

Shielding Your Business

— *Positive Pay Shields Business Checks From Check Fraud* —



Foreward

Check fraud costs you more than you think. Not only could you be paying for the increasing cost of fraud but you could be paying for your reputation as well. Check fraud affects your bottomline and your business relationships:

- Check fraud is an enormous problem and, without positive pay, your company is highly vulnerable.
- Your company may be held liable for check fraud, if you do not utilize your bank's positive pay services.
- A cost-effective implementation of positive pay exists.

Check Fraud Continues to Grow While Businesses Pay the Price

Check fraud is one of the biggest challenges facing businesses today. The most wanted criminals in the United States, according to the United States Secret Service website, are check or currency fraud criminals. As technology evolves, it has increased the ease with which criminals can create realistic counterfeit and fictitious checks, as well as false identification used to defraud businesses and financial institutions. Industry experts agree that check fraud is a growing problem and is projected to continue burgeoning for many years to come.

According to the 2007 AFP Payments Fraud Survey, check fraud in 2006 was widespread: "The majority of organizations responding to the survey—72 percent—were victims of attempted or actual payments fraud, up from 68 percent in 2005...Checks continue to be the preferred target of thieves, as nearly all organizations that experienced payments fraud were victims of attempted check fraud." With such a large portion of surveyed businesses experiencing check fraud, the importance of check fraud prevention becomes foremost.



Table of Contents

Foreward	2
Check Fraud Continues to Grow While Businesses Pay the Price	2
Why the Rise in Check Fraud Each Year?	3
Who is Liable for Check Fraud?	5
How Positive Pay Works	6
Positive Pay Protection in Two Easy Steps	6
References	7
Contact	7



Why the Rise in Check Fraud Each Year?

The continued popularity of paper checks is one reason check fraud is booming. Paul M. Connolly, First Vice President and Chief Operating Officer, Federal Reserve Bank of Boston at the Bankers Forum held on April 9, 2007, said "(Checks are still written —) maybe 30 billion or so annually. We will have billions of checks for years to come." The banking industry knows that checks and check fraud activity will be with us for a long time. With such a large volume of checks being processed at speeds of 2,500 items per minute, banks will never identify every fraudulent check through visual audits.

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 manipulate fraudulent bank transactions.

Although electronic data exchange of payments is growing, paper checks still dominate in terms of transaction dollar volume (Federal Reserve Payments Study 2007). So the checks being issued are of higher dollar value than in the past, making them an even more enticing target for criminals.

Another factor is check conversion, allowing banks to use check images in lieu of an actual check. The check truncation process increases the likelihood of

check fraud by removing the security information that exists on a real check at the point where the check is scanned in the clearing process.

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.

Simply put, committing check fraud is easy if positive pay is not safeguarding your bottomline by identifying fraudulent checks — your company is a target if you do not protect it from criminals.





Types of Check Fraud

Forgery

Internal forgery occurs when an employee falsifies an authorized signature on bogus payroll checks or checks from other company accounts. According to FBI statistics, most check fraud occurs externally when criminals steal, endorse, and present a check for payment at a retail location or at the bank teller window, using falsified personal identification.

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 numerous accounts are opened at two or more institutions and utilize "the float" or "processing time" to artificially inflate funds,

or overdraw the account. The check kiter takes advantage of the time required by a bank to clear a check and walks away with fraudulently-obtained funds.

Counterfeiting and Alteration

- Counterfeiting can either mean fabricating a check in its entirety or manipulating an existing 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 marks on the check, such as the payee's name or amount, it is called "spot alteration."



Who is Liable for Check Fraud?

It is important for companies to know that check fraud is not the exclusive responsibility of financial institutions. In 1990, revisions to the Uniform Commercial Code (UCC) introduced the concepts of comparative negligence and relative “standards of care” related to whether a bank or its customer 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 corporate treasurers adversaries in finger-pointing battles (and sometimes court cases) over who is responsible when check fraud occurs.

UCC Regulations Define the Rules

To encourage business customers to utilize special check security measures such as positive pay, banks often insert statements into deposit agreements that absolve the bank from liability when defensive measures are offered to its customers, but are not utilized. Under such an agreement, a bank would be protected in paying a check that has been verified using positive pay and would be justified in refusing to pay checks that do not pass 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.

*Criminals say
“Check Fraud Pays”*

Unfortunately, check fraud goes unreported or unprosecuted much of the time. According to the U.S. General Accounting Office, prosecutors on average fail to pursue 75% of bank check fraud cases. And, in major cities, where there is greater emphasis on using resources to prosecute violent crime, they fail to adjudicate 90% of check fraud cases on average.

Federal prosecutors on average will not pursue cases involving less than \$50,000, whereas larger cities will only prosecute cases that on average involve \$100,000 or more. Check fraud cases, if seen in a courtroom, are mainly prosecuted at the local level only.

Positive pay enables your company to protect itself from check fraud at every check disbursement.



Businesses are protecting themselves and promoting a technique called positive pay because it is the best method of fighting check fraud.

Positive Pay

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

— FRANK W. ABAGNALE

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

How Does Positive Pay Work?

With positive pay, the paying bank compares checks submitted for payment to an electronic file sent by the issuing company. If there is a discrepancy, the company is contacted for a decision on payment. By adopting a positive pay defense, businesses can substantially limit exposure and potential liability for fraudulent checks.

Is Positive Pay an Affordable Solution for Every Size Business?

Yes! AP Technology's SecurePay positive pay software provides an easy and affordable way for any size business to implement positive pay.

In the past, a company would have spent considerable amounts of time and money to integrate its accounting systems with its bank's individual positive pay applications. Due to the high implementation costs, many small and mid-size companies have not adopted positive pay, despite aggressive efforts by many banks to enroll all corporate accounts into positive pay services.

SecurePay software is designed to provide an easy way to convert check issue files from any accounting application into a bank's positive pay format. The solution works with any bank and is used by thousands of companies across the U.S. And, SecurePay is recommended by almost every major bank as a check fraud prevention method.

With SecurePay, positive pay protection is processed in two easy steps:

1. **Conversion:** SecurePay imports check data from any accounting package and converts it into a positive pay file that matches the bank's required specifications.
2. **Transmission:** SecurePay can automatically transmit check issue files to the bank and notify the client upon receipt.

Summary

Despite a changing payments landscape, check fraud remains a staggering problem and looks like it will be with us for years to come.

There is good news, however — check fraud does not have to affect your business. Positive pay prevents check fraud, helps attenuate your liabilities, and assists in maintaining your valuable reputation. Positive pay is an obvious best-practice for every business and SecurePay software from AP Technology makes implementing positive pay both easy and economical.

References

- 2007 AFP Payments Fraud Survey
<http://www.afponline.org/pub/pdf/2007PaymentsFraudSurvey.pdf>
- 2007 Federal Reserve Payments Study
http://www.frbervices.org/files/communications/pdf/research/2007_payments_study.pdf
- United States Secret Service
http://www.secretservice.gov/financial_crimes.shtml#Financial
- American Bankers Association
<http://aba.com>
- Stopcheckfraud.com
<http://www.stopcheckfraud.com>



Contact

For immediate attention
on SecurePay, contact
Adam Hansley at 760.602.5413
or
adam.hansley@aptechnology.com

AP Technology
5973 Avenida Encinas, Suite 140
Carlsbad, CA 92008
800.652.2877
sales@aptechnology.com
www.aptechnology.com