FIRST SAVINGS BANK®

Check Fraud Prevention Guide

HOW TO PROTECT YOUR COMPANY FROM CHECK FRAUD

Introduction

With cybercrime on the rise, the threat of check fraud remains a significant concern for businesses. According to a 2022 survey from the Association for Financial Professionals, two-thirds of businesses encountered check fraud incidents. And, physical checks were at the top of the list of payment methods vulnerable to fraudulent activity. It is now critical for companies, regardless of size or industry to prioritize check fraud prevention by improving internal processes.

First Savings Bank offers account protection and support to help businesses safeguard against fraudulent activities. However, it is ultimately the responsibility of each enterprise to adhere to best practices and integrate check fraud prevention into their financial management practices.

This guide outlines types of check fraud and actionable steps that, when used effectively, can help you identify and defend against check fraud.

Our team of experts is always available to assist you. Please reach out to your local branch for additional information.

We're Here For You!
Our team is available by phone during regular business hours. Call us toll free at 1-800-555-6895 or by contacting your local branch. Click here to view branch locations.

What is Check Fraud?

While cybercrime and electronic payment fraud often dominate security discussions, check fraud should not be underestimated or overlooked. Checks remain a prevalent method of payment for businesses of all types, making them a huge target for fraud.

Check fraud happens when an individual falsifies a check or manipulates its digital representation, with the intention of deceiving a person or organization into surrendering funds. There are two primary forms of check fraud: front-of-check fraud and back-of-check fraud. Counterfeiting or modifying the details on the face of the check constitutes front-of-check fraud, while back-of-check fraud involves endorsement issues—like forgery or the absence of a legitimate endorsement—and can extend to abuses in mobile deposit schemes.

Check fraud can be a tricky problem to solve, as it's a relatively easy type of fraud to commit. With just one intercepted check, a fraudster can obtain your checking and routing numbers, providing them with the necessary information to create counterfeit checks. Therefore, it is crucial to implement proper controls and account protections to establish a strong defense against check fraud.

First Savings Bank's Proactive Role in Combating Check Fraud:
We prioritize your security and take active measures to prevent fraud. These measures include screening transactions and verifying any suspicious activity. However, as the account holder, you are responsible for the movement of your funds. Our account disclosures outline the responsibilities of the bank, clients, and third parties involved. It's crucial to carefully read and fully understand these terms to prevent any fraudulent activity and potential losses.

Of those who were victims of payments fraud in 2022, more than one-fourth of organizations (27%) were able to successfully recover at least 75% of funds lost.

However, nearly half (44%) were unsuccessful in recouping any of the stolen funds. - AFP

WHAT IS CHECK FRAUD?

What you Need to Know

Strict reporting windows apply when it comes to check fraud. It is your responsibility to thoroughly review statements and promptly report any irregularities to us as soon as they are identified. Claims reported outside of these windows are liable to be denied by the bank. (Please see account disclosures for specific timelines.)

It's crucial to keep in mind that recovering funds lost to fraud cannot be guaranteed. During the investigation, you (as the client) and the intended payee will experience a loss of the amount for the duration of the investigation, regardless of the outcome. The recovery process can take anywhere from 90 to 120 business days on average, but it can take much longer.

Please understand that having a fraud protection product added to your account does not guarantee protection. In order to ensure maximum effectiveness, the product must be used in the manner intended. Failure to use the product correctly could result in liability for any losses incurred due to fraud. This is explained in greater detail in your account disclosures.

Important Notice Regarding the Use of Facsimile Signatures: Please be advised that if you suspect the misuse of your facsimile signature, you must notify us immediately. It is important to note that customers who choose to use a facsimile or mechanically reproduced signature are solely responsible for any check fraud. *(Please see account disclosures for specific details.)*

Keep Contact Information Up to Date with First Savings Bank
Let us get in touch quickly if we detect suspicious banking activity by regularly checking and updating your contact details.

BEST PRACTICES

- Verbal verification of payee information for any high-dollar payment requested (whether electronic or check).
- Payment thresholds above which payees must be paid directly via electronic methods.

When mailing checks:

- Always use a secure drop-off location such as the USPS mailbox.

When writing checks:

- Make sure the written and numeric amounts on the check are accurate and match.
- Fill in all spaces completely so numbers/letters cannot be added to the check.

Additionally:

- Don't give anyone a blank check or permit anyone to sign your name to a check, even trusted employees.
- Store checks and signature stamps in a secure location and frequently confirm that you are not missing checks.
- If you discover you are missing a check or signature stamp, notify the bank immediately.
- Record your transactions and reconcile your accounts on a regular basis.

First Savings Bank offers several options designed to protect clients against various forms of check fraud, including:

Positive Pay Services
You can use this to validate payee information, including payee names when checks are presented for payment. This product can help defend against both counterfeit and altered checks.

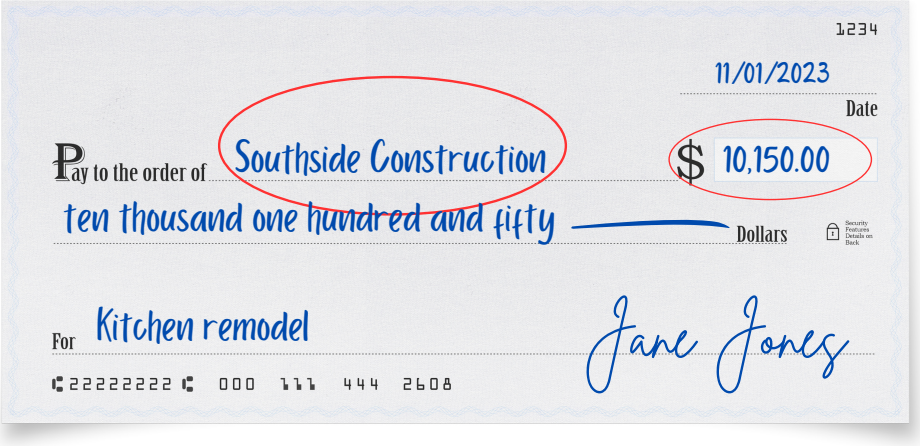
ACH Services
Automated Clearing House (ACH) services allow you to electronically pay employees payroll, pay vendor invoices and collect payments.

Dual Signatures
For large check transactions, businesses may benefit by requiring the signatures of two executives with the authority to issue such payments. This creates a higher level of scrutiny for these transactions.

FRONT OF CHECK FRAUD

Altered Checks

This is a common scheme where criminals modify the name or payment amount before depositing a check. To prevent such fraudulent activities, businesses can use Positive Pay with Payee Name Validation, which verifies that the check's information matches up with the business's records.



To safeguard your accounts against altered check fraud, it is crucial to activate Positive Pay features and to use the product correctly. Ensure that you carefully review all "exception" items before making a decision to pay, and keep account defaults set to "return" for exceptions. Failure to adhere to these guidelines may render you liable for altered-item losses.

While Positive Pay is a recommended feature, it alone may not be sufficient to detect all fraudulent changes. For example, a fraudster may intercept a check meant for a trusted third-party vendor and add "LLC" to the intercepted check after opening an account. Without a thorough review of the original item and proper use of Positive Pay with Payee Name Validation, this type of alteration could easily go unnoticed.

Consider another example where a client commonly made high-value payments via paper check. They mailed a check for over $1 million to a vendor, but at the time, the account did not have Positive Pay with Payee Name Validation activated. After a few weeks, the vendor informed the client that they had not received the check payment. The check had been intercepted by a fraudster while in transit, and the payee name was altered. The fraudster was able to successfully negotiate the check at another bank.

Be diligent in protecting your business and take advantage of available security features.

FRONT OF CHECK FRAUD

Counterfeit Checks

If a criminal has access to your checking account and routing numbers, along with the name and signature style of the authorized signer, they can produce fake checks using printers and desktop publishing software. To avoid this risk, consider using Positive Pay, a fraud protection service that can detect and stop the payment of counterfeit checks.

To prevent against both counterfeit and altered check fraud, we recommend using Account Reconciliation and Check Positive Pay with Payee Name Validation

Let's consider an example of counterfeit checks and how account tools are meant to catch fraud. In this case, a criminal was able to obtain bank account information. The fraudster then used the account details to issue multiple fraudulent checks, totaling over $1 million in fraudulent payments.

The targeted client's account did not have electronic payment thresholds related to high-dollar checks and was not using positive pay. Ultimately, this meant all these counterfeit checks could be presented without immediate detection.

Fortunately, the client noticed the fraud quickly and took swift action. Still, less than 20% of the funds were available for recovery, resulting in a client loss.

Train employees to recognize signs of check fraud, such as unusual alterations, suspicious payees, or mismatched signatures. Encourage prompt reporting of suspicions.

BACK OF CHECK FRAUD

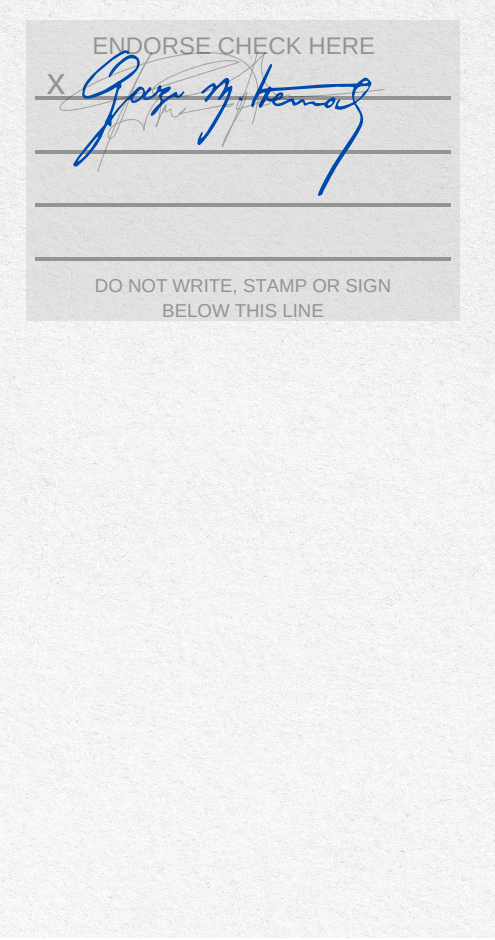
Forged, Missing or Improper Endorsement

In the majority of cases involving forged, missing or improper endorsement, a criminal will forge the endorsement on the back of a check and deposit it into a financial institution. However, there are also instances where the endorsement is absent altogether, or one of the two parties named on the check improperly endorses it.

Unfortunately, there are no current fraud protection products available to safeguard against this type of fraud. Although the accepting bank is typically responsible for any losses, retrieving funds is not guaranteed and may take up to 120 working days or more. If you receive a call from a vendor claiming non-payment, but you know the check was mailed, it's crucial to look into the status of the check as soon as possible since claims of forged or missing endorsements are time-sensitive.

Here are some best practices to minimize the risk of check fraud:

- Whenever possible, avoid multiple payee checks. It's best to include only one payee per check.
- Implement payment thresholds that require electronic payment methods for high-value transactions.
- Proactively confirm with intended recipients of high-value checks that the items were received.
- Always send high-dollar checks through trackable shipping methods instead of regular mail.



Investigate any checks with suspicious endorsements or signatures that appear inconsistent with the payee's usual signature.

BACK OF CHECK FRAUD

Mobile Deposit Fraud

While mobile check deposit offers significant benefits, it has also led to a surge in check fraud. What sets this form of fraud apart is that the perpetrator is typically the intended recipient. This type of fraud is often committed by employees who try to cash their paychecks twice after being fired from their job.

A business issues a check to an individual, who then images the front and back using their smartphone camera. The check is deposited into their account, and the physical check is taken to another bank or check-cashing store for payment. The problem arises when the check is presented for payment to the originating bank and is flagged as a duplicate. Dishonored checks could lead to a time-consuming and expensive claims process to determine who is liable for the funds.

To avoid this issue, electronic payments should be made directly to the payee. Mobile check fraud is largely identified due to Positive Pay being active on most clients' accounts, causing the check to appear as a duplicate against the mobile deposit. The duplicate is returned without the client realizing that it is a fraudulent check deposit (Holder in Due Course scenario). The paper holder (often a check-cashing facility) will demand payment from the “maker” of the check (the client).

Visit with your Banker about our ACH Services: Automated Clearing House (ACH) services allow you to electronically pay employees' wages for payroll or pay vendor invoices. You can also collect payments such as fees, dues, or donations. ACH streamlines your payment process and eliminates the costs associated with check processing. You choose between several methods of origination that best meet your company’s accounting needs. ACH expedites payments, improves your cash flow, and benefits your employees and vendors.

Mobile fraud occurs over a series of steps:

- An individual receives a check from a client.
- The individual completes a mobile deposit.
- The same individual goes to a check-cashing facility and cashes the paper check.
- The check-cashing facility presents the check to First Savings Bank for payment.
- The payment is flagged and the check is returned as a duplicate.
- A demand letter is sent from the check-cashing facility to the client. In turn, the client files a claim with First Savings Bank.
- If First Savings Bank is successful in recovering funds from the remote deposit capture bank, it pays out funds to the client and the client returns those funds to the check-cashing facility.

What to do if you Experience Check Fraud

> *Time is critical when dealing with instances of check fraud. To prevent further fraud, one of the most effective measures you can take is to eliminate check usage and switch to electronic payment methods.*

If it is not possible to eliminate checks entirely, you can take the following measures to protect your organization against fraud:

- Use Positive Pay with Exceptions on all check-writing accounts.
- Apply ACH debit filtering to accounts accepting ACH debits, and establish a reconciliation process to identify unauthorized transactions with enough time to report to the bank within 24 hours of posting.

However, be aware that if checks are absolutely necessary, an inherent risk may still exist, which may not be entirely mitigated.

Forged or missing endorsements require a claims process to recover funds from the bank of first deposit. It can take 120 business days or more for funds to be returned if the claim is not denied. To mitigate this risk, limit check usage to low volume and low dollar values, use courier services instead of USPS mail, and confirm receipt with the recipient. For Holder in Due Course, a claims process is also required to recover funds from a mobile bank.

Contact First Savings Bank Right Away if you Suspect Check Fraud
Our team is available by phone during regular business hours.
Call us toll-free at 1-800-555-6895 or by contacting your local branch.
Click here to view branch locations.

Next Steps

Now that you know how to spot and stop check fraud, how it occurs and some best practices to safeguard your accounts, what should you do?

We recommend that you review your accounts every 30 days at a minimum for signs of suspicious activity, reconciling payments and verifying any suspicious transactions. Review any accounts that issue checks and apply appropriate safeguards, like Check Positive Pay with Payee Name Validation.

Finally, when in doubt—take action! It's better to question a legitimate transaction now than to try and recover funds lost to check fraud later.

PC Execubanc®
Internet Banking for Businesses

Successful fraud prevention begins with secure business banking services. Visit with your Banker to ensure you have the tools you need to manage your business.

- *View Real-time Account Balances*
- *Review Check and Deposit Images*
- *Monitor Accounts with Alerts*
- *Take Advantage of Payroll Direct Deposit*
- *Utilize ACH Origination & Wire Transfers*
- *Assign Designated Employee Access*
- *All in a fully safe and secure environment*

Protect Your Business Against Check Fraud with Our Support

Ensuring your business is safeguarded against check fraud requires knowledge, proactivity, and staying informed about the latest trends in fraud. By implementing security practices and staying vigilant, you can significantly reduce the risk of fraudulent activities. As your trusted financial partner, we are committed to providing the necessary support to keep your finances secure. If you have any concerns about check fraud or account security, please do not hesitate to contact us. Together, we can strengthen the resilience of your business against financial threats.

Call us toll-free at 1-800-555-6895 or by contacting your local branch.
Click here to view branch locations.

FIRST SAVINGS BANK®

WWW.FIRSTSAVINGSBANKS.COM - MEMBER FDIC