Accredited Standards Committee X9 Inc.

Financial Industry Standards ®

INFORMATIVE REPORT

Mitigating Check Fraud Risk in the Modern Financial Ecosystem

Number: ASC X9 IR-13-2026

Published: May 7, 2026

Developed by: The X9 Check Fraud Industry Forum

i) Foreword

This Informative Report has been approved and released by Accredited Standards Committee X9, Incorporated ("ASC X9"), 275 West Street, Suite 107, Annapolis, MD 21401 USA. This document is copyrighted by ASC X9. It is not an American National Standard, and the material contained herein is informative and not normative in nature.

This Informative Report is a product of ASC X9. It was produced by the Check Fraud Industry Forum, which was created by the ASC X9 Board of Directors in February 2025 to canvas users of the various check standards and technical reports, like TR 8 Check Security, to solicit feedback on the standards and input on their needs.

The information in this report reflects the views and information available at the time of publication and may be revised as technology, standards, and industry practices evolve.

Comments, suggestions for improvement, and proposed revisions are welcome and should be sent to:

X9 Committee Secretariat
Accredited Standards Committee X9, Inc.
Financial Industry Standards
275 West Street, Suite 107
Annapolis, MD 21401 USA

This report is published by ASC X9 and is available to the public free of charge from the ASC X9 website at https://www.x9.org.

Published in the United States of America.

ii) X9 Board of Directors (List of Members):

At the time this Informative Report was published, the ASC X9 Board of Directors had the following member companies and company representatives and X9 had the following staff:

Corby Dear, X9 Board of Directors Chair
Ted Rothschild, X9 Board of Directors Vice Chair
Steve Stevens, X9 Executive Director
Janet Busch, Director of Operations
Ambria Calloway, Program Manager
Lindsay Conley, Project Manager

Organization Represented	*Representative*
Amazon	Smita Mahapatra
American Bankers Association	Karin Flynn
American Bankers Association	Ananda Radhakrishnan
American Bankers Association	Tab Stewart
American Bankers Association	Shannon Williams
American Express Travel Related Services Company	Matt Crothers
American Express Travel Related Services Company	Brian Politz
American Express Travel Related Services Company	Sophie Rainford
Bank of America	Rich Clow
Bank of America	Chuck Gruesbeck
Bank of America	Matt Sharp
Bank of America	Michael Smith
Bank of New York Mellon	Kevin Barnes
Bank of New York Mellon	Michael Kozol
BankVOD	Sean Dunlea
Bloomberg LP	Corby Dear
Bloomberg LP	Rich Robinson
Brook Path Partners, Inc. (representing FIX Protocol Ltd - FPL)	Lisa Taikitsadaporn
Capital One	Matthew Hines
Citigroup, Inc.	Sudha Iyer
Communications Security Establishment	Jonathan Hammell
CUSIP Global Services	Matthew Bastian
CUSIP Global Services	Roger Fahy
CUSIP Global Services	Gerard Faulkner
CUSIP Global Services	Scott Preiss
Deluxe Corporation	Margiore Romay
Deluxe Corporation	Andy Vo
Diebold Nixdorf	Bruce Chapa
Diebold Nixdorf	Anne Konecny
Diebold Nixdorf	Alexander Lindemeier
Digicert	Dean Coclin
Digicert	Tim Hollebeek
Discover Financial Services	Carey Ferro
Discover Financial Services	Gregory Wren
Dover Fueling Solutions	Harish Veeravalli
Early Warning Systems	Adam Klappholz
Early Warning Systems	Mark McInnes
FactSet Research Systems Inc	Michele Lieber
Federal Reserve Bank	Ainsley Hargest
Federal Reserve Bank	Mark Kielman
FirstBank	Ryan Buerger

FIS	Prashant Gupta
FIS	Tami Harris
FIS	Cary Jeffers
FIS	Gail Lumsden
FIS	Prajoy Prabhakaran
FIS	Gary Sliger
FIS	Joe Stein
Fiserv	Andrea Beatty
Fiserv	Jacqueline Dill
FIX Protocol Ltd - FPL	James Northey
Futurex	Ryan Smith
Harland Clarke/Vericast	Todd Herndon
Harland Clarke/Vericast	Andy Marek
Hyosung TNS Inc.	JaeWhan Shin
IBM Corporation	Richard Kisley
Ingenico	Steven Bowles
Ingenico	Wayne Burgess
Invenco by GVR	Scott Spiker
Invenco by GVR	Bruce Welch
ISITC	Jason Brasile
ISITC	Lisa Iagatta
ISITC	Rich Robinson
ITS, Inc. (SHAZAM Networks)	Scott Green
ITS, Inc. (SHAZAM Networks)	Manish Nathwani
J.P. Morgan Chase	Andrew Francis
J.P. Morgan Chase	Clinton Jones
J.P. Morgan Chase	Ted Rothschild
Keyfactor	Tomas Gustavsson
MasterCard Europe Sprl	Mark Kamers
Member Emeritus	Todd Arnold
Member Emeritus	Thomas Brown Jr.
Member Emeritus	Andi Coleman
Member Emeritus	Roy DeCicco
Member Emeritus	Dave Faoro
Member Emeritus	Charlie Harrow
Member Emeritus	Valerie Hodge
Member Emeritus	Darlene Kargel
Member Emeritus	Bryan Penny
Member Emeritus	Bill Poletti
Member Emeritus	Diane Poole
Member Emeritus	Ralph Poore
Member Emeritus	David Repking
Member Emeritus	Mark Tiggas
Member Emeritus	Bob Walker
Member Emeritus	Daniel Welch
Member Emeritus	Michelle Wright
Merchant Advisory Group	Troy Carrothers
Merchant Advisory Group	Steve Cole
Nacha The Electronic Payments Association	Kathy Levin
Nacha The Electronic Payments Association	Brad Smith
Nasdaq	Sofie DeSimone
Nasdaq	Jeff Kimsey
National Security Agency	Mike Boyle
NCR Atleos	Gordon Mackay
NCR Voyix	Jackie Farone

Office of Financial Research, U.S. Department of the Treasury ..... Paul D'Amico
Office of Financial Research, U.S. Treasury Department ..... Jennifer Bond-Caswell
PCI Security Standards Council ..... Doug Manchester
PNC Bank ..... Melinda Tobolewski
Safari SOP ..... Steve Jatnieks
Safari SOP ..... Tom Melling
Swift ..... Anne Suprenant
TECSEC Incorporated ..... Ed Scheidt
TECSEC Incorporated ..... Jay Wack
Thales DIS CPL USA Inc ..... James Torjussen
The Clearing House ..... Jackie Pagán
Thomson Reuters ..... Kyle Floyd
Thomson Reuters ..... Taimur Javed
U.S. Bank ..... Nicolas Westmoreland
University Bank ..... Stephen Ranzini
University Bank ..... Michael Talley
USDA Food and Nutrition Service ..... Lisa Gifaldi
USDA Food and Nutrition Service ..... Sara Klos
VeriFone, Inc. ..... Joachim Vance
Viewpointe Clearing, Settlement and Associations Services, LLC ..... Richard Luchak
VISA ..... Andreas Aabye
VISA ..... Adam Clark
VISA ..... Eric Le Saint
VISA ..... Kim Wagner
Wells Fargo Bank ..... Sotos Barkas
Wells Fargo Bank ..... Peter Bordow
Wells Fargo Bank ..... Dawn Elliot
Wells Fargo Bank ..... Alan Nguyen
Wells Fargo Bank ..... Jeff Stapleton
Wolters Kluwer ..... Andrea Hearn
Wolters Kluwer ..... Sayuj Nambiar

iii) X9 Check Fraud Industry Forum Members

At the time this informative report was published, the X9 Check Fraud Industry Forum had the following officers and members:

Jackie Pagán, Forum Group Chair
Matt Sharp, Forum Group Vice Chair
Principal Editor: Joe Gregory, OrboGraph

Special recognition: We are grateful to the following editors for contributing their time and expertise to this project:

- Matt Sharp, Bank of America
- Margiore Romay, Deluxe
- Scott Anchin, ICBA
- Joe Gregory and James Bi, OrboGraph
- Nick Westmoreland and John Martir, U.S. Bank
- Wally Burlingham, X9 Emeritus member

Organization Represented	*Representative*
Ally Financial	Kim Hlavaty
American Bankers Association	Paul Benda
Bank of America	Matt Sharp
Bank of New York Mellon	Amanda Ketter
Bank of New York Mellon	Scott Kreger
Bank of New York Mellon	Adam Mayak
Bank of New York Mellon	Aimee Rice
Beal Bank USA	Vanessa Garcia
Beal Bank USA	Jennifer Hochman
Beal Bank USA	Apryl Strass
Benchmark Community Bank	Emily Berry
BrightStar Credit Union	Ayleen Alfonso
C&F Bank	Molly Crawford
Central Bank	Crystal Hunter
Community National Bank	Charla Mulanax
Community National Bank	Alondra Varela
Deluxe Corporation	Margiore Romay
Deluxe Corporation	Anna Tallo
Deluxe Corporation	Leo Tintinalli
Discover Financial Services	Connie James
DuTrac Community Credit Union	Wionnia Mausser
ePayResources	Wanda Downs
ePayResources	Stephanie Hottle
ePayResources	Crissy Terry
EPCOR	Marcy Cauthon
Fayette Savings Bank	Darlene Brothers
Fayette Savings Bank	Corrie Scardino
Fayette Savings Bank	Gail Vacek
FDIC	Lloyd McIntyre
Federal Reserve Bank	Amanda Cooper
Federal Reserve Bank	Staci Shatsoff
Federal Reserve Bank	Michael Timoney
Fidelity Bank	Whitney Darcy
First Bank of Clewiston	Larissa Williams
Fiserv	Angela Crohn
Fiserv	William Kruse
FIX Protocol Ltd - FPL	James Northey
Grandview Bank	Samantha Fowler
Independent Community Bankers of America	Scott Anchin
J.P. Morgan Chase	Brian Hagaman
J.P. Morgan Chase	Yvonne Penny
Marine Bank and Trust	Kevin Barker
Marine Bank and Trust	Cari Cahill
Marine Bank and Trust	Nancy Connell
Marine Bank and Trust	Deanna McDermott
Marine Bank and Trust	Anna Sowell
Marine Bank and Trust	Casey Steele
Member Emeritus	Wally Burlingham
Member Emeritus	Daniel Welch
Mitek Systems	James Watts
Musselman Home Improvement	Lydell Little
National Bank and Trust	Errin Schneider
OAS FCU	Michaelina Busco

Orbograph	Joe Gregory
PaymentsFirst	Kari Kronberg
PaymentsFirst	Meredith Stubblefield
Pervasive Path Consulting	Amy Poteat
Piedmont Advantage Credit Union	Jessi Jones
Piedmont Advantage Credit Union	Hannah Vestal
PlainsCapital Bank	Lou Ann Rohne
Port Arthur Community Federal Credit Union	Teresa Bacon
Prosperity Bank	Jennifer Gortney
Prosperity Bank	Petra Hudson
R Bank	Amy Fajkus
Raiz Federal Credit Union	Christopher Montoya
Raymond James	Patrick Roche
Raymond James Bank	Jamie Coy
Republic Bank & Trust Company	Souhila Moussaoui
Rosetta Technologies	Andrew Pease
Rosetta Technologies	Bryce Pfeiffer
Rosetta Technologies	Matthias Regelsberger
Rosetta Technologies	Leonard Stone
Rosetta Technologies	Jim Walling
Security State Bank and Trust	Angela Willis
Southern Financial Exchange	Catherine Bishop
SQN Banking Systems	Stan Jaslar
The Clearing House	Jackie Pagán
The Clearing House	Christina Rice
The First National Bank of Ballinger	Cathy Elliot
The MetroHealth System	Paul Aboukhaled
The No Check Group, LLC	Chuck Kopko
Tower Federal Credit Union	Bryan Grimaldi
Tower Federal Credit Union	Leslie McDonald
Tower Federal Credit Union	Susan Rallston
Tower Federal Credit Union	Dylan Stocking
Tower Federal Credit Union	Lisa Wood-Mitchell
TransPecos Banks	Clara Reyes
U.S. Bank	Jeffrey Corcoran
U.S. Bank	Lisa Forman
U.S. Bank	Cynthia Levine
U.S. Bank	John Martir
U.S. Bank	Tammy Ostrander
U.S. Bank	Rhonda Strong
U.S. Bank	Philana Tso
U.S. Bank	Lucy Vongdeuan
U.S. Bank	Nicolas Westmoreland
UFCU	Kimberly Mayo
Viewpointe Clearing, Settlement and Associations Services, LLC	Richard Luchak
Vista Bank	Bentley Pollard
Wespay	Angie Smith

Mitigating Check Fraud Risk in the Modern Financial Ecosystem

Accredited Standards Committee X9, Inc.

Table of Contents

1. Preface

The Accredited Standards Committee X9 Inc. launched an industry forum dedicated to supporting the financial industry's fight against check fraud. This initiative, referred to as the Check Fraud Industry Forum ("Forum"), convened financial institutions, industry experts, and technology providers to examine emerging fraud patterns.

The ultimate objective is to identify practical strategies and tactics so financial institutions can mitigate fraud risk while maintaining operational efficiency and customer trust.

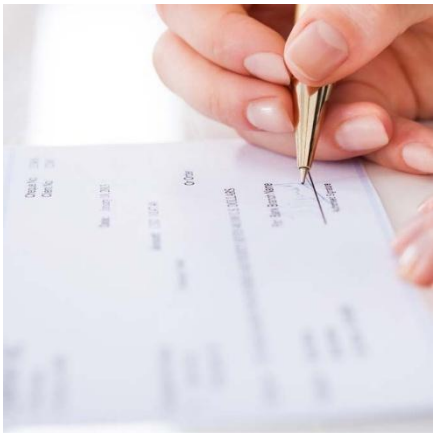
The Forum provides an assessment of the current landscape, scope, and impact of check fraud in the financial industry. Additionally, the white paper:

- Outlines check fraud categories and scenarios
- Evaluates detection and prevention tools and strategies
- Offers procedural recommendations alongside high-level regulatory reminders
- Provides details related to educational plans for financial institution employees and customers

Key findings from the Forum will be incorporated into the upcoming X9 informational publication, Technical Report 8: Check Security.

2. Introduction: The Continued Relevance of Checks

Despite the rapid adoption of digital payment systems, according to the 2025 AFP Payments Fraud Survey Report (Advanced Fraud Professionals), 90%+ of businesses still use checks for financial transactions for:



- Accounts payable
- Payroll exceptions
- Escrow transactions
- Large-dollar disbursements

Consumers continue to use checks for rent payments and other miscellaneous expenses. Government entities also issue benefits and tax-related payments via check.

As a result, checks remain a viable—and increasingly targeted—instrument for fraud.

Since 2020, the payments industry has experienced a sharp increase in check fraud attempts, resulting in substantial financial losses for institutions, businesses, and consumers. Criminal enterprises have adapted traditional fraud techniques to exploit various points in the check payment ecosystem including:

- Outdated systems
- Operational gaps
- Mail vulnerabilities
- Remote Deposit Capture (RDC) and self-service channels
- Social channels via engineering tactics
- Cost reduction in staffing
- Higher dollar thresholds

The combination of physical instruments and digital processing systems has created a hybrid risk environment that requires modernized detection and prevention strategies.

3. The Financial Industry and the Impact of Check Fraud

The financial industry operates on three core principles:

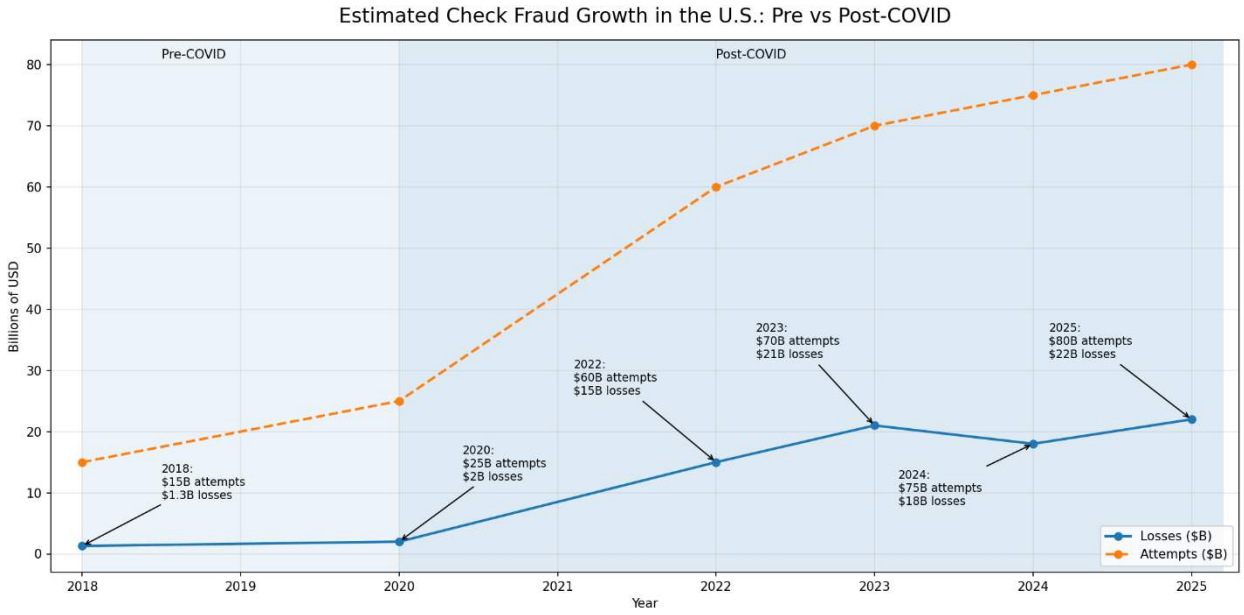
- Trust
- Speed
- Liquidity

Check fraud undermines all three.

Fraud losses create direct financial exposure for financial institutions and their customers while also increasing operational costs and introducing reputational and regulatory risks. These impacts affect profitability, operational efficiency, and overall customer confidence.

Data and Trends in Check Fraud

The increase in check fraud across the U.S. payments ecosystem since the COVID-19 pandemic has been substantial. Industry and vendor reports suggest:



Graphic above generated from data points below.

- Sharp upward trend post-2020
- Explosive growth in estimated attempts (dashed line), far outpacing losses (400%-800% compared to pre-2020)
- A visible structural shift after COVID, even with conservative estimates

A baseline reference comes from the American Bankers Association's 2020 Deposit Account Fraud Survey (Based on 2018 data), which estimated:

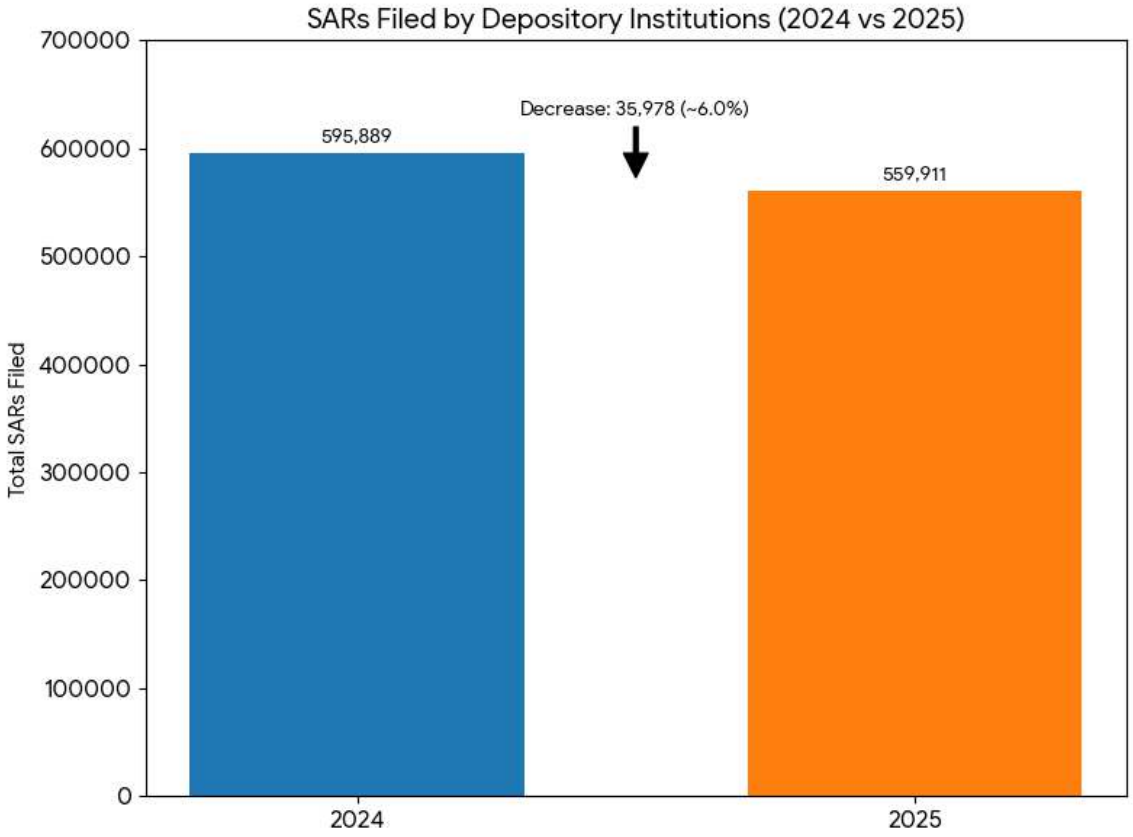
- $15 billion in check fraud **attempts**
- $1.3 billion in **losses** by financial institutions (based on 2018 data)
    - Ratio of attempts/losses = 11.5

Recent estimates are significantly higher. Key industry findings include:

- In 2023, reports indicated over $21 billion in check fraud losses in the United States. (source: chargebacks911.com)
- Industry analysts estimates more than $33 billion in annual losses tied to check fraud. (Source: NASDAQ report, Forbes.com report)
- Check fraud accounts for approximately 30% of total payments fraud, second only to debit card fraud at 39%. (source: (2024 Annual Federal Reserve Financial Services (FRFS) Financial Institution Risk Officer Survey)
    - Assuming a more conservative ratio of 4-5 (compared to 11.5 above), estimated check fraud **attempts** would approach $80-$100B in total.
- Hundreds of thousands of checks are stolen annually in the U.S. (likely 500,000+), with the true number potentially much higher due to underreporting and bulk theft activity. In 2025, FraudXchange monitoring surfaced nearly 3 million stolen checks circulating in criminal networks before any deposits occurred.


Other Noteworthy Trends:

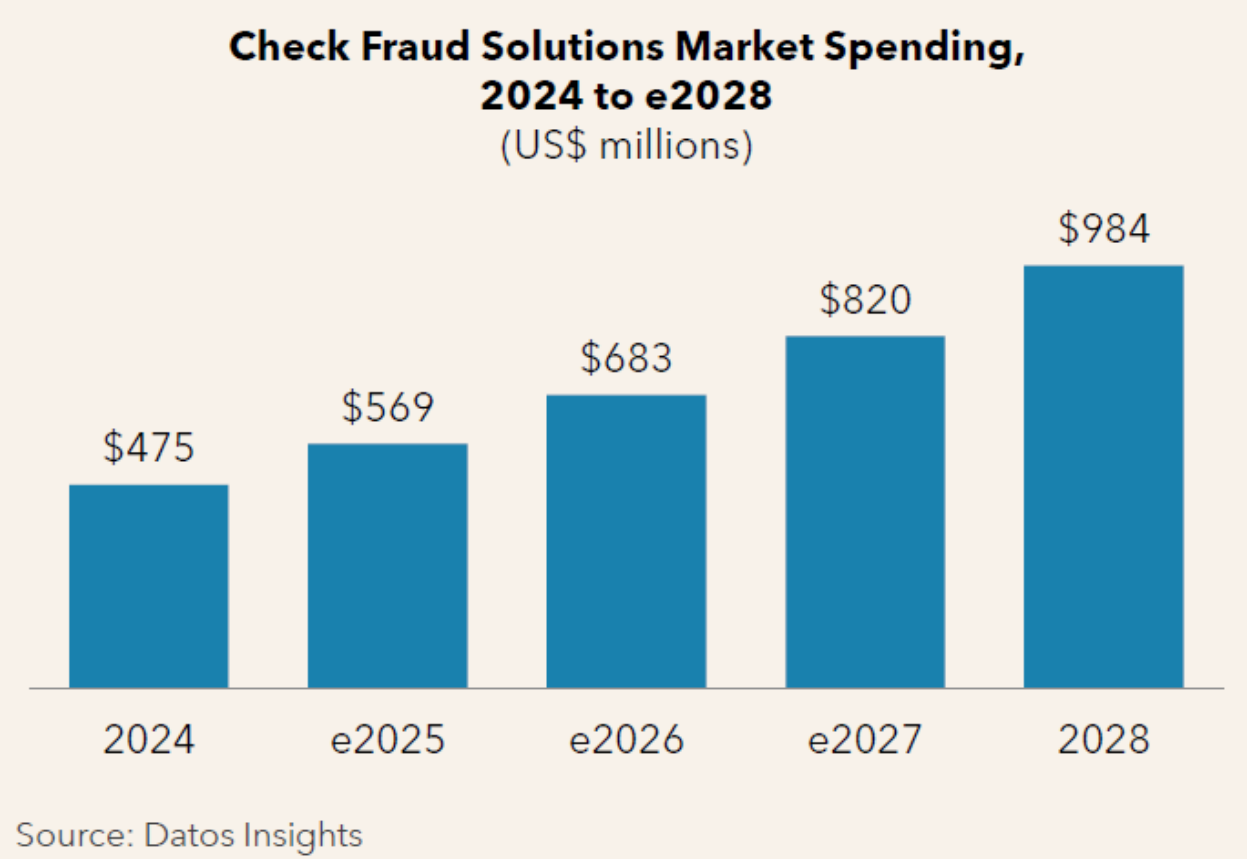
- The use of checks within Business Email Compromise fraud remains around 26%.
- The integration of fraud rings into mail theft is a continued source of stolen checks.
- Stolen check use, especially purchased via Telegram, was reported by the Reported Future: H1 2025 Check Fraud Report, to be moving toward more rural communities.
- Meanwhile, a comparison of Suspicious Activity Reports (SARs) filed by depository institutions, reported on FINCEN.



Overall, total SARs declined, a decrease of 35,978 (about 6%). It appears that SARs are decoupling from check fraud attempts.

Emerging Trends:

- Check fraud attempts may continue increasing through 2026, particularly among community financial institutions.
- Financial institutions are investing in modernization and fraud detection technologies, with the check fraud detection market projected to reach $984 million by 2028. (Source: Datos Insights).



- Use of Generative AI technologies to perpetrate various forms of fraud, including check fraud.

4. The Use of AI to Perpetrate Check Fraud

Artificial intelligence is reshaping check fraud tactics and prevention in the financial industry, enabling scaled operations for both criminals and defenders.

- Generate counterfeit checks: Leverage GANs (Generative Adversarial Network) and Machine Learning (ML) to replicate security features like watermarks, microprinting, and MICR lines from datasets, creating realistic forgeries with altered details.
- Create synthetic identities: Aggregate stolen data via Natural Language Processing to build personas with fake profiles, histories, and deepfakes for account openings or check cashing.
- Automate fraud schemes: Deploy bots and Large Language Models (LLMs) for phishing, timing deposits, and coordinating money mules to scale attacks efficiently.

How Financial Institutions Use AI

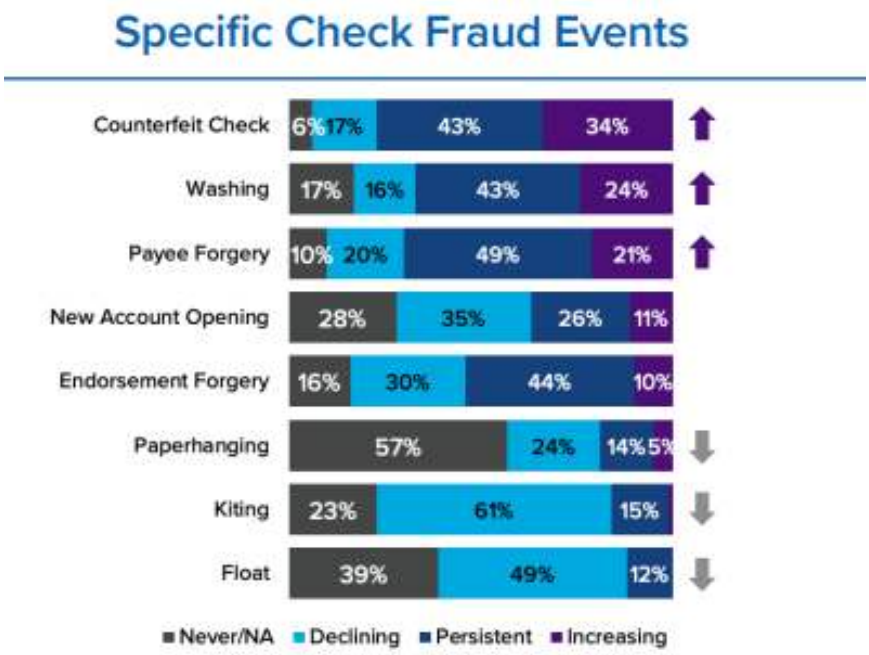
- Real-time anomaly detection: ML models flag irregularities in transactions, like unusual patterns or geolocation mismatches, halting fraud pre-disbursal.
- Behavioral analytics: Unsupervised learning profiles users to detect shifts in habits, scoring risks from biometrics and history.
- Image forensics: Convolutional/Recurrent Neural Networks analyze checks for tampering, like pixel inconsistencies or AI artifacts, automating rejections, coordinate comparisons, and signature verification.
- Predictive fraud modeling: Neural networks forecast threats from trends, using federated learning for shared insights to refine proactive strategies.

By ethically deploying AI with compliance, institutions mitigate billions in losses, boost trust, and minimize disruptions.

5. Check Fraud Categories

According to the Annual FRFS Financial Institution Risk Officer Survey (2024), the most common check fraud events include:

- Counterfeit checks
- Altered checks (often due to washing)
- Payee forgery
- New account fraud
- Forged endorsements



Counterfeit Checks

Counterfeit checks are generally the most prevalent forms of check fraud because there are so many methods available to create them including:

- Digital creation using desktop publishing software
- Duplication of legitimate checks using scanners or copiers
- Alteration of existing checks through chemical washing
- Use of stolen check templates or account information
- Synthetic fabrication combining valid bank codes with fictitious payer information
- Use of AI technologies to create the item

Counterfeit checks are often difficult to detect at the bank of first deposit because they are typically drawn on another institution. Due to clearing timelines, detection may be delayed one to three days.

Altered Checks

Altered checks have increased significantly due to rising mail theft. Criminals often steal checks and:

- Wash the ink to remove payee or amount fields
- Rewrite information before depositing or cashing the check
- In many cases, the signature is actually changed or altered, but this does not make the item a forgery

In some cases, criminals register a business with the same name as the intended payee in another state to bypass detection systems.

Forged Checks

Forged checks involve signing a check without authorization from the account holder. These incidents frequently occur when:

- Checkbooks are stolen
- Mail delivery is intercepted
- Employees misuse corporate check stock

Forged Endorsements

Forged endorsements occur when the individual depositing the check is not the intended payee. This is common at the bank of first deposit when the account holder name does not match the check payee.

- Impersonate the payee without altering the document

Duplicate Presentment

Duplicate presentment of a check to multiple financial institutions or check cashers. Fraudsters exploit:

- Workflow gaps, including RDC + branch presentment exploitation.
- Delayed returns
- Inconsistent warranty processes across institutions
- Lack of real-time data sharing.
- Fraud rings cashing items across institutions

Additional Fraud Scenarios

Other notable fraud scenarios include:

- Account takeover with check issuance: Criminals gain access to accounts through phishing or credential theft and issue checks directly from compromised accounts.
- RDC abuse: Fraudsters deposit checks via mobile channels and then attempt to negotiate the physical check elsewhere, creating duplicate presentment scenarios.

These examples highlight a central challenge: fraudsters exploit timing gaps between the issuance of a check, clearing, reconciliation, and exception handling.

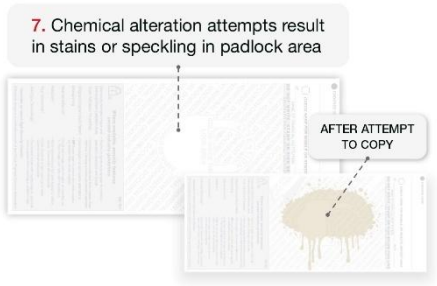
6. Recommendations for Improving Check Security and Reducing Fraud

In an era of sophisticated digital check fraud—driven by mail theft, check washing, and AI-generated counterfeits—physical check design remains a foundational layer of defense. While advanced analytics, image forensics, Positive Pay, and real-time monitoring provide powerful backend protection, the security of every check begins with the paper, ink, and print features themselves.

Thoughtfully engineered physical safeguards make counterfeiting and alteration significantly more difficult and detectable, especially during branch, mail, or forensic review. The recommendations below outline proven best practices for creating high-security checks. When combined with the multilayered operational and technological controls discussed earlier, they form a more resilient barrier against the check fraud trends that persisted through 2025.

1. Of genuine, mechanically produced watermark paper: Checks should be printed on paper containing true mechanical watermarks created during the paper-making process, rather than simulated or printed watermarks. Genuine watermarks are difficult to replicate and provide a reliable authenticity indicator during physical inspection. This approach mirrors the U.S. Treasury's reliance on specialized paper manufacturing for banknotes, where the security of the currency begins with tightly controlled paper production rather than relying solely on printed features.

2. Incorporate chemically sensitive (stain-reactive) security paper: Security paper that reacts visibly when exposed to common alteration chemicals can deter and reveal attempts to wash checks or modify payee and amount information. When the reactive chemistry is embedded in the paper itself, the response is immediate and difficult to conceal, strengthening protection against alteration fraud.



Source: Deluxe Corp.

3. Include microprinting and fine-line security patterns: Microprinting and intricate line patterns degrade when copied or scanned, increasing the effort and cost required to produce convincing counterfeits. While not impossible to reproduce with advanced equipment, these features remain effective deterrents and support forensic review.

4. Design checks to make alterations visually disruptive: Thoughtful layout and background design can help ensure that any attempt to alter critical fields—such as the payee name or amount—visibly disrupts the check's appearance. Integrating protection zones, controlled placement, and background patterns makes tampering easier to detect during review.

5. Apply layered security rather than relying on a single feature: No single security feature prevents all forms of check fraud. A layered approach—combining secure paper, print features, and thoughtful layout—significantly increases the difficulty of counterfeiting or alteration and improves detection across multiple inspection environments.

6. Maintain consistency in paper and security features: Consistent use of paper stock and security features helps financial institutions, processors, and reviewers more easily recognize authentic checks and spot anomalies. Frequent changes can unintentionally weaken detection by reducing familiarity.

7. Acknowledge limitations in image-based and remote deposit environments: Many traditional security features are most effective during physical inspection. As image-based and mobile deposit usage increases, physical security should be viewed as part of a broader fraud-mitigation strategy rather than a standalone solution.

8. Align physical check security with process and system controls: Physical check features are most effective when combined with operational controls such as verification processes, reconciliation, and fraud monitoring. Check security should be designed to complement downstream detection and review systems.

7. Check Fraud Detection and Prevention Strategies

Effective fraud mitigation requires a layered strategy combining multiple technologies, process controls, targeted tuning, and human oversight. In today's fraud ecosystem, this should involve multiple systems which are tightly integrated.

Financial institutions should also evaluate fraud risks across both on-us checks and deposited checks using specific tailored check fraud risk assessment techniques for each.

Key detection and prevention strategies include:

Greater Sophistication in Monitoring New Accounts

Fraudsters frequently exploit newly opened accounts to cash stolen or altered checks.

Institutions should implement:

- Multilayered fraud prevention framework
- Real-time monitoring for unusual activity for unusual or unauthorized behavior
- Geographic anomaly detection
- Device and authentication safeguards
- Identity verification controls
- Use of account risk score in check processing
- Use of rules to identify abnormal behaviors specific to the financial institution

Stolen paper checks are frequently used by criminals seeking to impersonate a legitimate customer, i.e., via payee alteration or modified account identity.

- Strengths: Real-time and AI-enhanced behavioral monitoring, advanced identity verification and consortium data sharing alternatives available
- Weaknesses: Vulnerability to synthetic identities and "aging" tactics, gaps in consistent implementation, over-reliance on initial onboarding vs. ongoing check-specific controls

Positive Pay and Payee Positive Pay

Positive Pay systems match presented checks against issued-check files to detect discrepancies in:

- Serial numbers
- Amounts
- Payee names

Payee Positive Pay enhances protection by validating payee information to prevent check washing.

Many financial institutions are now running positive pay in conjunction with other on-us and deposit fraud software modules to improve detection and move detection to day one.

- Strengths: Effective for blatant fraud attempts, fairly automated with minimal false positives.
- Weaknesses: Low adoption rates, administrative friction and file-maintenance burden, not 100% foolproof, and lacks functionality against specific fraud alteration use cases & schemes.

Advanced Analytics and Machine Learning

Analytics have evolved in many ways. Today, there are new transactional statistical models available, but predominantly AI-based machine learning models are used to identify anomalies in areas like:

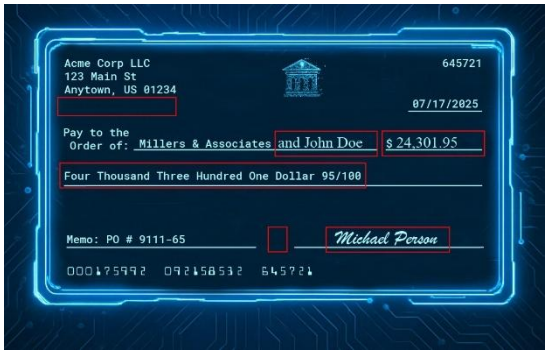
- Transaction behavior
- Deposit timing
- Geographic inconsistencies
- Transaction velocity
- Behavioral activity

Machine learning is not the end-all in fraud detection, as there are other considerations:

- Strengths: Real-time anomaly detection across key risk vectors, potential cross channel coverage when applied to multiple payments on same platform, adaptive learning and continuous improvement.
- Weaknesses: Lack of image feature analysis, persistent false positives/negatives, lack of explainability, arms-race vulnerability to AI-empowered fraudsters.

Image Forensics

Advanced image analysis tools can identify:



- Counterfeited checks
- Check washing alterations
- Font inconsistencies
- Payee and amount alterations
- Check fraud security features
- Strengths: Precision in detecting subtle visual manipulations, speed, scalability, and continuous adaptation, utilization of check fraud symbols on check are now available.
- Weaknesses: Legacy technologies are ineffective, vulnerable without complementary controls, dependence on image quality, strong false positive controls are needed.

Signature Verification

The use of automated signature verification has increased significantly due to improved accuracy and reduced false positives. Identifying forged signatures and altered items can be detected by comparing the check signatures to trusted reference data.

- Tampered
- Skilled forgeries
- Unskilled forgeries

AI-driven signature verification provides higher accuracy than legacy technologies, reduces false positives, and limits manual review.

- Strengths: Automation, speed, and reduced manual review, superior accuracy over legacy methods for forgery detection, seamless integration with broader image forensics.
- Weaknesses: Dependence on quality reference data, challenges with skilled forgeries and copied signatures, legacy system performance.

Deposit Controls and Funds Availability

Reg CC allows financial institutions to hold funds based on suspected fraudulent activity involving both deposited and inclearing checks. Criteria for holding funds includes several considerations as detailed by Federal Reserve:

- New accounts
- High-risk deposits
- Large-value checks
- Doubtful collectability
- Repeatedly overdrawn
- Prior fraudulent activity

- Strengths: Risk-based, targeted protection against high-risk deposits, proactive loss mitigation with built-in verification window, regulatory standardization and compliance alignment.
- Weaknesses: Customer friction and reputational risk, operational and documentation burden with potential gaps for “reasonable cause,” gaps in coverage for slow check fraud returns.

Cross-Channel Monitoring

Fraudsters now move money from one payment mechanism to another. By monitoring a wider range of transactions together, a centralized system can provide a holistic fraud detection approach when evaluating:

- ACH payments
- Online banking payments
- Real time payments
- Branch activity
- RDC transactions
- Wire transfers
- Strengths: Holistic detection of channel-hopping and layering schemes, potential measurable reduction in losses with fewer false positives, proactive risk mitigation aligned with regulatory and industry shifts.
- Weaknesses: Complex data integration and legacy system challenges, higher risk of alert fatigue or over-flagging without mature tuning, elevated privacy, compliance, and scalability demands.

Strengthen Frontline Training and Procedures

Human judgment remains essential in detecting forged checks. To address operational errors, financial institutions are strengthening training programs focused on:

- Verifying city and state codes
- Checking fractional MICR details
- Reviewing check stock security features
- Confirming customer identity and transaction purpose
- Recognizing signs of counterfeit or altered checks
- Implement new technologies at the teller line and self-service channels

Improved frontline training, supported by clearer internal guidance, creates greater consistency across institutions and reduces acceptance of fraudulent items.

Real-Time Fraud Screening

Financial institutions are shifting fraud detection earlier in the process. Real-time detection tools integrated into teller and deposit systems allow financial institutions to check items against fraud filters, exception lists, and customer profiles immediately.

Real-time alerts, vendor API integrations for payee validation, and Treasury verification services (such as TCVS for government checks) strengthen decision-making and reduce acceptance of fraudulent items.

Optimize Use of Consortium Data

Consortium data refers to pooled, anonymized fraud intelligence shared among financial institutions in a secure, collaborative network to enhance detection and prevention efforts. To use it, institutions join a consortium, contribute de-identified transaction data, and integrate the aggregated insights into their fraud analytics systems for real-time monitoring, machine learning model training, and risk scoring, ensuring compliance with privacy regulations like GDPR or CCPA.

Applications in Check Fraud Detection:

- Real-time anomaly detection: Analyzes deposit patterns across institutions to flag suspicious checks, such as altered or stolen items, at the point of presentment, preventing losses before funds clear.
- Pattern recognition and predictive modeling: Uses machine learning on vast consortium datasets to identify fraud trends, like counterfeit checks or synthetic identities, improving accuracy and reducing false positives.
- Cross-institutional risk assessment: Shares signals from many transactions to evaluate counterparty risks, enabling holistic views of threats like check kiting or fraud rings spanning multiple financial institutions.
- Enhanced in-clearing processes: Integrates consortium data with image analysis and behavioral analytics to detect fraud during check processing, minimizing operational disruptions and customer friction.

- Strengths: Cross-institutional risk assessment, potential improvement in Accuracy, Pattern Recognition, and False-Positive Reduction, Proactive, Privacy-Compliant Collaboration at Scale.
- Weaknesses: Dependency on network participation and data contribution, integration complexity and implementation costs, regional focus and potential for data gaps.

8. Tactical and Procedural Recommendations

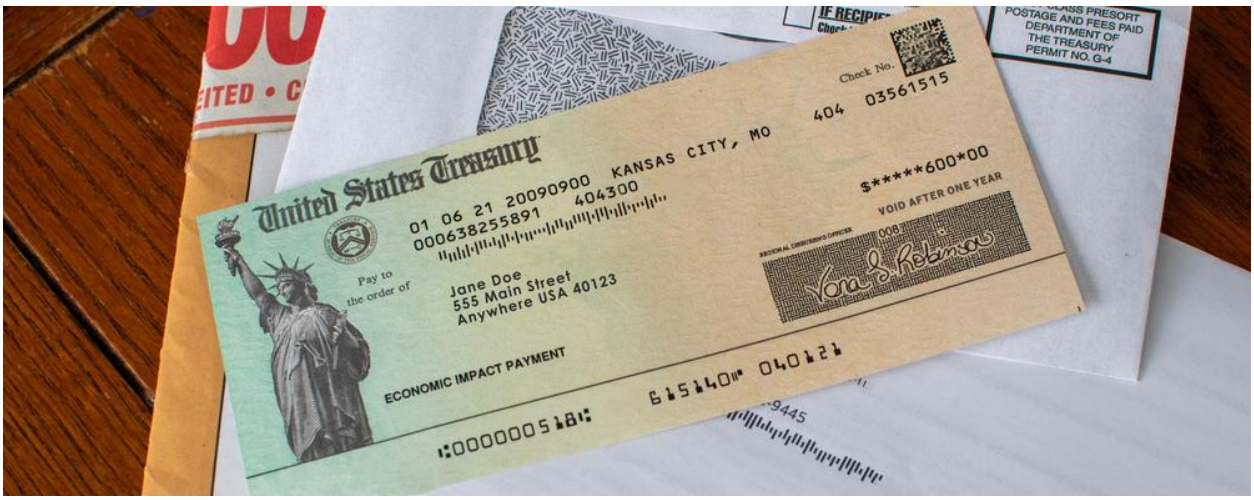
There are many check processing functions which are under the umbrella of check fraud detection. This section will highlight several of the key gaps with recommendations to address vulnerabilities of financial institutions. Initial gaps include:

- Teller acceptance of altered checks without inspection
- On-Us check cashing practices for non-customers
- Geographic fraud patterns
- Limited understanding of breach-of-warranty claims
- Counterfeit check creation using legitimate account data
- Organized fraud rings exploiting policy differences across institutions

Addressing these vulnerabilities requires stronger internal procedures and improved customer communications including:

- On-Us Check Cashing Practices: Financial Institutions cashing items from valid internal accounts for non-customers or unbanked individuals not associated with that specific account.
- Geographic Fraud: Perpetrators stealing checks and traveling to different cities to cash them, often using accounts with names slightly altered from the valid account holder's name.
- Regulatory Knowledge Gaps: Uncertainty regarding where and how to submit breach of warranty claims.
- Counterfeit Checks: Utilizing valid account information to create entirely new, fraudulent check instruments.
- Organized Scams and Information Silos: Collaborative fraud rings exploiting detailed knowledge of various banking policies, exacerbated by a lack of incident information sharing between financial institutions.

- Teller Protocols: Tellers accepting altered checks without thoroughly inspecting the physical instrument or verifying the identity and legitimacy of the customer presenting it.
- Internal Detection Failure: The same financial institution that captured the item failing to identify and flag fraudulent activity internally.
- U.S. Treasury Check Fraud: Difficulties and delays in gathering reclamation for U.S. Treasury check fraud due to specific, protracted regulatory processes.



- Managing On-Us Check Cashing for Non-Customers: Financial institutions must ensure robust training for both staff and customers on fundamental check processing procedures:
    - Verification using government-issued identification
    - Confirmation of available funds before releasing cash
    - Matching endorsements to presented identification
    - Management approval for large-value checks
    - Most institutions prohibit third-party check cashing for non-customers due to increased fraud risk

9. Education and Foundational Fraud Controls

Foundational check knowledge remains critical, even as fraud tools and technology advance. Education around check processing and understanding how checks can be used for fraudulent purposes is a shared responsibility between financial institutions, their employees and their customers. Gaps in understanding these basics can be exploited by criminals to carry out different check fraud schemes.

Customer Education

Financial institutions would benefit from educating their customers on the difference between how paper and electronic checks process, as well as providing clarification around the difference in funds availability and the settlement or collection timeframe. Customers may assume that because the funds from a check deposit are available in their account, it is a valid check that will not be returned. Fraudsters may take advantage of this knowledge gap if it is not made clear to the customer that deposited checks may be debited out of their account if they are not honored by the paying bank.

It is important for customers to be aware is that they should never share their online banking credentials with anyone. In addition, your financial institution will never ask for this type of information. When in doubt, they should call the direct phone line of their financial institution to validate any potential messages.

Financial institutions should educate customers on:

- Securing check stock
- Monitoring account activity
- Recognizing fraudulent checks
- Responding quickly to suspicious transactions

Prevention

Institutions may consider offering specific education to their business customers around how to mitigate check fraud. (Preventing Check Fraud: A Resource for Businesses)

Such as:

- Implementing internal controls
- Monitoring account activity
- Issuing checks securely
- Training employees
- Positive pay products and segregation of duties
- Even if the return timeframe is short, a Breach of Warranty can still be filed against the depositary institution for items like alterations and forged endorsements after the return timeframe (UCC §4-302 and Reg CC §229.31(b)) in which the BOFD may debit the amount from their customer account.

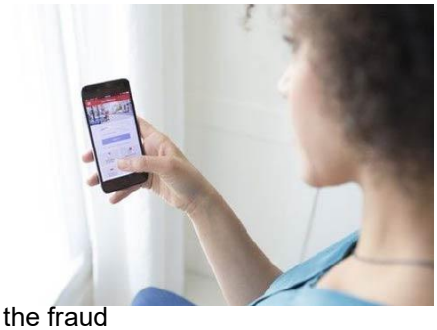
Detection

Education around detecting or identifying potentially fraudulent checks can also be helpful for both retail and business customers, this could include outlining red flags, such as:

- Visual identifiers: signs of alteration or the legal amount does not match the numerical amount
- Informational red flags: such as an unfamiliar issuer where the drawer of the check is a different entity than expected to be receiving a check from
- Behavioral flags: such as a sense of urgency or an unusual request

Response

Lastly, financial institutions can educate their customers on what steps to take if fraudulent checks are identified on their account. This will allow for quicker action to be taken to prevent additional fraudulent activity. Responding to check fraud concerns may include steps, such as:



- Review account activity
    - Check for other unauthorized activities
    - Confirm if account or profile changes were made (contact information, password, alerts, etc.)
- Contact your financial institution
    - Follow steps with the financial institution to report the fraud
    - Work with the financial institution to prevent additional fraud
- Consider filing a fraud report based on the type of fraud that may be involved
    - Federal Trade Commission (FTC)
    - U.S. Postal Inspectors (USPIS) – e.g. checks stolen from the mail
    - Local law enforcement
    - Internet Crimes Complaint Center: ic3.gov
- Monitor credit
    - Place alerts if concerns of credit risk exist
    - Monitor credit report
    - Explore identity theft protection

- Protect accounts / explore prevention services
    - Ask financial institution about services available to prevent check fraud
    - Change online banking password
    - Use multi-factor authentication if available
    - Set up account and transactions alerts or notifications

In summary, it is important for customers to know who they are paying and from whom they are receiving checks. Education around these small, simple steps can help customers prevent, identify, and feel prepared to respond to check fraud.

Employee Training

Understanding the basics can sometimes be overlooked, not because of a lack of experience or skill, but due to assumptions or the rush of daily tasks. It is essential to realize that fraud often exploits gaps in people and processes rather than technology. Through proper training, employees can align across all branches, contact centers, operations, and customer access channels.

Employees should receive training on:

- The check processing lifecycle
- Differences between funds availability and settlement
- Visual and behavioral fraud indicators
- Escalation procedures for suspected fraud

Consistent training ensures frontline staff remain vigilant and capable of identifying emerging fraud schemes.

Preventing and Detecting Check Fraud

Key elements in preventing check fraud include knowing your customer (KYC) and knowing your business (KYB). This involves verifying identity throughout all phases of the customer lifecycle and identifying red flags. Employees should be trained to recognize visual cues such as possible alterations, third-party endorsements, check stock alignment, and atypical formatting compared to other items accepted with the same MICR. Informational red flags might include new accounts or payee comparisons, while behavioral red flags could involve changes in deposit patterns. This paper provides specifics in how to identify these red flags that can be incorporated into employee training.

It is important to reiterate the significance of pausing to take thoughtful time for thorough review rather than making assumptions. Employees should be encouraged to stay vigilant and proactive in identifying and addressing potential fraud.

Response to Check Fraud

When check fraud is suspected, it is vital to have a clear and effective response plan. Employees should be educated on the steps they need to take, including holding the check, questioning its legitimacy, and who/how to escalate concerns. Reviewing documentation processes for their observations during the event is also essential.

By reinforcing these fundamentals, financial institutions can better equip their employees to prevent, detect, and respond to check fraud effectively.

10. Conclusions

Check fraud has re-emerged as a high-impact, systemically exploited risk—no longer confined to isolated incidents, but driven by organized networks leveraging mail theft, digital manipulation, and operational gaps across the payments lifecycle. The scale, speed, and coordination observed in today's environment make it clear: this is an enterprise risk issue, not a product-level problem.

For fraud leaders, the implication is direct—traditional controls and incremental enhancements are no longer sufficient. Institutions must reassess whether their current frameworks are truly aligned to the threat landscape, or simply optimized for a prior era of fraud.

Effective mitigation now requires intentional redesign across three domains:

- Detection Architecture: Shift from batch and post-event detection to real-time, decision-point intervention, leveraging AI, image intelligence, and cross-channel visibility.
- Operational Rigor: Eliminate inconsistencies in frontline execution, tighten high-risk workflows (e.g., on-us cashing, RDC, new accounts), and ensure controls are consistently enforced—not selectively applied.
- Network-Level Defense: Recognize that fraud is coordinated across institutions and channels—requiring active participation in consortium data, intelligence sharing, and industry alignment.

At the same time, leaders must ensure that foundational controls are not overlooked. Check design, issuance controls, and customer behavior remain critical points of failure—and opportunity.

The defining challenge is no longer detection capability alone—it is speed of response and organizational alignment. Fraudsters are exploiting timing gaps measured in hours; institutions that operate in days will continue to absorb losses.

The question for executive leaders is not whether tools exist—but whether their organization is operationally positioned to use them effectively, consistently, and at scale.

Winning institutions will be those that move detection earlier, act decisively at first presentment, and operate as part of a broader fraud intelligence ecosystem—not in isolation.

Appendix: Legal Framework for Fraudulent Checks

Appendix Legal Framework for Frau

Resources

Better Business Bureau:

Better Business Bureau scam prevention: https://www.bbb.org/all/scam-prevention

Better Business Bureau scam tracker: https://www.bbb.org/scamtracker/lookupscam

BBB Survival Toolkit: https://scamsurvivaltoolkit.bbbmarketplacetrust.org/

Check Fraud: A Practical Guide to Altered, Forged, and Counterfeit Checks Community Bankers – a comprehensive reference covering the check fraud landscape, prevention mechanisms, and the legal and regulatory framework governing checks. (https://www.icba.org/check-fraud-a-practical-guide)

ICBA (Independent Community Bankers Association):

Check Fraud: Detection Mechanisms – a high-level guide outlining available technology solutions and operational practices community financial institutions can use to detect check fraud. (https://www.icba.org/documents/d/asset-library-45247/check-fraud-detection-mechanisms)

Check Fraud: Engagement with Federal Bank Regulators – guidance on when and how community financial institutions should engage regulators regarding check fraud issues and reimbursement challenges. (https://www.icba.org/documents/45248/963855/Check+Fraud+-+Engagement+with+Federal+Bank+Regulators)

Positive Pay Guide – an overview of positive pay and reverse positive pay tools to help prevent and mitigate check and ACH fraud. (https://www.icba.org/d/asset-library-45247/positive-pay-guide)

ICBA–U.S. Postal Inspection Service Check Fraud Prevention Materials – consumer-facing flyers and educational materials focused on mail theft and check fraud prevention. (https://www.icba.org/d/asset-library-45247/uspis-check-fraud-scams-handout)

Federal Reserve - FedPayments Improvement:

https://fedpaymentsimprovement.org/resources/check-fraud-mitigation-toolkit/

https://www.frbservices.org/binaries/content/assets/crsocms/news/research/2024-risk-officer-survey-results.pdf

American Bankers Association

https://www.aba.com/banking-topics/risk-management/fraud/check-fraud

https://www.aba.com/news-research/analysis-guides/check-fraud-toolkit