

Championing Security

Selling Positive Pay to Your Corporate Clients

Selling positive pay services to your corporate clients requires making them aware of the relevant facts:

- The growing problem of check fraud and their vulnerability
- Potential liability and the importance of complying with standards of “ordinary care”
- How to cost-effectively implement positive pay

Check Fraud Continues to Grow While Businesses and Banks Feel the Pinch

Check fraud is one of the largest challenges facing financial institutions. As technology evolves, it has increased the ease with which criminals can create realistic counterfeit and fictitious checks, as well as false identification that can be used to defraud financial institutions. To protect banks and customers, it is crucial for both parties to be familiar with the problem of check fraud and the necessary prevention measures.

Industry experts agree that check fraud is a growing problem and is projected to continue growing for many years to come. Check fraud is the #1 crime facing banking institutions according to a survey done by US News. With each year showing an increase of 4-18% percent, check fraud is also the fastest growing crime.

Financial institutions look at the rising number of “smart” criminals and the increasing dollar amounts for check fraud and see a real epidemic for banks and businesses alike. Many of the most wanted criminals in the United States, according to the Secret Service website, are check or currency fraud criminals.

Why do we see an increase in check fraud each year?

The unfailing popularity of paper checks is one reason check fraud is booming. Banks have been working hard to transition customers from paper checks to electronic payments. However, bank customers continue to use checks with great frequency. Banks have realized that many customers prefer paper checks to other payment alternatives such as debit cards, automatic bill payments, electronic banking, and other paperless alternatives.

Adding to fraud potential is the speed at which banks process checks. Banks process over 64 billion checks a year at speeds of 2,500 items per minute. Banks cannot possibly review all checks thoroughly enough to identify every fraudulent check. Due to incredibly high volumes, many banks use third party verifiers that take in approximately 2.2 million bad checks each day, and this number is expected to continue rising in the future.

With the enactment of new regulations like Check 21 in October 2004, which has enabled banks to convert checks to electronic images and use these as substitutes for the real thing, the speed of processing checks is set to increase significantly. Conversion can increase the likelihood of check fraud by truncating the security information that may exist on a real check from the point in time when the check is scanned in the clearing process.

In addition, regulations and competitive pressures to accelerate availability, encourage banks to make funds available for checks before those checks have actually cleared, and this makes it easier for criminals to successfully negotiate fraudulent bank transactions.

Another reason for rising check fraud is the availability of low-cost, professional desktop publishing and copying technology. Using color copiers, laser printers, scanners and publishing software, counterfeiters can easily create excellent-quality duplicate, forged, or amount-altered checks. Criminals no longer need high-cost equipment or large resources to reproduce or alter checks.

Types of Check Fraud

Businesses remain the primary targets of check fraud criminals. Payroll checks and accounts payable checks are big targets for counterfeiting and alteration. Counterfeiting/duplication, alteration, forgery, paperhanging, and check kiting are some of the most common forms of check fraud that target both individuals and businesses.

Forgery

Internal forgery consists of an employee forging an authorized signature on bogus payroll checks or checks from other company accounts. According to FBI statistics, most check fraud occurs externally. This occurs when criminals steals, endorses, and presents a check for payment at a retail location or at the bank teller window, using bogus personal identification.

Counterfeiting and Alteration

- Counterfeiting can either mean fabricating a check in its entirety or doctoring up a check using readily available desktop publishing equipment.
- Alteration most often refers to using chemicals and solvents such as brake fluid, acetone, alcohols, carbon tetrachloride, and bleach to remove or modify handwriting and other pertinent information on a check. An attempt to erase all information from a check is often referred to as check washing. When performed on specific security locations on the check such as the payee's name or amount, it is called-spot alteration.

Paperhanging

Paperhanging involves the deliberate use of a closed checking account to write fraudulent checks. Criminals who commit paperhanging check fraud are usually hindered by a fixed number of checks. This being the case, these criminals often buy large ticket items and leave the area before discovery.

Check Kiting

Check kiting occurs when a person opens numerous accounts at two or more institutions and uses "the float or processing time" of available funds to create fraudulent balances or overdraw the account. The check kiter takes advantage of the time required by a bank to clear a check and in the mean time overdraws the account and walks away with funds.

Liability and Compliance

Unfortunately, check fraud is a relatively low-risk crime that goes unreported or un-prosecuted much of the time. Because of demands on law enforcement, prosecutors fail to pursue 75% of bank check fraud cases. And according to the U.S. General Accounting Office, in major cities where there is greater emphasis on using resources to prosecute violent crime, the number often exceeds 90%.

Many times federal prosecutors will not prosecute cases that are under \$50,000. Where larger cities like New York will only look at cases higher than \$100,000 before prosecuting. For this reason, prosecution is left at the local level, if it is seen in the courts at all.

UCC Regulations Define the Rules

It is important for a banks' corporate customers to be aware that check fraud is no longer the exclusive concern of financial institutions. In 1990, revisions in the Uniform Commercial Code (UCC) introduced the concepts of comparative negligence and relative "standards of care" related to whether a bank or its customers would be liable for check fraud losses. All but two states ratified the revisions by 1993 - the goal of which was to make banks and disbursing corporations allies in the war against check fraud. In fact, the 1990 changes have actually made banks and corporate treasurers adversaries in finger-pointing battles (and sometimes court cases) over who is to blame when check fraud occurs.

According to UCC Section 3-103 (7), "ordinary care" now requires corporate customers to follow "reasonable commercial standards" prevailing in their area for their industry or business. Under 3-406, if they fail to exercise "ordinary care", companies may be restricted from seeking restitution from their bank if their own failures contributed to a forged check or alteration. Additionally, Section 4-406 requires that customers exercise timeliness in reconciling bank statements and promptly notifying the bank if payment has been made on a counterfeit or forged check.

To encourage corporate customers to utilize special check security measures such as positive pay, banks often insert statements into their deposit agreements that absolve them from liability when those measures are offered to their customers, but are not utilized. Under such an agreement, a bank would be protected in paying a check that had been verified using positive pay and would be justified in refusing to pay checks that do not pass the security screens. The UCC however, prohibits a bank from disclaiming its responsibility (or limiting its damages) for lack of good faith or for failing to exercise ordinary care.

Banks and businesses alike are protecting themselves and promoting positive pay as the best method to fight check fraud.

"Positive Pay is the best product in 25 years to deal with the problem of forged, altered and counterfeit checks."

— Frank W. Abagnale

(Mr. Abagnale's legendary life story is told in the hit movie "Catch Me if You Can")

How Does Positive Pay Work?

The Positive Pay/Check Clearing Process

The depository bank sends checks submitted for payment to the paying bank. The paying bank compares the checks to an electronic file previously received from the issuing company. If there is a discrepancy,

the company is contacted for a decision on payment. By adopting a positive pay strategy, companies can substantially limit their exposure and potential liability for fraudulent checks.

But is Positive Pay an Affordable Solution for Every Size Business?

Yes! AP Technology's SecurePay positive pay software provides the answers your corporate clients are seeking.

With SecurePay, Positive Pay Protection is processed in two easy steps

1. Conversion: *SecurePay* imports check data from any accounting package, regardless of computer platform. It converts the check data into a positive pay file that matches the bank's required positive pay file specifications.

2. Transmission: *SecurePay* transmits this file to the bank and then it sends a notification to the client.

In the past, positive pay has been primarily adopted by large companies. Each of these companies has spent literally tens of thousands of dollars to integrate their accounting systems with their banks' individual positive pay applications. The complexity of positive pay implementation has been further compounded by a lack of industry or regional standardization and has resulted in a plethora of file transmission requirements based upon individual bank specifications. Further difficulties arise when banks go through evolutionary changes and alter how information should be transmitted between the bank and their business customers.

Due to high implementation costs, only a small percentage of small and mid-size businesses-comprising 90% of corporate America - have been able to adopt a positive pay strategy. Despite aggressive efforts by many banks to enroll their corporate accounts in positive pay programs, most companies have a difficult time converting check data into the format required by their bank. They lack the necessary financial and/or technical resources and must rely on expensive outside sources for custom programming.

Now any size business has a solution. SecurePay software is designed to provide an affordable easy-to-use interface that will convert almost any accounting check issue file into the bank's required positive pay format. For this reason, it is used by thousands of companies and banks across the U.S. SecurePay was first released in 1989 and today is used by almost every major bank - providing a needed bridge between banks and businesses.

ADDENDUM

Check Fraud Information & Statistics

“Counterfeiting has flourished for as long as there has been something worth forging. China, which invented paper money in the tenth century, once carried the grim warning on its currency that whoever forged or circulated counterfeit notes would be beheaded. England treated counterfeiting as a hanging offense, as some 600 unlucky forgers discovered before the law was repealed in 1832. Dante, in *The Inferno*, had such a poor opinion of counterfeiters that he placed them in one of the lowest circles of hell. And the Roman Catholic Church now includes check fraud and forgery as sins in its new catechism.”

Desktop Counterfeiting

By Doug McClellan

In 2003 check fraud exceeded \$20 billion per year, up from \$12 billion in 1996 and \$5 billion in 1993.

Nilson Report & US News

District Attorneys currently have a benchmark of \$5,000 before they prosecute check fraud crimes. The FBI, however, won't consider a case less than \$100,000. On the west coast and in large cities the figure is much higher. If a criminal commits check fraud internationally, the U.S Attorney gets involved, but only if it is above \$250,000.

Dept of Justice

Check fraud costs every man, woman, and child \$500 dollars a year in increased costs of goods and taxes.

United States Chamber of Commerce

Check fraud losses already are more than 15 times greater than combined losses from credit card fraud, ATM card fraud, and bank robberies. It is expected to grow at an annual rate of 12 to 15 percent over the next decade. Less than 15 percent of all check fraud loss is recovered.

Check Fraud Protection-A Report by the Office of the Metro Auditor

In 2003 counterfeit checks had the highest fraud median loss per case at \$3,059

ABA.com, John Hall

For the period of April 1st through September 30, 2003, the FBI received 268,536 Suspicious Activity Reports (SARs) for criminal activity related to check fraud, check kiting, counterfeit check, and counterfeit negotiable instruments. These fraudulent activities accounted for 47 percent of the 569,294 SARs filed by the U.S. financial institutions (excluding Bank Secrecy Act violations), and equaled approximately \$8 Billion in losses.

FBI Financial Institution Fraud and Failure Report for Fiscal Year ending Sept. 30, 2003

In 2004 there were 1474 arrests made against check fraud bandits. Of that 1474 arrested only 122 of them were convicted and 26 of those saw jail time.

Dept. of justice

Recent Secret Service investigations indicate that there has been an increase in... Counterfeiting of corporate checks and other negotiable instruments...created with the use of computer technology. The US Secret Service estimates \$5 Billion a year in losses in the United States alone. In fact, the chief of the agency's financial crimes division calls check fraud “the number one way criminals today are attacking our financial systems.”

US Secret Service

The top 1,000 U.S. companies have been surveyed, asking them to rank the crimes that hurt their business the most, both internally and externally. Check fraud made the list approximately 10 years ago, when it ranked ninth. Today, it ranks second.

KPMG International

A recent Nilson Report projects that the number of checks written annually will rise by two to four percent through the year 2020. At the same time, more than 1.2 million worthless checks enter the payment system daily.

Nilson Report

Check Fraud ranks second, behind embezzlement, on the list of crimes that most hurt America's top 1,000 companies.

American Payroll Association's PAYTECH magazine

More than 500 million checks are forged annually, with losses totaling more than \$10 billion.

Ernst & Young

55% of survey respondents indicate that their organization was a victim of payments fraud in 2004. Among these organizations, 94% indicate they were victims of check fraud. Check fraud was the most prevalent form of payments fraud. Since the majority of organizations make more than 80% of their payments by check, according to the 2004 AFP Electronic Payments Survey, it is not unexpected that the most frequently used payment method should be the most frequent target of attack.
Payments Fraud and Control Survey, Association of Financial Professionals, March 2005

Each day, 175,000 fraudulent checks are presented (low-end), representing approximately \$41 million in face value.
StopCheckFraud.com

Check fraud is among the fastest-growing problems affecting financial institutions with check fraud attempts at U.S. banks reaching \$4.3 billion in 2001, almost twice the \$2.2 billion in 1999.
2002 ABA Deposit Account Fraud Survey Report

Check fraud and counterfeiting are among the fastest-growing problems affecting the nation's financial system.
National Check Fraud Center

What Can Be Done To Prevent Check Fraud?

- *Don't use pre-printed check stock*
 - Pre-printed check stock makes fraud as easy as filling in the blanks. Use blank check stock in conjunction with advanced MICR laser check printing technology, such as SecureCheck from AP Technology.
- *Use security check stock and MICR toner*
 - Security Check Stock has specialized features that prevent copying or alteration.
- *Take advantage of check printing security features*
 - Advanced check printing solutions offer security features such as reverse fonts, watermarks, and print notifications.
- *Use tightly controlled check printing procedures*
 - Ensure that employees not involved in the accounting process do not have access to check printing equipment. Use a separate printer for check printing.
- *"Checks" and balances*
 - Separate procedures so that a person's activity will only affect part of the check production process.
- *Write fewer checks by using automatic deposits or electronic funds transfers*
 - However, forecasters say that within ten years, electronic transactions will have replaced only 25% of our check writing needs.
- *The best defense is to use a **Positive Pay***
 - Positive Pay remains the most effective weapon against check fraud. Positive Pay can be easily and cost-effectively implemented using SecurePay from AP Technology.

References

- “Bad Checks and Bogus Cards” article written by Monika Guttman
http://www.usnews.com/usnews/biztech/articles/941205/archive_012169.htm
- US Secret Service web site: http://www.secretservice.gov/financial_crimes.shtml#Financial
- American Bankers Association site: <http://aba.com>
- “Fraud - Check Fraud Statistics” article written by Michael Russell www.ezinearticles.com/?Fraud---Check-Fraud-Statistics&id=131847
- Federal Bureau of Investigations web site: <http://www.fbi.gov>
- National Check Fraud Center web site: <http://www.ckfraud.org/ckfraud.html>
- Federal Reserve System Check Fraud Report. <http://www.frbservices.org/Retail/pdf/CheckFraud.pdf>
- Frank W. Abagnale’s, an noted expert on check fraud, website: <http://www.abagnale.com/>
- "Positive Pay - Positively Pays: Check Fraud - The Rules Have Changed and You Are Exposed, Part II," article written by Kurt Pahl. <http://www.safechecks.com/articles/exposed.htm>
- "Check Fraud: A Guide to Avoiding Losses", written by the Check Fraud Working Group - a subgroup of the interagency Bank Fraud Working Group, including representatives from the Federal Bureau of Investigation, the Department of Justice, Federal Deposit Insurance Corporation, Federal Reserve Board, Internal Revenue Service, Office of the Comptroller of the Currency, Office of Thrift Supervision, U.S. Postal Inspection Service, National Credit Union Administration, and U.S. Secret Service.
<http://www.occ.treas.gov/chckfrd/chckfrd.pdf>
- Government Finance Review, "Understanding and Preventing Payment Fraud," December 2003 printed edition, article written by Michael Fletcher.
- The CPA Journal, "New Technologies to Combat Check Fraud," March 1999, written by Raymond Jeffords, Greg Thibadoux, and Marsha Scheidt.
<http://www.nysscpa.org/cpajournal/1999/0399/features/f300399.html>
- BankersOnline.com, Financial Institution Fraud Statistics, Friday June 23rd 2006, Written by Barbara Hurst.

Co-authored by Jessica Andrews & Adam Hansley, AP Technology