CHECK FRAUD PREVENTION GUIDEBOOK

Best Practices to Help Organizations Identify and Avoid Fraud

Huntington
Welcome.®

Table of Contents

CHECK FRAUD PREVENTION GUIDE BOOK

Introduction

Check fraud continues to pose a significant threat to businesses and organizations of all sizes, exposing them to financial losses, reputational damage, and operational challenges. In the payment landscape, checks remain the most vulnerable to fraud, with 65% of organizations reporting they have experienced actual or attempted check fraud†. Recovery attempts could take 120-180 days, meaning the payee and payer could be at a loss for months without a resolution. Fund recovery is also not guaranteed, which is what makes check fraud incidents so financially damaging.

65%

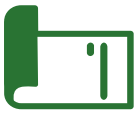
The number of surveyed organizations that report experiencing actual or attempted check fraud†.

For companies reliant on checks, understanding how these fraud schemes work – and how your business could help prevent them from happening – is key to protecting your finances. Huntington's Treasury Management, Cybersecurity Outreach, and Enterprise Fraud teams compiled this guide to check fraud prevention to equip you with the knowledge needed to help identify and defend against common check fraud schemes.

Understanding Check Fraud

Check fraud encompasses a wide array of deceptive practices, from altering check details to creating counterfeit documents. Fraudsters act by stealing checks from mailboxes, obtaining sensitive company information, or even working with insiders.

Check fraud can be divided into two categories:



Back-of-check fraud typically involves manipulating the endorsement area on a check through forgery or altering details. These tactics allow unauthorized individuals to claim ownership of the check to deposit or cash it.

Front-of-check fraud encompasses any modifications to the check's face value, payee name, or other details to increase the amount or change the intended payee and can also include a forgery of the check maker's signature.

The varied nature of check fraud requires diligent oversight and strong verification processes to detect and prevent. Companies should consider implementing fraud mitigation tools as well as ensuring employees are well-trained on common fraud tactics and how to handle suspicious payments.

SIX COMMON CHECK FRAUD TACTICS

#1: CHECK ALTERING

WHAT IS IT?

Check altering is a form of fraud that involves changing the details on a legitimate check, such as the payee name or amount. Fraudsters might use chemicals to erase or modify those details.

HOW IT HAPPENS

A check that was issued by a business is stolen or intercepted before it reaches the intended recipient. The fraudster then physically alters the information on the check – often the payee or amount – and then deposits or cashes it. Checks are typically stolen from the mail or obtained by someone with access to a company's outgoing payments.

PREVENTATIVE MEASURES

- **Secure checks:** Consider using checks with advanced security features that make it difficult to alter, such as watermarks or chemical-sensitive paper.
- **Use windowless envelopes:** Using a windowless envelope to send checks through the mail could make it more difficult for fraudsters to know it contains a check.
- Check Positive Pay and Teller Positive Pay: This service can provide early detection of fraudulent, altered, or counterfeit checks by comparing checks presented on your account against the checks issued daily.
    - **Teller Positive Pay:** Identifies potentially fraudulent, altered, or counterfeit check items presented at branches by comparing them in real-time with the check register file. If the information does not match, the check will not be cashed.
- **Enhance Check Positive Pay with Payee Positive Pay:** Allows you to add a layer of security by providing payee name with the check register file submitted for Check Positive Pay. When checks are presented, the dollar amount, check number, and payee information are compared with the check register file.
- **Regular account monitoring:** Institute a process to review bank statements and transactions on a regular basis to aid in early detection of check fraud.
- **If your business accepts checks for payment:** Review checks for signs of tampering before depositing them into your organization's account, including handwritten numbers or dates, signs of erasure, and stains or discoloration.

SIX COMMON CHECK FRAUD TACTICS

#2: COUNTERFEIT CHECKS

WHAT IS IT?

Counterfeit checks are fabricated using stolen account information to mimic real checks. Fraudsters use sophisticated printers and scanners to create these fake checks, so it can be difficult to distinguish between legitimate and fraudulent items.

HOW IT HAPPENS

Fraudsters typically obtain bank account details through methods such as phishing or by accessing physical documents. That information is used to produce and cash counterfeit checks that might incorporate your company logo, account names, or other details to enhance their legitimacy.

PREVENTATIVE MEASURES

- **Regular cybersecurity and fraud training:** Educating employees about phishing scams and other common cybersecurity attempts is an important step for organizations to help reduce the threat of fraud.
- **Secured data:** Use secured, encrypted channels for transmitting financial data within your organization to help prevent it from being accessed by cybercriminals.
- **If your business accepts checks for payment:** Be vigilant in examining checks from vendors and payees for irregularities in paper quality, printing, and security features to identify potential counterfeits.
- **If your business sends checks against your account:**
    - Check Positive Pay with and Teller Positive Pay: This service can provide early detection of fraudulent, altered, or counterfeit checks by comparing checks presented on your account against the checks issued daily.
        - **Payee Positive Pay:** Allows you to add a layer of security by providing payee name with the check register file submitted for Check Positive Pay. When checks are presented, the dollar amount, check number, and payee information are compared with the check register file.
        - **Teller Positive Pay:** Identifies potentially fraudulent, altered, or counterfeit check items presented at branches by comparing them in real-time with the check register file. If the information does not match, the check will not be cashed.
    - Reverse Positive Pay is a fraud mitigation service that provides a daily report of check activity to review and confirm transactions. A Reverse Positive Pay report includes check information as well as digital images of checks, which companies can review to determine whether any items need to be returned.
- **If your business does not send checks against your account**: Check block is a fraud mitigation tool that eliminates the risk of check fraud by designating a company's account as an electronic-only account. Enabling Check Block restricts your business account from allowing paper-based transactions and automatically rejects and returns them.

SIX COMMON CHECK FRAUD TACTICS

#3: FORGED CHECKS

WHAT IS IT?

Forged checks typically involve unauthorized individuals signing a check on behalf of someone else, essentially stealing funds from the victim's account.

HOW IT HAPPENS

A fraudster steals a legitimate, blank check from a company or creates a counterfeit check as described above and forges the account holder's signature, then cashes or submits it for deposit.

PREVENTATIVE MEASURES

- Reverse Positive Pay: This fraud mitigation service provides a daily report of check activity to review and confirm transactions. A Reverse Positive Pay report includes check information as well as digital images of checks, which companies can review to determine whether any items need to be returned.
- **Secure check storage:** Keep blank checks in a safe, locked location that can only be accessed by designated employees to prevent unauthorized access.
- **If your business accepts checks for payment:**
  -Be vigilant in examining checks from vendors and payees for irregularities in paper quality, printing, and security features to identify potential counterfeits.
  -Be attentive to discrepancies in check signatures and, when in doubt, take steps to verify the authenticity of the signer. Ensure your organization has a process for this that is clearly communicated to anyone handling checks.
- Check Positive Pay with and Teller Positive Pay: This service can provide early detection of fraudulent, altered, or counterfeit checks by comparing checks presented on your account against the checks issued daily.
  - **Payee Positive Pay:** Allows you to add a layer of security by providing payee name with the check register file submitted for Check Positive Pay. When checks are presented, the dollar amount, check number, and payee information are compared with the check register file.
  - **Teller Positive Pay:** Identifies potentially fraudulent, altered, or counterfeit check items presented at branches by comparing them in real-time with the check register file. If the information does not match, the check will not be cashed.

SIX COMMON CHECK FRAUD TACTICS

#4: ENDORSEMENT FRAUD

WHAT IS IT?

Endorsement fraud involves altering or forging the endorsement on the back of a check to illegally cash or deposit it.

HOW IT HAPPENS

A fraudster intercepts a check issued by a business and forges or alters the endorsement on the back of the check. They then attempt to deposit that check into their own bank account or cash it out. For example, a fraudster might find a check made out to a vendor and forge the vendor's endorsement to deposit the check into their own account.

Companies typically find out about this type of fraud when a vendor or third-party service notifies them that a check never arrived, despite the check having been cashed.

PREVENTATIVE MEASURES

Fraud prevention solutions do not provide protection for this type of fraud. Instead, organizations can opt to follow preventative best practices to help mitigate the risk.

- **Transitioning to more secure payment methods** can help lower risks associated with check fraud. Electronic payments, including corporate cards, ACH, Instant Payments, and wire transfers, offer enhanced security features that can reduce the opportunity for fraud. These payment options do not eliminate fraud risk, so companies should ensure they take appropriate measures to identify and mitigate electronic payment risk.
- **Restrictive endorsements:** Encourage the use of restrictive endorsements, such as "For Deposit Only," which limits how and where a check can be deposited.
- **If your business is required to send a check:** Consider sending it through UPS, certified mail, or another tracked mail system.
- **If your business accepts checks for payment:** Establish protocols for employees to secure checks received by vendors, customers, or other third parties until they are ready to be deposited.

SIX COMMON CHECK FRAUD TACTICS

#5: DUPLICATE PRESENTMENT

WHAT IS IT?

Duplicate presentment is a form of fraud where a check is presented for payment more than once, often through different deposit methods such as physical and electronic.

HOW IT HAPPENS

After a check is deposited electronically, fraudsters present the same check again for payment at a bank or through another mobile deposit account. These checks can be altered, forged, stolen, or counterfeit checks.

PREVENTATIVE MEASURES

- **Electronic deposit-only agreements:** Set up protocols within your organization and with authorized vendors to only allow electronic means of depositing checks. These agreements would prohibit attempts to deposit or cash checks once they've been electronically deposited.
- Check Positive Pay with Teller Positive Pay: Provides early detection of duplicate, fraudulent, altered, or counterfeit checks by comparing checks presented on your account against the checks issued daily.
    - **Teller Positive Pay:** As part of Check Positive Pay, this service identifies potentially fraudulent, duplicate, altered, or counterfeit check items presented at branches by comparing them in real-time with the check register file. If the information does not match, the check will not be cashed.
- Enhance Check Positive Pay with Payee Positive Pay: Allows you to add a layer of security by providing payee name with the check register file submitted for Check Positive Pay. When checks are presented, the dollar amount, check number, and payee information are compared with the check register file.
- **If your business accepts checks for payment:** Similar to the electronic deposit agreements with vendors or customers depositing checks from your business, implement an internal rule to only deposit checks electronically. Include a process for destroying checks after being deposited electronically to prevent them from being stolen and physically presented for deposit.

SIX COMMON CHECK FRAUD TACTICS

#6: MOBILE DEPOSIT FRAUD

WHAT IS IT?

With the rise of mobile banking, mobile deposit fraud has become an increasing concern. Fraud here can take many forms, including duplicate presentment (as explained above), account takeover, and deposit scams.

HOW IT HAPPENS

In the case of an account takeover, fraudsters gain unauthorized access to a company's banking credentials through social engineering, such as **business email compromise (BEC)** or other illegal methods. They then use the company's mobile deposit feature to deposit fraudulent checks into the account and quickly transfer the funds to other accounts under their control before fraud is detected.

Deposit scams involve deceiving employees into depositing fraudulent checks via mobile deposit, then transferring those funds to other accounts. This scam might involve overpayment for a service or purchase with a request to wire excess funds to a third party. Impersonation of business executives or other employees is often employed with this tactic.

PREVENTATIVE MEASURES

- **Regular social engineering training:** Ensure employees know how to spot BEC and phishing red flags in emails and establish strict protocols for handling suspicious communications.
- **Multi-factor authentication (MFA):** Implementing MFA strengthens mobile deposit and company account security. This multi-layered approach typically includes a **strong password**, security token, and biometric verification, such as an employee's fingerprint.
- **If your business accepts checks for payment and uses mobile deposit:** Verify the legitimacy of mobile deposits, especially for large sums, to help prevent falling victim to fraudulent activities. Set up a checks-and-balances system to ensure no one employee has access to both deposit and transfer funds. Additionally, use caution when accepting checks from unknown individuals or businesses.

WHAT TO DO IF YOU DETECT CHECK FRAUD

Your financial institution can help guide your business through the process of reporting check fraud and attempting to recover funds. However, fund recovery is not always possible, and there are strict timelines for reporting potential fraud.

1. Prioritize check fraud monitoring using the tools available to you.

Be aware that companies are often obligated to use fraud prevention services provided by their financial institution. These products are typically designed to discover or prevent unauthorized transactions, including unauthorized checks and ACH debits, forgeries, and alterations. Choosing to not use them could result in the bank no longer having liability for any fraudulent transaction that occurs on the account that those products were designed to discover or prevent.

Ensure your company reviews transactions, check activity, and statements in a timely manner and makes use of the check fraud tools available to you. If you choose not to use the services provided, there is no guarantee that unrecovered funds will be reimbursed.

2. Contact your bank immediately after identifying suspected fraudulent activity.

Companies are required to notify their bank within 30 days after their statement is mailed or made available, or as soon as possible, after discovering an error or fraudulent charge in the transaction history, or when notified by their payee. Failing to do so would result in the bank no longer being responsible for the errors or fraudulent charges. For this reason, companies should prioritize reviewing statements immediately upon receipt and be thorough in their review to avoid losses.

3. Be prepared to provide documentation.

You will likely need to provide documentation such as check images, transaction records and account statements.

4. Your bank will conduct a review and work toward a resolution, if possible.

Review times average 120-180 days. Though not guaranteed, even if fund recovery is successful, your company and the payee will be at a loss for that amount for the duration of the review. Consider planning for a fraud event with cash reserves or an alternate plan to avoid a check fraud incident disrupting operation, and/or by investing in a cybersecurity insurance policy.

CHECK FRAUD PREVENTION BEST PRACTICES

Companies should be aware of the important role they play in preventing fraud. Actively participating in monitoring accounts, reviewing statements, implementing internal controls, and remaining vigilant against check fraud attempts is critical in safeguarding financial assets.

These best practices can help organizations protect themselves against costly check fraud incidents.

CONSIDERATIONS FOR BUSINESS PROCESSES AND CONTROLS

- ✓ Separate employee fiduciary duties within your organization, so the person writing the checks isn't also responsible for cashing them and reconciling accounts.
- ✓ Implement detailed verification processes to help catch alterations before processing the checks.
- ✓ Establish strict protocols for check handling to prevent internal fraud.
- ✓ Review your financial statements immediately upon receiving them to make sure fraudulent activity is caught quickly.
- ✓ Frequently review accounts at least every 30 days at a minimum to look for signs of suspicious activity.
- ✓ In the event of check fraud, prompt reporting to financial institutions is essential.
- ✓ Reconcile your account regularly to ensure correct transactions are posting.

FRAUD MITIGATION TOOLS

- ✓ Take advantage of any fraud mitigation tools your financial institution might offer, which might include:
  - ACH Positive Pay
  - Wire Block
  - Check Positive Pay
  - Reverse Positive Pay
  - Check Block

ALTERNATE PAYMENT METHODS

- ✓ Transitioning to more secure payment methods can help mitigate the risks associated with check fraud. The following electronic payments offer enhanced security features, which significantly reduce the opportunity for fraud:
  - Corporate Card
  - ACH
  - Instant Payments
  - Wire Transfers
  - ChoicePay®
- ✓ Consider making recurring payments through online bill pay or ACH.

SECURE CHECK HANDLING AND DELIVERY

- ✓ Bring checks to a post office instead of putting them in an outgoing mailbox.
- ✓ Consider sending checks through USPS certified mail, UPS, or another tracked mail system.
- ✓ Implement secure storage and controlled check access to help minimize the risk of unauthorized handling.

HELP PROTECT YOUR ORGANIZATION AGAINST CHECK FRAUD

Awareness, employee education, and preventative measures play a pivotal role in navigating the complexities of check fraud.

Huntington is committed to protecting the safety and security of our organization. **Our payment and fraud** mitigation solutions are designed to make it easier for you to monitor your payments so you can stay one step ahead of threats to your business' finances.

Connect with your Relationship Manager or contact our Treasury Management team to learn more about the security solutions available to your business.

Huntington
Welcome.®

† Association for Financial Professionals. 2024. "2024 AFP Payments Fraud and Control Survey." Accessed April 19, 2024. 2024 AFP Payments Fraud and Control Survey Report (afponline.org)