

CHECK FRAUD



A Guide to
Minimizing Your Risk

JPMorgan Chase Treasury Services
jpmorganchase.com/ts

© 2005 JPMorgan Chase & Co. All rights reserved.
JPMorgan Chase Bank, N.A. Member FDIC 05/2005

JPMorganChase 

Check fraud is one of the greatest challenges facing businesses and financial institutions today. Technology has made it increasingly easier for criminals to create counterfeit checks, as well as fictitious identification documents that can be used to commit fraud. It has been estimated that check fraud costs our country \$20 billion per year. Either directly or indirectly, everyone involved with the check writing or clearing process is at risk of being a victim of check fraud.

Check Fraud Schemes

Check fraud schemes take various forms. Each type of fraud may require different prevention, detection and loss recovery approaches. Here are some of the more common forms of check fraud along with suggestions on how to help protect yourself against this costly crime.

Forged Signatures/Forged Endorsements – Forged signatures usually involve the use of legitimate blank checks with an imitation of the payor's signature on the signature line. This signature is often forged by a person known to the valid payor. Sometimes, signatures are forged on blank checks that have been stolen. This can happen during transit from the check printer to the account holder.

Forged endorsements are usually the result of valid, stolen checks that are endorsed and cashed or deposited by someone other than the named payee. Individuals who have access to the checks, and to corporate accounting records, are often the perpetrators of corporate forged endorsements.

Closed Account Fraud – Closed account fraud takes place when checks are written against closed accounts. This type of fraud relies on the clearing time involved in transactions between financial institutions.

Altered Checks – Altered checks involve the use of legitimate checks that have been changed in some way.

Counterfeit Checks – Counterfeit checks are one of the fastest-growing sources of fraudulent checks. Counterfeiters are able to produce exact imitations of genuine checks using readily available desktop publishing software and sophisticated color copiers or printers. Almost any type of check can be counterfeited, including cashier's, payroll, government and traveler's checks.

A criminal begins with a valid check. Chemicals or other means are used to erase or change information such as the payee name or the amount of the check. New information is added by typewriter, handwriting or laser or check printer.

Check Kiting – Check kiting occurs when a check drawn on one bank is deposited in a second bank without having proper funds to cover the check. When the deposit is made, the second bank grants the depositor conditional credit and allows the customer to draw checks against uncollected funds. The customer then writes a check on the second bank and deposits it in the first bank to cover the original check. Unless detected, this process can continue indefinitely.

Other Schemes Include the Fraudulent Use of:

- Checks written against accounts used primarily for deposits, ACH or wire activity
- Third-party bill paying services
- Demand drafts
- Telemarketing
- Deposits through ATMs
- Company information, supplies, or systems by company insiders

Responsibility for Check Fraud

Many laws that govern checks allocate the risk of loss resulting from check fraud to the person in the best position to have prevented the fraud. This means that companies may need to take additional steps to protect themselves from check fraud losses.

Minimizing Your Exposure to Check Fraud with Positive Pay

Positive Pay is a tool for authorizing the payment or return of exception items, offering a safeguard against loss from fraudulent check activity.

Many laws that govern checks allocate the risk of loss resulting from check fraud to the person in the best position to have prevented the fraud. In situations where a loss from fraudulent activity could have been prevented if the company had elected to use Positive Pay, such loss may be allocated to the company.

What it does

By using Positive Pay, you have the ability to make pay or return decisions on checks presented to your disbursement account for payment. Therefore, you reduce your risk of fraud because you retain control over each exception item and choose to either authorize payment or return the check.

Teller protection

Any checks presented to a teller at one of our banking centers* will also be able to match against a Positive Pay file. If the check appears on the file, it will be honored. If the check is not on the file, the presenter will be directed to contact the issuer of the check. And the check will not be accepted.

How it Works

- 1 Each day you issue checks, you will provide JPMorgan Chase with a data file containing check amounts, serial numbers and payee names.
- 2 We match information from checks presented for payment against your check issue data. Any discrepancies are reported to you.
- 3 Each business day you will receive a report detailing your discrepant checks. You will instruct us to either pay or return the discrepant items.

Payee Name Verification option

Enhance your Positive Pay service with an important option that provides greater protection against check fraud. Payee Name Verification detects altered payee names by capturing the payee line information, comparing it to the information in the Positive Pay issue file you have provided and flags suspect items.

You will be notified of payee name exceptions and asked to make a pay or return decision. Exception items can be viewed using our Client Internet Access Services.

* Not available in all banking centers.

What You Can Do to Minimize Your Risk

The Federal Reserve Board advises companies to be educated about the importance of procedures and controls that can deter dishonest employees from committing internal fraud. Here are some specific actions companies can take to help control check fraud:

- Use a fraud prevention service like our Positive Pay service on all disbursement accounts.
- Store check stock in a secure and locked environment. Keys and locks should be changed periodically, and inventory should be checked regularly. Signature plates should also be controlled and stored separately from the check stock. Use dual control for access to check stock, signature plates, etc., and set up an audit process to review checks written.
- Use image survivable check stock security features.
- Use separate accounts for collection and disbursement activity.
- Use bank transaction reporting to distinguish between a disbursement check on your account and a returned collection item.
- Use a separate account for payroll and accounts payable disbursements.
- Segregate high-volume accounts from low-volume petty cash or emergency payments that have to be monitored manually.
- Convert as many payments as possible to electronic delivery such as ACH, EDI, or wire.
- Make large-dollar payments from a separate account, with daily information reporting capability.
- Separate check issuance and check reconciliation duties.
- Use online reporting and reconciliation services for faster reconciliation.
- Reconcile your accounts as soon as you receive your bank statement. Generally, fraudulent activity must be reported within 30 days. Once reconciled, have a member of management review and approve the statement to ensure integrity.

What to do if you experience fraud on your account

- Call your customer service representative, banking center, or bank representative IMMEDIATELY to place a warning on your account.
- We will send you a fraud package, which includes instructions, affidavits and an incident report.
- We will contact you within 10 days of the receipt of a complete fraud packet if follow-up is required.
- File a police report if you feel you have been a victim of a crime.

For more information

If you have questions regarding check fraud or the information in this brochure, please contact your JPMorgan Chase sales representative.

Take the steps necessary to reduce your risk of paying fraudulent checks.

