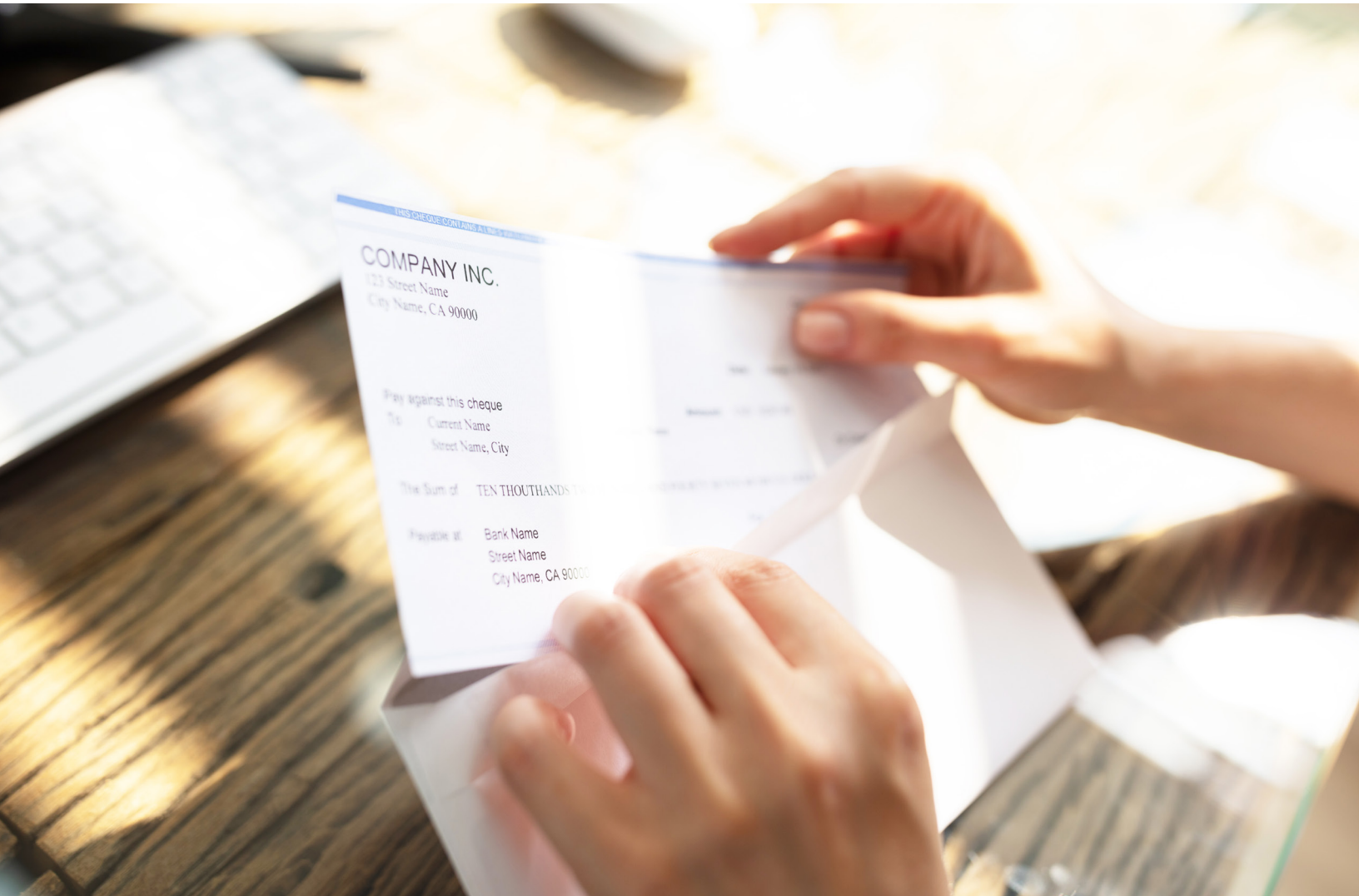
J.P.Morgan | CHASE

FRAUD + CYBERSECURITY

Your guide to protecting your company from check fraud



Introduction

Check fraud is a risk that companies must keep in mind, even as cybercrime increases. A 2023 survey from the Association for Financial Professionals (AFP) found that **63% of respondents reported being impacted by check fraud**. Overall, physical checks were the payment type most susceptible to fraud.

Knowing these risks, JPMorgan Chase makes a number of account fraud protections available to our clients. While there can never be a guarantee that you will not experience any fraud, it's ultimately up to your organization to take advantage of the fraud protection products and services we offer that can help protect your business.

That's why we've prepared this check fraud guide. It outlines the types of check fraud and how schemes unfold—and offers best practices and account protection information to help you identify and defend against check fraud.

We are here to help. Contact your relationship team for more information on check fraud protection products.

Sue Dean

Head of Solutions
Commercial Banking

Alec Grant

Head of Client Fraud Prevention
Commercial Banking

CONTENTS

Introduction
What is check fraud?
What you need to know
Altered checks
Counterfeit checks
Forged, missing or improper endorsement
Mobile deposit fraud
What to do if you experience check fraud
Next steps

What is check fraud?

Check fraud can sometimes fly under the radar, especially given all the attention paid to cybercrime and electronic payments fraud. However, checks are still widely used by organizations and companies of all types—making them a big target for fraudsters.

Check fraud occurs when a criminal manipulates a paper or digital deposit to defraud a legitimate payer. There are three main types of check fraud: front-of-check fraud and back-of-check fraud and mobile deposit fraud. Front-of-check fraud includes counterfeit checks and altered checks; back-of-check fraud includes forged, missing, or improper endorsement of checks.

This type of fraud can be challenging to combat given how easily it can be committed. One intercepted check provides a fraudster with your checking and routing numbers—all they would need to create counterfeits. That's why it's vitally important that you implement the right controls and account protections to have comprehensive defenses against check fraud.

JPMorgan Chase's role in combating check fraud:
We make every effort to protect you against fraud, including proactive screening of transactions and verification of potentially suspicious activity. However, you are ultimately responsible for movement of funds. Account terms and conditions clearly lay out the scope of responsibility for the bank, its clients and third parties. It is important to read these account terms carefully and fully understand your responsibility as a client to prevent fraud losses.

CONTENTS

Introduction

What is check fraud?

What you need to know

Altered checks

Counterfeit checks

Forged, missing or improper endorsement

Mobile deposit fraud

What to do if you experience check fraud

Next steps

WHAT IS CHECK FRAUD?

What you need to know

1. There are strict reporting windows related to check fraud. If fraud is reported to the bank outside of the reporting windows, claims are subject to denial. The general reporting timelines are:
   - **Front-of-check fraud:** 60 days from the date an item clears on your statement.
   - **Back-of-check fraud:** 6 months from the date an item clears on your statement.
   - Please see your account terms for specific timelines.
2. Recovery of funds lost to fraud **cannot be guaranteed**. It is important to remember that during the research of the claim, you as the client (and the intended payee) will be at a loss for the amount for the duration of the research, regardless of the outcome. Recovery time frames vary: 90 – 120 business days is typical, but this process can take much longer.
3. Simply adding a fraud protection product to an account does not mean you are protected. The product must be used in the way it was designed for maximum effectiveness. Not using the products correctly means you could still be liable for fraud losses (this is explained more fully in your account terms.)
   For accounts using Positive Pay products, you should carefully review all exceptions for payment and validate with the vendor or third party before paying, if needed. Also, the default decision for payments presented should be "return"—not "pay"—to further protect against fraud.

We offer multiple product options designed to protect clients against various forms of check fraud, including:

- **Post No Checks:** Automatically returns any check presented for payment on the account. This is a no-cost account feature that all clients are encouraged to use as a default.
- **Check Positive Pay and Reverse Positive Pay:** Enables you to validate items presented for payment.
- **Check Positive Pay with Payee Name Validation:** 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.

There are also multiple best practices we recommend, including:

- **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.
- **Use of appropriate check fraud protection products** for all your accounts, including Post No Checks as a default setting.

CONTENTS

Introduction

What is check fraud?

What you need to know

Altered checks

Counterfeit checks

Forged, missing or improper endorsement

Mobile deposit fraud

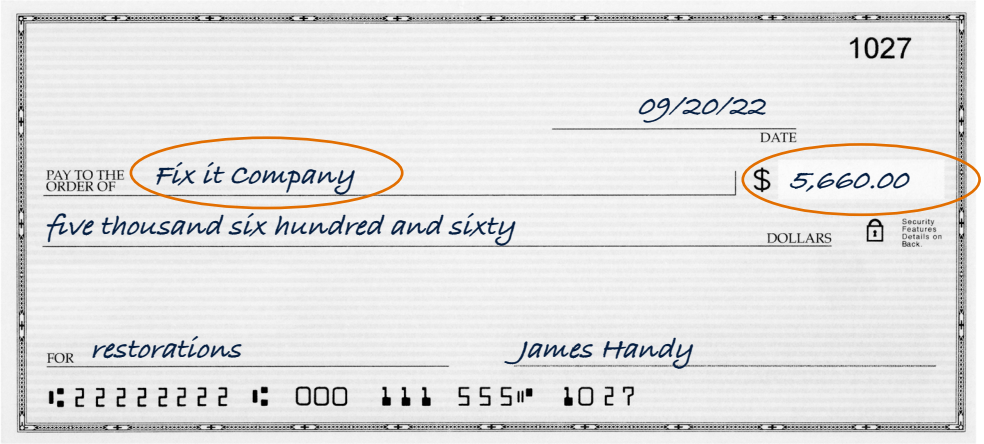
What to do if you experience check fraud

Next steps

FRONT-OF-CHECK FRAUD

Altered checks

In this scheme, the criminal will alter the name or the payment amount before depositing a check. Businesses can use Positive Pay with Payee Name Validation to confirm that a check's details match against the business's records.



To protect against altered check fraud, it is critical that you activate the Positive Pay features and use the product properly—i.e., reviewing all "exception" items closely before making a decision to pay and keeping account defaults set to "return" for exceptions. If these guidelines aren't followed, you may be liable for altered-item losses.

However, while Positive Pay is recommended for accounts, it alone may not necessarily detect all fraudulent changes.

For example, you need to make a payment to a trusted third-party vendor. However, a fraudster may be able to intercept a check payable to this vendor, and then open an account and add "LLC" to the intercepted check. Without careful review of the original item and correct use of Positive Pay with Payee Name Validation, this type of alteration could easily slip through the cracks.

Let's look at another example where a client was accustomed to making high-value payments via paper check and mailed a check for over $1 million to a vendor. At the time, the account did not have Positive Pay with Payee Name Validation active. After a few weeks, the vendor reached out to the client, saying that they had not received the check payment. It turned out that the check had been intercepted by a fraudster while in transit. The fraudster then altered the payee name and negotiated the check successfully at another bank.

CONTENTS

Introduction

What is check fraud?

What you need to know

Altered checks

Counterfeit checks

Forged, missing or improper endorsement

Mobile deposit fraud

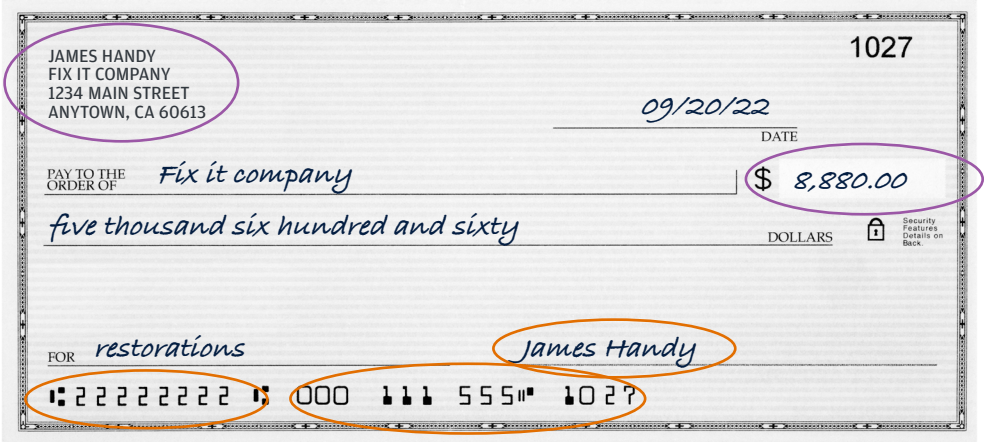
What to do if you experience check fraud

Next steps

FRONT-OF-CHECK FRAUD

Counterfeit checks

> Once a criminal obtains your checking account and routing numbers—as well as the name and signature style of the authorized signer—they may use printers and desktop publishing software to create counterfeit checks. Positive Pay and Reverse Positive Pay are fraud protection services that can help you identify and prevent payment of counterfeits.



To protect against this risk, we recommend all clients activate Post No Checks as a default setting. If your account will issue checks, Account Reconciliation and Check Positive Pay with Payee Name Validation are the recommended products to protect against both counterfeit and altered check fraud.

Let's consider an example of counterfeit checks and how account tools are meant to catch fraud. In this case, a fraudster 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 Post No Checks set as a default setting, 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.

CONTENTS

Introduction

What is check fraud?

What you need to know

Altered checks

Counterfeit checks

Forged, missing or improper endorsement

Mobile deposit fraud

What to do if you experience check fraud

Next steps

BACK-OF-CHECK FRAUD

Forged, missing or improper endorsement

In most cases of forged, missing or improper endorsement, a criminal forges the endorsement on the back of a check and deposits it at a financial institution. In other cases, they may choose to not endorse it at all, or perhaps one party improperly endorses a check that was payable to two parties.

There are no available fraud protection products to protect against this type of fraud. While it's true that the bank that accepts the deposit is usually liable, funds recovery is not guaranteed and can often take up to 120 business days, or more.

Claims of forged or missing endorsements are time-sensitive and subject to dollar limits set in the your account terms. If a vendor calls to say they haven't received payment, but you know the check was mailed, it's important to investigate the status of the check promptly.

To mitigate against this type of fraud, it's recommended to avoid multiple payees checks whenever possible. A good rule of thumb is one payee per check. Other best practices include implementing payment thresholds above which electronic payment methods are required and proactively confirming with intended recipients of high-value checks that the items were received. Always send high-dollar checks via trackable shipping methods, as opposed to regular mail.

CONTENTS

Introduction

What is check fraud?

What you need to know

Altered checks

Counterfeit checks

Forged, missing or improper endorsement

Mobile deposit fraud

What to do if you experience check fraud

Next steps

Mobile deposit fraud

> The convenience of mobile check deposit has benefits, but it's also enabled a rapid expansion of a new form of check fraud. What makes it notable is that mobile check fraud is usually perpetrated by the intended recipient. Often, it's used by employees who attempt to double-cash paychecks after being terminated from a company.

It unfolds like this:

A business issues a check to an individual, who remotely images the front and back of the check using their smartphone camera. After the deposit is made into the account, the recipient takes the same physical check to another bank or check-cashing store and receives payment (essentially receiving funds twice by drafting the same account for the same check, using two different methods). When the paper check is presented for payment to the originating bank a few days later, the check is flagged and dishonored as a duplicate. The dishonored check gets returned, and it could begin a time-consuming and expensive claims process to determine who is liable for the funds. The claims could bounce between the banks involved, the company that wrote the check or the intended payee. This type of fraud can primarily be avoided by making electronic payments directly to payees.

The reason that the paper check is dishonored in mobile check fraud is because most clients who have been subjected to this type of fraud have Positive Pay active on their accounts. The check presents as an exception, showing 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).

Mobile fraud occurs over a series of steps:

1. An individual receives a check from a client.
2. The individual completes a mobile deposit.
3. The same individual goes to a check-cashing facility and cashes the paper check.
4. The check-cashing facility presents the check to JPMorgan Chase for payment.
5. The payment is flagged and the check returned as a duplicate.
6. A demand letter is sent from the check-cashing facility to the client. In turn, the client files a claim with the JPMorgan Chase.
7. If JPMorgan Chase 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.

CONTENTS

Introduction

What is check fraud?

What you need to know

Altered checks

Counterfeit checks

Forged, missing or improper endorsement

Mobile deposit fraud

What to do if you experience check fraud

Next steps

What to do if you experience check fraud

> Time is of the essence when addressing instances of check fraud. One of the most effective steps you can take to prevent further fraud is to eliminate check use and transition to electronic payment methods.

If that's not possible, consider following these steps to protect your organization:

1. Apply Post No Checks to non-check-writing accounts
2. Use PVE on all check writing accounts
3. Apply ACH debit block to all accounts that should not receive ACH debits
4. Apply ACH debit filtering to all accounts that accept ACH debits and ensure there is a reconciliation process to identify unauthorized transactions with ample time to report to bank within 24 hours of posting (for example, a phone account may be an ID through which fraud can occur)

If checks are absolutely required, you must recognize there is an inherent risk that may not be able to be completely mitigated:

- Forged/missing endorsement—required to go through claims process to recover funds from bank of first deposit. If claim is not denied it can take 120 business days or more for funds to return.
- Mitigants—limit checks to low volume, low dollar values; send via courier service as opposed to USPS mail; confirm receipt with recipient.
- Holder in due course—required to go through claims process to recover funds from mobile bank.

FOR MORE INFORMATION

Visit our Fraud Solutions webpage to learn more about profducts and solutions.

CONTENTS

Introduction

What is check fraud?

What you need to know

Altered checks

Counterfeit checks

Forged, missing or improper endorsement

Mobile deposit fraud

What to do if you experience check fraud

Next steps

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. Double check any accounts that don't issue checks and ensure Post No Checks is an active feature on those accounts.

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.

WE ARE HERE TO HELP

Contact your relationship team to learn more about available fraud protection products for your accounts and other best practices.

CONTENTS

Introduction

What is check fraud?

What you need to know

Altered checks

Counterfeit checks

Forged, missing or improper endorsement

Mobile deposit fraud

What to do if you experience check fraud

Next steps

J.P.Morgan | CHASE