and identification documents sold on criminal channels to provide real-time alerts of potentially compromised accounts.

Utilizing both account and image-based data, Check Fraud Defender provides true check fraud coverage with the ability to inspect more than 24 key check attributes including; payee information, LAR and CAR style and location, check stock, date validation, handwriting style, signature style and location, MICR validation, memo line, and more.

As the financial industry continues to strive for faster payment turnarounds, Mitek aims to leverage its expertise as the inventor of Mobile Deposit technology to introduce realtime check fraud detection, for all deposit channels, at the time of capture. This solution will enable institutions of all sizes to address items at point of capture, rather than at end of the day or next day.

Mitek’s continuous innovation underscores our dedication to providing financial institutions with cutting-edge tools to protect their customers and assets, ensuring that CFD remains at the forefront of check fraud prevention in an increasingly complex financial landscape.

Control at your fingertips.

As a part of Mitek's Check Fraud Defender platform, the MiControl Fraud Management Console provides financial institutions with a comprehensive dashboard to quickly detect, analyze, and stop incoming check fraud.

Through a simple and intuitive user interface, back-office employees can seamlessly escalate or review check fraud through advanced visualization tools that yield greater efficiency and fewer errors. Its intuitive user interface makes single and multi-item reviews, escalations, and queue management a snap.

By leveraging adaptive business rules, actionable insights, and clear visual overlays, MiControl supports day-zero, prior to posting, analysis and decisioning of fraud suspects.

With its clear dashboard of actionable insights and the ability to create customized business rules selected by the bank and based on information shared through our consortium, MiControl can decrease the time it takes for a fraud analyst to review and decision a suspect check from between 5-10 minutes to about 90 seconds.

Your key to back-office efficiency.

Through proprietary visual inspection modeling, Check Fraud Defender helps decrease your operational costs without disrupting your current fraud prevention workflows. The platform itself requires very little integration effort, and your team can easily filter alerts and set business rules. This allows your institution to focus on the fraud that matters and helps your fraud team quickly triage flagged deposits and make decisions based on a high degree of available information, all through one centralized management console.

Minimize false positives
An advanced, visual-based system inspects more document attributes, so fewer checks are flagged for review, resulting in reduced false positives.

Accelerate reviews
Actionable insights and opacity overlays help reviewers validate checks faster and more efficiently.

Decrease operational costs
Proprietary, automated visual inspection modeling helps reduce manual reviews by providing automated, accurate check fraud detection.

Creating a better customer experience.

Financial institutions strive to give their customers a great experience at their bank. However, when customers are impacted by check fraud, they often face significant hidden costs and financial disruptions that can have lasting effects on their financial and emotional well-being. So, in addition to financial institutions being financially responsible for check fraud losses, incidents of check fraud can also cause a ripple effect on an institution's reputation, potentially leading to customer attrition and difficulty attracting new customers.

With Check Fraud Defender, you can give your customers the security and peace of mind they demand.

Check Fraud Defender can detect forgeries often missed by other fraud tools or not detected until much later in the check clearing process, like forged signatures, legal and courtesy amounts, and recipient name. With terminal status feedback from all participating financial institutions, Check Fraud Defender flags future check deposits tied to stolen checks and fraudulent checks, at risk account data, and duplicate deposits.

Built by bankers for bankers.

With a strong commitment to staying ahead of ever-evolving fraud trends, and forwardthinking development, Check Fraud Defender was created with the goal of ensuring a robust check fraud prevention solution that helps your institution proactively address the evolving threat of check fraud.

Our purpose-built fraud solutions were created and developed by industry experts from leading financial institutions, leveraging their expertise in fraud detection, prevention, and banking technologies to ensure we stay at the forefront of fraud affecting both banks and credit unions.

Now, more than ever, it's time to partner with the global leader in check fraud security and unite with other institutions to stay ahead of fraudsters and escalating threats. Through our robust fraud consortium, institutions can proactively defend against "migrating" fraud scams before they are victimized.

With security and compliance, top of mind, Mitek's check profiles are stored in a secure, cloud-hosted environment that utilizes end-to-end encryption and ISO 270001 certified security protocols.

THE NEXT GENERATION OF POSITIVE PAY

Positive Pay Plus

Check fraud is rising, but adoption of traditional prevention tools has not kept pace. According to Datos Insights, more than 90% of financial institutions report an increase in fraud attacks targeting business customers, yet adoption of Positive Pay remains inconsistent and often reactive.

In many cases, financial institutions only introduce Positive Pay after a client has already experienced fraud, with nearly 74% requiring it post-incident rather than proactively.

THE REACTIVE MODEL

This reactive model leaves a critical gap in protection and exposes both institutions and their business customers to avoidable losses.

The challenge with traditional positive pay

While Positive Pay remains a foundational fraud control, legacy approaches introduce friction and limit effectiveness:

- Manual file uploads create operational burden for business customers
- Limited validation capabilities leave exposure to altered and counterfeit checks
- Reactive deployment reduces effectiveness in preventing fraud
- Low adoption rates leave many commercial accounts unprotected

> Even when implemented, traditional Positive Pay often operates too late in the process, identifying discrepancies after checks have already entered clearing workflows.

Introducing Positive Pay Plus

Positive Pay Plus modernizes this approach by shifting detection earlier in the transaction lifecycle and reducing friction for both financial institutions and their business customers. It enables financial institutions to:

- Validate issued check data at the point of presentment, including at the Bank of First Deposit
- Detect altered, duplicate, and out-of-range checks before funds are released
- Integrate seamlessly into existing treasury workflows
- Reduce reliance on manual file handling and exception processing

A NEW STANDARD FOR BUSINESS BANKING FRAUD PROTECTION

Financial institutions are at an inflection point. As fraud continues to rise and business customers face increasing risk, Positive Pay can no longer be treated as an optional or reactive service. **Positive Pay Plus represents the next evolution, enabling earlier detection, improved adoption, and stronger protection for commercial accounts.**

Learn more at www.miteksystems.com

Follow Mitek on LinkedIn, YouTube, and read Mitek's latest blog posts here.

To learn more about how to stop check fraud at your institution, contact your sale representative today to see Check Fraud Defender in action.

Check Fraud Defender in action

Mitek (NASDAQ: is a global leader in digital identity and digital fraud prevention, with technology to bridge the physical and digital worlds. Mitek's advanced identity verification technologies and global platform make digital access faster and more secure than ever, providing companies new levels of control, deployment ease and operation, while protecting the entire customer journey. More than 7,800 organizations use Mitek to enable trust and convenience for mobile check deposit, new account opening and more.