

### CHECK FRAUD...A GROWING PROBLEM

Check Fraud, once the criminal specialty of professional forgers, has emerged from relative obscurity to become the "Crime of the Nineties" and beyond. According to recent studies, more than 500 million checks are forged annually, with losses totaling more than \$10 billion, and growing at a rate of about 2.5% annually.

#### What's the reason for the increase in check fraud incidents?

The American Bankers Association (ABA) attributes the increase in check fraud to the availability of sophisticated, low-cost technology – desktop computers, scanners, laser printers and desktop publishing software programs. Color copiers have provided the criminal element with the ability to mass-produce any type of check in the market.

#### How does check fraud occur? And who are the principal targets of check fraud activity?

Check fraud occurs in a number of ways. Checks are easily copied or otherwise reproduced, amount and payee information is changed, and checks are cashed with phony identification cards or other media. Gangs are deeply involved in this activity and account for major fraud activity in larger metropolitan areas, sometimes making as many as 40 to 50 bogus checks from a "good check" copy that has a valid signature and other corporate data and logo information on it. Corporate payroll and accounts payable departments are great targets. All types and sizes of companies, companies with remote offices -- out of state or within the state -- are targets. Large banks are particularly hard hit, but fraud occurs in every size and type of business and in every size of bank. Fraud is on the increase, and every company must prepare to defend itself against the damage that lack of "ordinary care" procedures may cause within their organization.

### THE UNIFORM COMMERCIAL CODE (UCC)

The current UCC code outlines specific responsibilities for banks and companies in the handling of check fraud cases. The UCC document itself was not substantially updated until 1993, when major revisions were developed as a result of major increases in check fraud incidents and dollar losses.

Since that time, the UCC has been adopted by all fifty (50) states, and legal precedents have been established that have shifted some of the burden of check fraud prevention to businesses and corporations, where before, banks had 100% of the responsibility in check fraud incidents. This includes dollar liability for some incidents.

The term "ordinary care" was introduced in the updated regulations, and it is important that you contact your bank and learn what your bank defines as your firm's responsibilities in exercising ordinary care to prevent check fraud. Your bank defines ordinary care as it pertains to your company and their security standards.

#### Why is my firm potentially liable for a fraud incident?

Some reasons for potential liability are:

- Lack of security control for the storage of check stock within your company's document storage area. Check stock must be stored in a secure, locked environment with controlled access only by authorized personnel.
- Lack of timely bank account reconciliation for payroll and accounts payable accounts.
- Lack of secure control over storage and access to signature stamps or signature machines.
- Lack of signature verification on canceled checks during the reconciliation process.
- Lack of timely reporting of potential check fraud occurrences to your bank.
- Lack of paper safety features in your check paper stock.
- Lack of procedures within your organization to inhibit the forging of signatures or alteration of amount
- Failure to supply current documentation to your bank on authorized signers.

### HOW CAN I PROTECT MY COMPANY AGAINST CHECK FRAUD?

Unfortunately, there is no absolute method available to protect your company against check fraud, BUT the following suggestions are recommended to you as a start.

1. Contact your bank and ask for a written copy of their suggested procedures for preventing check fraud, check stock considerations, and check reconciliation processes that they expect you to follow.
2. Ask your bank for the written procedures that they follow to reduce check fraud. (Their back office procedures, the "ordinary care" activities that they follow.)
3. Ask your bank if they have a "Positive Pay" program. Ask for details of the program and the processing cost, if any. Some banks do not charge for "Positive Pay." (See the last section of this document for additional information.)
4. Consider the following "Internal Procedures" for implementation within your company.
  - Review all hiring procedures. Utilize a background check for employees working in vendor assignment, check issuance or check reconciliation areas.
  - Ensure that at least two people are responsible for accounts payable, and ensure that the mailroom personnel and procedures are sound.
  - Keep all check stock or cash equivalents in a secure and locked facility. Verify that tops and bottoms of check boxes have not been opened and resealed.
  - Change keys or entry codes periodically to prevent routine access to storage areas.
  - Enforce mandatory vacation policies, particularly for those with financial access. Be alert for employees living beyond their means.
  - Conduct surprise audits. Do any employees appear nervous? Have you noticed a substantial change of lifestyle?
  - Read and understand your bank contracts regarding liability as well as your company's liability for fraud under the current UCC Regulations.

5. Consider the following "External Procedures" for implementation within your company.
  - Use bank services like "Positive Pay," expedited return information, and signature verification systems to protect your accounts payable, payroll and accounts receivable activities.
  - Purchase blank safety paper or specially designed check stock from established vendors or banks that offer this stock for your check printing operations.
  - Reconcile check disbursements and deposits regularly. Prompt account reconciliation is a must!
  - If you discover a check with a fraudulent payable amount, close the account as soon as possible.
  - Be cautious when using refund accounts, such as rebates for subscriptions. This is another target for check fraud since the checks are relatively easy to obtain and can be used for check fraud.
  - Find ways to replace paper documents with electronic payments, devices, and complete printing systems that control not only the creation of checks from blank safety stock, but which also include Positive Pay for the processing of your issued checks by the bank electronically.
  - Store or dispose of canceled checks properly and safeguard new checks. Do not disclose checking account numbers to individuals you do not know, even if they claim they are from your bank.
  - Compare payroll checks with your current employee records.
  - Question funds that are transferred between bank accounts; verify new business vendors and their associations with your company.
  - Review cancelled checks and endorsements on a monthly basis.

## ACOM SOLUTIONS, INC.

Based in Long Beach, California, ACOM is the leading "single source" provider of electronic payments and MICR laser check processing solutions, deemed by experts to be the most effective methods for deterring check fraud.

Running host-resident in the Windows or IBM iSeries (AS/400) operating environments, ACOM's EZPayManager Suite is an electronic payments and MICR laser check processing solution that enables users to generate corporate payments from a single software application. Using electronically stored form templates, users can send payments electronically through the banking systems ACH network, or print checks on a MICR-enhanced secure laser printer (a single pass through the printer generates all the corporate information, logos, amounts and signatures). ACOM's EZPayManager is compatible with all financial management software systems, ranging from legacy and general business systems such as Oracle Financial Applications, and JD Edwards, to specialized vertical packages such as WLT (healthcare) and PDS (payroll).

ACOM's integrated payment solutions provide unprecedented security, efficiency and control in disbursement-processing operations.

Elements of ACOM's Total Solution include:

- EZPayManager disbursement-processing software (including modules for e-payments, MICR laser checks, forms design, and Check Fraud Alert for positive pay)
- Xerox Network Laser Printers (MICR-enhanced by ACOM)
- Post-processing equipment for folding
- Blank security check stock (including watermarks, void pantographs, micro-printing, toner grip, and sequential numbering)
- Consumables (including MICR toner engineered to the specifications of each printer, fusers, etc.)
- Toll free tech support

ACOM customers tell us that our "single source" approach saves them time, money and confusion, since they only have to go to one place for:

- Hardware (printers and post-processing equipment)
- Software
- Installation
- Training
- Supplies
- Tech Support

ACOM has been in business since 1983, and currently has more than 3,000 active customers.

## REFERENCES

- Security Documents - On Guard, FORM Magazine, Susan Keen, (703) 836-6225
- Balancing Act, WASHINGTON Business Journal, Fred O. Williams
- Articles of the Uniform Commercial Code, Legal Information Institute, Cornell Law School
- Open Doors with Software Compatible Forms and Checks, Business Products Professional
- Check Fraud, Cardinal Business Media, Survey 1087
- Client Service Bulletin, Frank W. Abagnale & Associates
- Fraud Prevention and the Management, Management Accounting, Richard Turpen, CPA & Frank Messina, CPA
- What Is Negligence, Garon & Associates Co., L.P.A., Cleveland, OH 44113
- Strategies to Reduce the Potential for Check Fraud at Your Company, IOMA, Managing Accounts Payable
- Check Fraud: A Guide to Avoiding Losses, Office of the Comptroller of the Currency, United States Government
- Check Fraud – Liability and Defenses, Articles 3 & 4 – UCC, Brent S. Gorey & Daniel S. Bernheim

This document is for informational purposes only. It is not intended for usage as a legal reference. All information has been obtained from noted third party reference source and material. ACOM assumes no liability for the information contained herein.