



Identify and Prevent Check Fraud



Check Fraud is on the Rise

Checks have been utilized as a convenient payment method for decades, offering a variety of benefits as well as risks. While advances in technology have made it easier for customers and financial institutions to use checks, it has also given scammers and fraudsters new opportunities as well.

According to FinCen, the number of check fraud cases reported in 2022 was 680,000-and, it's expected to continue to rise. Even with a shift to online payments, billions of checks are still in circulation, putting millions of consumers at risk.

Financial services organizations have a responsibility to prevent fraud and other scams before it happens. Organizations need to be aware of the latest tactics associated with check fraud and train their employees to identify when check fraud might be happening and how to respond appropriately to it.

Understanding Checks to Detect and Prevent Fraud

Organizations should provide a comprehensive training program for employees which includes training on the components of a check and how to review those components to verify that check's legitimacy. Once employees have a solid understanding of this information, subsequent training should teach employees how to recognize and address red flags associated with check fraud and scams. Organizations should also have established procedures, so employees know how to respond appropriately.



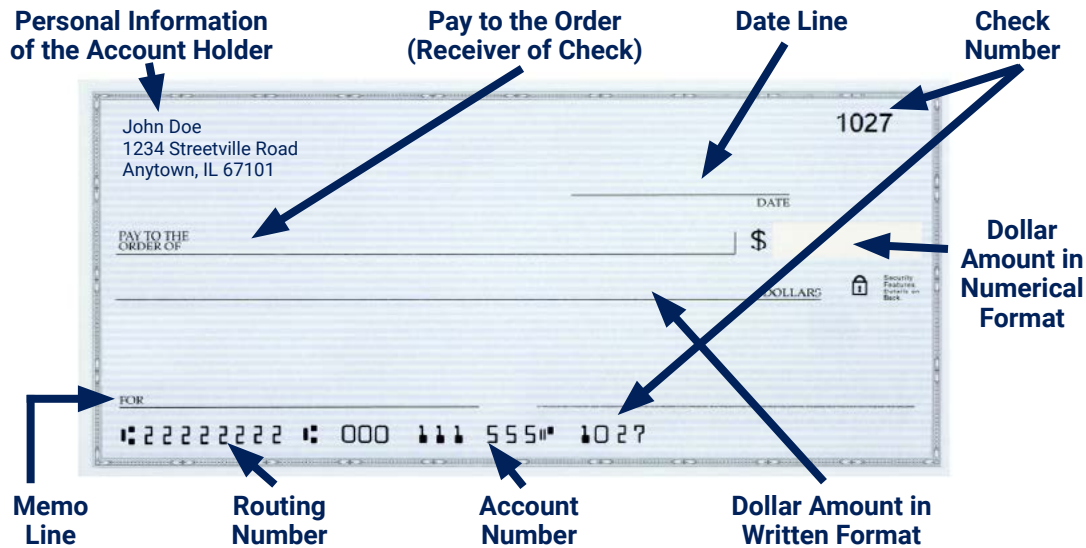
Stay Ahead. Act with Confidence.

[Contact us](#) to learn more.

Identify and Prevent Check Fraud

Understanding Check Components

Even though there are many different types of checks, they all contain the same components. The diagram below of the front of a check provides descriptions of each component:



Check Type

Training courses on checks should include information on the various types of checks listed below:

- Personal
- Certified
- Cashier's
- Payroll
- Traveler's

Negotiating Checks

Improper endorsement of a check can cause a delay to the customer/member from receiving their funds. The minimum required factors in making a check negotiable are:

- Must be in writing must be signed by the maker (front of check) and the drawer (back of check)
- A definite order to pay must be included ("I/We promise" or "Pay") on the front of the check
- Must be unconditional promise (i.e., no strings attached or conditions that must occur before it can be executed)
- Must be payable in cash or currency
- Must be an order or promise to pay a specific amount
- Must be payable under a finite amount of time
- Must be payable to a payee or bearer

A Check is a Negotiable Instrument

A negotiable instrument is a written document which is signed by both the maker and the drawer, containing a legal, unconditional promise to pay a specific amount of dollars and/or cents within a finite amount of time to one or multiple people known as the bearer(s).



Check Fraud Types

Check fraud refers to any deceptive act involving checks to illegally obtain money. This can include altering legitimate checks, forging signatures, creating counterfeit checks, or using stolen checks to make unauthorized transactions. Below are common check fraud types that should be covered in training courses:

Paperhanging: This generally involves a fraudster writing a bad check and quickly withdrawing funds or making purchases before the check bounces. The point of this tactic is to exploit the delay between check writing and check processing which can allow a fraudster to conduct transactions before a financial institution detects the fraud.

Check Washing: This is when a scammer steals a check and then chemically removes the ink to adjust various details of the check such as the payee's name, the amount, or other details. Then, they rewrite the check so they can easily deposit it to their own account.

Forgery: Criminals may steal blank checks from someone. Once they have their checks, they can alter the details and forge a signature to make it look like the owner issued the check.

Check Kiting: Kiting occurs when a scammer uses several bank accounts to write bad checks. Before the check clears, they transfer funds from another account or write a bad check from another account to cover the first check. This creates a temporary illusion of sufficient funds, exploiting the delay in the check clearing process.

Counterfeit Checks: These checks are fabricated to resemble legitimate checks issued by banks or businesses. Criminals generally use advanced printers and graphic design tools to replicate the look and feel of legitimate checks.



Electronic Check Fraud

In addition to physical check fraud, fraudsters may utilize digital methods to exploit people and defraud them. Electronic check (e-check) fraud essentially occurs when someone fraudulently gains access to a person's account and initiates e-check transactions without consent. There is also mobile deposit fraud which is when someone uses remote deposit technology to deposit the same check into multiple accounts or deposit stolen or counterfeit checks.

Check Scams

Check scams manipulate people into unintentionally participating in transactions based on counterfeit checks. It typically involves a criminal asking someone to deposit a check and then requesting a follow-up action, like transferring the money somewhere else or refunding part of the check funds back to the criminal.

There are a few scams both consumers and businesses should be aware of:

Overpayment: The scammer sends a check to the victim for an amount greater than the agreed-upon price. They then ask the victim to refund the excess amount before the check bounces.

Work-From-Home: Scammers pose as employers offering remote jobs. They send a check to cover initial expenses or equipment, instructing the victim to deposit it and wire a portion back before the bank identifies the check as fraudulent.

Lottery Prize: Victims receive a fake check and a notification that they've won a lottery or prize. They're instructed to deposit the check and return a portion to cover taxes or fees. The check eventually bounces.

Mystery Shopper: Victims are offered a mystery shopper position, receiving a check to purchase products or services. They're instructed to evaluate the experience and send back the leftover money. The check is counterfeit, and victims lose money.

Phishing: Similar to eCheck fraud, an email is sent to a victim asking them to provide their checking information to confirm payment of an expense. They send over their checking account info thinking their payment will go through, but the scammer can use that info to write themselves checks.

**Always positively identify customers before handling check requests.
(Verify their identity using proper identification, ensure signatures on
identification lines up with signature on checks, confirm addresses, etc.)**

How to Spot Check Fraud and Scams

Counterfeit checks are presented based on fraudulent identification or are false checks drawn on valid accounts. Counterfeit checks are most successful when false documents or instruments use actual valid accounts, technology, and check stock that makes them look and feel real.

To prevent counterfeit checks, the institution should:



Verify checks when possible before processing them as well as look for any imperfections in the checks.



Use anti-money laundering and fraud prevention software to catch potentially fraudulent checks.



Use the 314b option to reach out to other institutions for information to help with their investigations.

To reduce the risk of fraud, employees should take the following red flags into account when inspecting checks and monitoring customer behavior:

- A check that does not have a MICR line at the bottom.
- A routing code in the MICR line does not match the address of the drawee financial institution.
- The MICR ink looks shiny or feels raised.
- The magnetic ink is dull and legitimate printing produces characters that are flat on the paper.
- A check on which the name and address of the drawee financial institution is typed, rather than printed, or includes spelling errors.
- A check does not have a printed drawer name and address.
- A check on which information shows indications of having been altered, eradicated, or erased.
- A check drawn on a new account has no (or a low) sequence number or a high dollar amount.
- A signature is irregular-looking, shaky, or shows gaps in odd spots.
- A personal check has no perforated edge.
- A check is on poor quality paper that feels slippery.
- Check colors smear when rubbed with a moist finger. This suggests they were prepared on a color copier.
- Checks payable to a corporation are presented for cashing by an individual.
- Corporate or government checks show numbers that do not match in print style or otherwise suggest that the amount may have been increased.
- Checks presented at busy times by belligerent or distracting customers who try to bypass procedures.
- Checks have dollar amounts in numbers and in words that do not match.
- Items marked "void" or non-negotiable" are presented for cash or deposit.
- Customer demonstrates potential criminal behavior (i.e. paranoia, shielding, excuse making, etc.)

Using Technology to Detect Fraud

Outside of training employees, organizations can utilize advances in technology to identify and prevent fraudulent activity, which may include the use of:



Biometric scanning for both in person and online banking to ensure the appropriate person is cashing or depositing checks



Artificial intelligence to monitor deposit and withdrawal trends so potentially fraudulent activity can be flagged early

The technology that can be used will vary depending on the overall size of the company and the products they offer, but any organization that processes checks should be aware of the resources that are available to them to best protect themselves and their customers from fraud and scams.

Understanding what to look for on a check is crucial to being able to identify fraud and scams associated with checks. It is up to financial services organizations to provide adequate training to their staff members who handle and deal with checks to help them understand when fraudulent activity may be occurring and to prevent it before it affects anyone.

The ProSight Learning Manager—Your Key to Success

The ProSight Learning Manager not only focuses on teaching, but also encourages engagement and provides opportunities for growth. The ProSight Learning Manager gives financial services organizations the power to streamline training by allowing them to:

- Build and deliver tailored training programs.
- Assign highly targeted training plans.
- Track employee completion status.
- Track entire compliance programs electronically, including webinars and in-person training.
- Build more efficient and effective collaboration across your organization.

Enhance Your Training Programs with ProSight

ProSight Financial Association empowers financial services leaders to strengthen and advance our industry. Formed through the merger of ProSight and RMA—trusted organizations with rich histories and deep expertise in risk, fraud, compliance, and retail and commercial banking—we provide connections, training, insights, tools, and analytics to help you act with confidence.

Our work creates positive ripple effects throughout financial services organizations and the industry, generating new opportunities for growth and ultimately helping consumers, businesses, and communities thrive.

For more information on all the compliance and training solutions ProSight can provide your organization, contact us today!