FRANK W. ABAGNALE

CHECK FRAUD AND IDENTITY THEFT

VOLUME II

INSIDE THIS ISSUE

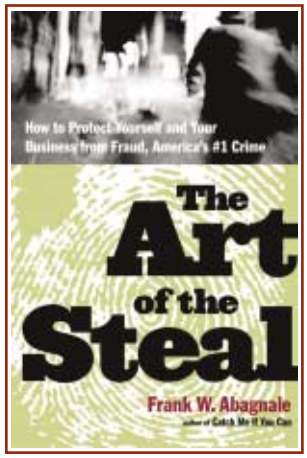
Frankly Speaking . . .

The fastest growing financial crimes in America today are check fraud and identity theft. The Nilson Report estimates check fraud losses to be about $20 billion a year. The American Bankers Association has stated that check fraud is growing 25 percent per year. Check fraud gangs are hardworking and creative. They constantly try new techniques to beat the banking system and steal money from depositors. Historically, the banks have been liable for these losses. However, recent changes in the Uniform Commercial Code now share the loss with the depositor.

The Wall Street Journal reported that nearly 700,000 Americans have been victims of identity theft. At $5 billion, identity theft is a small crime when compared to check fraud. But, it already surpasses credit card fraud. Because this is so simple to commit, I believe identity theft will become one of the most profitable criminal activities in history.

There are endless opportunities for a criminal to obtain the necessary information to commit identity theft. Let me illustrate just two, beginning with a visit to the doctor. As a new patient, the receptionist asks you to complete a form that asks for your name, address, phone number, and your employer's name, address and phone, and your health history. Then, they make a copy of your insurance card, which includes your Social Security number. You have just provided enough information for someone with access to those records to become you.

Another example. You walk into an upscale department store to make a purchase. You take your selection to the cashier and write a check. On that check is your name, address and home phone number, the name of your bank and its address, and your bank account number. The cashier asks for your driver's license. In 19 states, the license number is your Social Security number, which is written on the check. The cashier memorizes the birth date on your license, and then asks for your work phone number, which will lead them to the name and address of your employer. Once again, a thief has sufficient information to apply for credit in your name.



I am 54. As a teenager I did things that today, as a husband and father, an educator and consultant, I am not proud of. But, recounting one youthful experience may be illustrative.

In my old days, when I wanted to establish a new identity (so that I could open a bank account and pass bad checks), I would go to the Department of Vital Records (in any city I was in). I would ask to see the death records for 1948, the year I was born. Every fifth or sixth entry was an infant who had died at birth. I would write down the death information and later apply for a birth certificate in that name. I would fill out a form, pay $10, and obtain a legitimate birth certificate. I would go to the DMV and get a license with my picture, my description, and somebody else's name. I had 50 legitimate driver's licenses.

Now, 35 years later, you can buy a CD ROM with birth and death records, and can apply for a new birth certificate by mail. There are also a couple of Web sites that sell Social Security numbers for $49.95. Their advertisements claim that they can tell you anything about anybody. I researched these companies—all you have to provide is someone's name and address—and they will tell you everything you want to know, including spouse and children's names.

For the identity theft victim, the nightmare has just begun. On average, it costs a victim $1,173 and 175 man-hours to get their credit report straightened out. Fixing the problem is not as simple as saying "…that wasn't me." You must prove you did not apply for that auto loan. To fix things, you must first convince the credit card or finance company. Then, you must convince all three credit bureaus. In most cases, the credit bureaus refuse to delete the dispute from your credit files. Instead, they put an asterisk and say, "Customer disputes this Visa charge, claims they were a victim of identity theft." The result is that anyone accessing your credit report, whether a potential employer or a company considering granting you credit, may question whether you were really a victim or if you were just ripping somebody off.

I have been personally concerned about identity theft. A few years ago, I subscribed to a service that notifies me each time my credit report is accessed. Privacy Guard (www.privacyguard.com) provides me with the contact information of the company that obtained my credit report, as well as a means to correct false reports. I consider their annual fee money well spent.

This publication was written to help individuals and companies learn how to reduce their risk of check fraud, identity theft and embezzlement. I hope you find it useful. Because there was not space to cover every scam, I have included references to various agencies and organizations with useful products or information. I have written a book, *The Art of the Steal*, that covers numerous scams and solutions in detail. For individuals concerned about check fraud, I have designed the Supercheck, a high-security personal check. Manufactured with 12 safety features, there is nothing like it in America. It will be available only through financial institutions. For information and a sample check, visit www.supercheck.net.

Sincerely,

Frank W. Abagnale

www.supercheck.net

Check Fraud–A National Epidemic

The recent growth in check fraud has reached epidemic proportions, leaving no individual, company or municipality immune. More than 1.2 million worthless checks enter the banking system each day. The Nilson Report advises that annual check fraud losses now exceed $20 billion, which is up from $12 billion in 1996 and $5 billion in 1993. The American Bankers Association reports that check fraud is growing 25 percent per year.

Recent changes in the Uniform Commercial Code (UCC) distribute the problem by taking sole responsibility for check fraud from the bank and directing that it be shared with both banks and their customers. Losses and related expenses from check fraud will continue to increase the cost of doing business for banks and their customers, unless banks and customers form a strong partnership to prevent and control the problem.

Risk Management

Banks, companies, and municipalities face a substantial shared risk from check fraud. Financial executives must answer "How do we assess our risk? How much financial exposure are we willing to assume? What real and hidden costs will we bear if we become victims of check fraud? How might our image and reputation be damaged? How much are we willing to spend to reduce our risk?"

This bulletin serves as a guide for making those tough decisions.

Uniform Commercial Code Revisions Shift Liability

The legal basis for liability in check fraud losses is found in the Uniform Commercial Code (UCC). The revised UCC outlines specific responsibilities for banks and corporations, and recent court cases are providing clarification and establishing legal precedent. Failure to adhere to these new responsibilities may cause the negligent party to suffer a loss.

UCC revisions define responsibilities for check issuers and paying banks under the term "ordinary care." Under Sections 3-403(a) and 4-401(a), a bank can charge items against a customer's account only if they are "properly payable" and the check is signed by an authorized person. If a signature is forged, the issuer may be liable if one of the following exceptions applies.

According to UCC Section 3-406, if account holders fail to exercise "ordinary care," they may be restricted from seeking restitution from the payee bank if their own failures contributed to a forged or altered check. Under 3-103(7), ordinary care requires account holders to follow "reasonable commercial standards" prevailing in their area and for their industry or business.

Section 4-406 requires customers to reconcile their bank statements within a reasonable time and report unauthorized checks immediately. Typically this means reconciling bank statements as soon as they are received, and always within 30 days of its mailing.

The concept of comparative negligence in Sections 3-406(b) and 4-406(e) can also shift liability from the bank to the check issuer. If both the bank and the account holder have failed to exercise ordinary care, a loss may be allocated based on the extent that each party's failure contributed to the loss. The internal procedures used by a company when issuing checks will be questioned to determine negligence. Since banks are not required to physically examine every check, companies may be held liable for all or a substantial portion of a loss even if the bank did not review the signature on the fraudulent check.

Liability for counterfeit items that are virtually identical to original checks will be addressed on a case-by-case basis.

Read Bank Contracts

Carefully read your bank contracts to understand your company's liability for fraud losses under the revised Uniform Commercial Code. This specifically includes the small print on signature cards and disclosure statements. It is abundantly clear from recent court cases involving fraudulent checks that a bank's intentions must be stated clearly and without ambiguity in order to win a check fraud case against a customer. Accordingly, banks are rewriting their signature card agreements and are including new provisions and requirements in their disclosure statements. For a summary of the changes in the UCC, please visit www.FraudTips.net.

Impact Of Regulation CC

In 1992, the Federal Reserve Regulation CC reduced the time a bank was allowed to hold deposited funds as uncollected items. The new Regulation provides bank customers access to their funds in a shorter period of time, e.g., local checks within 2 days, non-local checks within 5 days, even if the actual check has not paid.

The Regulation's intent was to speed the availability of deposited funds to consumers. But the change has significantly increased fraud losses by shortening the time that banks can return checks paying against uncollected funds. Shortening the time has expanded the window available for criminals to perpetrate a fraud. Criminals often alter a check's routing and transit numbers, redirecting checks to an incorrect Federal Reserve District. When the fraudulent checks ultimately are returned to the correct bank, the deposited funds have been withdrawn.

Banks are also required to follow strict guidelines regarding new accounts. Any account that has been open for 30 days may no longer be considered a new account, with its extended "hold" period on deposited funds.

For a summary of changes in the UCC regarding check fraud liability, please visit www.FraudTips.net.

Check Fraud Prevention–Best Practices

When fighting check fraud, nothing is 100 percent. No feature or program can completely eliminate check fraud, and no prevention system is foolproof. However, specific practices can complicate a criminal's counterfeiting efforts. Following are the Best Practices for reducing risk.

Positive Pay

The most effective check fraud prevention tool is Positive Pay (Match Pay), an automated check-matching service that is unparalleled in detecting bogus checks. It is offered through the Cash Management Department of many banks. To use this service, the check issuer sends (transmits) a file of issued checks to the bank. Positive Pay is extremely effective when the customer sends issued-check information to the bank the same day checks are issued. Positive Pay compares the account number, check number, and dollar amount of checks presented for payment against the list of checks authorized and issued by the company. All three components of the check must match exactly or it becomes an "exception item." When an exception item is identified, the bank contacts the customer to determine its authenticity. If the check is fraudulent or the dollar amount was altered, the bank will return the check unpaid, and the forger is foiled.

Because recent revisions in the UCC impose liability for check fraud losses on both the bank and its customer, it is in everyone's interest to help prevent losses. When a company uses highly secure checks (with eight or more security features) and works with its bank to implement Positive Pay, its risk of and liability for check fraud will be substantially reduced. Many banks charge a modest fee for Positive Pay, which should be regarded as an "insurance premium" to help guard against check fraud losses.

Reverse Positive Pay

For organizations or individuals with relatively small check volume, Reverse Positive Pay should be considered. This service allows an account holder to conduct a daily check matching to identify unauthorized checks. The account holder downloads from the bank the list of paid checks and compares them to the issued check file. Suspect checks must be researched and the bank advised of items to be returned. While Reverse Positive Pay provides timely and manageable information on a small scale, for larger operations it is not a worthy substitute for Positive Pay.

Positive Pay is not Foolproof

Positive Pay and Reverse Positive Pay monitor the check number and dollar amount, but not the payee name. Neither will catch added or altered payees, or counterfeit checks using legitimate check numbers and dollar amounts with new payees. Several banks are developing Positive Pay systems that compare the payee name, called Payee Name Verification (PNV). PNV identifies the payee line through X,Y coordinates on the face of the check, and uses optical character recognition software to interpret and match the characters. Matching the payee name, check number and dollar amount will stop most check fraud attempts, but it is still not 100 percent effective. It will not prevent added payee names inserted above or below the authentic payee name line.

> ***"Positive Pay is the best product in 25 years to deal with the problem of forged, altered and counterfeit checks."***
>
> ***— Frank W. Abagnale***

Preventing Added Payees

Altering or adding a new payee name is the latest scam of sophisticated forgery rings. They fully understand the limitations of Positive Pay and simply add a new payee name above or below the original name (after removing the address). To help prevent added payee names, insert a string of asterisks above and after the payee name, and use a Secure Name Font (see example page 5). To help prevent altered payees, use highly secure checks to keep the asterisks and address from being removed.

ACH Filter or Block

Forgers have learned that Positive Pay cannot monitor electronic "checks," also known as Automated Clearing House (ACH) debits. Files containing ACH debits are created by a company or municipality and submitted to its bank. The bank processes the file through the Federal Reserve System and posts the ACH debit against the designated account. Because paperless transactions pose substantial financial risk, banks are careful to thoroughly screen any company that wants to send ACH debits. However, some dishonest individuals get through the screening process and victimize others.

To prevent electronic check fraud, ask your bank to place an ACH filter or block on your account. An ACH block rejects all ACH debits. For many organizations, a block is not feasible because legitimate ACH debits would be rejected. In this case, use an ACH filter.

In the electronic debit world, each ACH originator has a unique identifying number. An ACH filter posts debits only from preauthorized originators or in preauthorized dollar amounts. If your bank does not offer a filter, open up a new account exclusively for authorized ACH debits and restrict who has knowledge of that account number. Put a block on all other accounts.

High Security Checks

Using highly secure checks is a critical component in check fraud prevention. One cannot discuss check fraud and ignore this important tool. A highly secure check provides the only deterrent to altered names and dollar amounts by making alterations and replications more difficult. There is substantial evidence that highly secure checks motivate criminals to seek easier targets. This "tool" is easy to implement. Simply ask your check printer to add safety features to your checks on your next order. For a list of safety features, see Page 6.

Highly secure checks should contain at least eight (8) safety features, and more is better. Many check manufacturers sell checks that include a printed padlock icon, suggesting the check is secure. The padlock icon does not make a check secure, since only three safety features are required to use it.

Some legal experts suggest that a strong argument can be made that the failure by a business to use adequate security features to protect its checks constitutes negligence. By using highly secure checks, a company can legally demonstrate that care has been taken to protect their checks.

Reconcile Bank Statements Promptly

The revised UCC requires an organization to exercise "reasonable promptness" in examining its monthly statements, and specifically cites 30 days from the date of mailing from the bank. Carefully read your bank's current disclosure agreement that details the length of time you have to report discrepancies on the bank statement. Some banks have shortened the timeframe to less than 30 days. Failure to reconcile promptly is an invitation for employees to embezzle because they know their actions will not be discovered for a long time. The people issuing checks should not be the same people who reconcile the accounts.

If you are unable to reconcile on time, hire an outside reconciliation service provider and have the bank statements mailed to them directly. Independent reconciliation service providers, CPA firms, and many banks offer this valuable service.

Repeater Rule

The repeater rule limits a bank's liability. If a bank customer does not report a forged signature, and the same thief forges a signature on additional checks paid more than 30 days after the first statement containing the forged check was made available to the customer, the bank has no liability on the subsequent forged checks so long as it acted in good faith and was not negligent.

The one-year rule is another important guide. Bank customers are obligated to discover and report a forged signature on a check within one year, or less if the bank has amended the one-year rule. If the customer fails to make the discovery and report it to the bank within one year, they are barred from making any claim for recovery against the bank. This applies even if the bank was negligent.

Alterations

Forgers and dishonest employees can easily erase words in small type and cover their erasures with a larger type font. You can help prevent erasure alterations by printing checks using a 12 point or larger type font for the payee name and dollar amount.

Multiple Check Colors

Some companies with multiple divisions or branches use a single bank account against which all checks pay. To differentiate locations, they often use different check colors for each branch. This is not a good practice. When many different colors of checks routinely pay against an account, spotting counterfeit checks by color becomes an impossible task. A bank's Sight Review department cannot be expected to identify a fraudulent or chemically washed item when so many colors are used. Use a maximum of two colors in the same account.

Manually Issued Checks

Every organization occasionally issues manual checks. They are often typed on a self-correcting typewriter. These typewriters use ribbons that are black and shiny. This black shiny ribbon is made of polymer, a form of plastic. Plastic, not ink, is typed onto a check. The white correcting tape is a very durable form of coated transparent tape that lifts the plastic off when errors occur.

Forgers can alter manually issued checks with ordinary transparent tape. They simply lay tape over the letters to be removed, rub the tape lightly with a pen or pencil and lift off the tape. The typed letters are now on the tape, not on the check. Then they type in another payee name and dollar amount and cash the check, which has the original signature!

When issuing manual checks, use a "single strike" fabric ribbon, which can be found in the catalog of major office supply stores. Single strike ribbons ensure that the maximum amount of ink is driven into the fibers of the paper.

Check Stock Controls

Check stock must be kept in a secure, locked area. Change locks or combinations frequently to ensure they have not been compromised by unauthorized individuals. Keep check boxes sealed until they are needed. Inspect the checks upon receipt to confirm accuracy, and then re-tape the boxes. Write or sign across the tape and the box to provide evidence of tampering. Conduct physical Inventory audits to account for every check. Audits should be conducted on a regular and frequent basis by two persons, including someone not directly responsible for the actual check printing. When checks are printed, every check should be accounted for, including voided, jammed and cancelled checks, and those required to align the printer.

Annual Reports and Correspondence

Annual reports should not contain the actual signatures of the executive officers. Forgers scan and reproduce those signatures on checks, purchase orders, letters of credit, and other negotiable documents.

When possible, do not include account numbers in correspondence. Credit applications sent to a new supplier should include the name and phone number of the company's account officer at the bank, but not the bank account number. Nor should an authorized signer on the account sign the correspondence. You have no control over who handles this information once it is mailed or faxed, and it could be used to commit check fraud.

Wire Transfers

Forgers obtain bank account information by posing as customers requesting wiring instructions. These instructions contain all the information necessary to draft against a bank account. To avoid giving out primary account numbers, open a separate account that is used exclusively for incoming credits, such as ACH credits and wire transfers. Place the new account on "no check activity" status and make it a "zero balance account" (ZBA). These two parameters will automatically route incoming funds into the appropriate operating account at the end of the business day, while preventing checks from paying against the account.

Internal Revenue Service

If an embezzlement or check fraud loss does occur, whenever possible, file a 1099 on the perpetrators and let them deal with the IRS for the rest of their natural lives.

There are numerous external and internal threats to an organization's financial integrity. Wisely implementing these safeguards and controls can contain such threats.

Counterfeiters & New Technologies

Counterfeiting corporate checks has always existed. Today's counterfeiters have the availability of sophisticated technology that allows virtually anyone to alter, forge or replicate authentic checks. Desktop publishing software is the largest threat to today's check payment system. Counterfeiters alter or replicate payroll, accounts payable, refund and cashier's checks, even money orders and gift certificates. Several techniques are commonly used to alter legitimate checks or create counterfeit checks.

PCs and Scanners

To make counterfeits appear even more genuine, criminals use scanners to reproduce high-quality check images. Once an original check is scanned into the PC, the counterfeiter can manipulate the entire document. Changing payee information or dollar amounts requires only the push of a few buttons.

Color Copiers

Today's high-end color copiers reproduce color documents that cannot be discerned from the original by an untrained eye, even in side-by-side comparisons. These copiers also make authentic-looking U.S. paper currency.

Desktop Publishing

A PC with desktop publishing capabilities can easily produce high quality checks. A counterfeit check need not exactly match the genuine check in appearance; counterfeiters need only create a check that appears legitimate to the first and last recipients. They often contain accurate routing and Magnetic Ink Character Recognition (MICR) account information. Because many computer systems have MICR ink and fonts, criminals can produce fraudulent checks that will clear the banking system without detection.

Offset Printing

Years ago, counterfeiters used standard offset printing equipment to generate high quality checks. However, the cost of equipment and the technical expertise needed to run the presses have made desktop publishing fraud much more popular.

Cut and Paste and Chemical Alterations

Original documents may be altered by cut and paste methods or by chemicals that dissolve ink. One chemical will completely dissolve the check paper over a period of days, thus destroying all evidence of the fraud.

Authentic checks printed by laser printers can be altered by removing inadequately fused toner from the check with tape. New names or dollar amounts are then inserted.

Mail Order

Criminals use catalogs or order forms from magazines or newspapers to acquire original check stock by mail. Bogus checks may be ordered with a company's correct name and account number and shipped to a P.O. box under a forger's control. While these checks might not look exactly like the company's real checks, the quality is good and they will most likely be accepted as legitimate checks by third parties.

Laser Printers

Once criminals have a high quality image to print, they often use high resolution laser printers or color copiers connected to a personal computer to create authentic-looking checks. Some laser printers use magnetic ink as toner to create a "live" check that easily clears the bank. Off-the-shelf computer systems can be purchased for as little as $20.

Other Cash Management Services

In addition to Positive Pay and Reverse Positive Pay, banks offer other cash management products that help prevent check fraud losses.

Electronic Payment Services

Companies and municipalities can reduce their exposure to check fraud by reducing the number of checks they issue. Electronic funds transfer (EFT), including wire transfers and automated clearing house (ACH) technology for vendor payments and payroll direct deposits eliminate check fraud risk. Virtually all online banking services offer access-restrictive security features. These include primary and secondary levels of authorization and personal identification numbers (PINs). However, even with these levels of security, there are very real risks associated with any electronic payment program. While EFT will eliminate paper check fraud, electronic checks can move seamlessly throughout the world in a day or two, and if there is a loss, electronic audit trails are more time-consuming to trace than are paper trails.

Outsourcing Services

Companies can reduce their check fraud exposure by outsourcing their payables and payroll functions to a bank or other financial services provider. The provider generally assumes responsibility for processing payments on a timely and accurate basis. Because the very nature of outsourcing presumes the company will lose direct control over the disbursement process, the contract should be reviewed carefully to ensure that the service provider assumes liability for check fraud losses for the checks that are issued. If the service provider will not assume the risk, rethink your decision to outsource.

Outsourcing is ideal for companies that want electronic payment methods (ACH/EFT) and electronic data interchange (EDI), but do not want to spend the time or money to develop and maintain an in-house system. EFT payments are very cost-effective in disbursing funds, and completely eliminate the risk of altered checks.

Account Reconciliation

This service has been offered on disbursement accounts for many years. Positive Pay is a daily version of the bank's full month-end account reconciliation. On a daily, weekly, or monthly basis, account reconciliation customers provide the bank with issued check data that are matched to the bank's paid check file. While a month-end review will not catch fraudulent checks quickly enough to prevent a loss, it does provide the company with a timely reconciliation and is an excellent tool to assist in segregating financial duties.

A Primer on Laser Printing

Many companies and municipalities are considering implementing or have already implemented laser printers with Magnetic Ink Character Recognition (MICR) capabilities in their payment process. When proper controls are in place, this rapidly advancing technology creates an efficient platform for printing and distributing checks. Without proper controls, laser printing technology invites financial disaster.

Risks in laser printing environments can be reduced by arming the system with passwords, securing the imaged facsimile signatures, and controlling the check stock.

Password Protection—

is critical for the protection of any computer system. While a skilled and determined hacker may well be able to break through any firewall, a company has significant exposure from dishonest employees. At least two levels of authority (passwords) should be required to print checks, add new vendors and add or change employees and pay rates. Employee passwords should be changed from time to time, and audit procedures must ensure that passwords are never shared.

Generic Check Stock—

that is readily available entirely blank should be avoided. If a printer or computer company will sell you entirely blank generic checks, they are selling the identical blank checks to others, who, in effect, have your check stock! Ensure that your check design is not available entirely blank to others in laser format. Request a blank check stock that is uniquely designed for your company.

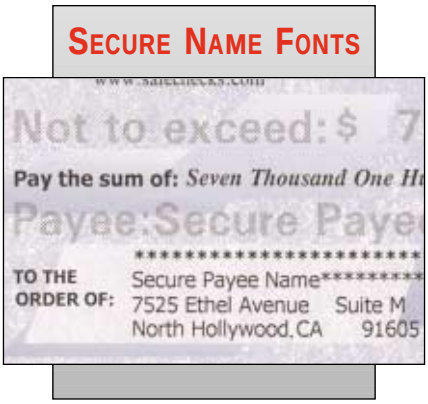
Recent court cases have ruled that issuers using plain checks may have contributed to the alteration or duplication of a check. Issuers of such checks may be held liable for fraud losses resulting from duplications or alterations.

Inventory Control Numbers—

are numbers printed in sequence on the back of all non-pre-numbered laser checks. The control number is completely independent of the check number printed on the face of the check. They are essential on laser check stock that is not pre-numbered because they assist in tracking each sheet and in maintaining compliance with auditors. Insist that your check manufacturer print a sequenced control number on the back of each unnumbered check.

Secure Name Fonts—

help prevent altering the payee name. Payee name alteration is the latest scam among sophisticated forgery rings because it allows them to circumvent Positive Pay. Use a Secure Name Font that uses a unique image or screened dot pattern to print the payee name. The uniqueness of the image is important because forgers have access to all the standard true type and Adobe fonts. Size matters. Large fonts are more difficult to remove without leaving telltale signs. Use a 12 point font or higher, and bold the payee name



Secure Number Fonts—

prevent the dollar amount on the check from being removed or altered without detection. For instance, the dollar amount image can be reversed, that is, printed white on black with the name of the number spelled inside the number symbol. Often the cent amounts are black and white with the letters "CTS" running under each number.

Toner Anchorage—

is a chemical coating applied to the face of the check paper. When the check passes through a hot laser printer, the toner is permanently bonded into the paper. Without it, laser checks can be altered by removing the toner with tape or by scraping. Toner anchorage, also referred to as Laser Lock™ or Toner Grip™, must be specifically requested when ordering laser checks. While it does cost extra, the additional cost is far less than the price of an altered check.

String of Asterisks —

should fill blank payee name areas. Forgers often alter checks by simply adding a new payee name above or after the original payee name. To prevent these alterations, insert a string of asterisks above and after the original payee name.

Facsimile Signatures —

are often applied to a check by the laser printer. When not printing checks, the cartridge containing the signature should be removed and locked in an area separate from the check stock. It must not be left in the printer overnight.

Because a bank's Sight Review or Signature Verification department cannot distinguish an original facsimile signature from one that has been scanned and replicated by a forger, internal check issuing procedures should require that large dollar checks also include an original manual signature. Positive Pay is imperative when checks are not manually signed. See page 2.

Check Security Features

In response to growing concerns about counterfeit checks, the check printing industry has developed a wealth of new security features. In this section, several of the best features are described. While individual security features cannot make checks completely counterfeit-proof, combining several of them, eight or more, into a highly secure check will help deter most criminals. This list is not all-inclusive; new safety features and security check papers are steadily being introduced.

Controlled Paper—

is security paper that is securely distributed and monitored by the paper manufacturer. Insist on a controlled paper stock, as its use will help control fraud. Well organized counterfeiting rings often acquire and use original check paper when making fraudulent checks. The check paper you choose must be very tightly controlled, with limited distribution. Because paper manufacturers try to amortize their fixed costs over a large customer base, there are very few controlled papers. One of the best papers in America is *Pentagon* by Boise Cascade.

Multichemical Reactive Papers—

produce a stain or the word "VOID" in multiple languages when activated with ink eradicator class chemicals, making it extremely difficult to chemically alter a check without detection. Checks should be reactive to at least 18 chemicals.

Multichemical Reactive Papers

Thermochromatic Inks—

react to changes in temperature. Some inks begin to fade away at 78° F and disappear at 85° F. The ink reappears when the temperature cools to 78°. Proper thermochromatic ink cannot be accurately color copied because the copier machine temperature is above 85 degrees, making the ink disappear.

Thermochromatic Ink

Copy Void Pantographs—

are patented designs developed to protect a document from being duplicated. When copied or scanned, words such as "VOID" or "COPY" become visible on the copy, making the copy non-negotiable. This feature can be circumvented by high-end color copiers.

Copy Void Pantographs

Fourdrinier Watermarks

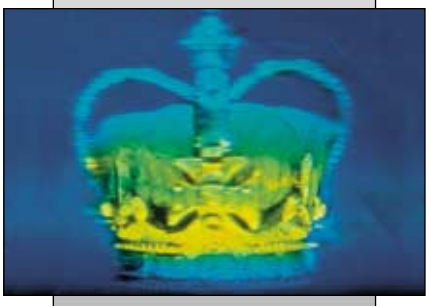
are faint designs pressed into the paper while it is being manufactured. When held to the light, these true watermarks are easily visible from either side of the paper for instant authentication. Copiers and scanners are incapable of duplicating Fourdrinier watermarks.

Fourdrinier Watermarks

Holograms—

are multicolored three-dimensional images that appear in a reflective material when viewed at an angle. They are an excellent but expensive defense against counterfeiting in a controlled environment. Holograms are usually not cost-effective on checks, but are valuable in settings such as retail stores where a salesperson or attendant visually reviews each item before acceptance. Admission passes, gift certificates and identification cards are enhanced by holograms.

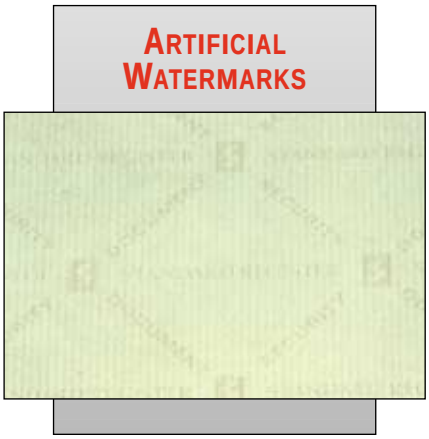
Holograms



Some security features are better than others. This page contains those that are the most useful and effective.

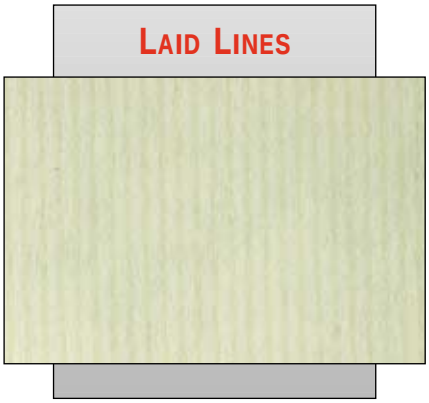
Artificial Watermarks—

are subdued representations of a logo or word printed on the paper. These marks can be viewed while holding the document at a 45 degree angle. Copiers and scanners capture images at 90 degree angles and cannot see these marks.



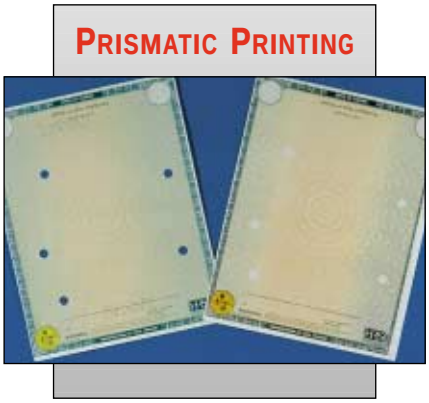
Laid Lines—

are unevenly spaced parallel lines on the back of the check. They make it difficult to physically cut and paste dollar amounts and payee names without detection.



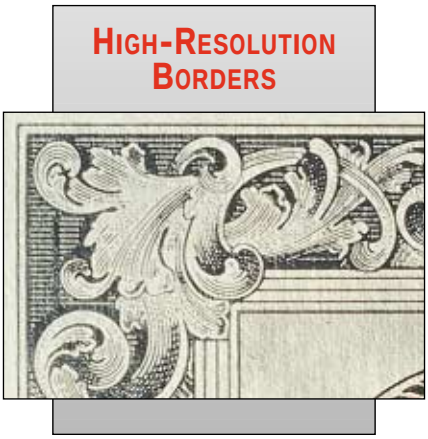
Prismatic Printing—

is a multicolored printed background with gradations that are difficult to accurately reproduce on most color copiers.



High-Resolution Borders—

are intricately designed borders that are difficult to duplicate. They are ideal for covert security as the design distorts when copied.



Microprinting—

is printing so small that it appears as a solid line or pattern to the naked eye. Under magnification, a word or phrase appears. This level of detail cannot be replicated by most copiers or desktop scanners.

High-Security Checks—

help deter check fraud attempts by complicating the criminal's task of altering or replicating an original check.

High-security checks should have at least eight (8) safety features, and more is better. Among the best safety features are a controlled paper that is reactive to at least 18 chemicals, a true watermark, thermochromatic ink, and toner anchorage on laser checks.

Warning Bands—

are printed messages that call attention to the security features that have been added to protect the document. These bands should advise the recipient to inspect a document before accepting it, and may deter criminals from experimenting.

Dual Image Numbering—

creates a red halo around the serial number or in the MICR line of a check. The special red ink also bleeds through to the back of the document so it can be verified for authenticity. Color copiers cannot accurately replicate these images back-to-back.

Safety Papers—

were designed to combat erasures. For years, paper manufacturers sold safety papers with multiple layers of colored fibers. When forgers try to erase the paper, it bleeds. However, generic safety papers are easily obtained from office supply stores and mail order catalogs, severely diminishing their usefulness. Controlled specialty papers are vastly superior because they are much more difficult to obtain and contain additional safeguards.

Recent Court Rulings

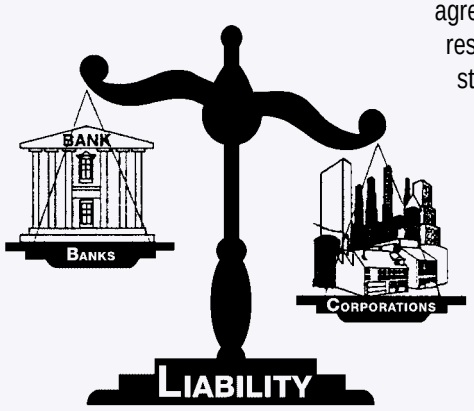
Facsimile Signatures May Invite Fraud Losses

Arkwright Mutual Ins. Co. v. NationsBank, N.A. (South)
Original Case No. 96-2969-CIV-GOLD; (SD Fla. 1999)
Appeal Case 2000 WL 679165,41; Rep.2d 726 (11th Circuit 2000)

In another victory for banks, the Florida 11th Circuit Court of Appeals upheld NationsBank's (now Bank of America) interpretation of its carefully worded Deposit Agreement. This agreement effectively shifted the burden of responsibility from the bank to its customer in cases of forgery. The phrase "purporting to bear the facsimile signature" saved NationsBank over $4 million in losses caused by forged checks.

Florida Power and Light (FPL), a customer of NationsBank, used a facsimile machine to sign most of its corporate checks, nearly 20,000 each month. Unfortunately, 27 fake checks were cashed over a two-month period in 1993, totaling $4,387,057. They bore exact replicas of the facsimile signature and used actual serial numbers from real FPL checks that had been voided or canceled.

Because all of the counterfeit checks were over the $25,000 sight review threshold established by NationsBank, each one was sent to the "signature control department" and compared by hand with the authorized signatures. The fake checks appeared authentic and signatures were identical to the signature card, and therefore were paid "in good faith."



When FPL discovered the counterfeits, they contacted NationsBank, which in turn contacted its upstream collecting banks. However, because the 24-hour rescission period had long since passed, NationsBank was denied its request for reimbursement. It therefore refused to credit FPL's account for the loss.

Arkwright Mutual Insurance, who insured FPL against commercial crime, reimbursed the company. It then sued NationsBank for damages. Arkwright claimed that the checks were not "properly payable" because nothing in the contracts between the two had authorized NationsBank to pay checks with forged facsimile signatures.

NationsBank disputed this, pointing out that FPL had agreed to a provision in its Deposit Agreement that said, "If your items are signed using any facsimile signature or non-manual form of signature, you acknowledge that it is solely for your benefit and convenience. You accept sole responsibility for maintaining security over any device affixing the signature. Such signature will be effective as your signature regardless of whether the person affixing it was authorized to do so."

As part of the Deposit Agreement contract, FPL had passed a resolution authorizing NationsBank to pay checks for $500,000 or less "when bearing or purporting to bear" selected facsimile signatures.

This is extremely significant. Banks are bound by the regulations of the Uniform Commercial Code (UCC), which has historically placed the responsibility for detecting forgery on the bank. However, the UCC also specifically allows a bank and its customers to alter, through contractual agreement, the liability for fraud losses.

"The effect of the provisions of this chapter (4-103) may be varied by agreement, but the parties cannot disclaim a bank's responsibility for its lack of good faith or failure to exercise ordinary care or limit the measure of damages for the lack of failure. However, the parties may determine by agreement the standards by which the bank's responsibility is to be measured, if those standards are not manifestly unreasonable."

In other words, the parties may set their own ground rules as long as it is not overly one-sided.

The Official Comments to Chapter 4-103 expand on this idea:

"…In view of the technical complexity in the field of bank collections, the enormous number of items handled by banks, the certainty that there will be variations from the normal in each day's work in each bank, the certainty of changing conditions and the possibility of developing improved methods of collection to speed the process, it would be unwise to freeze the present methods of operation by mandatory rules. This section, therefore, permits within wide limits variation of the effects of provisions of this Article by agreement…[Subsection [1]] confers blanket power to vary all provisions of this Article by agreements of the ordinary kind."

The Florida court granted summary judgment to NationsBank, agreeing that these two contractual agreements shifted the liability for the forged checks to FPL.

Clearly, the courts are upholding the freedom-of-contract language between a bank and its customers, requiring a company to abide by the agreements it has signed. These legal precedents should encourage banks to be precise when drafting documents outlining customer responsibilities with respect to fraud, and customers to read, fully understand, and agree to "the fine print."

The better course would be to avoid this type of fraud altogether by implementing fraud prevention measures such as Positive Pay and highly secure controlled check stock, which would have caught the forged checks.

Timely Account Reconciliation is Essential

Borowski v. Firstar Bank Milwaukee, NA
579NM2d 247, 35 UCC
Rep.2d 221 (Wis. Ct. App. 1998)

Are you reconciling your bank accounts on a timely basis? A Wisconsin man learned too late that his bank had shortened the timeframe to report unauthorized items, and it cost him $130,000.

UCC 4-406 requires an account holder to exercise "reasonable promptness" in examining monthly statements and reporting unauthorized signatures or alterations. Under the revised UCC, now adopted by all states except New York and South Carolina, "reasonable promptness" is considered 30 days. Subsection (f) sets a one-year outside limit for reporting discrepancies or errors "without regard to care or lack of care of either the customer or the bank."

UCC 4-103 allows for contractual amendments of the UCC rules, provided the bank does not try to disclaim its own negligence. Many banks throughout the country have shortened the one-year timeframe for reporting discrepancies, and in light of the following Wisconsin case, many more are likely to do so.

In Borowski v. Firstar Bank Milwaukee, the account holder, Borowski, maintained two checking accounts with Firstar Bank (now US Bank)—his personal account and an account for his father's estate. Borowski alleged that his fiancè stole $100,000 from the estate account and $50,000 from his personal account, using forged checks, unauthorized telephone transfers, and forged handwritten notes requesting cashier's checks that were left in the bank's night depository box. When the monthly statements and $20,000 in cashier's checks were sent to Borowski, his fiancè intercepted them. When Borowski discovered his loss of both money and faith, he sued the bank to get his money back. (We presume he also called off the marriage, thus mitigating future financial outlays for wedding expenses, divorce attorney fees, and alimony.)

In court, the bank moved for summary judgment based on the signature card agreements on the two accounts. The personal account agreement required that the bank be notified ". . . of any unauthorized or altered item shown on your statement within fourteen (14) days of the statement date." The estate account required notification ". . . of an unauthorized signature or alteration on an item within 14 days after we send or make available to you your statement and items or copies of the items." The bank argued that these two specific provisions completely barred Borowski's claims. For his part, Borowski acknowledged that he had not reviewed the statements because his fiancè intercepted them and then lied to cover their receipt. But he argued that the bank was negligent in the handling of his accounts.

The court ruled in favor of the bank. It found that Borowski's failure to reconcile on a timely basis because of the deception of his betrothed was irrelevant as long as the bank had mailed them to the customer's proper address. The burden of receipt falls upon the customer. The issue of alleged bank negligence was deemed irrelevant because the shortened timeframe to report errors was an allowable contractual variation of the one-year rule, which the bank had made part of the signature card agreement. The court did rule in favor of Borowski regarding the $20,000 in cashier's checks that were issued on the basis of fraudulent hand-written notes, because the bank failed to make those notes available with the bank statement.

A Bank Cannot Contract Away Its Own Responsibilities

Civil Action 96-399
U.S. District Court for the
Western District of Pennsylvania

On June 9, 1997 the director of treasury operations for Kaiser Aluminum and Chemical, Thomas Edwards, spent the day in court defending his firm against an attempt by Mellon Bank to make Kaiser absorb $262,000 in losses from two forged checks. Mellon Bank claimed the firm was liable because it did not use Positive Pay, the bank's electronic check matching service.

Kaiser prevailed, attributing the victory to its tight internal controls, timely reconciliations and good security measures. The company, which issues 11,000 checks a month, keeps its check stock locked up and accessible to only a few persons. While the forged facsimile signatures were good quality, the fraudulent checks did not resemble Kaiser's highly secure checks. Mellon Bank was ordered to pay the cost of the two checks and $26,000 in interest.

The crux of the case rests on two sections of the Uniform Commercial Code, UCC 3-406(b) and 4-103(a). When a bank is not able to establish its customer's negligence, it will bear the loss. Mellon failed to establish Kaiser's negligence. Rather, it relied on an agreement letter with Kaiser that stated "Unless the Bank is negligent or does not act in good faith with respect to its performance of the Service, the Company agrees to hold the Bank harmless and indemnify the Bank from any and all liabilities, losses, claims, or damages…." The court found Mellon's agreement too one-sided, void and unenforceable as a matter of law, and would not allow Mellon to shift to Kaiser the entire risk of loss for the payment of checks bearing unauthorized facsimile signatures.

The Code and other federal law require that a bank seeking "exculpatory or indemnity provisions" must state the intention of the parties with the greatest particularity. Mellon's agreement did not provide for indemnity in the context of forgery loss nor did the language specifically shift the risk of forgery loss in the circumstances of forged facsimile signatures. Banks may cause corporate issuers to bear part of the burden of check fraud losses by using properly worded deposit and facsimile signature agreements.

For example, a bank might state in its disclosure statement that its business customers should ". . . use Positive Pay and high security checks with eight (8) or more safety features. Failure to do so may result in a check fraud loss for which you may be held liable in all or part, based upon the revised Uniform Commercial Code."

Identity Theft Is On The Rise

Identity theft has grown exponentially over the past few years, spurred by the financial rewards, the relative ease of committing the crime, and the low probability of being caught. According to the Federal Trade Commission, nearly 500,000 Americans are victimized each year, costing financial institutions over $5 billion. To clean up one's credit report and associated complications requires an average of $800 and 175 hours.

Stealing wallets or purses was once the primary method to obtain another person's personal information. Today, "dumpster diving," combined with Internet Web sites and search engines, help criminals identify and exploit their victims.

Identity thieves are very brazen. In one incident, the identity thief took out a life insurance policy on his victim. In another incident, an identity thief was arrested after two victims living in the same apartment complex struck up a conversation about their travails. This coincidental conversation ultimately led the police to arrest a person that worked in the business office of the complex and had access to the rental applications and credit reports of present and past tenants.

Criminals gain access to individuals' credit reports by posing as potential landlords, employers or loan officers. They "shoulder surf" at checkout lines and videotape transactions at ATM machines to capture PIN numbers. They steal mail from mailboxes for bank or credit card statements and newly issued credit cards, and "dumpster dive" in trash bins for credit card and loan applications that have not been shredded.

After combining key pieces of individuals' identities, they are able to impersonate their victims and obtain loans and spend money as fast as possible. Generally, victims of banking and credit card fraud will be liable for no more than the first $50 of the loss. However, the victim must notify financial institutions within two days of learning of the loss to avoid being responsible for the fraud activity.

Even though victims are usually not responsible for paying their imposters' bills, their credit report is always left in shambles. It takes months or even years to regain their financial health. In the meantime, they have difficulty writing checks, obtaining loans and housing, and even getting hired. Victims of identity theft seldom find help from the legal authorities as they attempt to untangle the web of deception created by their imposter.

Recommendations

Consider these recommendations to reduce your potential risk of identity theft:

1. Guard your Social Security number zealously. It is the key to your credit report and banking accounts and is the prime target of criminals.

2. Monitor your credit report. It contains your SSN, present and prior employers, a listing of all account numbers, including those that have been closed, and your overall credit score. After applying for a loan, credit card, rental, or anything else that requires a credit report, request that your SSN on the application be truncated or completely obliterated, and your original credit report be shredded before your eyes or returned to you once a decision has been made. (A lender or rental manager needs to retain only your name and credit score to justify his/her decision.)

3. Shred all old bank and credit card statements and "junk mail" credit card offers before trashing them. Use a crosscut shredder. Crosscut shredders cost more than regular shredders but are superior. When Iranian students in Tehran stormed the US embassy in 1979, the embassy staff had shredded the most important documents; however, they used a regular shredder. The enterprising students hired carpet weavers and reconstructed the shredded documents.

4. Remove your name from the marketing lists of the three credit reporting bureaus to reduce the number of pre-approved credit offers you receive.

5. Add your name to the name deletion lists of the Direct Marketing Association's Mail Preference Service and the Telephone Preference Service used by banks and other marketers.

6. Do not carry extra credit cards or other important identity documents except when needed.

7. Place the contents of your wallet on a photocopy machine. Copy both sides of each license and credit card so you have all the account numbers, expiration dates and phone numbers if your wallet or purse is stolen.

8. Do not mail bill payments and checks from home. They can be stolen from your mailbox and washed clean in chemicals. Take them to the post office.

9. Do not print your SSN on your checks.

10. Order your Social Security Earnings and Benefits Statement once a year to check for fraud.

11. Examine the charges on your credit card statements before paying them.

12. Cancel unused credit card accounts.

13. Never give your credit card number or personal information over the phone unless you have initiated the call and trust that business.

14. Subscribe to Privacy Guard or another similar service.

If You Are A Victim

Even though one may take every possible precaution, identity theft still happens. Consider these suggestions:

- Report the crime to the police immediately and get a police report number.
- Keep a log of all conversations with authorities and financial institutions, including names, dates, and time.
- Call your credit card issuers immediately, and follow up with a letter and the police report.
- Notify your bank immediately.
- Call the fraud units of credit reporting companies to place a fraud alert on your name and SSN.

References

- Federal Trade Commission:
  877-IDTHEFT (877-438-4338)
  www.ftc.gov
  www.consumer.gov/idtheft/
  www.consumer.gov/sentinel/
- Privacy Guard:
  800-374-8273
  www.privacyguard.com
- Privacy Rights Clearinghouse:
  619-298-3396
  www.privacyrights.org
- Identity Theft Resource Center:
  858-693-7935
  www.idtheftcenter.org
- Equifax:
  800-525-6285
  P.O. Box 740250
  Atlanta GA 30374
  www.equifax.com
- Experian (once TRW):
  888-397-3742
  P.O. Box 1017
  Allen, TX 75013
  www.experian.com
- Trans Union:
  800-680-7289
  P.O. Box 6790
  Fullerton, CA 92634
  www.tuc.com
- Social Security Administration Fraud Line:
  800-269-0271
- CheckRite: 800-766-2748
- ChexSystems: 800-428-9623
- CrossCheck: 800-552-1900
- National Processing Co. (NPC):
  800-526-5380
- SCAN: 800-262-7771
- TeleCheck: 800-710-9898

False Identification

A person obtains false identification because they have something to hide, such as their age or their true identity. Our society's primary threat from false identification is not from under-age students trying to buy alcohol or illegal immigrants seeking honest employment.

Today's threat is from a more insidious group—ex-convicts, sexual predators, terrorists, and the like. New laws allowing public notification of sexual predators' identities and addresses, and stepped up Homeland Security efforts against potential terrorists are serious issues, and will fuel the demand for false identification.

To change identities, the best form of "legitimate" identification is a driver's license and a Social Security card. A person can easily obtain both of these documents after getting a birth certificate through a county's Department of Vital Records. A clean, unencumbered birth certificate can be obtained by using the birth information taken from the death certificate of an infant or young child because the two departments (birth certificates and death certificates) are often unconnected. The solution is to mark "DECEASED" on the birth certificates of people who have died.

In many states, birth certificates and death records are part of the public record and are readily available for the asking. In other states, only the next of kin or an attorney can request a birth certificate. For purposes of obtaining a birth certificate, however, one need not attend law school to "become" an attorney. Simply printing up cards and stationery at a local quick print shop or visiting a legitimate attorney's office to obtain a business card can provide anyone with sufficient legal legitimacy.

The policies controlling birth certificates at many counties' Department of Vital Records (DVR) were designed decades ago to accommodate the honest public. Today, these out-dated policies often assist criminals by providing them with authentic birth certificates that are then used to create false identities and commit crimes. In creating these false identities, criminals know no shame. Not long ago, the director of the DVR in a large metropolitan area admitted to being aware of instances when unknown individuals requested and obtained half a dozen different birth certificates at one time!

Maintaining a computerized log of persons and addresses that requested birth certificates, and taking thumbprints of individuals appearing in person to obtain a birth certificate may help deter criminal activity.

Frank Abagnale's Document Verification Manual (pictured left) contains information useful to help authenticate a person or a document. The manual has full size, full color specimens of all U.S. and Canadian driver's licenses, traveler's checks, money orders and credit cards, and a Social Security number reference chart, etc.

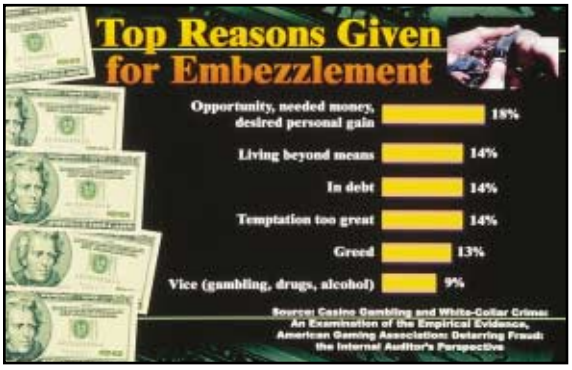
For more information, call (800) 237-7443 or visit www.abagnale.com and click on products.

Preventing Embezzlement

If you make it easy for people to steal from you, they will.
- Frank W. Abagnale

For the past 25 years, the accounting firm KPMG International has surveyed the top 1000 firms in the United States, asking them to rank the crimes that hurt their company the most, both internally and externally. KPMG does not ask how many dollars were lost, only the ranking of the types of crime.

Since the survey began, embezzlement has ranked Number 1 among these firms. Check fraud did not make the list until 10 years ago, when it ranked ninth. Today, it ranks Number 2.



Under the revised Uniform Commercial Code (UCC), employers have sole responsibility for the actions of their employees. Employers are in a far better position to avoid losses by carefully selecting and supervising their employees, and by adopting other internal fraud prevention measures. By strictly following basic internal financial controls, companies can prevent or substantially reduce these crimes.

Hiring Practices

Use hiring procedures that keep people with questionable backgrounds out of your organization. Thoroughly check all references. Confirm employment dates and look for time gaps in a résumé. When filling positions in sensitive areas, conduct complete background checks. Use bonded temporaries in financial functions.

Prevent ghost employees and improperly altered pay rates by restricting access to the personnel master file records. Adding new employees or changing pay rates should require supervisory approval and supporting documentation.

Establish internal procedures to prevent the theft of incoming or outgoing checks. Mail room personnel must have clean backgrounds. Bonding makes sense. Many crime victims have traced the source to their own mail rooms!

Controlling Check Stock

Establishing tight controls over the storage and distribution of check stock is essential in preventing the theft and unauthorized use of corporate checks. Under Articles 3 and 4 of the UCC, if a bank customer is negligent with their checks, and if that negligence contributes substantially to a forgery, the bank may have no liability.

All check reorder forms and checks, whether preprinted or entirely blank, must be stored in a locked area, cabinet, or room with access restricted to only those persons responsible for issuing checks. Only these people should have keys or combinations to the secure storage area. Maintain a detailed inventory log of all checks received into the supply area. Conduct a physical inventory at least quarterly and account for every check. Keep check boxes sealed until they are required for use. Turn the sealed boxes over monthly to verify that the bottom has not been sliced open and checks removed. Cleaning crews must not have access to the area where checks are stored. Change keys and combination locks that safeguard checks annually.

Empty the printer after every check run and return them to the locked storage area. If unused checks from the last check run are not immediately returned to secure storage, an unauthorized employee or a cleaning crew member could find the checks in the printer and use them for unauthorized purposes. Emptying the printer seems obvious, but it is a practice frequently overlooked.

True Story: A major apparel maker in the Northwest fell victim to a scam involving the theft of a few blank checks left behind from a check run. The company was initially puzzled over how the checks could have been stolen, but a review by an accounts payable audit firm revealed that the source of the stolen checks was an unemptied printer tray.

Zero-amount checks and checks that have been cancelled or voided should immediately be written or stamped with "void" or "cancelled." Cancelled or voided checks should not be left unattended in someone's In-box. Someone other than the accounts payable processor who made the original transaction should be responsible for handling voided or cancelled checks. When shredding negotiable documents, have two people present, or use a bonded shredder.

Timely Reconciliations

Timely account reconciliation is an extremely important control to prevent embezzlement and detect check fraud. Checking accounts should be reconciled as soon as the bank statement arrives. The reconciliation should be reviewed by the appropriate manager, with any discrepancies investigated immediately. It is the account holder's responsibility to ensure that statements are received, reconciled and reviewed for any forged or altered checks. Suspicious items must be reported to the bank immediately.

True Story: The payroll department of a city in the West had a practice of throwing checks that had been crumpled by the printer into the trash without voiding them. The cleaning crew retrieved those checks, forged signatures, and cashed them for large amounts of money. The thefts were not discovered until the account was overdrawn, but by then, over $1,000,000 was stolen. The city, it was discovered, had not reconciled its accounts in over six months, and its own practices had contributed substantially to the loss. The bank lost the customer, but was not liable except for the first few checks.

Holder in Due Course

Obsolete check stock should be destroyed as soon as possible and never left unattended. Some people believe there is no need for concern about checks drawn on a closed account. This is not true. Checks are checks and must be kept under lock and key. Although an account may be closed, someone could steal and pass the old checks to an unsuspecting third party. Under the UCC, a "holder in due course" could successfully sue the check maker, who would be deemed

negligent and held responsible for the loss. (Visit www.FraudTips.net.)

Accounts Payable and Payroll Controls

The payroll and accounts payable functions are particularly vulnerable to embezzlement, and controls over those functions are needed to prevent payments to ghost employees or vendors. Corporations are totally responsible for any unauthorized payments made by a dishonest employee.

To help identify and reduce exposure to fraud in the payables area, engage an accounts payable audit firm with the experience to properly audit this area. The better firms provide a detailed review of a company's disbursement procedures as part of their audit, which is generally conducted on a no-fee contingency basis.

Vendor Master File

Protect the accounts payable and procurement functions by controlling how vendors are added to the system and how invoices are processed. Access to the vendor master file records should be tightly restricted. Changing vendor records or adding new vendors should require supervisory approval and supporting documentation. Someone independent of the buying and payment processing functions should review all new supplier entries. The review should always include a telephone call to the new supplier using a phone number obtained from an external directory source such as 411. Verify the name, address, and Federal tax ID number.

Payroll controls should ensure that only legitimate employees can be added to the system and that the rate of pay cannot be changed without supervisor approval and supporting documentation.

Vendor Payments

Checks should always be mailed directly to the vendor or payee, and not returned to the requesting operating unit, department, division, or branch office. Returning checks to the requester is open invitation for fraud because of the risk of alteration.

True Story: An employee of a large company was caught altering payees on checks intended for charities. Because the charitable contributions were within budget, and because charities don't invoice, nothing was missed. The embezzlement was found by an accounts payable auditor.

Audits

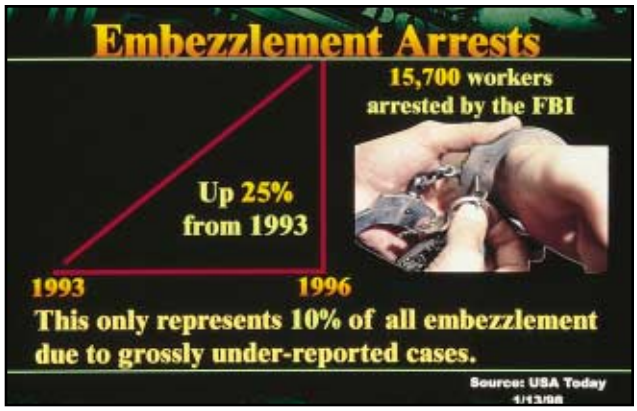
Conduct periodic surprise audits of the various check control functions. Audits should test the overall system to ensure that it is functioning as it should. Independent, experienced individuals trained in software systems and theft detection should conduct these audits.

Create audit trails by restricting access to the master file records. Most computer systems can create an audit trail of all changes made to the master file records, including who made them and who approved them. Someone independent should regularly print and review a report detailing the changes. This report is sometimes referred to as an "access matrix." The access matrix should list each person with system access and the person's level of access by module. Comparing the access authority of each employee should be part of this review. Determine a standard "access profile" for each employee position and restrict the master file records to these persons. Immediately delete the names of employees who are terminated or have their positions modified, and investigate any unusual or suspicious activity.

True Story: A major manufacturer discovered that an accounts payable supervisor had edited a supplier record in the master file before the accounts payable checks were printed. The employee had access to set up and edit records in the supplier master file, but the oversight function was not in place. A vendor's name had been changed to the employee's mortgage company, along with a reference to his loan number. Most mortgage companies accept large principal reductions outside of regular monthly payments only with specific written instructions to do so. Since the employee could not intercept mailing of the payment, a written note was not included. The fraud was discovered when the mortgage company returned the check to the manufacturer.

Separate Financial Responsibilities

Make sure separate groups of people are responsible for the accounts payable, accounts receivable, and banking functions. Divide financial responsibilities to ensure that the people adding new vendors to the master vendor file are not approving invoices for payment. The people issuing checks should not reconcile the account. If duties are not separated, a dishonest employee could issue a check to him or herself or to a co-conspirator, remove the check from the bank statement, and adjust accounting records to hide the embezzlement. Receipts and deposits must balance each day, and separate people should perform these duties to prevent forged endorsements.



Mailed checks that are returned by the Post Office as undeliverable should not be returned to the person who wrote them. Someone independent from the disbursement process should handle these exceptions and investigate the reason for their return. A separate post office box should be established for returned checks. Replace your company name and address on disbursement envelopes with a simple post office box number.

True Story: An uncashed disbursement check was returned to an accounts payable clerk because she originated the invoice entry. The clerk put the check in a desk drawer and forgot about it for several months. Upon cleaning her desk, she discovered the returned check. When she checked the paid history, she realized the supplier had returned the check when it was determined to be a duplicate payment of an invoice. She also noticed that the payee name had been printed slightly below "Payee" on the check. With a bit of effort she managed to align the check and insert her name above the original payee in a print similar to the original, along with "or" following her name. An accounts payable auditor searching for duplicate payments discovered the fraud. The auditor was asked by the supplier to provide copies of both cancelled checks as proof of duplicate payment. This example is another reason to engage a qualified accounts payable audit firm to review your disbursements.

Frank W. Abagnale & Associates
P.O. Box 701290
Tulsa, Oklahoma 74170-1290
(800) 237 7443
www.abagnale.com