Nasdaq
Verafin

Tactics Exposed:
Understanding Check Fraud Typologies

Table of Contents

Modern Check Fraud Typologies: From Mailbox to Mayhem

In the modern age, you might think check fraud is less prominent. But while deep fakes and AI dominate the financial crime conversation, checks are being stolen from the mail[1] or duplicated to exploit legacy systems and fragmented data. Recent check fraud losses exceeded $21 billion in the U.S.,[2] a staggering figure that continues to climb.

In a recent report, FinCEN highlighted 15,417 BSA reports involving 841 financial institutions linked to checks stolen from the mail.[3]

These stolen checks were grouped into three dominant fraudulent check typologies:

- Altered and deposited (44 percent).
- Used as templates to create counterfeit checks (26 percent).
- Fraudulently signed and deposited (20 percent).

While these are the most prevalent, there are several more ways check fraud contributes to a global $3.1 trillion financial crime problem.[4]

This ebook is your guide to the evolving landscape of check fraud. With this resource in the hands of your frontline staff, you'll be ready to stop these frauds from impacting your institution and customers.

Sources

1. FIN-2024-Alert003, FinCEN, 2023
2. Global Financial Crime Report, Nasdaq, 2024
3. Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, FinCEN, 2023
4. Global Financial Crime Report, Nasdaq, 2024

Who Are the Victims of Check Fraud?

Unfortunately, anybody who uses checks can fall victim to a check fraud scheme. Even a freshly-ordered batch of checks can disappear in the mail and turn up in a slightly different form on the dark web. However, most targets include:

- Consumers whose checks are stolen, altered or replicated.
- Businesses whose checks are stolen, altered or replicated.
- Financial institutions that issue checks.
- Retailers that provide cash back on fraudulent checks.
- Vendors or payees who never receive the intended funds.

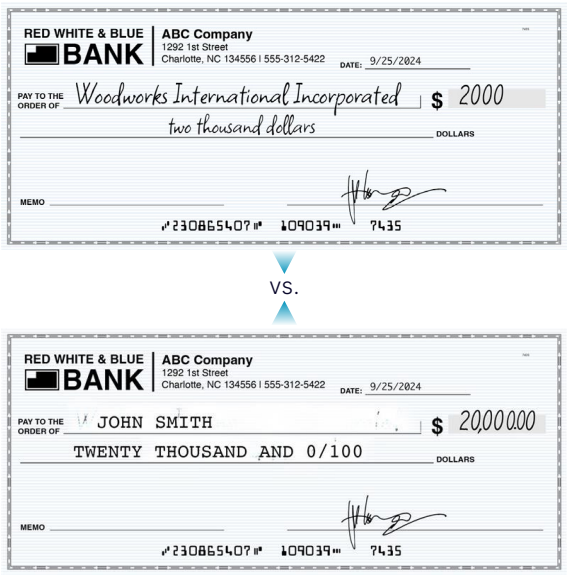
Altered Checks

What is it?

Altered checks are legitimate checks that have been doctored either manually or digitally to misrepresent crucial details. This typically includes changes to the recipient, check value and other physically altered characteristics to deceive financial institutions.

How does it work?

Fraudsters tamper with checks to change the appearance of crucial details. This includes using chemical solvents or abrasive tools to erase and replace the payee's name and/or check amount,[4] and rewriting them using similar ink or handwriting. These changes are often subtle and require close scrutiny to detect.



Source

[4] Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, FinCEN, 2023

Visual Red Flags

- Ink inconsistencies (e.g. different shades or types of ink)
- Erasure marks, abrasions, faded handwriting or torn edges[4]
- Font inconsistencies

Behavioral Red Flags

- Inflated payment amount
- Uncharacteristic payee
- First-time payee account activity

How to Mitigate the Problem?

- Utilize deposit-side risk and counterparty data to evaluate the payee
- Use tamper-evident check stock with chemical-sensitive paper and embedded security features
- Train staff to inspect for physical and visual inconsistencies
- Use image analysis, optical character recognition (OCR), and heat mapping tools to detect anomalies
- Contact customers to verify high check amounts

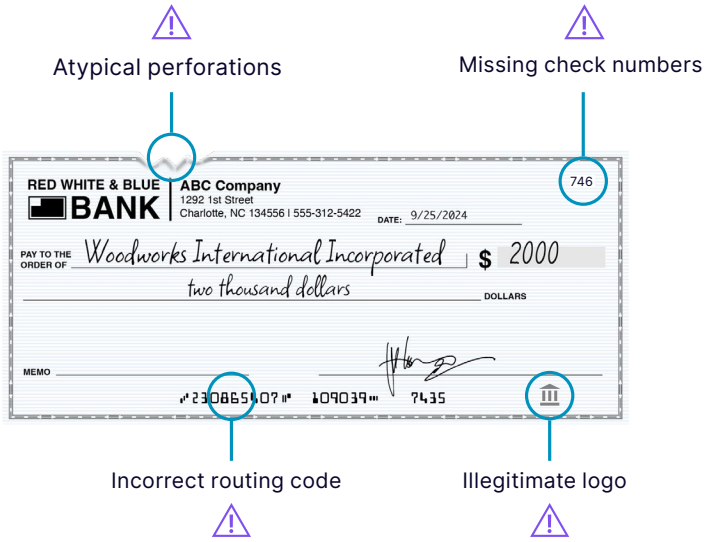
Counterfeit Checks

What is it?

Counterfeit checks are fraudulent reproductions of legitimate checks, often created using stolen originals as templates. In some instances, these checks can be mass-produced and sold on the dark web, then used to defraud financial institutions across jurisdictions. Unlike altered checks, which modify existing checks, counterfeits are created from scratch to mimic authentic payments.

How does it work?

Fraudsters steal legitimate checks — often from the mail[5] — and use them as templates to generate as many counterfeit versions as they wish. These replicas may include copied logos, account numbers and even security features. Once created, these counterfeits are sold or circulated and deposited into accounts controlled by fraudsters, who may exploit gaps in verification systems to bypass detection.



Source

[5] FIN-2023-Alert003, FinCEN, 2023

Visual Red Flags

- Low-resolution, inconsistent or sloppy printing
- Missing or altered security features (e.g. microprint, watermarks, atypical perforations)
- Inaccurate or outdated logos and branding
- Unusual paper quality or texture changes
- Misaligned text or off-center elements
- MICR line mismatches

Behavioral Red Flags

- Account holder identity cannot be verified
- Inconsistent or non-existent payee transaction history
- Payee accounts are uncharacteristic for payers
- Suspicious payment patterns, such as rapid or high-volume deposits
- Checks deposited from or into unfamiliar, distant locations

How to Mitigate the Problem?

- Leverage deposit-side risk and consortium data to identify suspicious accounts and checks
- Cross-reference check data with account behavior and transaction history
- Train staff to recognize counterfeit indicators and escalate suspicious items
- Use an image analysis tool that evaluates both the front and back of checks

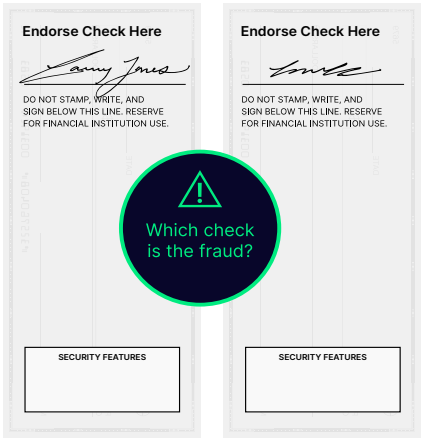
Fraudulent & Forged Endorsement

What is it?

A fraudulently endorsed check is a legitimate check that has been stolen and deposited with a forged endorsement signature.[6] Unlike counterfeit or altered checks, the check's MICR line, sequence number and even the payee name often remain unchanged. The forged endorsement typically matches the name on the front of the check, making this an extremely difficult fraud to detect.

How does it work?

Fraudsters intercept legitimate checks and deposit them into unauthorized accounts using a forged signature on the back. Because the check is authentic and the endorsement matches the payee's name, it can bypass some verification systems.



Visual Red Flags

- Signature inconsistencies
- Endorsement irregularities, such as missing or incorrect dates
- Alterations or erasures on the back of the check
- Multiple endorsements on a single check

Behavioral Red Flags

- Suspicious endorsement patterns (e.g. multiple checks endorsed by the same unknown individual)
- Customer complaints about missing or misdirected payments
- First-time payee account activity
- First-time deposits to a new account

How to Mitigate the Problem?

- Leverage deposit-side risk and consortium data to identify suspicious accounts and checks
- Use image analysis tools to detect inconsistencies in endorsement areas
- Educate customers on reporting stolen or suspicious checks
- Cross-reference endorsements with known payee profiles

Sources

[6] Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, FinCEN, 2023

Duplicate Presentment

What is it?

Duplicate presentment occurs when the same check is deposited more than once, either at multiple institutions or using both digital and physical channels. This can be done intentionally as a form of check fraud or accidentally, such as when a spouse or coworker deposits a check that has already been deposited on a mobile device.

How does it work?

Fraudsters typically deposit a digital image of a check using mobile or remote deposit capture, then attempt to cash or deposit the original paper check at a different financial institution or check-cashing service. Because communication between banks isn't immediate, this delay can be exploited to withdraw funds before the duplicate is detected. In deliberate cases, fraudsters often:

- Use two different financial institutions or a bank and a non-bank entity.
- Withdraw the maximum available funds immediately after the first deposit.
- Present the paper check at full value before the duplicate is flagged.

Visual Red Flags

- Absence of a restrictive endorsement (e.g. For Mobile Deposit Only)
- Altered or erased endorsement area
- Multiple endorsement marks on the back of the check
- Check appears worn or previously handled despite being presented as new

Behavioral Red Flags

- Same check number deposited at multiple institutions
- Check image is the same as another submitted in the past

How to Mitigate the Problem?

- Leverage deposit-side risk and consortium data to identify suspicious accounts and checks
- Use duplicate detection systems that flag repeated check numbers or images
- Monitor for cross-institution duplicate activity
- Contact the customer to verify the cheque's authenticity

Fraudulent Clusters

What is It?

A fraudulent cluster is when a fraudster submits a large number of smaller checks in a short timeframe. Because financial institutions clear many checks on a daily basis, most have implemented a minimum dollar value threshold below which they will not analyze the checks for fraud.

How Does it Work?

Fraudsters will use various systems to create a large number of fraudulent checks, either through check washing or cooking, giving them a low deposit value in order to avoid immediate scrutiny. These methods are often used in combination with other deposit mechanisms to distance themselves from illicit activity, such as mobile deposit apps, newly opened accounts and cross-institution tactics to maximize gain and reduce traceability.

Visual Red Flags

- Altered handwriting or mismatched fonts or ink
- Signs of erasure or overwriting on check surfaces
- Inconsistent endorsement areas (e.g., missing dates, irregular spacing)
- Multiple checks with similar formatting or design anomalies

Behavioral Red Flags

- Unusual check amounts that are consistently small and repetitive
- Checks deposited shortly after being mailed, especially if the recipient never received them

How to Mitigate the Problem?

- Flag accounts with repetitive, low amount check activity
- Share fraud intelligence across institutions to identify coordinated activity
- Evaluate payee account characteristics for suspicious behavior

HELOC Fraud

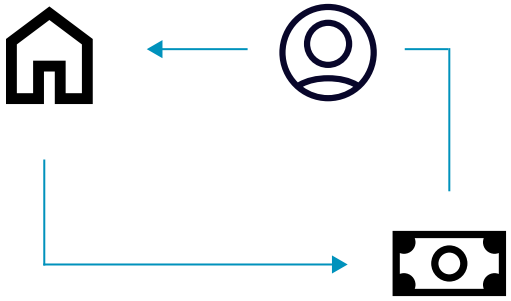
What is HELOC Fraud?

HELOC (Home Equity Line of Credit) fraud occurs when criminals gain unauthorized access to a homeowner's credit line, often through identity theft, and steal funds. HELOCs are attractive to fraudsters because revolving credit lines backed by home equity allow them to secure larger payouts.

Victims often discover the fraud only after receiving missed payment notices, calls from lenders or spotting errors on their credit reports — making detection difficult until it is too late to recover the funds.

How Does the Scheme Work?

Fraudsters exploit HELOCs by stealing personal information through phishing attacks, public records or data breaches. Criminals impersonate the homeowner to set up fake online banking profiles, order checks linked to the HELOC and transfer funds to fraudulent accounts. Fraudsters may also create fake checks that draw from a HELOC's funds using public record information.



Visual Red Flags

- Unfamiliar checks drawn against a HELOC account
- Altered or suspicious check designs linked to HELOCs
- Missing or inconsistent endorsement markings on HELOC checks

Behavioral Red Flags

- Unfamiliar withdrawals or transactions on a HELOC account, such as:
  - Higher value than usual
  - Unnecessary borrowing
  - Uncharacteristic payee
- Requests to increase HELOC limits

How to Mitigate the Problem?

- Instruct customers never to share personal information via text, email, or unverified websites
- Review non-routine payment activity with the customer
- Regularly review HELOC account activity and financial statements
- Enable alerts for large withdrawals or account changes

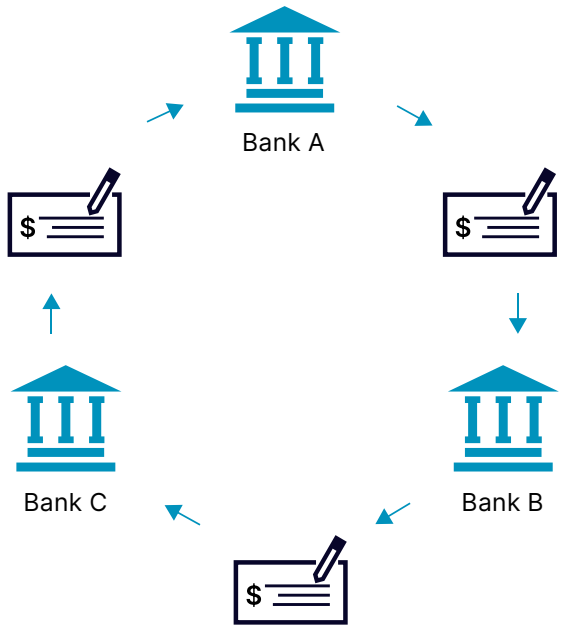
Check Kiting

What is Check Kiting?

Check kiting is a form of fraud that exploits the float period (the time it takes for a check to clear) to create the illusion of available funds. It allows individuals or groups to use non-existent money as unauthorized credit. While some use it to bridge short-term cash gaps, others use it to fraudulently inflate balances and withdraw funds before the checks bounce.

How Does the Scheme Work?

Check kiting schemes happen when a fraudster writes checks between accounts at different banks to artificially inflate balances. A check is drawn on one account containing insufficient funds, and the funds are then deposited into another account. During the check's in-clearing period, funds are withdrawn from the account.



Visual Red Flags

Check kiting activities are enacted by the owner of the account, and detection relies solely on behavioral red flags since the checks themselves were not fraudulent until they were drawn against an account with insufficient funds.

Behavioral Red Flags

- Frequent deposits with increasing amounts
- Accounts with low average balances but high check activity
- Excessive balance inquiries (kiters monitor closely to time withdrawals)
- High volume of checks written between accounts at different banks
- Sudden spikes in deposit and withdrawal activity
- Use of multiple banks or financial institutions in short timeframes
- Repeated use of cash-back transactions at retailers
- Checks made payable to the owner of account being drawn from

How to Mitigate the Problem?

- Monitor for patterns of circular deposits and withdrawals
- Flag accounts with excessive non-sufficient fund activity or balance inquiries
- Delay funds availability for high-risk or new accounts
- Require enhanced verification for large or frequent check deposits
- Share suspicious activity reports across institutions to detect cross-bank schemes

Solving a Complex Problem Together

Check fraud is challenging institutions with significant losses, exposing investigative limitations. Although most check frauds could be mitigated by reviewing account activity and a thorough analysis of the check, legacy solutions cannot perform every layer of analysis in one place. And for many institutions, the volume of checks being deposited renders this level of scrutiny impractical. This is how fraudulent checks slip through the cracks.

There's a shift underway. A consortium approach to prevention, reinforced by machine learning and real-time analysis, provides superior detection at deposit and in-clearing. With these tools, the financial industry can finally outpace one of the oldest threats in finance.

Nasdaq Verafin's solution leverages these three types of analysis to provide the industry's only completely holistic solution, capturing:

- Insight into the risk of the payor, payee and bank of first deposit.
- Security features on the back and front side of checks.
- Historical account behavior.

This helps institutions reduce false positives and spend more time analyzing the most high-risk activity — detecting more fraud and swiftly stopping transactions before the funds are lost.

Visit verafin.com for more information about how we will help you protect your customer relationships.

Quick Reference Guide

Nasdaq Verafin

Check Fraud Typologies

TYPOLOGY	DEFINITION	VISUAL RED FLAGS	BEHAVIORAL RED FLAGS
Altered Checks	• Legitimate checks that have been doctored to misrepresent crucial details, including changes to the recipient, check value and other physically altered characteristics	• Ink inconsistencies (e.g., different shades or types of ink) • Erasure marks, abrasions, faded handwriting or torn edges[4] • Font inconsistencies	• Inflated payment amount • Uncharacteristic payee • First-time payee account activity
Counterfeit Checks	• Fraudulent reproductions of legitimate checks, often created using stolen originals as templates	• Low-resolution, inconsistent or sloppy printing • Missing or altered security features (e.g. microprint, watermarks, atypical perforations) • Inaccurate or outdated logos and branding • Unusual paper quality or texture changes • Misaligned text or off-center elements • MICR line mismatches	• Account holder identity cannot be verified • Inconsistent or non-existent payee transaction history • Payee accounts are uncharacteristic for payers • Suspicious payment patterns, such as rapid or high-volume deposits • Checks deposited from or into unfamiliar, distant locations
Fraudulent & Forged Endorsement	• A legitimate check that has been stolen and deposited with a forged endorsement signature	• Signature inconsistencies • Endorsement irregularities, such as missing or incorrect dates • Alterations or erasures on the back of the check • Multiple endorsements on a single check	• Suspicious endorsement patterns (e.g. multiple checks endorsed by the same unknown individual) • Customer complaints about missing or misdirected payments • First-time payee account activity • First-time deposits to a new account
Duplicate Presentment	• When the same check is deposited more than once, either at multiple institutions or using both digital and physical channels	• Absence of a restrictive endorsement (e.g. For Mobile Deposit Only) • Altered or erased endorsement area • Multiple endorsement marks on the back of the check • Check appears worn or previously handled despite being presented as new	• Same check number deposited at multiple institutions • Check image is the same as another submitted in the past

Nasdaq Verafin

Quick Reference Guide : Check Fraud Typologies Continued

TYPOLOGY	DEFINITION	VISUAL RED FLAGS	BEHAVIORAL RED FLAGS
Fraudulent Clusters	• When a fraudster submits a large number of smaller checks in a short time-frame	• Altered handwriting or mismatched fonts or ink • Signs of erasure or overwriting on check surfaces • Inconsistent endorsement areas (e.g., missing dates, irregular spacing) • Multiple checks with similar formatting or design anomalies	• Unusual check amounts that are consistently small and repetitive • Checks deposited shortly after being mailed, especially if the recipient never received them

HELOC Fraud	• Fraudsters gain unauthorized access to a homeowner's credit line through identity theft	• Poor paper quality
		• Low-resolution, inconsistent or sloppy printing
		• Missing or altered security features (e.g., microprint, watermarks)
		• Inaccurate or outdated logos and branding
		• Incorrect or mismatched check and routing numbers
		• Unusual paper quality or texture changes
		• Misaligned printing or off-center elements
		• Missing or altered security features (e.g., no watermark, missing microtext)
		• Logo or branding errors
		• MICR line mismatches
			• Unfamiliar withdrawals or transactions on a HELOC account, such as:
			  • Higher value than usual
			  • Unnecessary borrowing
			  • Uncharacteristic payee
			• Requests to increase HELOC limits

Check Kiting	• A legitimate check that has been stolen and deposited with a forged endorsement signature	• Fraudsters exploit the float period and write checks between accounts at different banks to artificially inflate balances	• Frequent deposits with increasing amounts • Accounts with low average balances but high check activity • Excessive balance inquiries (kiters monitor closely to time withdrawals) • High volume of checks written between accounts at different banks • Sudden spikes in deposit and withdrawal activity

Nasdaq Verafin

Nasdaq Verafin provides cloud-based Financial Crime Management Technology solutions for Fraud Detection, AML/CFT Compliance, High-Risk Customer Management, Sanctions Screening and Management, and Information Sharing.

More than 2,600 financial institutions globally, representing over $10T in collective assets, use Nasdaq Verafin to prevent fraud and strengthen AML/CFT efforts.

Leveraging our unique consortium data approach in targeted analytics with artifical intelligence and machine learning, Nasdaq Verafin significantly reduces false positive alerts and delivers context-rich insights to fight financial crime more efficiently and effectively.

To learn how Nasdaq Verafin can help your institution fight fraud and money laundering:

Visit: **www.verafin.com**
Email: **info@verafin.com**
Call: **1.877.368.9986**

Legal www.nasdaq.com/legal
© 2024 Nasdaq Verafin Inc. All rights reserved.
Updated Q4, 2025