Combating Fraud on Corporate Checking Accounts

A Bank of America White Paper
One in a series of white papers prepared by Bank of America on key issues of interest to corporate treasurers.

The information contained in this publication is not legal advice. You may wish to consult your own legal advisor to discuss your company’s legal needs.
Understanding Fraud

According to the FBI, thieves steal more through check fraud than through bank robberies. Today, companies and financial institutions combined are losing billions of dollars annually to rising check and electronic transaction fraud occurrences. To successfully combat fraud, both parties must partner responsibly and act aggressively.

Since 1990, when revisions to Articles 3 and 4 of the Uniform Commercial Code were adopted in almost every state, subsequent case law has supported changes that assign responsibility and financial losses from check fraud to companies, or apportion losses between banks and companies, based upon comparable negligence. Thus, if or when companies fail to exercise “ordinary care,” which is the adherence to reasonable commercial standards prevailing in their region and industry, financial institutions may no longer be held wholly liable. Furthermore, for ACH entries, companies are required to identify and return fraudulent items on business-to-business electronic transactions within a very narrow time frame, generally within 24 hours. As a result of these regulatory changes, companies now own greater responsibility for losses sustained from check and electronic transaction fraud. Likewise, financial institutions must also exercise “ordinary care” in today’s high volume, highly automated environment of processing checks and share responsibility for establishing systems and controls to help prevent fraud on deposit accounts from occurring.

Contributing Factors to a Growing Problem

First, the bad news: there are a number of factors contributing to increased check and electronic transaction fraud. The good news, however, is that there are now a variety of methods available to help companies and financial institutions combat fraud. Let’s examine the primary factors contributing to the trend in increased check fraud.

Technology

Today, anyone intent on committing check fraud can easily do so through inexpensive software programs once they have obtained account information. When used with sophisticated scanning devices and laser printers, these programs facilitate reproduction of almost any document, including checks, as well as duplication of signatures. They also make it easy to add a company’s name and logo onto the fraudulent check.

Regulations

Another major factor contributing to the growth in check fraud is the requirement for banks to comply with the Expedited Funds Availability Act and Federal Regulation CC (Reg CC). This requirement has unintentionally assisted the growth of check fraud because it requires banks to make funds deposited into an account by check available sooner. As a result, the fraud perpetrator can receive funds before companies and
banks can identify the items as fraudulent. Positive Pay and Teller Positive Pay are fraud prevention services offered by banks to help companies identify fraudulent checks as quickly as possible. We will review both Positive Pay and Teller Positive Pay later, in more detail.

**Can fraud be eliminated with electronic payments?**

To streamline payment processes and to help prevent check fraud, more and more companies are using the ACH network to electronically complete their payment obligations. However, electronic transactions are not immune to fraud. The shift towards electronic payments invites another opportunity for fraud, particularly through online purchases. Once account information is obtained, fraud perpetrators need to only provide an account number to the online merchant for the purchase of goods and services. Given the ease of initiating a fraudulent transaction, companies should monitor account activity on a daily basis in order to return fraudulent items on business-to-business transactions within the very short timeframe, as mandated by NACHA, the National Automated Clearing House Association. If companies do not review account activity on a daily basis, these transactions could easily go undetected for days, weeks or even months.

**Preventing Check and Electronic Transaction Fraud**

There are a number of services offered by financial institutions that can help reduce exposure to and impacts from check and electronic transaction fraud. Additionally, banks must also establish procedures that help prevent fraud attempts. On the other hand, companies should also take advantage of the bank services designed to help prevent fraud as well as implement internal practices and procedures to further combat fraud. The following section outlines suggested services and procedures for preventing fraud. They are suggestions only and are not a guaranty against fraud loss and are not meant to substitute for internal procedures that are appropriate for your company.

**Bank services and company procedures**

**Check cashing procedures**

In today’s environment, it is critical for financial institutions to implement thorough check cashing procedures and invest in technology that will aid in the identification of fraud at the earliest opportunity in order to protect their customers and themselves. As a result, financial institutions are moving beyond the traditional requirement of proper personal identification. Procedures include isolating check cashing by non-account holders to the banking center lobbies, requiring companies to use Teller Positive Pay (described below) in conjunction with traditional Positive Pay and requiring thumb printing for non-bank customers when they present a check. The combination of Teller Positive Pay and thumb printing non-bank customers will help identify and deter potential fraud perpetrators as well as assist in the recovery of losses once a fraudulent check is cashed.
Positive Pay

A key fraud-fighting tool is the Positive Pay service for disbursement accounts. This service establishes a daily checks and balance process that provides an early warning system for check fraud:

- Positive Pay automatically compares companies’ electronic record of issued checks with the bank’s record of checks presented for payment
- Early each day, companies receive a report of non-matching items, also referred to as “exception items,” to review
- Companies are given a period of time to review exceptions and render a pay or return decision to the bank
- Items that are deemed to be fraudulent are returned to the bank of first deposit immediately

For Positive Pay service to be effective in detecting fraud, companies have the responsibility to:

- Send the bank their check file before the checks are distributed
- Authorize individual(s) within the company to submit a pay or return decision on exception items within the established time, usually within hours from the time the check is presented for payment
- Establish a dual control system that removes the person issuing the check from the process of making the pay or return decision

Positive Pay has evolved over recent years to offer various options: Image Positive Pay, Teller Positive Pay and Reverse Positive Pay. These options are detailed in Figure 1.1 and 1.2.

Emerging technologies allow banks to continuously expand Positive Pay functionality. Companies have the ability to electronically submit payee name information as part of their check issue file. Some banks can match this additional issue information to their Positive Pay system, identify non-matches and even present the payee name to their teller cashing the check. Also, some banks are using bar coding and digital seal technology that provides original document and non-alteration verification. Finally, banks and retailers are currently reviewing how a fraud database might be shared in order to provide further protection against losses. These capabilities will facilitate faster identification of fraudulent checks and capture of the perpetrator.

Figure 1.1

Positive Pay options:

- **Image Positive Pay** – View items before deciding to pay or return
- **Teller Positive Pay** – Stop fraud at the teller line before the money goes out the door
- **Reverse Positive Pay** – Notify banks of exception items
Image Positive Pay

Many banks now use image technology to provide companies with digitized images of paid checks for daily Positive Pay reporting.

- Image Positive Pay allows companies to review both the front and back of checks, as well as verify payee names, check stock and endorsements.
- With real-time access to these images, companies are able to make more informed decisions on whether to pay or return an item.

Teller Positive Pay

Some banks now offer a more enhanced Positive Pay service called Teller Positive Pay. With this service, bank tellers are better equipped to detect fraudulent checks before they are cashed because the teller systems are linked to check issue files the company sends to the bank.

- When a check is presented to the teller that is drawn on a company’s account at that bank, the teller system automatically compares the amount and serial number of the check to the corresponding company’s check issue file.
- If the data does not match, the teller is instructed not to cash the check; or, if there is a discrepancy noted, the teller receives a message with instructions to seek additional approval before cashing the check. This might include contacting an authorized person at the company to verify legitimacy of the check.

Reverse Positive Pay

The positive pay process can also be reversed by having the company maintain its own database of issued checks and compare lists of checks issued against checks paid on a same day basis. Reverse Positive Pay is typically used when sending an issue file to the bank prior to disbursing checks is not feasible. A practical example is an insurance company issuing claims checks on the spot for damage resulting from disastrous situations such as earthquakes, tornados and hurricanes. It works this way:

- After checks are presented, the bank prepares a file listing check serial numbers and amounts and sends that file to the company early in the morning.
- The company immediately compares the paid item check file with its internal records and informs the bank of any items identified as exceptions.
- The bank researches those checks that do not match and corrects any misreading or encoding errors.
- For checks that still do not match the issue file, the company instructs the bank to return these items immediately.
ACH Blocks and Filters

As previously noted, many companies are moving away from a completely paper-based disbursement process to an enhanced electronic process. In addition, increased use of ACH debits for corporate-to-corporate payments as well as proposed ACH legislation to allow corporate check conversion has sparked an increased awareness of the need for electronic fraud protection. To this end, the ACH Blocks and Filters service was developed to help companies protect their accounts against unauthorized ACH transactions.

The ACH Blocks and Filters service offers companies the ability to authorize incoming ACH transactions that post to their account. There are two levels of protection available with ACH Blocks and Filters to help companies meet their specific account needs:

- The first level allows companies to block all incoming ACH debit or credit transactions, or both.
- The second level allows blocking of all incoming ACH transactions except those items specifically defined by the company. The company instructs and authorizes the bank to pay specific transactions based on specific criteria they define.

Card Solutions

Card programs provide another alternative to paper disbursements. They help companies reduce check fraud by significantly reducing the number of checks issued for various payment applications. Most card programs offered by banks cover a variety of disbursement types including payroll, purchasing and travel and entertainment.

- **Corporate Cards** – A number of different corporate card types are available to companies seeking to better manage vendor payments associated with purchasing supplies, managing travel and entertainment expenses as well as fleet expenses. Companies define authorization parameters for how and where cards may be used as well as individual spending guidelines. Corporate cards are also covered by liability protection against card misuse.

- **Payroll Cards** – An alternative to traditional direct deposit and paper paychecks, payroll cards allow companies to offer a payroll method in electronic format to employees who do not have traditional banking accounts or who do not want their pay deposited into their regular checking or savings account.

- **Prepaid cards** – These cards are pre-funded by the company electronically and eliminate checks issued as a one-time or recurring payment to individuals. Common applications include expense management (relocation, petty cash, and infrequent traveler), rewards and recognition as well as customer care (insurance claims, loyalty programs and loan proceeds).

Corporate policies and practices

All companies, regardless of size, should consult with their legal and audit departments and other necessary advisors to establish and implement internal measures to address security concerns. Preventative measures begin with thorough verification of newly hired employees and training of all personnel involved with disbursing funds.
Training should include a comprehensive review of legal and regulatory guidelines for disbursing funds, as well as common methods used to defraud companies. Other recommended practices for preventing fraud include:

- Ensure audits are conducted on a regular basis.
- Reinforce that all levels of management take the audit results very seriously.
- Ensure security of all financial information. One common area of vulnerability for companies is the sharing of passwords or posting of passwords publicly with vendors, maintenance staff, visitors or equipment repair personnel. It is recommended that passwords or control words be changed on a regular basis to protect accounts and other confidential information.

**Internal check-writing responsibilities**

Additional policies and procedures should include a clear separation of responsibilities for signing checks and reconciling accounts. To this end, companies should consider assigning two different employees to manage these functions. Companies should also ensure that procedures are in place for manually processing any kind of check and that upper management approval is obtained. Statistics show that internal theft of checks and check reorder forms and fraudulent disbursements made to “miscellaneous” vendors and/or fictitious employees are all very common and a significant risk for companies.

**Check stock security measures**

The security of check stock and related materials is critical to a company’s success at fighting internal and external fraud. Therefore, access to check stock should be carefully managed and monitored, perhaps implementing a policy of random rotation of assignments for these functions. In addition, companies should conduct regular inventory reviews of check stock and have their auditors assess the results, including the physical security of the items. Security experts also advise that blank check stock and signature plates should be stored in separate and secure locations.

In addition to careful management of inventory, there are a variety of security tools specific to check stock and related materials available to companies. For example, companies may decide to:

- Include a distinctive watermark or other special feature that makes reproduction of checks more difficult.
- Opt for checks that carry a “pantograph” or patented design in the background of the check. When these checks are photocopied, the unique design changes to read “VOID” on the check, which diminishes the opportunity to cash fraudulent checks.
- Treat check stock with chemicals that are not detectable to potential fraud perpetrators. These inks react with eradication chemicals, causing the word “VOID” to appear on the check and making it more difficult for forgers to modify amounts or payee names.
• Utilize high-resolution micro printing for the signature line of a check and the border. While the border may appear to be part of the design, when magnified, it actually contains a series of words that thread together or become wholly illegible if the check is photocopied or scanned.

• Include three-dimensional reflective “holostripes” on checks. These metallic strips contain one or more holograms (like credit cards) that are printed on checks. They are difficult to forge, scan or reproduce because they are based on a laser etching process.

As noted above, companies need to carefully review their policies and procedures to identify what measures need to be implemented to ensure the safety and security of their check stock. As decisions are made, it is important to note that treatments need to be easily identifiable for bank tellers and check cashing companies. Given the importance of these security measures for fighting fraud, this may be one instance where the lowest price may not be the most cost-effective decision in the long-term. Furthermore, the best solution to prevent fraud and gain economies of scale may be to outsource the physical production of your checks to a bank or other value-added vendor.

Next Steps

A comprehensive review of current policies should be conducted. The following Check and Electronic Transaction Fraud Checklist is a useful tool that will help you begin such a review; however, it needs to be further defined depending on your company, industry or operating environment. Bank of America welcomes the opportunity to work with you, your auditors or security specialists to help create an environment that protects all of us against check and electronic transaction fraud.

For More Information

It is important that banks and treasury managers continue to discuss key issues that face us today. We welcome any comments or questions you may have about check and electronic fraud. Please call your Bank of America representative, or access our Web site at corp.bankofamerica.com.
Check and Electronic Transaction Fraud Checklist

To help safeguard your business against fraud, you need to develop strong internal safeguards and controls. Here is a brief summary of specific steps you may want to consider taking:

- Reconcile accounts timely.
- Convert as many payments as possible to an electronic format.
- Implement ACH Blocks and Filters to protect all your disbursement accounts.
  - If you elect to have your account debited by another entity, consider separating your accounts, using one account to receive electronic transactions and a separate account for check writing.
  - Segregate account functionality to make it easier for you to monitor specific electronic or paper account activity. Use one account for electronic transactions, which can be monitored daily and protected with ACH Blocks and Filters. Use another paper transaction account that is protected with Positive Pay and ACH Blocks and Filters.
- Use Positive Pay and Teller Positive Pay service on all paper-only disbursement accounts. Failure to use these services may be considered lack of “ordinary care.” Be sure to review and respond to Positive Pay exception items by the deadline daily.
- Make frequent, unannounced audits of your check stock and electronic payment system.
- Incorporate check writing policies designed to prevent internal and external fraud, including but not limited to:
  - Centralize the check-writing function and limit access to check stock and signature plates.
  - Use check stock with fraud prevention security features.
  - Maintain a log of access to check stock and signature plates.
  - Keep blank check stock and facsimile signature plates under lock and key, in separate locations and under dual control.
  - Limit the number of signatures, and immediately notify your bank of changes in signing authorization. Be sure to update signature card and resolution as soon as possible.
  - Separate the check writing and account reconcilement functions.
- Set up a separate account for large dollar payments and a separate account for manual check issuance with a maximum dollar limit.
- Consider a comprehensive disbursement outsourcing service.
- Report any fraudulent or unauthorized transactions immediately.

These steps are suggestions only and are not meant to substitute for internal procedures that are appropriate for your company.