

# A guide to payments fraud solutions



# Mitigating payments fraud risk

## A critical treasury duty

The fraud landscape is both alarming and evolving. The fraudsters targeting your organization are no longer just individuals operating alone. Increasingly, the bad actors are part of sophisticated and often global criminal organizations armed with extensive human resources, the latest technology and plenty of creativity. There's an entire profit-driven industry out there built to defraud companies.

The foe is formidable and the risk is significant: A single large-dollar attack could cripple an enterprise, as companies very often bear liability for payments fraud-related losses.

80% of organizations reported being victims of payments fraud attacks, and nearly 40% of victims said they recouped less than 10% of funds stolen.

— 2024 AFP PAYMENTS FRAUD AND CONTROL SURVEY

At U.S. Bank we understand that fraud risk mitigation is a critical responsibility of our treasury clients. And since our mission is ensuring your success, we've made partnering with you in the fight against payments fraud a major priority.

Inside this guide, we describe specific fraud threats across both paper and electronic payment methods, report on U.S. Bank solutions, suggest best practices, and direct you to more information on fraud scams and prevention strategies.





## Check fraud: A continuing threat

With new cyber scams emerging daily, check fraud can sometimes fall outside the limelight. But it remains a major threat.

In fact, according to the 2024 AFP Payments Fraud and Control Survey Report, 65% of respondents reported their organizations faced check fraud activity.

A major trend impacting check fraud volume: The U.S. Treasury Department has reported a surge in mail theft-related check fraud. Criminals are targeting U.S. Postal Service blue collection

boxes and often steal business checks from boxes in commercial buildings. The fraudsters may alter or “wash” the stolen checks, replacing the payee information with their own or fraudulent identities linked to accounts they control. They often increase the dollar amounts on the checks by hundreds or thousands of dollars before cashing or depositing them.

Washed checks may also be copied, printed and sold to third-party fraudsters on the dark web, generating even more fraudulent transactions.

Once a fraudster steals your check MICR line information, by whatever means, it’s also easy for them to issue authentic-looking counterfeits to any payee name they choose, in any desired amount.

Checks are  
the payment  
method most  
vulnerable  
to fraud, a  
trend that  
has remained  
consistent  
for years.

— 2024 AFP PAYMENTS FRAUD AND  
CONTROL SURVEY

# Detering check fraud

At U.S. Bank, we offer a comprehensive set of positive pay solutions designed to allow you to identify and reject potentially fraudulent, altered or counterfeit items – including the most effective form of protection, **Payee Positive Pay**.

With both Payee Positive Pay and our standard Positive Pay services, each day your business transmits a file to the bank that includes information on each issued item such as the account number, check number and amount. The bank compares that information to the checks presented for payment and reports those that don't match, allowing you to reject exception items.

With Payee Positive Pay, you also include payee information in the issuance file to thwart the many fraudsters who alter payee names or include unauthorized payees on counterfeits.

As part of these services, we also identify potentially fraudulent items presented at our branches by comparing them in real time with check-issuance information.

In addition, our SinglePoint® Image Access and SinglePoint Image File Delivery services allow you to view check images online. This eliminates the need to secure canceled checks at your location. Similarly, you can avoid storing check stock on premises by outsourcing check printing using our Check Payables service.

Best protection	Effective	Basic protection	Other options
Payee Positive Pay	Positive Pay	Reverse Positive Pay	Check Filter
<ul style="list-style-type: none"><li>• Checks presented are matched to items issued using basic check information <b>and</b> payee names.</li><li>• Exceptions are reported to you.</li></ul>	<ul style="list-style-type: none"><li>• Checks presented are matched to items issued using basic check information.</li><li>• Exceptions are reported to you.</li></ul>	<ul style="list-style-type: none"><li>• Checks presented for payment are sent to you to match against your issue file.</li></ul>	<ul style="list-style-type: none"><li>• Prevents check transactions over a certain designated dollar amount from posting to your account.</li></ul>

# Electronic payments fraud: An increasing threat

**Vendor email compromise**, a form of business email compromise (BEC), is one of the most prevalent forms of fraud impacting electronic payments these days. Fraudsters impersonate a legitimate vendor and contact your business – often through email – and request that account payment information be changed. If you comply, you end up sending invoice payments via wire transfer, ACH or one of the newer instant payments channels to the fraudster’s account instead of to your vendor.

Another increasingly common fraud is **website/URL spoofing**. The fraudsters purchase sponsored sites online that are designed to lure authorized users to click on a link to a false online banking platform login page and then key in their online banking credentials. Using the captured credentials, the criminals can initiate electronic transactions on your accounts.

Many companies are also being victimized by **bank impersonation scams**. For instance, a caller purporting to be from your bank will use social engineering to convince someone in treasury that your company’s account is under attack and

they must transfer funds to a safekeeping account controlled by the fraudsters. In another impersonation scheme, the caller tries to convince the treasury employee to download a call forwarding app to their phone; then, when the bank sees fraudulent activity and tries to notify you, the call goes to the fraudsters.



# A host of electronic payment fraud solutions

As payments increasingly go digital, and with many being instant and irrevocable, it's more important than ever that you protect your transactions and accounts. Here are some key objectives and U.S. Bank tools that can help:

1

## Confirm the payment is going to the desired payee.

- » **Account Validation** tells you if the account you are being asked to send a payment to is open and owned by the intended payee. The service scores the proposed transaction and can raise a red flag to suggest the need for investigation. It's ideal for combatting schemes like vendor email compromise where fraudsters attempt to fool you into misdirecting payments to them.

2

## Ensure the payment is authorized.

- » **ACH Blocks and Filters** allow you to authorize specific ACH debits and/or credits or prevent all ACH transactions from posting to your account.
- » Using **SinglePoint ACH Positive Pay**, you can go online to review any incoming ACH debits that don't exactly match those you have authorized, and then choose whether to allow payment.
- » **eCheck Block** enables you to prevent potentially unauthorized transactions from posting to business checking and money market accounts.

3




## Protect proprietary banking information.






- » A **Universal Payment Identification Code (UPIC)** is a unique remittance number that allows you to receive ACH credit payments without revealing sensitive bank information.
- » **Payee Token+** enables you to tokenize sensitive payee data for a variety of electronic payment types, such as Zelle®, ACH, real-time payments, wires, checks and credit card information. There is an optional add of account validation to confirm account details prior to returning a payee token to ensure you are sending payment to the correct account.




# Best practices for thwarting electronic payment fraud

While bank solutions are an essential element of your defense, the greatest power to prevent fraud resides with your company and its employees. The best way to stop the scams described in this guide is to adhere to basic best practices:

-  **Regularly review information reporting** through your online banking platform to spot questionable transactions on a timely basis.
-  **Leverage electronic fraud prevention services and automation** as much as possible to efficiently flag suspicious transactions.
-  **Establish procedures and controls** for processing money movement change requests and follow them diligently. This is critical in fending off business email compromise attacks.

-  **Confirm the validity of requests** to change payment instructions using independent verification. Don't verify using a phone number in the email. Instead, use a different, trusted phone number or seek out the emailer for in-person verification.
-  **Employ dual authorization.** This requires one authorized person to access online banking and initiate a payment, and a second to log in to review and approve it.
-  **Never access a banking platform through a search engine.** Always use a trusted link (or a bookmark saved from a trusted link).
-  **Make sure employees know U.S. Bank will never ask them to provide credentials,** redirect a payment to a different account, or ask them to download a call-forwarding app onto their phone.
-  **Take advantage of alerts and notifications.** Customized alerts make you aware of payment events, such as a wire over a certain amount being initiated.

 [View our Fraud Prevention Checklist](#), an extensive list of best practices to help you maintain a strong fraud prevention program.



# Stay vigilant

Too often businesses fail to implement best practices and employ bank solutions until they’ve experienced a fraud loss. So, ask yourself: Are you doing everything you can at your organization to control payments, protect accounts and minimize fraud? Are you prepared for the inevitable attacks?

To ensure you are, we suggest two key steps: Continue to educate yourself and your staff on the current threat landscape, and partner with U.S. Bank to learn what combination of fraud risk-mitigation solutions makes the most sense for your treasury operation.



## Experienced a fraud attack?

Report it immediately to U.S. Bank Commercial Customer Service at 866-856-9063. For business banking, contact the Business Service Center at 800-872-2657. The faster you report the crime, the greater the odds of recovery.



# Want to learn more online?

- » [U.S. Bank Payments Fraud Protection page](#)
- » [2024 AFP Payments Fraud & Control Survey results](#)
- » [FBI’s Internet Crime Complaint Center.](#)  
Central hub for reporting cybercrime that offers education on the latest cyber threats.
- » [Financial Crimes Enforcement Network alert on nationwide surge in mail theft-related check fraud schemes – Feb. 27, 2023 \(PDF\)](#)
- » [Nacha](#)