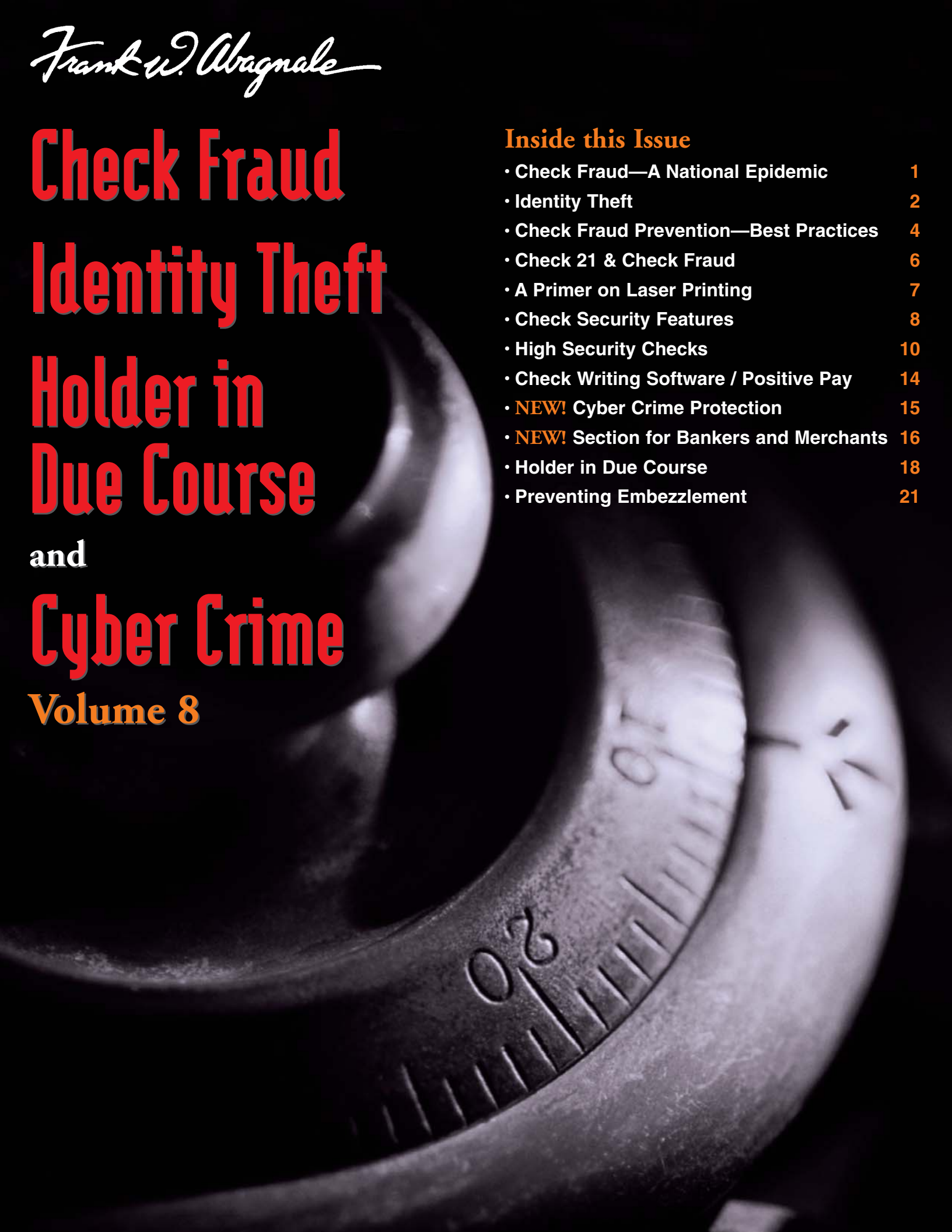
Frank W. Abagnale

# Check Fraud Identity Theft Holder in Due Course and Cyber Crime

## Volume 8



### Inside this Issue

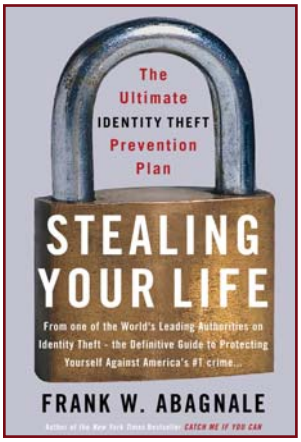
# Frankly Speaking . . .

Some of the most serious financial crimes in America are check fraud and identity theft. The Nilson Report estimates check fraud losses to be about $20 billion a year. Check fraud is by far the most dominant form of payment fraud and produces the greatest losses. Check fraud gangs are hardworking and creative. They constantly try new techniques to beat the banking system and steal money. Historically, the banks have been liable for these losses. However, changes in the Uniform Commercial Code now share the loss with the depositor.

The Federal Trade Commission reported that nearly 15 million Americans have been victims of identity theft, costing consumers $5 billion and banks and businesses $56 billion every year. Because this crime 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 your visit to a 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. They copy your insurance card, which includes your Social Security number. Your co-pay is paid with a check drawn on your bank account. You have just provided enough information for someone to become you.

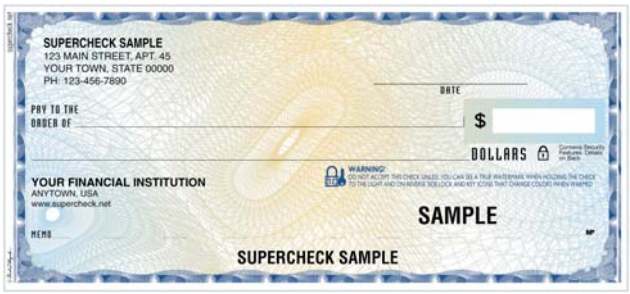
Another example. You walk into an upscale department store to make a purchase. You take your selection to the cashier and write a check. On that check is your name, address and home phone number, the name of your bank and its address, and your bank account number. The cashier asks for your driver's license.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




I am 61. 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 youth, 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, 40 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 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 provide is someone's name, address and DOB—and they will tell you everything you want to know, including spouse and children's names.




www.supercheck.net

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 "…I did not apply for that loan." You must prove you did not apply for that 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 am 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/frank) provides me with the contact information of any company that obtained my credit report, as well as the means to correct false data. 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 three books, *The Art of the Steal, The Real U Guide to Identity Theft* and *Stealing Your Life* that cover numerous scams and solutions in detail. For individuals concerned about check fraud, I designed the **Supercheck**, a high-security personal check with 12 safety features. I also designed the **SuperBusinessCheck** and **SAFEChecks** for companies and organizations that want extremely secure checks.

**See Pages 10 through 13.**

Sincerely,

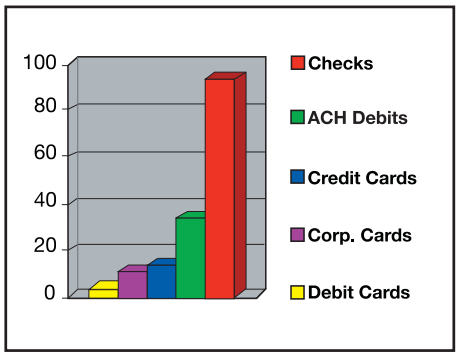
Frank W. Abagnale

# Check Fraud–A National Epidemic

Mark Twain wrote in 1897, "…the report of my death was an exaggeration." So, too, was the predicted demise of the paper check in 1973. Now, 35 years later, not only are checks still being used, they represent the largest category of non-cash payment instruments. Not surprisingly, check fraud – the paper check's evil twin – is the most dominant method of fraudulent payments, and produces the greatest losses. Check fraud continues to be one of America's most serious and least prosecuted financial crimes, and every checking account holder, company, and organization is at risk of becoming a victim.

In the *Payments Fraud and Control Survey* released by the Association of Financial Professionals (AFP) in March 2005, 55% of the organizations who responded confirmed that they had been a victim of payments fraud. The vast majority – 94% – indicated they were victims of check fraud. This was true whether the organization was large or small.

**Percentage of Fraudulent Payments**



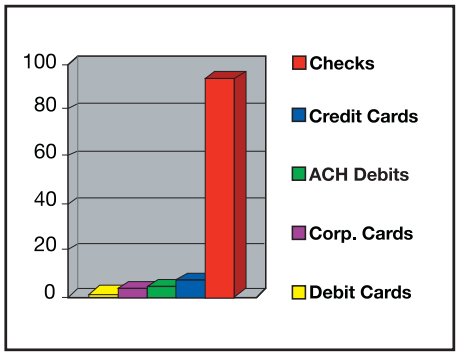

In the AFP survey, only 7% of the companies reporting a fraud attempt did not lose money. In other words, 93% of those reporting a fraud attempt did lose money. This data supports Mr. Abagnale's conclusion: **"Prevention is the only viable course of action."**

A past Nilson Report said that annual check fraud losses now exceed $20 billion, up from $5 billion in 1993. BankInfoSecurity.com stated in November 2007 that while reported check fraud cases decreased between 2003 and 2006, the average loss per case increased 57%, from $1,098 to $1,727.

## Risk Management

These statistics show that financial institutions and checking account holders face a substantial shared risk from check fraud. 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?"

**Percentage of Greatest Fraud Losses**




## Uniform Commercial Code Revisions Shift Liability

The legal basis for liability in check fraud losses is found in the Uniform Commercial Code (UCC), which was revised in 1993. The UCC now places responsibility for check fraud losses on both the bank and its customers. Responsibility for check issuers and paying banks falls under the term "ordinary care." Ordinary care requires account holders to follow "reasonable commercial standards" prevailing in their area and for their industry or business. 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 with an authorized signature. If a signature is forged, the account holder may still be liable if one of the following exceptions applies:

First, if account holders' own failures contributed to a forged or altered check, they may be restricted from seeking restitution from the bank. 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 the bank statements being mailed.

Second, 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 controls 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.

## Stop Payments and Holder in Due Course

Placing a Stop Payment on a check does not end your liability to pay the check. Holder in Due Course trumps Stop Payments and Positive Pay exception items. **See Page 18, Robert J. Triffin vs. Cigna Insurance Co.**

Further, a company can be held liable for counterfeit items that look virtually identical to its original checks. **See Page 18, Robert J. Triffin vs. Somerset Valley Bank and Hauser Contracting Co.**

## Read Bank Contracts

Read your bank contracts to understand your liability for fraud losses under the revised Uniform Commercial Code. This specifically includes the small print on signature cards and disclosure statements. It is clear from recent court cases involving fraudulent checks that a bank's intentions must be stated clearly to prevail in a check fraud case against a customer. Accordingly, banks are re-writing their signature card agreements to include new provisions and requirements in their disclosure statements. For a summary of the revised UCC, visit www.FraudTips.net.

## Remotely Created Checks

Remotely created checks (RCC), also referred to as "demand drafts", "preauthorized drafts," or "telephone checks" are created by the payee on the authority of the account holder on which the check is drawn. In place of a signature, the check bears a statement in the signature area that the account holder authorized the check. They serve a useful purpose in that consumers can pay bills and avoid late charges, or purchase goods over the phone. Because remotely created checks are vulnerable to fraud, the bank that accepts a fraudulent RCC is liable for any losses. Read more at www.FraudTips.net and click on Remotely Created Checks.

# 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 15 million Americans are victimized each year, costing consumers $5 billion, and banks and corporations $56 billion every year. To clean up one's credit report and associated complications requires an average of $1173 and 175 hours.

Stealing wallets or purses is still 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.

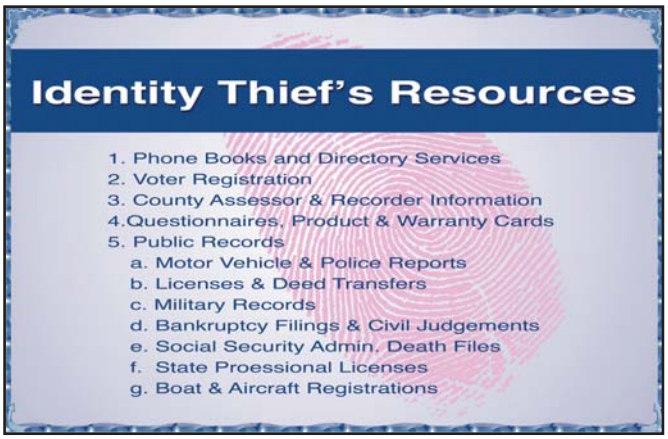
Criminals gain access to individuals' credit reports by posing as potential landlords, employers or loan officers. They "shoulder surf" at checkout lines and videotape transactions at ATM machines to capture PIN numbers. They steal mail from mailboxes for bank or credit card statements and newly issued 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, obtain loans and steal the money.

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.

Contrary to popular belief, even people with bad credit can be victims of identity theft.

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 fraudulent 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 a job. Victims of identity theft seldom find help from the legal authorities as they untangle the web of deception created by their imposter.




## Recommendations

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

### Social Security Number

1. Guard your Social Security number vigilantly. It is the key to your credit report and is the criminals' prime target.

2. Do not print your SSN on your checks.

3. Order your Social Security Earnings and Benefits Statement once a year and look for employers you didn't work for. Someone may be using your identity for a job.

4. Monitor your credit report. It contains your SSN, present and past employers, a listing of all account numbers, including those that have been closed, and your 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 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.)

### Internet / Computers

5. Make sure your computer is protected with Internet security software that is updated regularly. **See Cyber Crime, Page 15**.

6. Do not download anything from the Internet that you did not solicit. Activate the pop-up blocker on your computer.

7. Shop only on secure websites. The web address should begin with https://. It must have the "s" or it is not a secure site. You can also look for a padlock or key in the bottom right corner of your screen.

8. Avoid using a debit card when shopping online. Credit cards have a maximum liability of $50 for fraudulent charges; debit cards can go up to $500 or more.

9. Use a strong password. While it is easier for you to have one that is simple, it is also easier for crooks.

10. When possible, choose to have a second-level password on an account. Choose a password that is more difficult.

11. Never leave your laptop anywhere you wouldn't leave your baby….in the car, in a gym bag, at a restaurant. According to Amitron.org, stolen laptops and computers account for nearly 40% of security breaches.

12. Before donating your computer to a recycling center, completely wipe out all confidential information. This requires special software, and more than just reformatting.

### Credit Cards

13. Shred old bank and credit card statements, "junk mail" credit card offers and old tax returns. 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 their most important documents; however, they used a regular shredder. The enterprising students hired carpet weavers and they reconstructed the shredded documents.

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

15. When you are shopping or dining, be aware of how salespeople or waiters handle your card. Make sure they do not have a chance to copy your card.

16. Examine the charges on your credit card when your statement arrives. Also, keep track of the billing cycles of your cards. If a statement doesn't arrive when it should, it could mean that a thief has changed the mailing address on your account.

17. Minimize the number of credit cards you own to reduce the opportunity for a criminal to steal a card.

18. Carry extra credit cards or other identity documents only when needed.

19. Shred the card on unused credit card accounts. If you close the account, it may lower your credit score because of reduced credit availability.

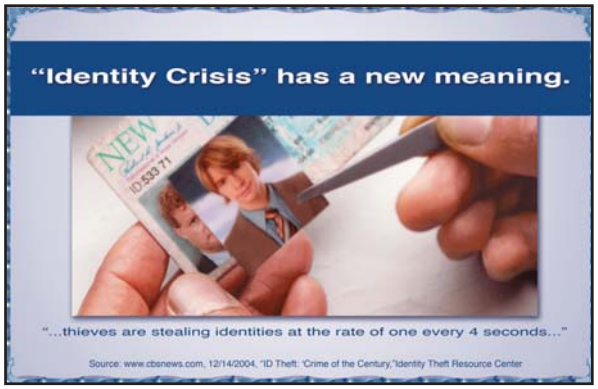
20. Put a fraud alert tag on your credit report, which will limit a thief's ability to open accounts in your name.

**Bank Accounts/Checks/PINS**

21. Use high security checks like those shown on **Pages 10 – 13**. Criminals "wash" ordinary checks in chemicals, dissolving what you wrote without affecting the check. When the check is dry, forgers insert new data. High security checks react to chemicals, showing that they have been washed.

22. Do not mail checks from home. They can be stolen from your mailbox, chemically washed and re-used. Go to the post office.

23. When writing manual checks, use the uni-ball® 207 gel pen. Its ink will not dissolve in chemicals.




24. When writing manual checks, use the uni-ball® 207 gel pen. Its ink will not dissolve in chemicals.

25. Protect your PIN. Forgers steal wallets and cell phones, then sort through the contacts for the spouse. They then send a text message to the spouse asking to be reminded of the PIN.

**Miscellaneous**

26. Be highly suspicious of unsolicited emails or letters that say you won money.

27. Remove your name from the marketing lists of the three credit reporting bureaus to reduce pre-approved credit offers.

28. Add your name to the Name Deletion List of the Direct Marketing Association (www.dmachoice/consumerassistance.php).

29. Subscribe to Privacy Guard or another similar service to alert you if your credit history is being requested.

30. Avoid ATMs that are not connected to a bank or a reputable business. Shield the keypad when entering your PIN.

31. Protect your incoming mail by picking it up ASAP. If you will be away for a period of time, have your mail held at the post office.

32. Keep your purse or wallet in a locked drawer at work. Find out how the company protects your personal information, and who has access to your direct deposit information.

33. Photocopy and retain the contents of your wallet. Copy both sides of each license and credit card so you have the account numbers, expiration dates and phone numbers if your wallet or purse is stolen.

34. Keep Social Security cards, birth certificates and passports in a locked box.

35. Read the privacy policies of the companies with whom you do business. Opt out of having your information shared.

36. Protect a dead relative. Contact the credit bureaus and put a "deceased" alert on the person's reports. Send copies of the death certificate to institutions where the person had an account.

## Check Fraud Scam Alert

Thousands of people have been burned by a simple check fraud scam. It involves checks that look real to consumers and tellers, but are counterfeit. There are several variations, but the basic scam works like this: You receive a letter in the mail, often preceded by an email, announcing that you have won a large prize, award, lottery, etc. The letter includes a real-looking check. You are told that taxes must be pre-paid on the award, but the enclosed check includes the taxes and a portion of your award. It is explained that once you have paid the taxes, the balance of your award money will be mailed to you. You are instructed to deposit the check, wire transfer the tax portion of the money to the company that sent you the check, and to keep the balance.

Of course, the check is bogus and is returned unpaid. You are liable to the bank for the dollar amount of the check, which is charged back to your account. Moral: If something seems too good to be true, don't deposit the check! Search "check fraud scams" on the Internet.

## All the resources you need. All in one place.

Even though you may take every possible precaution, identity theft can still happen to you. Consider these suggestions:

- Report the crime to the police immediately and get a copy of the police report.
- Keep a record of all conversations with authorities, lending and financial institutions, including names, dates, and time of day.
- 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 agencies to place a fraud alert on your name and SSN.

## Resources

- Equifax:
  1-800-525-6285
  www.equifax.com
- Experian:
  1-888-397-3742
  www.experian.com
- TransUnion:
  1-800-680-7289
  www.transunion.com
- Federal Trade Commission:
  1-877-IDTHEFT (877-438-4338)
  www.consumer.gov/idtheft
- Privacy Guard:
  1-866-482-7363
  www.privacyguard.com/frank
- Privacy Rights Clearinghouse:
  1-619-298-3396
  www.privacyrights.org
- Fight Identity Theft:
  info@fightidentitytheft.com
  www.fightidentitytheft.com
- Identity Theft Resource Center:
  1-858-693-7935
  www.idtheftcenter.org
- National White Collar Crime Center:
  1-800-221-4424
  www.nw3c.org
- Social Security Administration
  1-800-269-0271
  www.socialsecurity.gov
- U.S. Postal Service:
  1-800-275-8777
  www.usps.com/postalinspectors

# 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 discourage a criminal from attempting fraud, and can thwart his counterfeiting efforts. The following are recommendations for reducing risk.

## Positive Pay

One of the most effective check fraud prevention tool is Positive Pay, an automated check-matching service that is unparalleled in detecting most bogus checks. It is offered through the Cash Management Department of many banks. To use this service, the check issuer transmits to the bank a file containing information about the checks it has issued. Positive Pay compares the account number, the check number, dollar amount and sometimes payee name on checks presented for payment against the list of checks issued and authorized by the company. All the components of the check must match exactly or it becomes an "exception item." The bank contacts the customer to determine each exception item's authenticity. If the check is fraudulent or has been altered, the bank will return the check unpaid, and the fraud is foiled. For Positive Pay to be effective, the customer must send the data to the bank before the checks are released.

Because 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 high security checks with Positive Pay, the risk and liability for check fraud are substantially reduced. Many banks charge a modest fee for Positive Pay, which should be regarded as an "insurance premium" to help prevent 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 review in-clearing checks daily to identify unauthorized items. The account holder downloads the list of checks from the bank and compares them to the issued check file. Suspect checks must be researched and the bank notified of items to be returned. While Reverse Positive Pay provides timely 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. Several banks have developed Payee Positive Pay (PPP) that also compares the payee name. PPP identifies the payee line by 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 because of added Payees above the X, Y field. A Secure Name Font stops added Payees. **See Page 7 and 14.**

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

## ACH Filter or Block

Forgers have learned that Positive Pay doesn't monitor electronic "checks," also known as Automated Clearing House (ACH) debits. Files containing ACH debits are created by an organization or company and submitted to its bank. The bank processes the file through the Federal Reserve System and posts the ACH debit against the designated accounts. Because paperless transactions pose substantial financial risk, most banks are careful to thoroughly screen any company that wants to send ACH debits. However, some dishonest individuals still get through the screening process and victimize others. Banks have liability for allowing these lapses.

To prevent electronic check fraud, ask your bank to place an ACH block or filter on your accounts. 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 allows 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. ACH block all other accounts.

## Preventing Added Payees

Adding a new payee name is a major scam used by sophisticated forgery rings. They understand the limitations of Positive Pay and simply add a new payee name above or beside the original name. To help prevent added payee names, insert a row of asterisks above the payee name, or use a Secure Name Font **(see example Page 7)**. To help prevent altered payees, use high security checks like **SAFEChecks** or the **SuperBusinessCheck**, and good quality toner to keep the asterisks and **Secure Name Font** from being removed.

## High Security Checks

Check fraud prevention begins with high security checks. Checks are the first line of defense, and help prevent altered payee names or dollar amounts. There is substantial evidence that high security checks motivate criminals to seek softer targets.

High security checks should contain at least ten (10) safety features. More is better. **Pages 10 through 13** show high security checks designed by Frank Abagnale. Many check manufacturers claim their checks are secure because they include a printed padlock icon. The padlock icon does not make a check secure, since only three safety features are required to use the icon.

Some legal experts suggest that the failure of a business to use adequate security features to protect its checks constitutes negligence. By using high security checks, a company can legally demonstrate that care has been taken to protect its checks.

## Check Washing

Washing a check in chemicals is a common method used by criminals to alter a check. The check is soaked in solvents to dissolve the ink or toner. The original data is replaced with false information. When a check reacts to many chemicals, the "washing" can be detected when the check dries. To defend

against washing, use checks that are reactive to many chemicals. Chemically reactive checks become spotted or stained when soaked in chemicals. A Chemical Wash Detection Box on the back of the check warns recipients to look for evidence of chemical washing. **See Page 13.**

## Prompt Reconciliation

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 disclosure agreement that details the length of time you have to report discrepancies on the bank statement. Some banks have shortened the reporting 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 or accountant and have the bank statements mailed to them directly.

## 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.

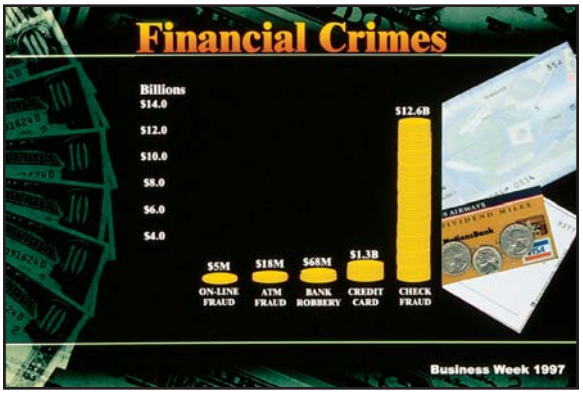
The one-year rule is another important guide. Bank customers are obligated to discover and report a forged signature on a check within one year, or less if the bank has shortened the one-year rule. If the customer fails to make the discovery and report it to the bank within one year, they are barred 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 printed in small type and cover their erasures with a larger type font. Prevent erasure alterations by printing checks using a 12 or 14 point font for the payee name, dollar amount, city, state and zip code. **See Page 7 on Laser Printing.**

## Multiple Check Colors

Some companies with multiple divisions or branches use a single bank account against which all checks pay. To differentiate locations, they use different check colors for each branch. This is not a good practice. When many colors of checks 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 many colors are used. Use a maximum of two colors in the same account, and find other ways to differentiate locations.




## Manually Issued Checks

Every organization occasionally issues manual checks. Some are typed on a self-correcting typewriter. These typewriters use ribbons that are black and shiny. These black shiny ribbons are made of polymer, a form of plastic. Plastic is typed onto a check.

Forgers can alter manually issued checks with ordinary translucent tape. They simply lay tape over the letters to be removed, rub the tape firmly 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, with the original signature!

When issuing manual checks, use a "single strike" fabric ribbon, which uses ink, not polymer. They can be found in the catalog of major office supply stores. Single strike ribbons maximize the ink driven into the fibers of the paper by the typewriter.

## 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 when received 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 used to align the printer.

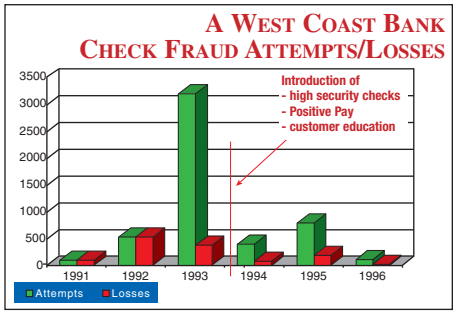
## Annual Reports and Correspondence

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, etc.

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 fraud.

## Wire Transfers

Forgers obtain bank account information by posing as customers requesting wiring instructions. Wire 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, and prevent unauthorized checks from paying.




*Check fraud attempts and losses fell by 95% over three years after a West Coast bank educated its customers and introduced high security checks and Positive Pay.*

# Check 21 & Check Fraud

Check Clearing for the 21st Century Act, aka "Check 21" was passed into law October 28, 2004. Check 21 allows banks to 1) convert original paper checks into electronic images; 2) truncate the original check; 3) process the images electronically; and 4) create "substitute checks" for delivery to banks that do not accept checks electronically. The legislation does not require a bank to create or accept an electronic check image, nor does it give an electronic image the legal equivalence of an original paper check.

Check 21 does give legal equivalence to a "properly prepared substitute check." A substitute check, also known as an image replacement document (IRD), is a new negotiable instrument that is a paper reproduction of an electronic image of an original paper check. A substitute check 1) contains an image of the front and back of the original check; 2) bears a MICR line containing all the information of the original MICR line; 3) conforms to industry standards for substitute checks; and 4) is suitable for automated processing just like the original check. To be properly prepared, the substitute check must accurately represent all the information on the front and back of the original check, and bears a legend that states "This is a legal copy of your check. You can use it the same way you would use the original check." While Check 21 does not mandate that any check be imaged and truncated, all checks are eligible for conversion to a substitute check.

## Warranties and Indemnity

Check 21 does not require a bank to convert and truncate paper checks. It is voluntary. A bank that chooses to convert a paper check into an electronic image and substitute check provides two warranties and an indemnity that travel with the substitute check. The two warranties are 1) that the substitute check is properly prepared, and 2) that no bank will be asked to make payment on a check that has already paid (no double debit).

The Indemnity is very powerful, and gives banks and companies a clear defensive strategy against losses caused by substitute checks. It may also deter banks and companies eager to convert high-dollar checks. The warranties and indemnity continue for one year from the date the injured party first learns of the loss[1].

The Final Rule issued by the Federal Reserve Board states, a bank "that transfers, presents, or returns a substitute check…shall indemnify the recipient and any subsequent recipient…for any loss incurred by any recipient of a substitute check if that loss occurred due to the receipt of a substitute check instead of the original check."[2] It goes on to say that if a loss "…results in whole or in part from the indemnified party's negligence or failure to act in good faith, then the indemnity amount …shall be reduced in proportion to the amount of negligence or bad faith attributable to the indemnified party." The indemnity would not cover a loss that was not ultimately directly traceable to the receipt of a substitute check instead of the original check.

The Fed gives this example. "A paying bank makes payment based on a substitute check that was derived from a fraudulent original cashier's check. The amount and other characteristics of the original cashier's check are such that, had the original check been presented instead, the paying bank would have inspected the original check for security features and likely would have detected the fraud and returned the original check before its midnight deadline. The security features the bank would have inspected were security features that did not survive the imaging process. Under these circumstances, the paying bank could assert an indemnity claim against the bank that presented the substitute check.

"By contrast with the previous example, the indemnity would not apply if the characteristics of the presented substitute check were such that the bank's security policies and procedures would not have detected the fraud even if the original had been presented. For example, if the check was under the threshold amount the bank has established for examining security features, the bank likely would not have caught the error and accordingly would have suffered a loss even if it had received the original check."[3]

## Remote Deposit Capture

Remote Deposit Capture is a service that allows a business to scan, image and transmit to its bank the checks it normally would deposit. While the technology is exciting, you must understand your risk. Under the law, an organization that images and converts a check issues the warranties and indemnity, and may be held liable for any Check 21 loss. The statute of limitations in the law for these types of losses is one year after the injured party discovers the financial loss.

## Check Safety Features

The purpose of safety features is to thwart criminals trying to alter or replicate checks. The minimum number of safety features a check should have is 10, and more is better. The best safety features are fourdrinier (true) watermarks in the paper, thermochromatic ink, and paper or ink that is reactive to at least 15 chemicals. These safety features cannot be imaged and replicated, and are the best!

When an individual or organization uses high security checks that include these safety features, they are positioned for a built-in indemnity claim against the converting bank, as allowed under Check 21. This assumes that their bank has a Sight Review threshold such that the original check would have been physically examined.

## Check 21 Fraud Strategies

In a Check 21 world, the strategies are straightforward. 1) Every bank should offer Positive Pay at an affordable price, and every company and organization should use the service. Most banks charge for Positive Pay; consider the fee an insurance premium. For useful information about Positive Pay, visit PositivePay.net and SafePay123.com.
2) Make large dollar payments electronically.
3) Every company, organization and individual should use high security checks with 10 or more safety features. The checks should include a true watermark, thermochromatic ink and 16+ chemical sensitivity. The **Supercheck**, the **SuperBusinessCheck**, and **SAFEChecks** **(See Pages 10-13)** were designed by Frank Abagnale with these and many additional safety features so prudent individuals, companies and organizations could enjoy maximum document security in a controlled check. Visit **Supercheck.net** and **SafeChecks.com** to request a sample.
4) Avoid using laser checks that can be purchased by multiple people entirely blank because the stock is not controlled.
5) Banks should lower their Sight Review thresholds and re-train inspectors, and encourage their customers to use high security checks and Positive Pay.

[1]Visit www.FraudTips.net for a copy of the Act, and the Federal Reserve Board's Final Rule governing Check 21 issued July 26, 2004. Read Page 67(c) Jurisdiction.
[2]The Fed's Final Rule, page 58, Substitute Check Indemnity.
[3]ibid., pages 99-100, Substitute Check Indemnity.
Frank Abagnale has co-authored a white paper on Check 21 and image survivable safety features. Downloaded it at www.FraudTips.net under Check 21.

# A Primer on Laser Printing

Many companies and organizations print checks on a laser printer. This technology is highly efficient, but proper controls must be in place or laser printing can invite disaster.

## Toner Anchorage, Toner, Printers

To prevent laser checks from being easily altered, the toner must bond properly to the paper. This requires check stock with toner anchorage, good quality toner, and a hot laser printer.

Toner anchorage is an invisible chemical coating applied to the face of check paper. When the check passes through a hot laser printer, the toner melds with the toner anchorage and binds onto the paper. Without toner anchorage, the toner can easily be scraped off, or lifted off the check with tape.

High quality toner should be used because poor quality toner does not meld properly with the toner anchorage. Also, if the printer is not hot enough, the toner and anchorage will not meld sufficiently. The fuser heat setting can be adjusted on most laser printers through the front panel; hotter is better.


## Blank Check Stock

that is not customized for each customer should be avoided. If a printer or computer company will sell you entirely blank checks, they may be selling the identical checks to others, who, in effect, have your check stock! Ensure that your check stock is not available entirely blank to others. It should be uniquely customized in some way for each user.

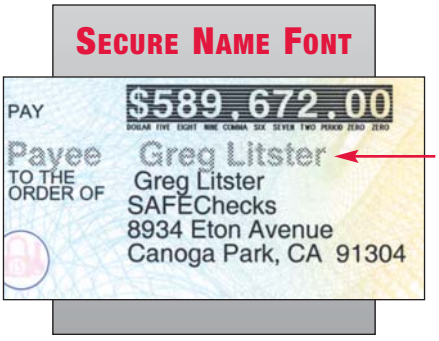
Recent court cases have shown using plain checks may contribute to the alteration or replication of a check. Issuers of such checks may be liable for the resulting losses. **See Page 14 Robert J. Triffin v. Somerset Valley Bank and Hauser Contracting Company.**

## Image Survivable "Secure Seal" Technology

is a new, state-of-the-art encrypted barcode that is laser printed on the face of a check. The barcode contains all the critical information on a check – payee name, dollar amount, check number, routing and account numbers, and issue date. The barcode can be "read" using Optical Character Recognition (OCR) technology and compared with the printed information on the check. If the printed data does not match the barcode, the check can be rejected. This technology is image survivable. Some software providers also include Secure Name and Number Fonts.

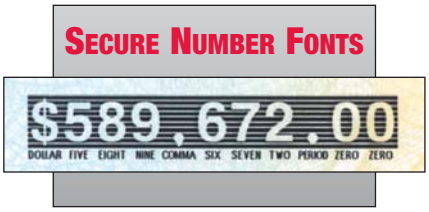

## Secure Name Fonts

help prevent added or altered payee name. In many cases, altering the Payee name allows the forger to circumvent Positive Pay. A Secure Name Font uses a unique image or screened dot pattern in a large font size to print the payee name. This makes it extremely difficult to remove or change the payee name without leaving evidence.




## Secure Number Fonts

prevent the dollar amount on the check from being altered without detection. Some fonts have the dollar amount image reversed out, with the name of the number spelled inside the number symbol. Although Positive Pay makes this feature redundant, it is a strong visual deterrent to criminals.




## Password Protection

is critical for every computer system. A company has more exposure from dishonest employees than from a hacker. 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.

## String of Asterisks

placed above the payee line can prevent added payee names. Forgers often add 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. (Do not use asterisks when using Payee Positive Pay. The asterisks cause false positives.) Asterisks can be pre-printed on the checks by the check vendor.

## Sequenced Inventory Control Numbers

are numbers printed in sequence on the back of non-pre-numbered laser checks. The control number is completely independent of the check number printed on the face of the check. Numbering is essential on laser checks that are 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, and keep a log of every check run.

# Check Security Features

In response to the alarming growth of check fraud, the check printing industry has developed many new security features. The best features are illustrated here. While nothing is 100%, combining ten (10) or more security features into a check will deter or expose most check fraud attempts.

## Controlled Paper

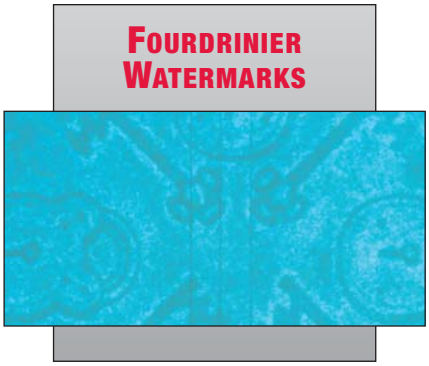
is manufactured with many built-in security features, such as a true watermark, visible and invisible (UV light-sensitive) fibers, and multi-chemical sensitivity. To keep the paper out of the hands of forgers, the paper manufacturers have written agreements that restrict the paper's use and distribution. Ask for and read the written agreement. If there is none, the paper may not be controlled.

## Controlled Check Stock

are high security checks that are printed on controlled paper. The check manufacturer does not allow the checks to be sold entirely blank without it first being customized. Ask your check printer for their written policy about blank check stock. If there is none, the check stock may not be controlled.

## 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 not capable of replicating dual-tone Fourdrinier (true) watermarks.




## Thermochromatic Inks

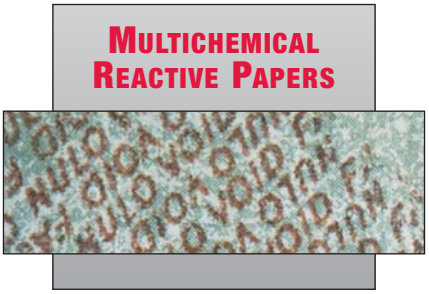
react to changes in temperature. Some thermo inks begin to fade away at 80°F and disappear completely at 90°F. The ink then reappears when the temperature cools to 78°F. Thermo ink's reaction to temperature changes cannot be replicated on a color copier or laser printer.


## Explicit Warning Bands

are printed messages that call attention to the security features found on the check. These bands should instruct the recipient to inspect a document before accepting it, not merely list features, and may discourage criminals from attempting the fraud.

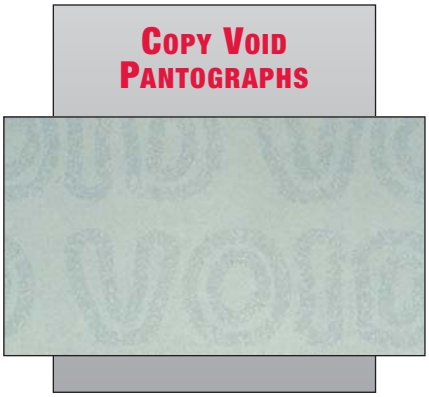

## Multi-chemical Reactive Papers

produce a stain or speckles 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 15 chemicals.



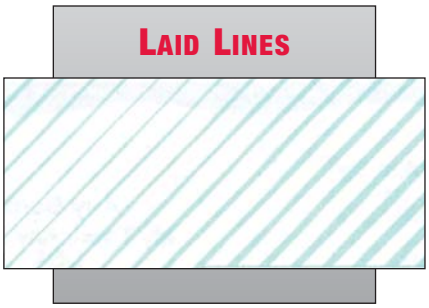

## Copy Void Pantographs

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



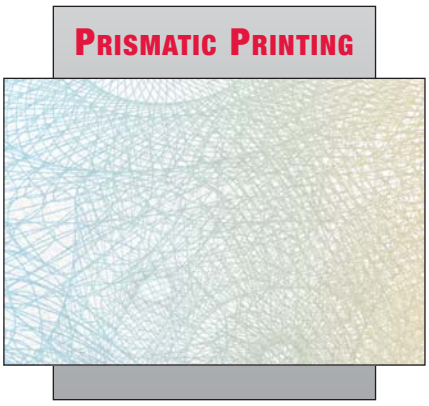

## Laid Lines

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 many color copiers.

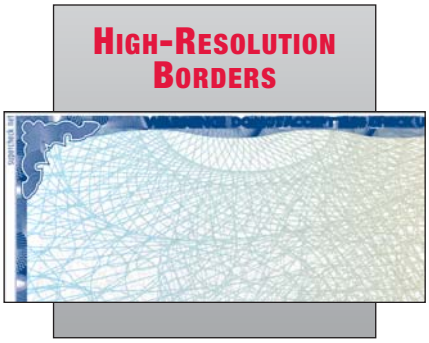


## Image Survivable Secure Seal

is an encrypted barcode that is laser printed on the face of the check. The barcode contains all the critical information found on the check. **See Page 7.**


## High-Resolution Borders

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

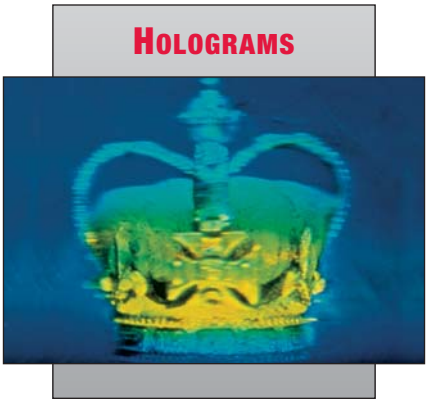



## Ultraviolet Light-Sensitive Ink and Fibers

Ultraviolet light-sensitive ink and fibers can be seen under ultraviolet light (black light) and serve as a useful authentication tool.

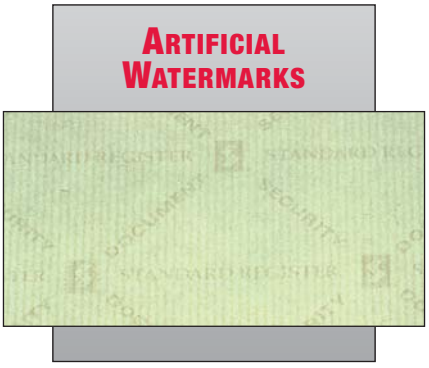

## Holograms

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. Holograms enhance admission passes, gift certificates and identification cards.



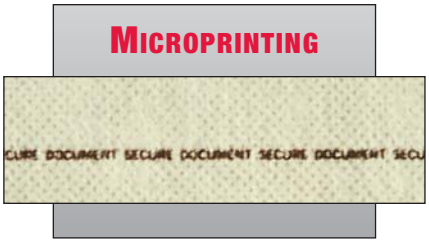

## Artificial Watermarks

are subdued representations of a logo or word printed on the paper. These marks can be viewed while holding the document at a 45º angle. Customized artificial watermarks are superior to generics. Copiers and scanners capture images at 90º angles and cannot see these marks. However, to the untrained eye, their appearance can be replicated by using a 3% print screen.



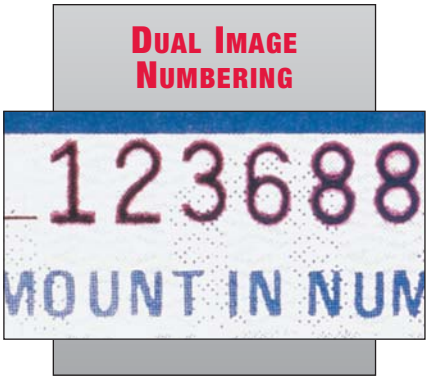

## Microprinting

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.




## 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.




## High Security Checks

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

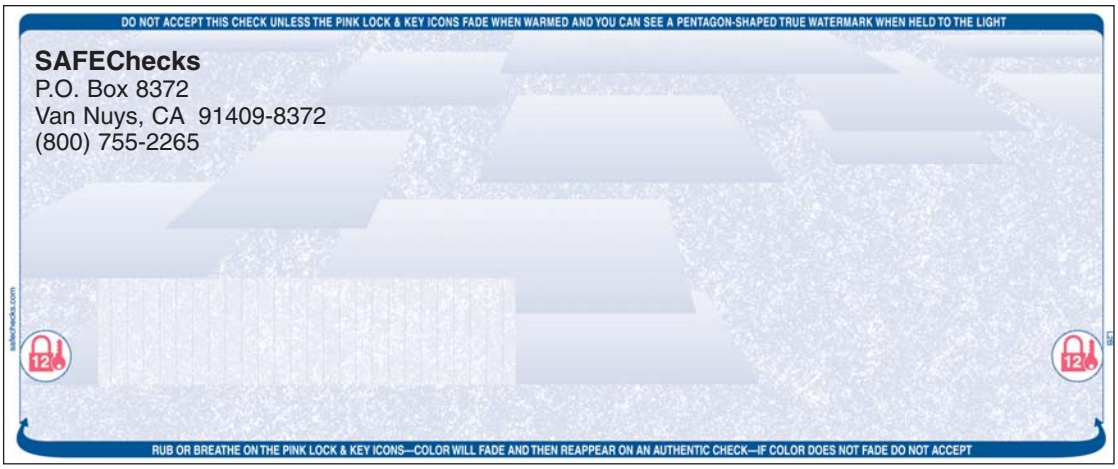
They also establish the basis for an indemnity claim charge-back under Check 21's indemnity provision. **See Page 6.**

High-security checks should have at least ten (10) safety features. Among the best safety features are a controlled paper, a true watermark, thermochromatic ink, and toner anchorage on laser checks.

Frank Abagnale designed the **Supercheck**, the **SuperBusinessCheck** and **SAFEChecks** to help consumers, businesses and organizations have access to high security checks at affordable prices. **See Pages 10-13.**

# SAFEChecks

SAFEChecks were designed by Frank Abagnale with 12 security features, and are virtually impossible to replicate accurately using desktop publishing tools or a color copier. SAFEChecks are printed on controlled, true-watermarked security paper. To prevent unauthorized use, checks are never sold blank without first being customized for each specific customer.




## 12 Safety Features

### Covert Security Features

**Controlled Paper Stock**
**Fluorescent Fibers –** Become visible under ultraviolet light.
**Chemical Reactivity –** to 85 chemicals.
**Toner Anchorage on Laser Checks**
**Copy Void Pantograph**

### Overt Security Features

**Thermochromatic Ink –** The pink lock and key icons fade away when warmed above 90º and reappear at 78º. This reaction cannot be replicated on images created by a color copier.
**Fourdrinier (True) Watermark –** The true watermark is visible from either side when the check is held toward a light source. It cannot be color copied or scanned.
**Explicit Warning Bands**
**Chemical Wash Detection Box –** **See Figure 2 on page 13.**
**Sequenced Inventory Control Numbers**
**Microprinting**
**Laid Lines**

## Available Styles

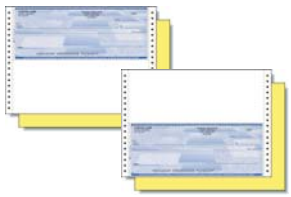
Laser - Top

Laser - Middle

Laser - Bottom

Continuous - 1 part

Continuous - 2 part



Legal Laser - Top

Legal Laser - Second Panel

Legal Laser - Panels 2 & 4

Continuous - 3 part

## Pressure Seal Checks Also Available

**NOT USING POSITIVE PAY?**
You should! Talk to your banker ASAP.
Visit
PositivePay.net
SafePay123.com

MORE FRAUD PREVENTION TIPS
Visit
FraudTips.net
Supercheck.net
PositivePay.net

# Abagnale SuperBusinessCheck

The SuperBusinessCheck is the most secure business check in the world. Designed by Frank Abagnale with 16 security features, the check is virtually impossible to replicate or alter without leaving evidence. The SuperBusinessCheck is printed on very tightly controlled, true-watermarked security paper. For your protection, checks are never sold blank without first being customized for each specific customer. Available styles are shown below. **Pricing can be found on the Web at SAFEChecks.com or Supercheck.net.**

## 16 Safety Features

**COVERT SECURITY FEATURES**

- Controlled Paper Stock
- Fluorescent Ink
- Fluorescent Fibers
- Chemical Sensitivity
- Toner Anchorage
- Copy Void Pantograph
- Microprinting
- Chemical Reactive Ink

**OVERT SECURITY FEATURES**

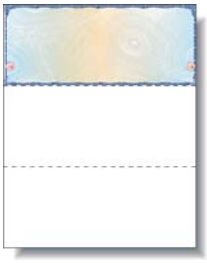
- Thermochromatic Ink
- Fourdrinier (True) Watermark
- High-Resolution Border
- Prismatic Printing
- Explicit Warning Bands
- Chemical Wash Detection Box
- Sequenced Inventory Control Numbers
- Laid Lines

*"After years of designing checks for Fortune 500 companies and major banks, I designed the Supercheck, the SuperBusinessCheck and SAFEChecks to help consumers, medium and small businesses, and organizations protect their checking accounts."*

Frank W. Abagnale


## Available Styles

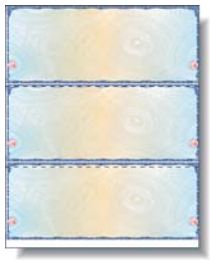
Laser - Top



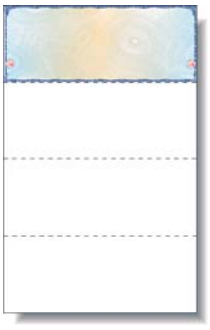
Laser - Middle

Laser - Bottom

Laser 3-On-a-Sheet



Legal Laser - Top



Legal Laser - Second Panel

## Pressure Seal Checks Also Available

3-on-A-Page

### Secure Ordering Procedures

To prevent unauthorized persons from ordering checks on your account, SAFEChecks verifies all new check orders with your bank. We confirm that the name, address and account number on the order form match the data on file with the bank. Check orders are shipped to the address on file with the bank. Reorders with a change of address are re-confirmed with the bank. Our Secure Ordering Procedures are in place for your protection, and we are unparalleled in the check printing industry.

# PLEASE PHOTOCOPY THIS FORM TO ORDER CHECKS

**SAFE Checks®**


Download a price list at SAFEChecks.com

8934 Eton Avenue (800) 755-2265
Canoga Park, CA 91304 Fax (800) 615-2265


**How did you hear about us?** ☐ Seminar by Frank Abagnale ☐ Seminar by _____ ☐ Other _____

CUSTOMER NAME, ADDRESS AND PHONE NUMBER

☐ To be printed on checks ☐ For file information (not printed on checks)

Phone ( )

**Please send a voided original check with this completed form. We will call you to confirm receipt.**

**BANK NAME AND ADDRESS**

☐ To be printed on checks ☐ For file information (not printed on checks)

Ship-To Address (if different from address on checks)

Attention:

| Account Number | |
|---|---|
| Routing / Transit: | Bank Fraction: |
| Bank Representative | Bank Representative's Phone # |

| Check Starting Number | Quantity |
|---|---|
| Text to be printed above signature lines | |

☐ Check this box for two signature lines

☐ **Custom Logo** - Camera-ready art or electronic file (diskette or e-mail) is required. Send to: graphics@safechecks.com
JPG, EPS, PSD, TIFF & BMP are acceptable formats

☐ Standard Turnaround (most orders ship in 5-7 business days)
☐ RUSH (RUSH FEE APPLIES) Date you must receive checks _____

Shipping Instructions: ☐ Overnight UPS ☐ Two-day UPS ☐ Ground UPS
☐ Other: _____

## LASER CHECKS

☐ **8½ X 11 Frank Abagnale's SuperBusinessCheck** (one color design only)
- ☐ Top Check
- ☐ Middle Check
- ☐ Bottom Check
- ☐ 3 Laser Checks per Sheet

☐ **8½ X 14 Frank Abagnale's SuperBusinessCheck** (one color design only)
- ☐ Top Check
- ☐ Check in 2nd Panel

☐ **8½ X 11 SAFE Checks®**

| | | | | | |
|---|---|---|---|---|---|
| ☐ Top Check | ☐ Blue | ☐ Green | ☐ Red | ☐ Plum | |
| ☐ Middle Check | ☐ Blue | ☐ Green | | | |
| ☐ Bottom Check | ☐ Blue | ☐ Green | | | |

☐ **8½ X 14 SAFE Checks®**

| | | | |
|---|---|---|---|
| ☐ Top Check | ☐ Blue | ☐ Green | ☐ Red |
| ☐ Check in 2nd Panel | ☐ Blue | ☐ Green | |
| ☐ Check in 2nd & 4th Panels | ☐ Blue | ☐ Green | |

How are your laser checks placed in the printer? ☐ Face Up ☐ Face Down

Software Name | Version #

## CONTINUOUS CHECKS

| | | | | |
|---|---|---|---|---|
| ☐ **Single** | ☐ Blue | ☐ Green | Check: ☐ **Top** | ☐ **Bottom** |
| ☐ **Duplicate** | ☐ Blue | ☐ Green | | |
| ☐ **Triplicate** | ☐ Blue | ☐ Green | ☐ Red | |

Software Name | Version #

## PRESSURE SEAL

Pressure seal checks are custom designed. Call (800) 755-2265 ext. 3306.

Make and Model # of Folder/Sealer: _____

Make and Model # of Printer: _____

## SAFE Checks® SECURE ORDERING PROCEDURES

To prevent unauthorized persons from ordering checks on your account, all new check orders are verified with your bank. We confirm that the name, address and account number on the order form match the information on file with the bank. Check orders are shipped to the address on file with the bank. Reorders with a change of address are re-confirmed with the bank.

## THREE-ON-A-PAGE HANDWRITTEN CHECKS

☐ **Single Stub (General Check) Frank Abagnale's SuperBusinessCheck**

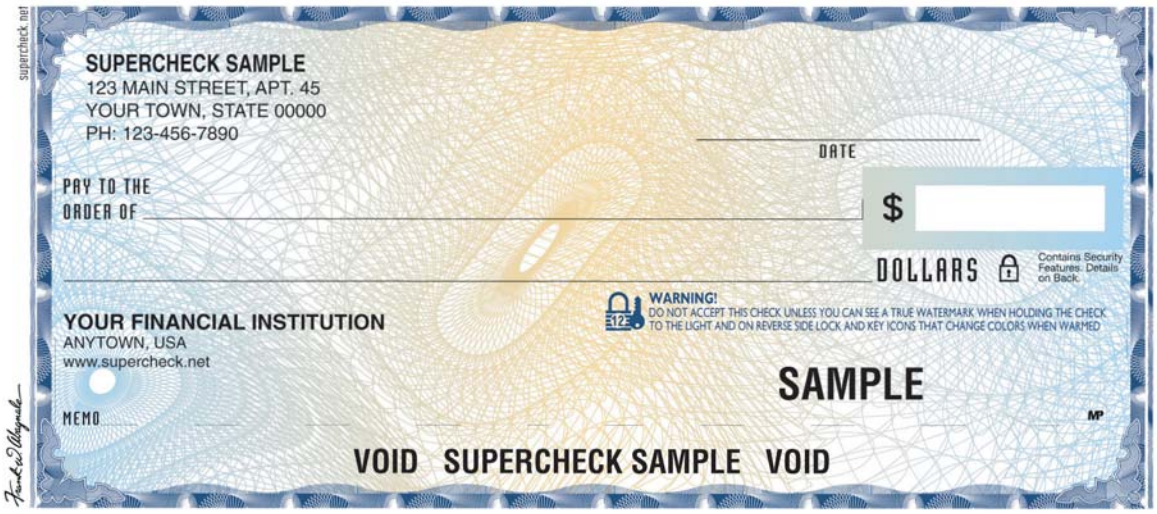
☐ **Three-on-a-Page Binder**

Prepared by *(print)*: _____ Phone Number: _____ Date: _____

# ABAGNALE SUPERCHECK

The Supercheck is a high security personal check designed by Frank Abagnale to help consumers protect their checking accounts. The Supercheck contains 12 security features, is reactive to 85 chemicals, is Check 21 compatible, and is nearly impossible to replicate or to alter without leaving evidence. It is "the check for people with something to lose."

*"The check for people with something to lose"*




## STYLES

Supercheck Wallet Single

Supercheck Wallet Duplicate

## 12 SAFETY FEATURES

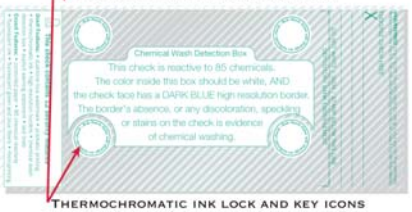
**Controlled Paper Stock**
**Fourdrinier (True) Watermark**
**Thermochromatic Ink**
**Chemical Sensitivity**
**Explicit Warning Bands**
**Prismatic Printing**
**Chemical Wash Detection Box**
**High-Resolution Border**
**Laid Lines**
**Fluorescent Fibers**
**Fluorescent Ink**
**Microprinting**

FIGURE 1 — FRONT VIEW OF THE SUPERCHECK


FIGURE 2 — BACK VIEW UNDER NORMAL LIGHT AND TEMPERATURE

FIGURE 3 — BACK VIEW UNDER ULTRAVIOLET LIGHT

FIGURE 4 — BACK VIEW OF CHECK ABOVE 90° F



THERMOCHROMATIC INK LOCK AND KEY ICONS FADE AWAY AT 90° F AND REAPPEAR AT 78° F.

**PLEASE PHOTOCOPY THIS FORM TO ORDER CHECKS**

### CHECK ORDER FORM AND INFORMATION

*Our* **Secure Ordering Procedures** *are unmatched in the check printing industry. For your protection, we verify that the name, account number, and mailing address match the information on file with your financial institution. Checks are shipped to the address on file or directly to your financial institution. Reorders with a change of address are re-verified with your financial institution.*

| We need all three (3) items below to complete your order: | Please mail to: | Delivery Times: |
|---|---|---|
| 1. Completed ORDER FORM<br>2. VOIDED CHECK (indicate any changes on the face)<br>3. VOIDED DEPOSIT SLIP | SAFEChecks<br>P.O. Box 8372<br>Van Nuys, CA 91409-8372 | Allow 3 weeks for delivery.<br>Expedited service is available.<br>Call (800) 755-2265 ext 3304 |

Name _____ Primary Telephone (We do not give or sell your information to anyone.)

Email Address _____ Alternate phone where you can be reached

Please mail checks to the:

____Address on checks (this address must be on file with the financial institution)

____Financial institution _____
Branch Address City State Zip

____Other _____
Address must be on file with bank

| ORDER SUMMARY | Check Start # | # of Boxes | Total (price + s/h) |
|---|---|---|---|
| Wallet Supercheck Single | | | |
| Wallet Supercheck Duplicate | | | |
| | | SubTotal | |
| | | California residents add sales tax | |
| | | TOTAL | |

Single - $29.95 per box of 150
Duplicate - $32.95 per box of 125
Shipping/Handling - $2.00 per box

### PAYMENT OPTIONS:

_____Debit this checking account _____Check or Money Order enclosed (made payable to SAFEChecks)

_____Bill my credit card: _____MasterCard _____Visa

_____ __ __ __ __
Credit Card Account Number / Expiration Date Security Code

Cardholder Name

Authorized Signature

Billing address of credit card if different from address on checks

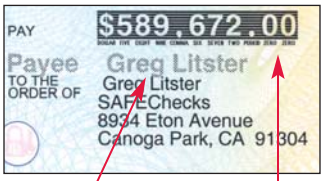
# Secure Software

## Secure Check Writing Software


SAFEChecks partners with a software company that specializes in laser check writing systems. A recent security advancement is a state-of-the-art encrypted "secure seal" barcode that is laser printed on the face of a check. The barcode is created using a print driver, and each barcode is unique to that check. The barcode is the newest weapon in the fight against check fraud. It contains all the critical information found on a check, including payee name, dollar amount, check number, routing and account number, and issue date. It is like on-board Positive Pay, without needing to transmit the check data to the bank. (The bank must have barcode reading software.)

The barcode data is "read" using Optical Character Recognition (OCR) technology, and compared with the printed information on the check. If the information on the check does not match the barcode, the check will be rejected. The secure seal barcode is "image survivable" and retains its fraud prevention effectiveness in a Check 21 imaging environment.

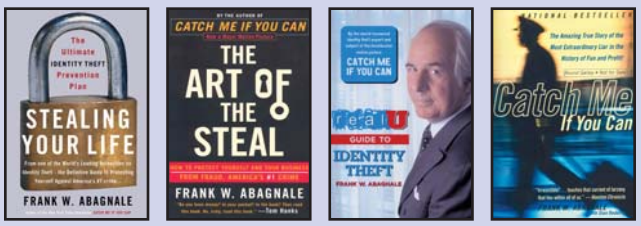
ChequeGuard
Secure Seal Barcode




Secure Name Font
Secure Number Font

As illustrated above, the ChequeGuard print driver can include the barcode, a Secure Name Font to prevent added payee names, and a Secure Number Font to prevent altered dollar amounts.

**For software information, contact SAFEChecks (800) 755-2265 x 3301 or greg@safechecks.com**




**Books authored by Frank W. Abagnale**
**Available online or from local booksellers**
**Catch Me If You Can is also available on DVD**

## Positive Pay

Positive Pay is one of the most important tools available to prevent check fraud. Developed by bankers years ago, Positive Pay is an automated check matching service offered by many banks to businesses and organizations. It helps stop most (not all) counterfeit and altered checks. When Positive Pay is used with high security checks, such as the Abagnale SuperBusinessCheck or SAFEChecks **(see Pages 10 - 11)** fraud losses can be cut dramatically.

Positive Pay requires a check issue file (information about checks that have been issued) to be sent to the bank before the checks are disbursed. The most common obstacle to using Positive Pay is a company's inability to format the check issue file and securely transmit the information to its bank. SAFEChecks created **SafePay** to help companies and organizations use their banks' Positive Pay service. **SafePay** is PC-based and is compatible with virtually all accounting systems and check writing software.

The **SafePay** package (SafePay123.com) sells for $299 and includes a free order of the SuperBusinessCheck or SAFEChecks, and a free order of the Supercheck. **(see Pages 10 – 13)**


***Caution: Some companies have the mistaken notion that if they use Positive Pay they do not need to use high security checks.***

**<u>This is a serious misconception.</u>** **<u>Positive Pay and Payee Positive Pay are not foolproof!</u>** Consider this analogy: Using Positive Pay is like catching a thief standing in your living room, holding your jewels. Although it is good that the thief was caught, it would be better to have the thief look at your house and go elsewhere. This is where high security checks are important. They DETER, or discourage, many criminals from attempting fraud against your account.

***High security checks <u>and</u> Positive Pay are critical companions in effective check fraud prevention strategy.***

**Supercheck.net SafePay123.net PositivePay.net**

Frank Abagnale and SAFEChecks recommend the
**uni-ball® 207™ Gel Pen**

The **uni-ball® 207™** pen uses specially formulated gel inks with color pigments that are nearly impossible to chemically "wash." It retails for under $2, is retractable and refillable, and images perfectly. It can be found at most office supply stores.

# Cyber Crime Protection

A Midwestern company's computer system became infected with a virus that tracked keystrokes. The hacker was able to decipher the log-on keystrokes to the company's bank, logged on, and sent $160,000 in ACH credits to various bank accounts. The money was sent overseas to bank accounts controlled by the thief. The company was shocked when its bank denied liability for the loss because the log-on was authentic. A bank is not responsible for the integrity of a customer's computer.

Of the companies responding to the 2008 CSI Computer Crime and Security Survey, the overall average annual loss due to computer security incidents was almost $300,000 per company. At the end of 2007, Symantec had detected 499,811 new malicious code threats, a 571% increase over the second half of 2006.

Computer crime is becoming "professionalized" and criminals have adopted stealthier attack techniques. They now target end users on individual computers through the Web, rather than attempting widespread broadcast attacks to infiltrate networks. The Web is now the primary avenue for attacks, as demonstrated by the 11,253 site-specific vulnerabilities versus the 2,134 traditional vulnerabilities verified by Symantec in 2007. Social networks like Facebook and MySpace are prime targets for cyber crime activities.

Bots are programs secretly installed on a computer, allowing a malicious user to control it remotely. Attackers scan the Internet to find computers that are unprotected, and then install software through "open doors." For example, attachments, links or images in spam email, if opened, can install hidden "bot" software. Sometimes visiting a website or downloading files may cause a "drive-by download," which installs malicious software, turning your computer into a "bot." An attacker controls a large number of "bot" computers in a botnet, which can then be used to launch coordinated attacks. If you find unknown messages in your out box, or if messages bounce back that you did not send, it's a sign that your computer may be part of a botnet.

The Verizon 2008 Data Breach Investigations Report found that of the 500 data breaches that were investigated, more than half only required minimal skills to commit. Basic security protections and procedures would have thwarted them. Here are some of the ways individuals and companies can protect themselves. For more details, see **"Resources"** below.

## For Individuals

- Use anti-virus and anti-spyware software that removes or quarantines viruses, and set it to perform daily automatic updates. Consider Norton Internet Security 2009 (no longer a resource hog), AVG, Kaspersky, McAfee, etc.
- Use a properly-configured firewall, which helps make you invisible on the Internet and blocks incoming communications from unauthorized sources.
- Do not follow links found in emails messages from untrusted sources, as these may be links to spoofed Web sites. Manually type the URL into your browser bar.
- Unplug your Internet connection when you're away.
- Never reply to an email, text, or pop-up message that asks for personal or financial information.

- Never open an email attachment unless you are expecting it or know what it contains.
- Download software only from trusted sites.
- Restrict which applications you install on social networks, and never install a codec from a random Web site.
- Don't send sensitive files over a Wi-Fi network unless it is secure. Most public "hot spots" are not secure.
- When you're not using Wi-Fi, turn off the wireless connection to your laptop.
- Don't respond to a message asking you to call a phone number to update your account or give your personal information. If you need to reach an organization, look the number up yourself.
- You can track your child's keystrokes, emails, IM, MySpace, Facebook and websites visited with **Spector Pro** (spectorsoft.com). You can also have their emails forwarded to you by including eBlaster. Never divulge the source of your "parent's intuition."

## For Companies and Organizations

- The recommendations for individuals (above) also apply to companies and organizations.
- Implement security policies to restrict unauthorized access to sensitive data.
- Require that all sensitive data be encrypted or password protected before transmission. Adobe Acrobat 7 and higher does this easily.
- Regularly review updated patches for your operating system software, and install those that tighten your security.
- Develop written policies for using flash drives, etc. Some companies fill in the flash drive port with epoxy to stop data theft.
- Install software to limit the sites users may access; be cautious about visiting unknown or untrusted Web sites.
- Use a network-based Intrusion Prevention System (IPS)
- Maintain a whitelist of trusted Web sites, and disable individual plug-ins and scripting capabilities for others.
- Educate in-house developers about secure development practices, such as the Security Development Lifecycle.
- When employees leave the company, immediately disconnect their access to the company's network and building, shut down remote connections, and collect their cell phones, iPDAs, etc.
- Ask your bank about using a **TOKEN**


as part of your bank log-on and password sequence to thwart keystroke logger viruses.

## Resources

*2008 CSI Computer Crime and Security Survey*
*Symantec Global Internet Security Threat Report (2006, 2007)*
*Verizon 2008 Data Breach Investigations Report*
*OnGuardOnline.gov*
*fbi.gov/cyberinvest/protect_online.htm (several articles on website)*
*getnetwise.org*
*pcisecuritystandards.org*
*PC Magazine (pcmag.com)*
*CNET Networks (cnet.com)*
*"Small Business Security, New Entrepreneurial Solutions" Brigham Young University, Marriott School of Management Alumni Magazine, Fall 2008*

# ★★★ FOR BANKERS AND MERCHANTS / RETAILERS ★★★

**Cashiers and tellers are the "front line" in the fight against check fraud. Below are several simple procedures to follow to help catch fraudulent and altered checks.**

• Don't let a customer's appearance lull you into a false sence of security. Frank Abagnale once cashed a $50 check written on a cocktail napkin, before a hidden camera for television, because the bank teller was more impressed by his appearance than by the "check." When you are in a hurry, or want to make an exception, consider how you will defend your decision if the check is returned. Then, only the check itself will matter, not the circumstances in which you took it.

• When viewing a license for identification, always ask yourself: Is the person in the photo and in front of you the same person? Do the addresses on the check and the license match? Has the license expired? If so, do not accept it.

• Be cautious of new checking accounts. Most "hot" checks come from accounts less than a year old. The consecutive number in the right hand corner often begin with 101; be careful when taking low numbered checks. Some banks now print a date code on the check of when the account opened.

• On drafts issued by savings banks, the routing number may start with 2 or 3. Credit union drafts are honored by the bank on which they are drawn. U.S. Government checks have the routing number 000000518. Traveler's Checks have routing numbers starting with 8000.

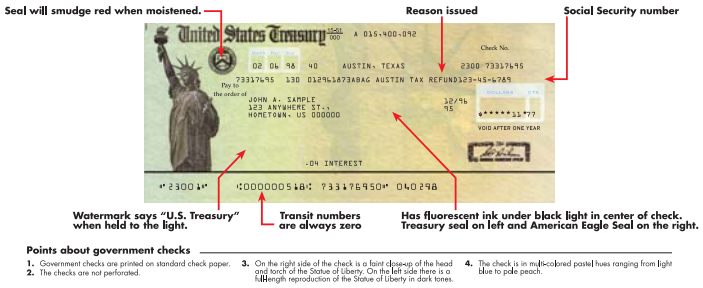

FEDERAL RESERVE BANK CODES:

01—Massachusetts, Maine, New Hampshire, Connecticut, Vermont, Rhode Island
02—New York, New Jersey, Connecticut
03—Pennsylvania, Delaware, New Jersey
04—Ohio, Pennsylvania, Kentucky, West Virginia
05—Virginia, Maryland, North Carolina, Washington D.C., South Carolina, West Virginia
06—Georgia, Alabama, Florida, Tennessee, Louisiana, Mississippi
07—Illinois, Michigan, Indiana, Iowa, Wisconsin
08—Missouri, Arkansas, Kentucky, Tennessee, Indiana, Illinois, Mississippi
09—Minnesota, Montana, North Dakota, South Dakota, Wisconsin, Michigan
10—Missouri, Colorado, Oklahoma, Nebraska, Wyoming, Kansas, New Mexico
11—Texas, New Mexico, Louisiana
12—California, Oregon, Washington, Utah, Hawaii, Alaska, Idaho, Nevada, Arizona


## Things to look for in a check:

1. **Perforations.** There will be at least one perforated edge on all legitimate checks (except for government checks, card stock checks, and counter or temporary checks that do not have pre-printed names.)
2. **Routing Code.** There are nine numbers between two colons on the bottom of the check. The first two numbers indicate in which of the 12 Federal Reserve Districts the bank is located. (See graphic, above right.) Criminals often change the routing number, causing the check to be sent to the wrong Federal Reserve District for processing, thus giving them more time to continue their crime.
3. **Magnetic Ink.** This special ink for printing a check's MICR line is flat and dull. If it looks bright and shiny, it's counterfeit. Also, the MICR numbers on a counterfeit check may smear with moisture from your fingers.
4. **Warning banner on face of the check.** Read it and follow it. If security features are listed, look for those features. Do not accept the check if they are missing or if the check appears to be altered.
5. **Watermarks.** True watermarks can be seen by holding the check to the light. Artificial watermarks can be seen when viewed at an angle.
6. **Thermochromatic ink.** Test the heat sensitive ink by gently breathing on or by rubbing it. If the ink does not fade, do not accept the check.
7. **Dollar amounts or payee names** that do not line up, or that have a type font that is inconsistent.
8. **Discoloration or speckles on the face or back of the check.** Any discoloration or speckles indicates chemical "washing."
9. **Added Payee names.** If a name has been added above or beside the original name and the check is being cashed by that second person, it may have been added fraudulently. Examine the alignment carefully.
10. **Photocopy.** A check that looks like it is a photocopy probably is one. It may be shiny or have the word "void" showing lightly in the background of the check. Amazingly, photocopied checks have been cashed by tellers and cashiers!
11. **Laid lines** (thin, parallel lines on the back of the check) that do not line up with each other. If they don't align, then a "cut and paste" alteration may have occurred.
12. **Microprinting** (words printed so small they look like a solid line to the naked eye) that looks blurred under a magnifying glass.

## HOW TO AUTHENTICATE GOVERNMENT CHECKS




## HOW TO AUTHENTICATE TRAVELERS CHECKS

**American Express** – Turn check over. Moisten fingertip and rub the left denomination. If it smears, it is good. Right side will not smear.
**VISA** – When held above eye level, a dove appears on the left side in the white area. (Old format: a globe of the world appears on the front left and a dove in the upper right.) **Mastercard and Thomas Cook** – When held above eye level, a Greek goddess will appear on the right side of the check in a circle. **Citicorp** – When held above eye level, a Greek god's face will appear on the right.

# SHORT CHANGE ARTISTS: HOW THEY DO IT

**Short-change artists always deal with cash transactions. Victims of short-change artists often do not know exactly what happened or how it happened. The short-change artist is hard to spot because he or she looks like everyone else.**

**The Artist May:**

…be any age, even an elderly person or a small child,
…look ordinary and respectable,
…act pleasant and unsuspicious, and
…easily gain confidence and trust.

**The Artist Will Usually Do The Following:**

…purchase a small item (often less than $1.00),
…pay for the item with a large bill (a $20, $50 or $100),
…request that change be broken down even further,
…try to create confusion about the amount of change involved in the transaction.

**The following is a sample Short-Change situation:**

*"Good afternoon, miss. Let me take these razor blades."*

*"98¢, sir."*

*"98¢? Here's a $20 bill, miss."*

*"Thank you sir, that's 98¢ out of $20."*

*"Here's your change. 2¢ makes a dollar, that's 2, 3, 4; 1 is 5; 5 is 10 and 10 is 20. Have a nice day, sir."*

*"Tell you what, miss. I really didn't want all this change. Do you think I might just trouble you for a $10 for $5 and $5 ones?"*

*"Certainly sir. Here is a $10."*

*"And here is the $5 and $5 ones. You might want to count that. Make sure I gave you the right change."*

*"Thank you, sir."*

*"I'm glad you said that. You only gave me $9.00. I'm afraid you owe me one more dollar."*

*"Look miss, this is ridiculous. What did you do with my $20?"*

*"It's right here on my register, sir, where it's supposed to be."*

*"I'll tell you what miss, let me just get my $20 back. You say you have $9.00 there?"*

*"Here's $1 makes $10 and here's $10 more, makes $20. Have a nice day!"*

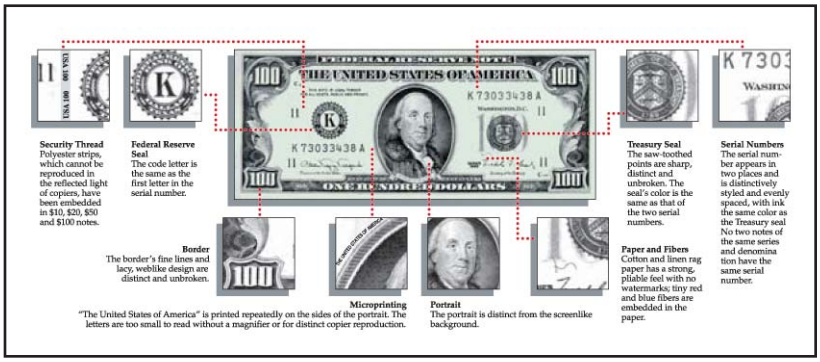
**How much was she short-changed?**

$10. If she had been given a $50 she would have been short $20. If she had been given a $100 she would have been short $40.

**To Stop the Short-Change Artist**

Never try to do more than one transaction at a time. Always close out the first transaction before moving on to the next. Always have the customer's money before you make change.

## RECOGNIZE COUNTERFEIT CURRENCY




**For details on all U.S. Currency security features, visit www.FraudTips.net/AbagnaleTips**

## CREDIT CARD SECURITY FEATURES


**To view the complete images, detailed credit card security features and Government checks, visit www.FraudTips.net/AbagnaleTips.**

# Court Cases

## Holder In Due Course

Holder in Due Course (HIDC) is part of the Uniform Commercial Code (UCC) that significantly impacts an organization's liability for check fraud and the checks it issues. After learning about HIDC, prudent companies are often motivated to use high security checks and change check disbursement procedures to protect themselves. Anyone responsible for check disbursements or fraud prevention should understand this law. Following is a brief description of Holder in Due Course, and three Federal Appellate Court rulings.

In simple terms, a Holder in Due Course is anyone who accepts a check for payment. On the face of the check there is no evidence of forgery or alteration, nor does the recipient have knowledge of any fraud related to the check. Under these conditions, the recipient is an HIDC and is entitled to be paid for the check. The statute of limitations under the UCC for an HIDC to sue the check's maker for its face value is 10 years from the issue date, or three years from the date the check was first deposited and returned unpaid, whichever comes first. An HIDC can assign, sell, give, or otherwise transfer its rights to another party, who assumes the same legal rights as the original Holder.

The following three Federal Appellate Court cases illustrate the far-reaching power of Holder in Due Course.

### ROBERT J. TRIFFIN v. CIGNA INSURANCE

**Issue: Placing A Stop Payment Does Not Eliminate Your Obligation To Pay A Check**

In July 1993, Cigna Insurance issued James Mills a Worker's Compensation check for $484. Mills falsely claimed he did not receive it due to an address change, and requested a replacement. Cigna placed a stop payment on the initial check and issued a new check. Mills nevertheless cashed the first check at Sun's Market (Sun). Sun then presented the check for payment through its bank.

Cigna's bank dishonored the check, stamped it "Stop Payment," and returned the check to Sun's bank. Had Sun filed an HIDC claim against Cigna as the issuer of the check, Sun would have been entitled to be paid because of its status as a Holder in Due Course. Apparently Sun either did not know about HIDC or chose not to pursue it, because they merely pinned the check on a bulletin board in the store, for two years.

Robert Triffin bought the check from Sun, assumed its HIDC rights, and filed this lawsuit in August 1995, over two years after the check was returned unpaid (statute of limitations is three years). The Court ruled in favor of Robert Triffin, and ordered Cigna to pay him $484, plus interest.

**Recommendation:** Cause a check to "expire" before replacing it, or you may be held liable for both checks. Print an expiration statement on the check face such as, "THIS CHECK EXPIRES AND IS VOID 20 DAYS FROM ISSUE DATE." If a check is lost, wait 20 + 2 days from the initial issue date before reissuing. Many companies print "VOID AFTER 90 DAYS" but cannot reasonably wait that long before re-issuing a check. A party that accepts an expired check has no legal basis to sue as an HIDC if the check is returned unpaid.

**Superior Court of New Jersey, Appellate Division, A-163-00T5**
**lawlibrary.rutgers.edu/courts/appellate/a0163-00.opn.html**

### ROBERT J. TRIFFIN V. SOMERSET VALLEY BANK AND HAUSER CONTRACTING CO.

**Issue: You May Be Held Responsible For Checks You Did Not Issue or Authorize**

Hauser Contracting Co. used ADP for payroll services. A thief obtained check stock that looked identical to ADP's checks and created 80 counterfeit payroll checks totaling nearly $25,000 that were identical to Hauser Contracting Co.'s.

A retailer who knew Mr. Hauser became suspicious and called him. Somerset Valley Bank also called. Mr. Hauser reviewed the in-clearing checks, which looked just like his, and confirmed the checks were unauthorized and the payees were not his employees. The bank returned the checks marked as "Stolen Check - Do Not Present Again."

Mr. Triffin bought 18 of these checks totalling $8800 from four check cashing agencies, claimed HIDC status, and sued both Mr. Hauser and his bank for negligence for not safeguarding the payroll checks and facsimile stamp. Because the counterfeit and authentic checks looked identical, the lower court ruled for Triffin. Hauser appealed, but the Federal Appellate Court upheld the lower court. The Court said the counterfeit check met the definition of a negotiable instrument, and because the check and signature were identical to an authentic check, the check cashing agency could not have known it was not authentic.

**Recommendation:** Use a controlled check stock, which means using checks that are uniquely designed or customized for your organization and are not available blank to others. **SAFEChecks** and the **SuperBusinessCheck** are controlled check stocks.

**Superior Court of New Jersey, Appellate Division, A-163-00T5**
**lawlibrary.rutgers.edu/courts/appellate/a0163-00.opn.html**

## ROBERT J. TRIFFIN V. POMERANTZ STAFFING SERVICES, LLC

**Issue: High Security Checks May Protect You From Some Holder in Due Course Claims**

Pomerantz Staffing Services used high security checks that included heat sensitive (thermochromatic) ink on the back and a warning banner on the face that said, "THE BACK OF THIS CHECK HAS HEAT SENSITIVE INK TO CONFIRM AUTHENTICITY." Someone made copies of Pomerantz's checks, but without the thermo ink on the back. They cashed 18 checks totaling $7000 at Friendly Check Cashing Company. Friendly's cashiers failed to heed the warning on the check face, and did not look for the thermo ink on the back. All 18 checks were returned unpaid, likely caught by Positive Pay.

Mr. Triffin bought the checks, claimed Holder in Due Course status, and sued Pomerantz. Pomerantz counter-sued and won! The judge correctly asserted that if Friendly had looked for the thermo ink as instructed, they could have determined the checks were counterfeit. Because they were provided a means to verify authenticity and failed to do so, they were not an HIDC and had no rights to transfer to Mr. Triffin.

This case illustrates the value of check security features, a properly worded warning band, and a controlled check stock. Pomerantz was protected by his checks.

**Recommendation:** Use high security checks with overt and covert security features, including explicitly worded warning bands. Such security features will also help prevent other kinds of check fraud. The **SuperBusinessCheck** is a properly designed high security check with 16 security features.

**http://lawlibrary.rutgers.edu/courts/appellate/a2002-02.opn.html**

***Visit www.fraudtips.net for an in-depth article, Holder in Due Course and Check Fraud, written by Frank Abagnale and Greg Litster. Click on Holder in Due Course.***

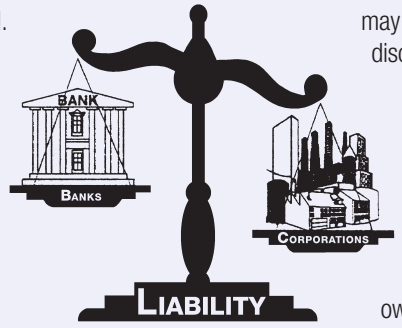
# FACSIMILE SIGNATURES MAY INVITE FRAUD LOSSES

**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 resulting from 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 cancelled.

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 visually compared 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 for the loss.

Arkwright Mutual Insurance, who insured FPL against commercial crime, reimbursed the company. It then sued NationsBank. 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 Florida court granted summary judgment to NationsBank, agreeing that these two contractual agreements shifted the liability for the forged checks to Florida Power and Light.

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."

Conclusion: Implement fraud prevention measures such as Positive Pay and highly secure controlled check stock, which would have caught the forged checks and stymied the forger.

# Timely Account Reconciliation is Essential

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

Do you reconcile 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.

# Small Business and Security Compliance

Merchants and retailers are becoming more dependent on information-processing systems, and thieves are becoming more sophisticated in their ability to penetrate those systems for fraudulent purposes. In today's economy, it is critical for a company's systems to be secure.

Organizations are now required to develop methods to protect the privacy and financial information of their customers. Payment Card Industry (PCI) Standards have been developed that impose security requirements on all merchants who store, transmit, or process credit card information. There is increasing pressure on companies to become "PCI Compliant."

In addition, consumers are now more conscious about security issues, and take their business elsewhere if a company has problems in this area. In an online survey conducted by TNS PLC, a London-based market research company, 75 percent of shoppers reportedly discontinued shopping from sites because of security concerns. A report from the Ponemon Institute indicated that when merchants experienced a data breach, 74 percent lost customers, 59 percent faced potential lawsuits, 33 percent faced potential fines, and the share value decreased for 32 percent of respondents. These serious, multi-faceted consequences make it even more imperative for companies to protect themselves and their customers from cyber crime.

Large companies have long been aware of compliance with PCI Standards. Smaller organizations are now under pressure to become compliant, but many lack the in-house knowledge or the financial resources to do so. Here are two scenarios: First, a small restaurant that accepts credit cards. The bank has told the owner to comply with PCI Standards or it will withdraw card-processing privileges. However, the Standards are very technical and the owner doesn't understand them. After calling a few security vendors, it becomes clear that even uncomplicated solutions cost several thousand dollars, which is unaffordable. He cannot change banks, and is essentially stuck.

Next, imagine that most of a bank's merchant customers do not comply with PCI Standards, and the bank is facing numerous fines and penalties. Although it has strongly encouraged its customers to become compliant, they have not done so because of cost constraints. The bank, like the restaurant, is in a difficult position.

Many new enterprises are emerging that offer compliance solutions for small organizations. Panoptic Securities allows merchants to asses their security needs online for free. It then provides low-cost solutions for them to bring their standards into line. Other companies offering security services include Qualys, Comodo HackerGuardian, VeriShield System by VeriFone, Magnesafe by MagTek, MAXX Business Solutions, mailMax by Trustwave, and SonicWALL. Hacker Safe Search Feed automatically integrates the Hacker Safe seal into comparison-shopping listings; companies using this service have seen a substantial increase in revenues compared to sites that did not implement the service.

The need for compliance to higher security standards has given rise to many new firms with resourceful answers. Companies that take advantage of these solutions will be able to better avoid compromising situations and retain the trust of their clients, in addition to avoiding fines and penalties for non-compliance.

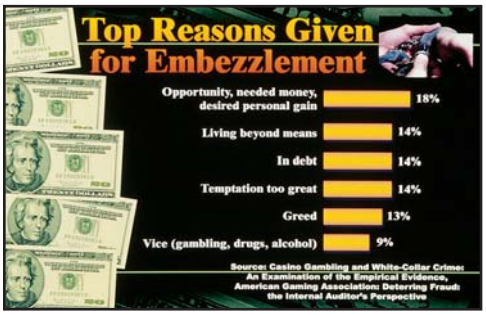
***Excerpted from "Small Business Security, Entrepreneurial Solutions" by W. Gibb Dyer, Jr., PhD. Brigham Young University Marrriott School of Management Alumni Magazine, Fall 2008. To read the complete article, visit www.FraudTips.Net/BYUMagFall2008***

# 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. 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, check fraud ranks Number 2.




Under the revised Uniform Commercial Code (UCC), employers have 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 following basic internal financial controls, companies can prevent or substantially reduce their risk of embezzlement.

## Hiring Practices

Use hiring procedures that keep people with questionable backgrounds out of your organization. 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.

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

## 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.

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.

To help identify and reduce exposure to fraud in the accounts 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

Access to the master vendor file 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.

Mailed checks returned by the Post Office as undeliverable should not be returned to the person who processed 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.

## Audits

Conduct periodic surprise audits of the various check control functions. Audits should test the overall system to ensure that it is secure and 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 suspicious activity.

## 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 vendor 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 on stolen checks.

# Frank W. Abagnale

Frank W. Abagnale is one of the world's most respected authorities on the subjects of forgery, embezzlement and secure documents. For over 30 years he has lectured to and consulted with hundreds of financial institutions, corporations and government agencies around the world.

Mr. Abagnale has been associated with the Federal Bureau of Investigation for over 30 years. He lectures extensively at the FBI Academy and for the field offices of the FBI. More than 14,000 financial institutions, corporations and law enforcement agencies use his fraud prevention materials. In 1998, he was selected as a distinguished member of "Pinnacle 400" by CNN Financial News. He is also the author and subject of *Catch Me If You Can*, a Steven Spielberg movie that starred Tom Hanks and Leonardo DiCaprio.

**Mr. Abagnale believes that the punishment for fraud and the recovery of stolen funds are so rare, prevention is the only viable course of action.**

## SAFE*Checks*®

*America's Premier Check Fraud Specialists*

Checks offered by SAFE*Checks*® were designed by Frank Abagnale. As a former master forger, Mr. Abagnale's experience designing checks is unsurpassed. The story of Frank Abagnale and the origin of **SAFE***Checks* follows.

**SAFE***Checks* began in 1994 as a division of a California business bank. In the early 1990s, the bank experienced an enormous number of fraudulent checks paying against its customers' accounts. Over a three-year period, the bank saw altered and counterfeit checks increase from $90,000 to over $3,000,000. Many of these checks were perfect replications of authentic checks.

Greg Litster, then Senior Vice President and head of the bank's Financial Services Division, summoned the bank's primary check vendors and made a simple request: "Provide our business customers with checks that forgers cannot replicate or alter." These vendors included some of the largest check printers in the nation, yet none of them offered a high-security check.

With fraud losses mounting, Mr. Litster hired Frank Abagnale to assist the bank in its fight against forgers. Mr. Abagnale helped the bank strengthen its internal controls, and in 1994, at the bank's request, designed a new, high security business check. That check became **SAFE***Checks*. Over the next three years the bank caused its corporate customers to use **SAFE***Checks*, and fraud attempts and losses began to drop immediately. By the end of 1996, check fraud attempts fell to $120,000, a 95 percent decrease from 1993 levels. Mr. Litster acquired the **SAFE***Checks* operation from the bank in 1997, and is its president.

**SAFE***Checks* offers high-security checks, including the Supercheck, the SuperBusinessCheck, and SAFEChecks business checks. **SAFE***Checks* also offers Positive Pay file transmission software (see SafePay123.com), and MICR laser check printing systems with a Secure Name and Number font to help prevent altered payee names and dollar amounts.


SAFE*Checks*®

*America's Premier Check Fraud Specialists*

**(800) 755-2265**

safechecks.com

**8934 Eton Avenue**
**Canoga Park, CA 91304**
**(800) 755-2265**
**Fax (800) 615-2265**
**info@safechecks.com**