AmericanBank

HELPFUL HINTS ON MINIMIZING FRAUD, THEFT AND EMBEZZLEMENT

Depending on the type of business you are in, some of these tips may be more applicable than others. For example, retailers will be more interested in sales, credit card, refund and over-ring information than other types of businesses. We encourage you to review all the hints. You may find some thought-provoking ideas, even among those not directly applicable to your type of business.

Your Bank Statement

Statements

□ **If you own your own business, have your business account bank statements mailed to your home.**

□ Watch for check numbers paid out of order.

□ Determine if there are an unusual number of checks made payable to the same payee.

Returned Check Images

□ Review your returned check images to see if the payee has been altered. Alterations can be made by marking through the payee and writing another payee above or beside it, using correcting fluid or simply modifying the original payee (i.e., Bill Jones changed to Bill Jones, Jr. or the initials F. M. C. changed to Frank M. Capps).

□ Check to see if the numerical and written dollar amounts of the checks match.

□ Check the amount to see if it has been increased (a $50 check increased to $150).

□ Check to see if the writing of the amount matches the writing of the payee's name.

□ Verify that the encoded amount at the bottom of the check matches the written dollar amount.

□ Look for typed or handwritten checks where computer generated checks are the norm.

□ Compare invoices back to the check payments. A common method of theft is for an accounts payable clerk to add the amount of their personal utility or telephone bill to the employer's bill. This same scenario can apply to any payee common to the company and the employee such as Visa, MasterCard or American Express.

□ Do not allow telephone or Internet payments to be initiated from the account.

□ Compare invoices back to electronic debits to the account.

Internal Controls

All Sales

□ Reference cash, credit card and check sales by the register sequence number.

□ Make sure there is an audit trail for cash and cash back.

Credit Card Sales

□ Close out your credit card terminal and balance the transactions each day.

□ Look for multiple sales using the same credit card number or the same dollar amount.

□ Make credit card refunds available only through a credit to the card. (Otherwise a refund can be shown as cash and the cash can be pocketed. You are not required to provide a refund on a credit card sale if the proper verbiage is printed on the customer's receipt.)

□ Be alert to the fact that a credit card number may be used to falsely process a sale to cover up for cash pocketed.

Checks

□ Watch for altered checks; they can be used to help a clerk pocket cash.

□ Periodically, remove checks from the register and store them in a secure place. (This will help prevent an employee from taking a check from the register on one business day and putting it in place of cash that they have pocketed on another business day.)

□ Secure your cancelled checks as well as your blank checks. Cancelled checks can be used to create fraudulent checks.

□ If you sign blank checks for retail purchases such as those at an office supply store or Sam's Club, verify that the items on the receipt are for business use. Also, verify that the check amount and the receipt's total are the same. Some stores accept checks for an amount greater than the actual sale and give cash back.

Cash

□ Build audit trails for any time cash is handled.

□ Remove $100 and $50 denomination bills from the register as soon as possible, and store them in a secure place.

□ Establish dual control procedures to open and close a register.

- □ Start the register with the same amount of cash each day. In balancing cash at the end of the day, register cash should equal the cash to be deposited at the bank. This prevents employees from replacing register cash with their own personal check.
- □ Require a separate register tray for employees relieving other employees.
- □ Conduct surprise register audits.

Refunds

- □ Require the customer's signature.
- □ Establish a procedure that requires a second employee's approval for refunds.

Over-rings

- □ Require a second employee's approval.

Collusion

- □ Observe employees' relatives or acquaintances who frequent your business.
- □ Look for fraudulent or insufficient checks by relatives or friends.
- □ Watch for employees giving friends or relatives too much cash back on purchases.
- □ Implement a policy that prohibits employees from ringing up sales or doing refunds for relatives or friends.

Security

- □ Provide a separate register for each cashier.
- □ Utilize security cameras and monitors; tape activity.
- □ Install security mirrors.

Ink

- □ Use ink on all written forms and balancing sheets. This prevents tickets from being altered and will help you identify someone who is "force" balancing cash.

Company Credit Cards and Debit Cards

- □ If you provide a business credit card or debit card for your employees' use, compare actual receipts to the credit card bill and bank statement to make certain all purchases are for a business purpose and not for personal use.
- □ Do not allow cash withdrawals with a debit card from ATMs. Set the cash withdrawal limit to zero.
- □ Review the daily spending limit for each employee based on actual need and set the limit by employee accordingly.

Bank Deposits

- □ On the deposit slip, list cash deposited separately from checks deposited.
- □ Upon receipt, endorse all checks "for deposit only."
- □ Do not sign the deposit slip for cash back until you arrive at the bank. (For your protection, cash back is normally not allowed on a commercial deposit.)
- □ Safeguard your blank deposit slips. Someone can use them to deposit a fraudulent check into your account and take cash back. (Cash back normally occurs on personal accounts only.)
- □ When making a deposit, do the following:
  - ▪ Keep your deposit/bank bag concealed. Don't carry it in the trunk of your car. The time it takes you to exit your car, open the trunk, retrieve the deposit and close the trunk increases your risk.
  - ▪ Keep your car doors locked from the time you enter your car with the deposit until you exit the car at the bank.
  - ▪ Have your night drop key and deposit ready when you leave your car.
  - ▪ Always be aware of your surroundings. Do not get out of your car or stop at the night drop if anything looks suspicious.
  - ▪ If you make deposits daily or several times a week, vary your route to and from the bank.
  - ▪ Be very suspicious of anyone approaching you outside the bank. The bank does not allow solicitation on its premises.
  - ▪ If anything appears suspicious, report it to the bank during banking hours or to the police after hours.
- □ If you use employees to make bank deposits, vary them so the same person is not always making the deposit.
- □ Require the person making a deposit during banking hours to return a deposit receipt to you.
- □ If you store your deposit overnight, have two employees remove it from storage and place it in a locked bank bag for delivery to the bank. The person making the deposit should not have access to the bag's key.

Deposited Checks Being Returned

- □ If you do not use a collection agency, make sure the returned items are sent to the attention of someone other than the employee preparing deposits or responsible for reconciling the account.

Employee Check Cashing

- □ Consider the risks before allowing employees to cash checks.
- □ If you decide to allow employee check cashing, make sure checks are cashed out of a register or drawer for which the employee cashing the check is not responsible.
- □ Have two people (other than the employee cashing the check) initial it: the person whose register/drawer the check is being cashed from and one other employee.
- □ Establish a low dollar limit for employee check cashing.
- □ To avoid cashing employees' payroll checks, consider direct deposit for payroll.

Payroll

- □ Watch for payroll checks being made payable to former or fictitious employees.

Petty Cash

- □ Do not allow employees to cash personal checks from petty cash.
- □ Keep your petty cash under dual control.
- □ Conduct surprise audits on petty cash.

Counterfeiting

Look for the following features to guard against counterfeit bills:

Color-shifting Ink

Tilt the front of the bill back and forth to see the color on the numeral located on the lower right corner of the note change from a distinct green to black and back again.

Watermark

Hold the bill up to a light source to see the watermark in the blank space to the right of the portrait. Because the watermark is in the paper, not printed on it, the watermark looks the same from the reverse.

Security Thread

This is a thin strip of plastic imbedded in the paper that is visible only when you hold the bill up to a light source. This thread glows under ultraviolet light.

Concentric Fine Lines

Look at the very fine lines behind the portrait. Turn the note over to be certain that the lines on both sides are clear – not splotchy, wavy or composed of dots.

Microprinting

Look at the security thread with a magnifying glass to see the words "USA" and "The United States of America" microprinted on the note.

Comparison

Compare the note against a note you know to be authentic to look for differences in the features as well as the texture of the paper.

If you receive a counterfeit note:

Keep the bill from the passer (if you can safely do so);
Delay the passer, if possible;
Observe the passer's description and that of any companion or vehicle used;
Telephone the police - or
Surrender the bill to your bank for delivery to the local police or the U.S. Secret Service.

Avoiding ACH Fraud

Controls and Practices to Deter Corporate Account Takeover

These recommendations were developed by the FS-ISAC and NACHA for you to protect your online business banking credentials and strengthen ACH and wire security procedures.

Account Controls:

- □ Learn about account features that may protect your accounts, such as check cashing limitations and automated payment filters.
- □ Reconcile all banking transactions on a daily basis.
- □ Initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.

Best Practices:

Among the recommendations to secure computer systems:

- □ If possible, and in particular if you do high value or large numbers of online transactions, carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which e-mail and Web browsing are not possible.

(Continued on back)

□ Be suspicious of e-mails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information. Opening file attachments or clicking on web links in suspicious emails could expose your system to malicious code that could hijack your computer.

□ Install a dedicated, actively managed firewall, especially if you have a broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.

□ Create a strong password with at least 10 characters that includes a combination of mixed case letters, numbers and special characters.

□ Prohibit the use of "shared" usernames and passwords for online banking systems.

□ Use a different password for each website that is accessed.

□ Change the password a few times each year.

□ Never share username and password information for Online Services with third-party providers.

□ Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.

□ Install commercial anti-virus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.

□ Ensure virus protection and security software are updated regularly.

□ Ensure computers are patched regularly, particularly operating system and key applications, with security patches. It may be possible to sign up for automatic updates for the operating system and many applications.

□ Consider installing spyware detection programs.

□ Clear the browser cache before and after starting an Online Banking session in order to eliminate copies of web pages that have been stored on the hard drive. How the cache is cleared will depend on the browser and version. This function is generally found in the browser's preferences menu.

□ Verify use of a secure session (https not http) in the browser for all online banking.

□ Avoid using automatic login features that save usernames and passwords for online banking.

□ Never leave a computer unattended while using any online banking or investing service.

□ Never access bank, brokerage or other financial services information at Internet cafes, public libraries, etc. Unauthorized software may have been installed to trap account number and sign on information, leaving you vulnerable to possible fraud.

□ Familiarize yourself with the bank's account agreement and with your liability for fraud under the agreement and the Uniform Commercial Code as adopted in the jurisdiction.

□ Stay in touch with other businesses to share information regarding suspected fraud activity.

□ Immediately escalate any suspicious transactions to your bank, particularly ACH or wire transfers. There is a limited recovery window for these transactions and immediate escalation may prevent you from further loss.

Avoiding ACH Fraud tips are provided courtesy of www.BankInfoSecurity.com.

Written by:
Linda McGlasson
Managing Editor
BankInfoSecurity.com