

Stop, Thief!

Best Practices in Fighting Payment Fraud

BY CHERYL GURZ,

North American Payments Market Manager,
Global Transaction Services, Citi

Payment fraud is now a multi-billion-dollar industry. Here's how to protect your organization's bottom line.

It's as old as commerce. For as long as currency has been exchanged for goods and services, there has been fraud. And in recent years, as the number of payment methods has expanded, the incidence of fakery has, predictably, kept pace.

By far the most prevalent is check fraud, which costs American businesses up to \$14 billion annually, with those volumes growing at a rate of up to 3% per year.¹ In a recent AFP survey, 73% of respondents said they were victimized by attempted or actual payment fraud in 2009, with 90% of those incidents in the form of check fraud.²

That unnerving set of statistics is a key driver of a major corporate trend: a migration from checks to electronic payments. Today, the use of check payments for B2B products and services in the U.S. is in decline. In 2007, nearly three-quarters of all B2B payments were made via check; by 2010, that figure had dropped to 57%.³

Of course, as fast as any new technology emerges, there are criminals who will devise nefarious workarounds to abuse and illegally profit from that technology. And electronic payment is no different. While it has eliminated many of the vulnerabilities of checks, electronic payment has its own holes that have been discovered, and exploited.

Types of payment fraud

To assess the risks of, and combat, payment fraud in an organization, one must first have a cursory understanding of its many facets. Here is a rundown of the predominant types of payment fraud, of both the check and electronic variety:

Check Fraud. The most common forms of check fraud include:

- *Altered checks.* This includes checks that had already been issued and received, by the payee or a third party, then subsequently altered. One of the most popular alteration methods is "check washing." Data is deleted from a check field and replaced with false information – usually the dollar amount and the name of the payee.
- *Forgeries.* This includes found or stolen checks that have their endorsements forged. In many cases, the thief/forger is a friend or family member of the payer. Forged endorsements (unauthorized use of the payee's signature on the check signature line) are more typically found in a B2C environment, while forged signatures (stolen checks that are endorsed and cashed by someone other than the intended payee) are more prevalent in the B2B space.
- *Counterfeit checks.* With the rise and growing sophistication of desktop computing applications and advanced printers, it's become easier to print imitations of original checks. All that's needed is a company's bank account information. With the right tools, a counterfeit check can be produced with rather alarming ease.
- *Remotely created checks.* Remote checks are created by the payee on the authority of the account holder. In place of a signature, a statement in the signature area indicates that the account holder has authorized the check. That statement can be duplicated as part of a fraud.

Electronic Fraud. Although electronic payments substantially reduce fraud, criminals have found cracks in the technology. Among them:

- *Unauthorized ACH transactions.* Hacking bank account information obtained from public or internal sources, fraudsters initiate ACH debits against an account, either to purchase merchandise or to make deposits to fake bank accounts.
- *Corporate account takeover.* An employee or external cyber-attacker finds and compromises a customer's credentials in your business account files, then uses a payment origination system to make payments in that customer's name.
- *Check conversion counterfeits.* The conversion of a check to ACH is prone to fraud. Here, ACH debits are generated through electronic conversion of a counterfeit check.

A strategy for detection and prevention

Armed with the above knowledge, a company can begin to formulate a solid, successful strategy for detecting and preventing payment fraud – a strategy that can help eliminate fraud losses and protect a company's bottom line.

It begins with knowledge. First, be sure to understand your company's liabilities under your bank agreements, as well as the legal governance of various payment instruments. For example, with changes in the Uniform Commercial Code (UCC), responsibility for check fraud loss is now on the party who was most negligent in preventing it. That could be you.

Beyond familiarizing yourself with your legal responsibilities and potential liabilities, one of the most powerful and proven effective ways to combat payment fraud is by partnering with a financial institution with the expertise, controls and auditing tools to combat it with you. Citi, for example, is renowned for having one

of the industry's most formidable suites of fraud-fighting solutions.

Ways to protect against check fraud...

Positive Pay/Payee. Check Positive Pay/Payee is an automated check-matching service offered by banks such as Citi to discover fraudulent checks. You send check issuance data – account numbers, check numbers and dollar amounts, payee data – to your bank. You're immediately notified if information doesn't match up when a check is presented for payment. If any data are fraudulent, the check is returned unpaid... and fraud loss is prevented.

Bank account reconciliation. The best defense against check fraud is an ounce of prevention. Frequent, even daily, reconciliation of your account is critical to identifying unauthorized transactions. Your bank can help, with solutions such as Citi's Account Reconciliation service dramatically reducing costly errors and fraud write-offs.

Secure check stock. In recent years, the check printing industry has developed several fraud-fighting security measures. Ask Citi, which provides check printing services, about controlled paper, controlled check stock, Fourdrinier watermarks, thermo-chromatic ink, explicit warning

bands, multi-chemical reactive paper, copy void pantographs, laid lines, prismatic printing, image survivable seal, high resolution borders, ultraviolet light-sensitive ink and fibers, holograms, artificial watermarks, microprinting, and dual image numbering.

Check issuance data structuring. Don't overlook some rather simple check fraud deterrents, such as using a secure name font on your checks. You might also consider adding a row of asterisks above the payee name, to prevent a fraudster from adding his/her name to a stolen check.

Ways to protect against electronic fraud...

Universal Payment Identification Code. Developed by the Electronic Payments Network (EPN), a UPIC is a unique account identifier issued by financial institutions. It allows your organization to receive electronic payments without divulging confidential banking information.

ACH Positive Pay. Your bank can alert you to ACH transactions that don't meet your predefined criteria. Citi, for example, notifies you of such transactions for your review. You can then decide to approve or decline the transaction.

ACH Block. If your account isn't authorized for ACH transactions, you can place a "block" to prevent ACH activity. This provides you with protection against fraudsters who may be looking to confirm an active account number.

A trusted crime fighter

As part of a robust, organization-wide due diligence program, you can combine the above best practices – some internally, some in conjunction with your bank – to protect yourself against payment fraud. While there isn't a single solution that's 100% effective, using a well-planned, consistent mix of these tools can discourage many attempted fraudulent attacks against your company.

No bank offers as robust or effective a suite of fraud detection/prevention methods as Citi. The proof is in the results: Citi clients enjoy one of the lowest fraud write-off ratios in the industry – year after year.

¹ Source: Industry sources quoted by the Federal Reserve System

² Source: 2010 AFP Payments Fraud and Control Survey

³ Source: 2010 AFP Electronic Payments Survey

For more information, please visit
www.transactionservices.citi.com

© 2011 Citibank, N.A. All rights reserved. Citi and Arc Design is a trademark and service mark of Citigroup Inc., used and registered throughout the world.

761167 2/11

