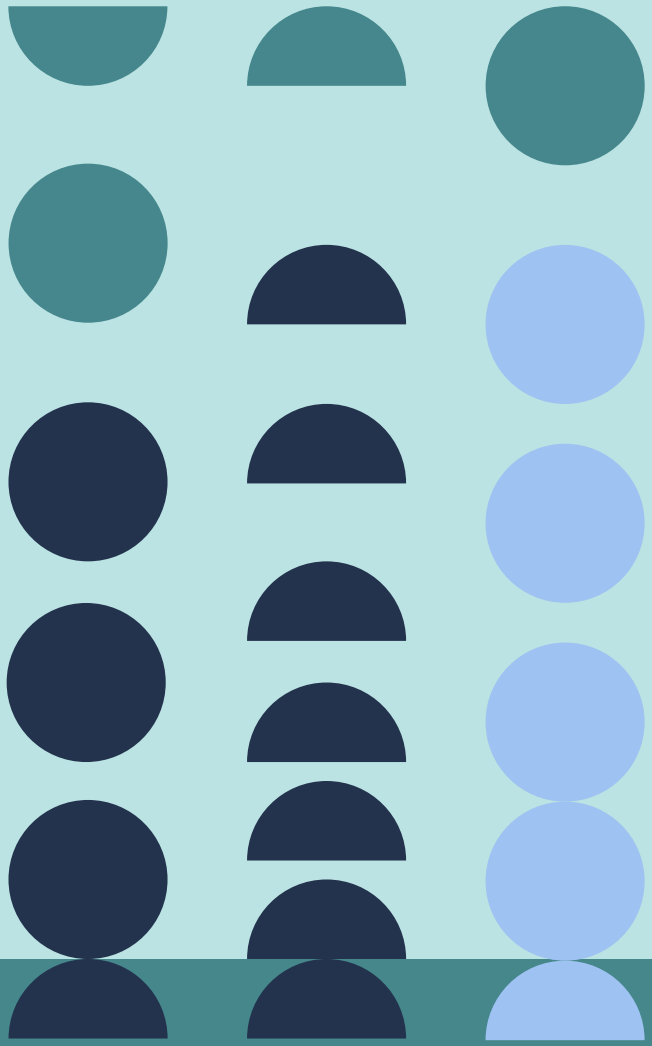
Early Warning®

Check Fraud Prevention:
4 Best Practices to Combat Escalating Attacks

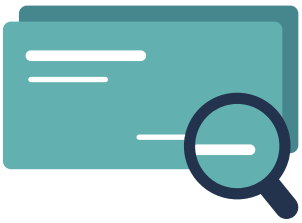


Introduction

Check fraud losses continue to grow at a shocking pace. More than three quarters of financial services companies reported escalating losses from check fraud over a two-year period ending in late 2023, with some unlucky financial institutions (FIs) citing triple-digit increases in losses.[1]

While check fraud is an age-old threat, its resurgence is catching even the most forward-thinking banks and credit unions off guard.

Check usage continues dropping in favor of credit cards, debit cards and digital payment methods, yet over 3.1 billion commercial checks were collected through the Federal Reserve in 2023. And the average value per check doubled from $1,329 in 2013 to $2,685 in 2023[2], making checks a lucrative target for bad actors.



CLICK HERE TO LEARN MORE

This is not your grandfather's check fraud.

Traditional forms of check fraud like counterfeiting, forgery and alteration persist, but modern-day criminals are using new methods to exploit weaknesses in the banking system. Below are common check fraud tactics.

MAIL THEFT

What it is: Stealing checks from the mail with the intent of accessing the account's funds, generally by altering the payee's name and dollar amount.

What's new: Organized crime rings now engage in mail theft on a broader scale. Increasingly, criminals are using stolen or counterfeit USPS master keys to open blue collection boxes, as well as mailboxes in apartment complexes, commercial buildings and residential communities that use cluster mailboxes. In short, criminals are getting their hands on more checks, more quickly.

CHECK WASHING

What it is: Removing the ink from valid checks using chemicals or other techniques—in order to change the payee's name and often, drastically increase the dollar amount.

What's new: Criminals have devised more advanced processes to dissolve the ink. Some schemes involve printing multiple copies of the washed checks—which they can use in the future or sell to other criminals on the dark web.

DUPLICATE DEPOSIT

What it is: A criminal deposits the same check into multiple accounts they hold at various institutions—using each FI's mobile app—then quickly withdraws the available funds. In some cases, the criminal will deposit (and cash out) the physical check one final time at the teller window or ATM.

What's new: This tactic wasn't possible prior to remote deposit capture technology because the criminal needs to hold onto the physical check for the scheme to work. (It's worth noting that even honest customers can inadvertently make a duplicate deposit—with the physical check still on hand, they may simply forget they already deposited it.)

CHECK OVERPAYMENT SCAM

What it is: The criminal purposely overpays an individual or business for goods or services using a bad check, then requests a refund for the surplus amount. The scammer then makes off with the refund payment along with the original item or service they "purchased."

What's new: Faster payment technologies like mobile payment apps, real-time ACH and other electronic money transfer options make it easier for scammers to receive, deposit and cash out the 'refund' payment before the fraud is detected.

CLICK HERE TO LEARN MORE

Check fraud harms FIs in more ways than one.

As check fraud goes up, the impact on FIs is compounding. Each attack leads to direct and indirect bottom-line losses.

Repayment costs: Because banks and credit unions typically reimburse customers affected by check fraud, they often incur the direct loss of the theft.

Associated costs: FIs must deploy staff to investigate the theft, attempt to recover the funds and determine who is liable for the loss (i.e., the bank of first deposit, the initiating bank, or the customer). It's a long, drawn-out process. As attacks increase, so does the drain on the institution's resources.

Reputational costs: In some cases, customers suffer major losses. With counterfeit checks, for example, the person who makes the deposit is often liable for repaying the funds. Even when FIs do reimburse customers for check fraud losses, the process can be time-consuming and frustrating. Failing to protect customers affected by check fraud can erode brand trust and increase customer attrition.

CLICK HERE TO LEARN MORE

Criminals are exploiting weaknesses in check handling systems.

Digital banking has improved the overall security of financial transactions. But it also creates new check fraud challenges. Due to the speed of digital transactions, a criminal can deposit a check and make off with the money before the check is processed and the fraud is detected.

Criminals aren't just targeting digital channels. Some still deposit bad checks at the teller window. Modern check washing, altering and counterfeiting processes make the fraudulent checks difficult to spot. What's more, some crime rings are creating sophisticated fake IDs—and training "walkers", or people who actually walk into the bank to cash these checks, how to do so without raising suspicions.

In the ever-evolving landscape of check fraud, implementing robust prevention measures is crucial. Below are four best practices for safeguarding your institution and your customers.

CHECK FRAUD PREVENTION BEST PRACTICES

1

Educate your employees and customers. Communicate regularly with customers and staff about trending check fraud tactics and how to stay vigilant.

- Train your employees to watch for red flags, such as the following listed in a 2023 FinCEN alert:
- Non-characteristic large withdrawals on a customer's account via check to a new payee
- Checks used to withdraw funds from a customer's account appearing different from the bank's legitimate transactions
- Existing customers with no history of check deposits suddenly making check deposits and withdrawals or transfers of funds
- Non-characteristic, sudden and abnormal deposits of checks, often electronically, followed by rapid withdrawal or fund transfer.[3]

Education should also extend to your customers. Keep your individual and business customers updated on common check fraud methods and the risks of using paper checks. In so doing, you'll protect your customers, strengthen relationships and improve brand trust.

CLICK HERE TO LEARN MORE

2

Pool your data.

Many check fraud scams rely on depositing checks originating from different banks. Consortia and/or bank-contributed data provides valuable information for assessing risk and detecting potential fraudulent transactions effectively.

Early Warning customers, for example, have access to The National Shared Database℠, which includes deposit performance data contributed by more than 3,500 participating banks and credit unions. When you have deep insight into an individual's current and past account behavior across institutions, you can more easily spot suspicious activities.

3

Encourage electronic payment methods.

Promoting the adoption of electronic payment options—and thereby reducing check usage—is perhaps the most straightforward way to prevent check fraud. But it's easier said than done.

Three-fourths of organizations currently using checks do not plan to discontinue issuing them.[4]

Businesses and individuals are often reticent to stop using checks due to a lack of information. Focus on educating your customers about various electronic payment options, such as mobile payments, digital wallets and same-day ACH. Empowering customers with knowledge about the ease and security these payment alternatives offer can help motivate them to make the switch.

4

Monitor, classify and analyze losses.

To outpace fraudsters, you must identify their trends and tactics—then proactively counter them.

Modern solutions that combine real-time monitoring with advanced analytics can help you detect and prevent check fraud. By observing check deposits and withdrawals as they happen—whether it's at the teller windows, ATMs or via remote deposit capture—you can swiftly spot potential fraud.

Predictive intelligence tools can help you further analyze historical deposit and transaction data to assess risk and identify potentially fraudulent activity. By screening off-us or on-us checks against the National Shared Database℠, for example, Deposit Chek® from Early Warning lets you confirm the status of an account and determine the likelihood that a check will be paid. In 2023, Deposit Chek® helped the U.S. financial system save $1.76 billion in total potential fraud loss.

CLICK HERE TO LEARN MORE

BY ADOPTING THESE CHECK FRAUD PREVENTION BEST PRACTICES, YOU'LL BE BETTER EQUIPPED TO SAFEGUARD YOUR CUSTOMERS AND YOUR INSTITUTION FROM COSTLY CHECK FRAUD LOSSES.

Learn more about how Early Warning helps banks and credit unions prevent check fraud and protect customers.

Sources

1 Trends in Fraud for 2024 and Beyond, Datos Insights, Feb. 2024
2 Commercial Checks Collected Through the Federal Reserve, Federal Reserve, Last Updated Feb. 2024
3 FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail, U.S. Treasury Financial Crimes Enforcement Network, 2023
4 2024 AFP Payments Fraud and Control Survey Report, Association for Financial Professionals, 2024

ABOUT EARLY WARNING

Early Warning Services, LLC, a financial services technology leader, has been empowering and protecting consumers, small businesses, and the U.S. financial system with cutting-edge fraud and payment solutions for more than three decades. We are also the company behind Zelle®, and the soon-to-launch Paze℠, a wallet that reimagines e-commerce payments. Early Warning partners with more than 2,500 banks and credit unions to increase access to financial services and products, and protect financial transactions.
Learn more at www.earlywarning.com.

CLICK HERE TO LEARN MORE