TreasuryPulse
delivering excellence
A Passion to Perform.
Deutsche Bank

Summer 2008

Protecting Your Company from Payments Fraud

Advances on the Internet as well as in computer and photocopier technology continue to make fraud a major concern. New and different threats to the security of bank and corporate assets emerge every day. Below are answers to frequently asked questions about payments fraud that include a number of prevention tips.

What are some current payments fraud trends?
Global changes have contributed to the growth and complexity of financial fraud worldwide. The globalization of commerce along with the rise of the Internet and worldwide communication created new opportunities to perpetrate fraudulent activities. More victims can be reached and the perpetrators are able to operate with anonymity.

Much of today's transactional fraud is initiated via the Internet. Some of the most common types of Internet fraud schemes involve "social engineering," fraudulent faxed authorizations and active fee scams such as lottery and inheritance fraud.

Social engineering fraud is a collection of techniques used to manipulate people into performing actions or divulging confidential information. Some of the techniques used are pretexting — pretending to offer a business or job opportunity — phishing and malware.

What are some steps companies can take to prevent payments fraud?
Organized criminal elements familiar with the banking systems and corporations target weaknesses and look for opportunities to commit fraud. Anti-counterfeiting technology, employee/customer education and heightened awareness, and anti-fraud measures such as positive pay and transaction monitoring are key practices in preventing fraud.

Certain regulations may help to prevent fraud. Know Your Customer and new account opening rules provide banks with the opportunity to gain more information about their clients.

To prevent fraud you need to have good internal controls in place. Additionally, it is important to know your employees. Companies need to educate and train employees on fraud prevention, review hiring and mailroom procedures and monitor new accounts.

What are some of the operational risks and countermeasures?
To counteract employee fraud, enforce a "four-eyes" processing requirement. Deutsche Bank's systems call for every transaction to be created, repaired and approved by two different operators. We follow a "high-risk media" policy and procedure for instructions received by phone, fax and paper, including verification of the authorized sender's signature,

callbacks to the sending party and use of recorded phone lines. Audit trails provide the history of all actions taken on a transaction and identify an operator for each action.

Companies face the risk of fraudulent messages being received as well as intentional misrouting or cancellation of electronic messages that await manual intervention. As a result, strict application security administration is required for all messaging applications. Audit trails, advanced protocols to guarantee electronic message delivery and facilitate reconcilement, as well as encryption of sensitive file transfers are effective countermeasures. Companies can benefit from adopting industry and bank-specific services and products that ensure secure and encrypted means of communication.

Whenever physical media is involved, the challenges to prevent fraud multiply. Checks are handled and transported multiple times. A tight control on check stock inventory is a necessity and check stock should have built-in security features (MICR, watermarks, micro-line text, etc). Since these security features may be "lost" during conversion of a paper check to a substitute check or check image, insist on positive pay with payee recognition. For wires, limit use of manual instruction media to emergencies and make sure you have tight internal procedures in place for authorizing and reconciling their use.

Which innocent party is responsible if fraud does occur?
Under the Uniform Commercial Code (UCC), the general principle is that the burden of loss is on the innocent party best able to prevent it. Allocation of risk is impacted by clearinghouse rules and/or contract. When checks are altered or contain forged endorsements, UCC shifts losses up the collection stream to the presenting and depositary bank. But the payor bank remains liable for the counterfeit check or one containing the forged drawer's signature.

With a remotely created check, the loss created by the unauthorized check rests with the depositary bank. For the exchange of check images — which is not yet addressed in the UCC — liability generally will rest with the first party that converts the paper check to an electronic image. In all these cases, a bank's client may be stuck with the loss if its negligence substantially contributed to the fraud, its employee committed the fraud or the customer was induced to issue the check by an imposter.

Any other best practices in payments fraud prevention?
Keep in mind the value of information to the fraudster. Be suspicious of unsolicited phone calls or e-mails requesting internal information, and always verify the caller's identity and company affiliation. If you believe the contact may be illegitimate, contact the financial institution yourself. From a personal perspective, always ensure that your home-based computers have the most up-to-date security software.

Also, make sure you have detailed procedures for requesting user accounts and assigning entitlements. It is critical to monitor failed log-in attempts, followed by notifications to the affected users and their respective managers. Proactive reconcilement of user accounts and entitlements to the global directory is key, including removal of accounts for employees who have left the company.

And understand the liability for fraud. New technologies such as positive pay mean new rules. Banks and customers have agreed by contract to vary liability rules to reflect these new technologies and all parties should be aware of their responsibilities and be proactive in preventing fraud.