



## How to 'Void' Check Fraud at Your Organization

Every year, organizations lose billions of dollars to fraud schemes and scam artists – for some that loss is as high as 5% of annual revenue, according to Association of Certified Fraud Examiners data.

Business checks topped the list of payment methods most frequently subjected to fraud attacks, with 74% of organizations reporting actual or attempted check fraud in a recent Association for Financial Professionals (AFP) survey.

### What is Check Fraud?

Experian defines check fraud as follows: Check fraud occurs when checks are stolen or reproduced in order to cash those checks from a business or personal bank account. Methods of check fraud include:

- Forgery – endorsing a check not payable to the endorser or signing a check without authorization
- Theft – stealing checks for fraudulent purposes
- Paper hanging – writing checks on closed accounts
- Check kiting – intentionally gaining access to funds deposited in one account before the bank collects them from another
- Washing – removing information from a check with chemicals
- Counterfeiting – using information from the victim's account on illegally printed checks; AFP reports that a skilled fraudster can create a check that looks completely legitimate in just 15 minutes.

### Who are the Victims?

Organizations and businesses large and small are targets of check fraud.

### \$49,000 Loss for Small Business in Wisconsin

In 2018, a fraudulent check cleared the checking account of a small business in Wisconsin. The payment discrepancy became apparent when their vendor alerted them of their past-due invoice. The serial check number and dollar amount matched a legitimate check they'd paid, however, while reviewing the check image they noted the payee on the check was altered to be payable to a person, not the vendor they'd paid. Everything except the payable information matched the original, so the fraud wasn't detected in their visual review of checks clearing their account.

### Thieves Steal D.C. Local's Checks

In 2019, IATSE Local 22 became a victim of check fraud when several checks were forged on the Local's account at a bank in Maryland. Thieves stole the mailed checks from a USPS mailbox in the D.C. metro. The checks were altered and two were cashed before Local 22 became aware of the fraud.

### How Can You Reduce Your Risk?

The Motley Fool shares some advice that can help limit check fraud risk:

### Always check ID when accepting a check

The first rule for accepting checks is to check the ID of the customer writing the check. In every case, the ID should always match the name on the check. If it doesn't, request an alternate payment method.

Continued on page 2...

## Improve audit controls and reconcile bank statements promptly

Timely review of bank statements can help catch fraud. Jennifer Sands, Vice President – Security Officer at Bank of Labor, advises customers to regularly review bank statements for any inaccuracies and, if you notice anything that looks out of place, report it to the bank immediately. Services like [Positive Pay](#) and [Account Reconciliation](#) also help spot-check fraud early.

Finding a case of check fraud four months after it occurs will make it much more difficult to track down the perpetrator and less likely that stolen funds will be reimbursed.



## Only accept checks from known customers

If you've always accepted checks from certain customers, the odds of them defrauding you are low. This might be the best way to continue accepting checks without increasing your risk of check fraud.

## Start using other bill-paying methods

Start looking at other methods to pay your bills. [ACH](#) or [Direct Deposit](#) for bill payment, can help eliminate the need to write as many business checks. It also reduces the threat of stolen or misused checks.

## Examine the check closely

When accepting a check, be sure to look at it closely. Does the coloring -- or the numbers -- seem off? If a check looks suspicious, examine the routing number to see if it's legitimate. Verify the check with the bank that the check is written from.

## Keep your checks locked up

Many check scams occur because checks are stolen and used fraudulently. With computer technology, they can also be easily reproduced and used by thieves.

## The Difference a Few Easy Changes Can Make

Bill Dean, a Trustee with International Ironworkers (IMPACT), noted that they have been using Bank of Labor's Positive Pay system since opening their accounts.

"The Positive Pay platform is built into the bank's website portal so it's easy to use," explained Dean. "We process around 500 checks a month and the system plays a key role in making sure that only legitimate checks are credited against our account."

Dean reported that, in just the past month, Positive Pay flagged and rejected three attempts that were made to deposit fraudulent checks against IMPACT's account.

**"Without the system," said Dean, "IMPACT would have been out the \$10,000 and left to pursue other costly remedies.**

And remember the earlier reference to check fraud experienced by IATSE Local 22? After that incident, Local 22 moved their accounts to Bank of Labor and signed on for Positive Pay.

"We process around 100 checks a month and the system plays a key role in making sure that only legitimate checks are credited against our account," explained the Local's Secretary/Treasurer, John Page.

Bank of Labor's Positive Pay system sends alerts for every check written and allows the organization to easily control authorization.

"Since implementing this software we have not had any fraudulent attempts against our account," said Page.

For more ideas on steps your organization can take to avoid check fraud and other business scams, call Bank of Labor's Treasury Team at 855.24.LABOR, visit the Better Business Bureau (BBB) Scam Tracker <https://www.bbb.org/scamtracker> and sign up for the BBB's Scam Alert Notifications: <https://signup.e2ma.net/signup/1900156/1902645/>.