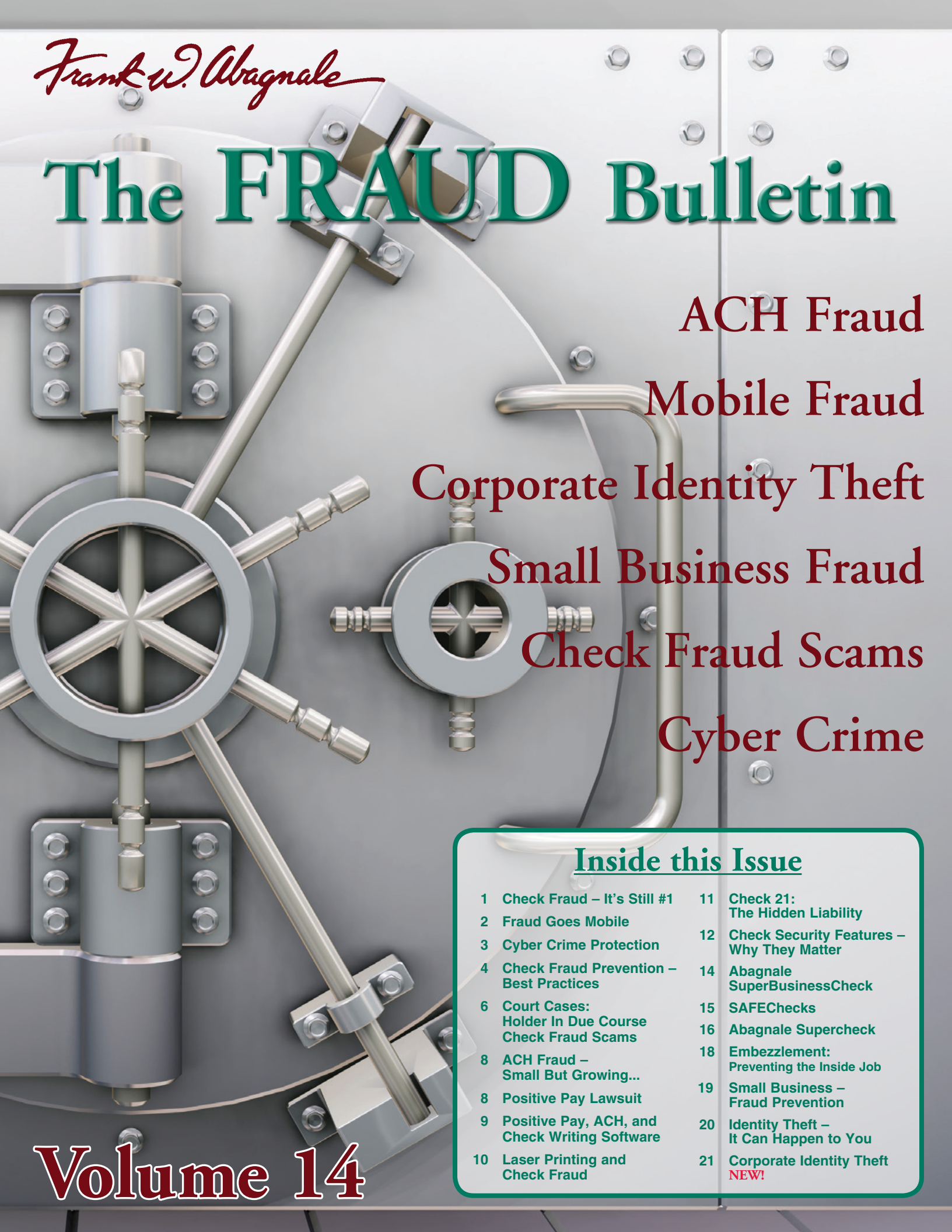
Frank W. Abagnale

The FRAUD Bulletin



ACH Fraud

Mobile Fraud

Corporate Identity Theft

Small Business Fraud

Check Fraud Scams

Cyber Crime

Inside this Issue

1 Check Fraud – It's Still #1
2 Fraud Goes Mobile
3 Cyber Crime Protection
4 Check Fraud Prevention – Best Practices
6 Court Cases: Holder In Due Course Check Fraud Scams
8 ACH Fraud – Small But Growing...
8 Positive Pay Lawsuit
9 Positive Pay, ACH, and Check Writing Software
10 Laser Printing and Check Fraud
11 Check 21: The Hidden Liability
12 Check Security Features – Why They Matter
14 Abagnale SuperBusinessCheck
15 SAFEChecks
16 Abagnale Supercheck
18 Embezzlement: Preventing the Inside Job
19 Small Business – Fraud Prevention
20 Identity Theft – It Can Happen to You
21 Corporate Identity Theft NEW!

Volume 14

Frankly Speaking . . .

Check fraud and identity theft are some of the most serious financial crimes in America. Every research report available has placed check fraud in the *tens of billions* of dollars each year. The Bureau of Justice Statistics reported that financial losses from identity theft totaled almost $25 billion, with almost 17 million victims.

Check Fraud

Check fraud is the most dominant form of payment fraud, representing 45 percent of all payment fraud losses, surpassing credit card fraud, ACH fraud and wire fraud. Clever check fraud gangs constantly try new techniques to beat the banking system and steal money. While one might expect banks to be liable for these losses, revisions in the Uniform Commercial Code (UCC) have shifted the liability from the bank to the party in the best position to prevent the loss. Today, the losses are shared between a bank and its customer based upon each party's comparative negligence. I designed the **SuperBusinessCheck, SAFEChecks** and the **Supercheck** to help organizations and individuals protect themselves against check fraud. **See Pages 14 through 17**.

Corporate Identity Theft

I believe identity theft will become one of the most profitable criminal activities in history because it is so easy to commit and so difficult to prosecute. Identity theft is no longer solely restricted to individuals. Corporations are increasingly being targeted, hacked, and victimized. Let me give three examples of new twists on corporate identity theft.

CASE 1 – Cyber criminals infiltrated a company's computer system, accessed its accounts receivable database, and sent bogus change-of-bank notifications to some customers. The bogus notices instructed customers to remit payment to a new PO Box or to the new bank, with updated wiring instructions. (The hackers controlled both the new PO Box and the new bank account.)

SOLUTION Avoid falling for bogus change-of-bank-notices allegedly sent by your vendors, whether those changes came via email or USPS. All changes of remittance address or bank wiring or ACH instructions must be verified with your vendor. Verifications should be documented and audited. In this case, the company narrowly avoided a substantial loss because its bank had implemented a policy of confirming all bank changes on repetitive wires going to Asia or Eastern Europe. Using this protocol, the bank also recently stopped an improper wire for $900,000 going to China and a wire for $1,400,000 going to Eastern Europe.

RECOVERY If you fall victim to this scheme and mailed a check to a P.O. Box, your remedy for recovery may be a forged endorsement claim against the bank of first deposit. Consult an attorney with expertise in banking law. If you paid by ACH or wire, the money is gone. Recovery will likely be through an insurance claim. Ask your insurance agent about check fraud and cyber crime coverage.

CASE 2 – A company was hacked when an employee's computer got a keystroke tracking virus. The cyber thieves captured the bank logon, and then targeted the company's VoIP phone system. The hackers eavesdropped on calls made to and from the bank, and learned the company's responses when the bank called to confirm wires. The hackers then sent a wire to Asia from the infected computer, allegedly to a vendor, but changed the vendor's banking information to a bank account they controlled. Immediately after sending the wire, the hackers reprogrammed the VoIP phone system and rerouted calls from the bank to an outside accomplice to verify the wire.

SOLUTION Page 3 of this Bulletin has many tips for mitigating and preventing cyber crime losses. Most banks have protocols to authenticate wire transfers; fewer have protocols to monitor bank changes on repetitive outbound wires. In this case, the company was very fortunate that its bank had a policy of confirming vendor bank changes on repetitive wire transfers leaving the USA. When the bank called to confirm the vendor's bank change, the call was routed to the outside accomplice who could not give the proper response. The banker hung up and called back. The call was again rerouted, and the bank was again given an incorrect response. The banker then called their primary contact on his cell phone. He confirmed the company had not received any calls from the bank that morning, and that both the bank change and wire were unauthorized. The bank's policy of verifying bank changes on repetitive foreign wires prevented a significant loss. Ask your bank for its verification policy.

RECOVERY Unfortunately, recovery will most likely be through an insurance claim. Speak with your insurance agent about cyber crime insurance.

CASE 3 – A title insurance company emailed a preliminary title report to an escrow agent. The prelim included their bank's wiring instructions. The escrow agent's email server was hacked, and the title officer's email attachment was opened and the bank information was altered. When the transaction closed, the escrow agent wired funds according to the altered preliminary title report instructions she had received. The funds went to the hacker. An investigation revealed the original email and attachment sent by the title company were intact.

SOLUTION When emailing pdf documents with banking or confidential information, password-protect the template or document so it cannot be easily opened and altered.

Individual Identity Theft

Being a victim of identity theft is a nightmare, costing an individual significant time and money to get their credit cleaned up. I am personally concerned, therefore I subscribe to a monitoring service that notifies me each time my credit report is accessed. Any effective identity theft prevention service should monitor all three credit reporting agencies, and notify you in real time if your credit has been accessed. Additional suggestions to prevent identity theft can be found on Page 20.

This Fraud Bulletin was created to help individuals, families, and companies learn how to protect themselves. I hope you find it useful. I have also written three books that cover numerous scams in detail **(See Page 21).**

Sincerely,

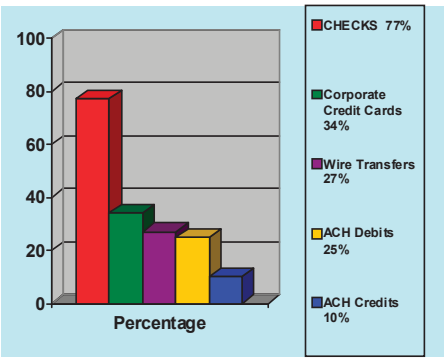
Frank W. Abagnale

www.abagnale.com

Check Fraud–It's Still #1

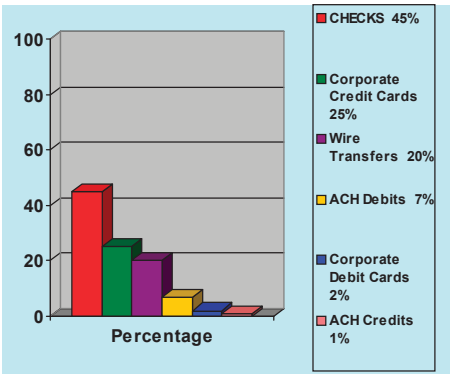
Check fraud litigation began in 1762 with Price v. Neal, and check fraud has continued unabated for the last 250 years. With 50% of today's organizations still issuing checks, check fraud will not be going away anytime soon. The 2015 *AFP Payments Fraud and Control Survey* indicates that "checks remain the most-often targeted payment method by those committing fraud attacks" with 77% of affected organizations reporting that their checks were targeted.

How Organizations Experience Payment Fraud



Not only are checks the dominant vehicle for committing payment fraud, they are the greatest source of actual losses, with 45% of financial losses coming from check fraud. All types and sizes of organizations are targeted, and those that are successfully defrauded once are often targeted repeatedly.

Greatest Financial Losses by Method



In the 2014 AFP Survey, 62% said that the most prevalent check fraud method was "counterfeiting by altering the MICR line on the check." Other types of counterfeit checks used a fake company name. More than half – 52% – of check fraud attempts involved altered payee names, and 37% were altered dollar amounts. This is up from 49% and 25% respectively in 2012. Such alterations may have been prevented by using high security checks. **(See Pages 14 – 16.)**

There were additional reasons for check fraud losses, all of which were within the organization's control: in 34% of the cases, Positive Pay or account reconciliation was not timely, and 24% of the time the losses came from internal fraud. Internal fraud was up from 13% in 2012. Another 15% had gaps in online security control and/or criminal account takeover which contributed to check fraud losses.

Holder in Due Course

In 38% of the check fraud losses, the fraudulent check was cashed by a check cashing service, initiating a Holder In Due Course claim. This is up from 22%, showing a large rise in losses stemming from Holder In Due Course claims. Holder in Due Course (HIDC) is a powerful part of the Uniform Commercial Code which regulates an organization's liability for check fraud. Under HIDC, a company can be held liable for counterfeit items that look "genuine," or are virtually identical to its own checks. If a genuine-looking counterfeit check was cashed by the bank, even if the account was on Positive Pay, the issuer can still be held liable. Placing a stop paym ent on a check does not end the issuer's liability to pay the check. HIDC trumps stop payments and Positive Pay. This is the reason to use a **controlled check stock**, and to have a short expiration date printed on the check. **See Holder In Due Course, Page 6.**

Uniform Commercial Code

The legal basis for liability in check fraud losses is found in the Uniform Commercial Code (UCC). The UCC 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. For example, in the AFP 2015 survey, 79% of all organizations use Positive Pay. A bank can argue that a company not using Positive Pay is not exercising "ordinary care." **See "Cincinnati" on Page 8.** 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. Second, the concept of "comparative negligence" in Sections 3-406(b) and 4-406(e) can also shift liability from the bank to the account holder. If both the bank and the account holder have failed to exercise ordinary care, a loss may be allocated based upon how each party's failure contributed to the loss.

Read Bank Contracts

Read your bank contracts and disclosure agreements to understand your liability for fraud losses under the UCC. This includes the small print on signature cards and disclosure statements. A bank's intentions must be stated clearly to prevail against a customer in a check fraud case. Banks are re-writing their signature card agreements and adding new provisions to their disclosure statements. For a summary of the UCC, visit www.FraudTips.net.

Risk Management

Financial institutions and bank customers face a 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 payment fraud? How might our image and reputation be damaged? How much are we willing to spend to reduce this exposure?"

Prevention Is For Everyone

Everyone has a responsibility to help prevent check fraud. Financial institutions still list check fraud as one of their top three threats, and view a lack of customer awareness as one of their biggest challenges in fraud prevention. Given that 50% of today's organizations still issue checks, financial professionals must use a number of tools and strategies to protect their organizations. The Federal Reserve recently required all banks to educate their customers on how to prevent fraud. Fraud mitigation tools are discussed throughout this Fraud Bulletin, and should be reviewed with your bank.

Frank Abagnale has observed:
"Punishment for fraud and recovery of stolen funds are so rare, prevention is the only viable course of action."

Resources

Association for Financial Professionals (AFP) 2014 and 2015 Payments Fraud and Control Surveys

Fraud Goes Mobile...

Mobile fraud continues to skyrocket, and is becoming much more sophisticated. Malicious activity on mobile platforms is growing much more quickly than it did on PC platforms. The vast majority of mobile malware is aimed at Android phones, with almost 30,000 new strains of malware in 2014 alone.

Most malicious mobile code consists of Trojans that imitate legitimate apps or games. They are uploaded to mobile app marketplaces, intending for users to download and install them, allowing criminals to infiltrate the users' systems.

One effective method for spreading malicious apps was through a mobile email account. An email message provided a link and invited the user to download and install an app. If installed, the user's contacts were gathered from the phone's address book and the "invitation" went out to those contacts as well.

Other major concerns for mobile users are links to malicious websites. The links may be imbedded in emails, attachments, social networks or text messages, and are activated when the victim clicks on the link or visits the site with their mobile device.

Smishing is a new mobile fraud strategy, sending unsolicited text messages to capture a victim's personal data. Once spammers capture the information, they either sell it or use it to commit fraud.

Mobile Banking Fraud

In the world's top 90 app stores, there are 350,000 apps which reference banking. (See www.RiskIQ.com and www.infosecurity-magazine.com.) Of these, 40,000 were deemed to be "suspicious." About half contained Trojan malware, and a significant percentage included adware, spyware, explicit code, and malicious Java script. A large number had excessive permissions, which allow criminals to capture device logs, record audio, write to contacts lists, read SMS messages, disable key guards, access GPS information, and install malicious packages into a user's phone.

Many of the malicious mobile apps were "fake" versions of official mobile apps. Malicious banking apps can capture a bank customer's user name and password, and can intercept text messages the bank sends to its customer for authentication. The malicious parties can then access the account and transfer funds.

Additionally, mobile remote check deposit has become one of the most desirable mobile banking applications. Almost all banks now offer or plan to offer Remote Deposit Capture (RDC) for mobile phones. Fraudsters have largely left mobile RDC alone, perhaps because of low daily deposit limits. However, cases of double-depositing checks via mobile banking are growing.

The Federal Reserve Board predicts that almost half of all mobile users will adopt mobile banking in one capacity or another. It will behoove all mobile phone users and financial institutions alike to be alert and vigilant toward fraud prevention.

iStock Photos

Mobile Deposits & Double Debits

The legal basis for creating and depositing a digital image of a check is Check 21. Check 21 has a rule ("warranty") that specifically prohibits a check or its image from being presented for payment more than once, and provides a powerful recovery remedy if it occurs. Example: John receives a check and deposits the check (its electronic image) via his smart phone app. He still has the physical check, which he later cashes at a check-cashing store. When the check casher deposits the original physical check and it hits the drawer's bank account, that second presentment of the check breaches the Warranty that John made when the electronic image was deposited.

Remedy: Under Check 21, the first presentment of the check (via smartphone) can be charged back to the bank of first deposit as a breach of Warranty (due to the second presentment) for up to one year from the date the injured party discovers the loss.

Mobile Deposits & Holder In Due Course

Scenario: John Doe picks up a check made payable to "John Doe" from a business or individual. He walks outside and deposits the check remotely using his smartphone. He then walks back inside and returns the check, asking that it be replaced with a new check made payable to John Doe OR Jane Doe. The issuing person or company reissues a new check payable to John Doe or Jane Doe. They don't think to place a Stop Payment on the first check because it is in their physical possession. John Doe cashes the second check, and waits overnight for the first check to clear before withdrawing the money from the first check. Unfortunately, the drawer issuing the check can be held liable for both checks. Reason: The second check was cashed at the bank, and the first check was deposited remotely. While banks often cooperate to stop fraudulent activity, John Doe's bank is a Holder In Due Course and is under no obligation to return the funds to the issuer.

To prevent this kind of theft, if a check leaves your possession for any length of time and is returned for a replacement, place a Stop Payment on that check. Cause the recipient to sign an affidavit declaring the check has not been remotely deposited, and accepts liability for all expenses to recover any stolen funds. **See Check 21, Page 11.**

Protect your mobile device from malware by updating to the latest operating system and using mobile security apps. Read reviews of security apps on respected mobile security websites. Be wary of unsolicited app offers, especially if it comes to you via a text message. Trustworthy apps will have many users, and will have many user reviews written in correct English. Check your mobile phone bill for unknown or unusual charges. Remember: for mobile fraud prevention, the best defense is to use common sense.

Cyber Crime Protection

Cyber crime is a mature, underground international business with well-organized and well-financed syndicates. These syndicates sell customized malware and instant hacking tools to novice cyber criminals, allowing them to quickly join the criminal community. Individuals and institutions of every size and industry are potential victims. Cyber criminals are increasingly more inventive, sophisticated, and malicious, and the battle against them will never end. Organizations and individuals must be continually vigilant, and devote time and resources to thwart these attacks.

New Twists on Cyber Crime

Describing the many methods criminals are now using to infiltrate computer systems and mobile devices – and how you can block them – is beyond the scope of this Bulletin. However, we have assembled many excellent articles and links that will provide you with this information. Visit **www.safechecks.com/articles**, and see **Resources** at the bottom of this page.

Malware and hacking are the main methods used to infiltrate an organization's computer system. There are two types of malware – "auto-executable code" that can happen merely by visiting an infected website, and code that requires interaction by users, e.g. opening an email attachment or clicking on an imbedded link. Because online threats are so rampant and insidious, assume that your computers now being used for email and web searches are already infected. However, even if a computer becomes compromised, preventing online intruders from stealing your money is simple.

Preventing Unauthorized Transfers

In four easy steps you can prevent unauthorized online money transfers: 1) Purchase a new computer that is dedicated to online banking only. It connects to the bank, and nothing else. A basic, inexpensive computer will suffice. 2) Require two different computers and users/passwords to send money out of your account. One or more employees can initiate a wire or ACH transfer using their everyday computers, but require that all initiated transfers be released using only the dedicated banking computer. Persons authorized to release the transfers must use different user names and passwords than those used to initiate the transfer. 3) Update your bank's Electronic Funds Transfer (EFT) agreement to reflect your revised, two-computer initiation-release procedures. 4) Implement all additional controls and technologies your bank recommends. Failure to implement the controls the bank recommends may result in your being liable for any cyber losses.

The justification for using a dedicated computer to release money transfers is best illustrated by a cyber crime case in California.

In 2010, the owner of an escrow company in California received an e-mail informing her that a UPS package she had been sent was lost, and urged her to open the attached invoice. When she opened the attached file, nothing happened, so she forwarded it to her assistant who also

tried to open it. The alleged "invoice" contained a keystroke logger virus that captured the passwords used on both the owner's computer and the PC belonging to her assistant, who was the second person needed to approve wire transfers. After the passwords were captured, cyber thieves sent 26 wire transfers totaling $465,000 to 20 individuals around the world. This loss could have been prevented if the company had used a dedicated, "clean" computer to release wires/ACH transfers.

Companies / Organizations

- Review the latest reports from Verizon, Symantec, and other reputable organizations that do in-depth cyber crime research, and implement their recommendations.
- Perform thorough background checks on new employees.
- Implement security policies to restrict unauthorized access to sensitive data.
- Require that all sensitive data be encrypted or password protected before transmission.
- Regularly review and install updated patches for your operating system software. Frequently review network log data to identify any unusual or unauthorized events.
- Establish policies and install software that limits the sites users may access; use caution when visiting unknown websites.
- Use a network-based Intrusion Prevention System (IPS).
- Educate in-house developers about secure development practices, such as Microsoft's Security Development Lifecycle.
- When employees leave the company, immediately disconnect all their access to the company's network and building, shut down remote connections, and collect their cell phones, iPDAs, smartphones, etc. Delete any passwords they used.

Individuals / Families

- Use anti-virus and anti-spyware software on your computer, and update frequently.
- Use a properly-configured firewall.
- Add security software to your smartphone, IPad, tablet, etc.
- Do not follow links found in email messages from untrusted sources; they may be links to spoofed websites. Manually type the URL.
- Completely close down your Internet browser after doing online banking or shopping.
- 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, cell phones.
- Don't send sensitive files over a Wi-Fi network unless it is secure. Public "hot spots" are not secure.
- When you are not using Wi-Fi, close down 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. Look the number up yourself.
- Protect your children from online predators by tracking their keystrokes, emails, MySpace, Facebook, IM, and websites they visit on their computers and cell phones. See **Spector Pro, PhoneSheriff, eBlaster**, etc.

Resources

2010-2014 Verizon Data Breach Investigations Report
2006-2014 Symantec Internet Security Threat Reports
2009-2013 CSI Computer Crime and Security Survey
2014 WhiteHat Website Security Statistics Report
PC Magazine (pcmag.com) CNET Networks (cnet.com)
www.counciloncybersecurity.org
www.fbi.gov/about-us/investigate/cyber

Check Fraud Prevention—Best Practices

No product, program or policy can provide 100% protection against check fraud. However, specific practices can significantly reduce check fraud risk by discouraging a criminal from alteration or replication attempts, and by thwarting his counterfeiting efforts. The following are important recommendations for reducing risk.

High Security Checks

Check fraud prevention begins with high security checks. High security checks are the first line of defense against forgers, and there is substantial evidence that they significantly reduce check fraud attempts: Every loss begins with an attempt–eliminating the attempt eliminates the loss! High security checks also help prevent altered payee names or dollar amounts.

High security checks should contain at least ten (10) safety features. More is better. **Pages 14 through 17 show high security checks designed by Frank Abagnale.** Many check manufacturers claim their checks are secure because they include a padlock icon. The padlock icon does not mean a check is secure; only three safety features are needed in order 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.

Positive Pay

In addition to high security checks, Positive Pay is one of the most effective check fraud prevention tools. It is an automated check-matching service that can detect most bogus checks. It is offered through all major banks and many smaller banks. To use this service, the check issuer transmits to the bank an electronic 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 being presented for payment against the previously submitted list of checks issued by the company. All the components of the check must match exactly or it becomes an "exception item." The bank provides the customer with an image of the suspect check 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 **(see Pages 4 and 9)**.

Because revisions in the UCC impose liability for check fraud losses on both the bank and its customer, it is important for everyone 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.

> ***"Positive Pay is the best product in 30 years to deal with the problem of forged, altered and counterfeit checks."***
>
> ***— Frank W. Abagnale***

Reverse Positive Pay

Organizations or individuals with small check volume can use Reverse Positive Pay. This service allows an account holder to log on and review in-clearing checks daily to identify unauthorized items. The account holder can download the list of checks from the bank and compare them to their issued check file. Suspect checks must be researched and the bank notified of items to be returned that day. While Reverse Positive Pay provides timely information on a small scale, for larger check volume it is not a worthy substitute for Positive Pay.

Payee 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 name by using the X, Y coordinates on the check face and 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. However, **PPP is not 100% foolproof because criminals can add a fraudulent Payee Name two lines above the original Payee Name**, outside of the bank's X,Y coordinates. The bogus added Payee Name will not be detected by Payee Positive Pay, resulting in the altered check being paid **(see Page 9)**.

Preventing Added Payees

Adding a new Payee Name is a major scam used by sophisticated forgery rings. They understand Payee Positive Pay's limitations and simply add a new payee name above the original name. They then cash the check using bogus documents in the name of the added payee. To help prevent added payee names, use a Secure Name Font **(see Pages 9 and 10)** or insert a row of asterisks above the payee name. To help prevent altered payees, use high security checks like the **SuperBusinessCheck** or **SAFEChecks**, and good quality toner to keep the **Secure Name Font** or asterisks from being removed without leaving evidence. Cheap toner will peel off with common office tape.

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.

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. To defend against washing, use high security checks that are reactive to many chemicals. When a check reacts to chemicals, the "washing" can often be detected when the check dries. 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 16.**

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 10 on Laser Printing.**

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. If you are unable to reconcile on time, hire your accountant or an outside reconciliation service provider and have the bank statements sent directly to them.

The people issuing checks should not be the same people who reconcile the accounts.

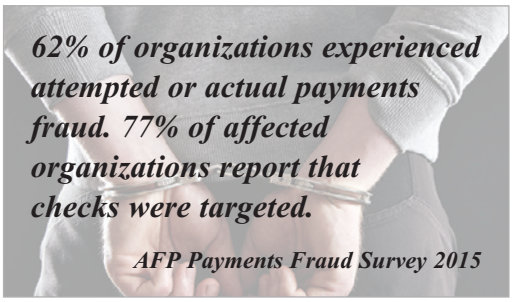
Repeater Rule

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.

Controlled Check Stock

Generic check stock that is sold completely blank is known as uncontrolled check stock. It is readily available to everyone, including criminals, and is a major contributor to check fraud. If multiple companies use the same blank, uncontrolled check stock, they are



iStock Photos

left with no legal defense against their bank if the bank pays a counterfeit check which is made on check stock identical to their own. **(See Robert J. Triffin V. Somerset Valley Bank and Hauser Contracting Company, Page 7.)**

Controlled check stock is customized in some unique way for each organization. It should also be numbered on the back of the check with sequenced inventory control numbers to prevent internal fraud. **See Pages 14 and 15.**

Manually Issued Checks

Every organization occasionally issues manual checks. Some are typed on a self-correcting typewriter which uses a black, shiny ribbon. This black shiny ribbon is made of polymer, a form of plastic. Plastic is typed onto the check. Forgers can easily remove this typing with ordinary office tape, type in new, fraudulent information, and then cash the signed, original check!

When typing manual checks, use a "single strike" fabric ribbon, which uses ink, not polymer. They can be found online in the catalog of major office supply stores.

Check Stock Controls

Check stock must be kept in a secure, locked area. Change locks or combinations periodically. 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 by two people not directly responsible for the actual check printing. When checks are printed, every check should be accounted for, including voided, jammed and cancelled checks. After the check run, remove the unused check stock from the printer tray and return it to the secure storage location.

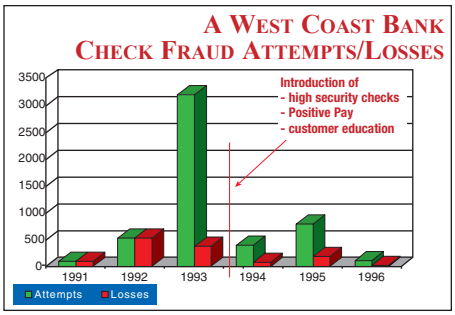
Wire Transfers

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.

Annual Reports and Correspondence

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

Do not include account numbers in correspondence. Credit applications should include the name and phone number of the company's banker, 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 sent, and it could be used to commit fraud.



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

Court Cases

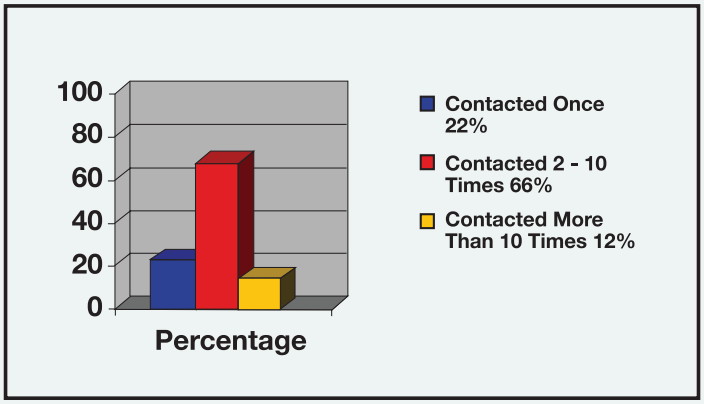
Holder In Due Course

Holder in Due Course, a powerful part of the Uniform Commercial Code, can adversely impact an organization's liability for check fraud, including those checks on which a "stop payment" has been placed.

Who or what is a Holder in Due Course? A Holder in Due Course (HIDC) is anyone who accepts a check for payment, and on the face of the check there is no evidence of alteration or forgery, 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 full face value is 10 years from the issue date, or three years from the date the check was deposited and returned unpaid, whichever comes first.

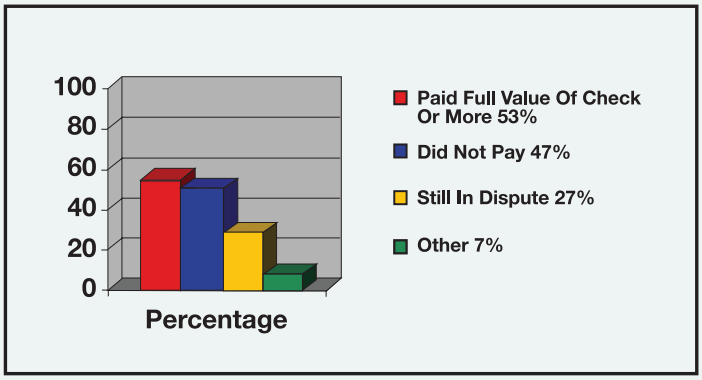
Frequency of HIDC Claims



Holder in Due Course trumps stop payments and Positive Pay exceptions. Further, an HIDC can assign, sell, give, or otherwise transfer its rights to another party, who assumes the same legal rights as the original Holder.

In the 2012 AFP Payments Fraud and Control Survey, 48 percent of organizations' check fraud losses were a result of payouts to check cashers (bank and non-bank) from Holder In Due Course claims. This is up from 37 percent in the 2009 survey, indicating a growing and serious concern.

Actions Taken in Response to Holder in Due Course Claims



Prudent companies use controlled high security checks to protect themselves from some HIDC claims.

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

ROBERT J. TRIFFIN v. CIGNA INSURANCE

Placing A Stop Payment Does Not End 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, which Mills received and cashed. Later, Mills cashed the first check at Sun's Market (Sun). Sun presented the check for payment through its bank.

Cigna's bank dishonored the first check, stamped it "Stop Payment," and returned the check to Sun's bank, who charged it back against Sun's account. Sun was a Holder In Due Course, and if Sun had filed an HIDC claim against Cigna as the issuer of the check, it would have been entitled to be paid. Apparently, Sun did not know about HIDC, because it merely pinned the check on a bulletin board in the store, where the check stayed 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: Allow a check to "expire" before replacing it, or you may be held liable for both checks. **A party that accepts an expired check has no legal standing to sue as a Holder in Due Course if the check is returned unpaid.**

Print an expiration statement on the check face such as, "THIS CHECK EXPIRES AND IS VOID 30 DAYS FROM ISSUE DATE." If a check is lost, wait 30 + 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.

Superior Court of New Jersey, Appellate Division, A-163-00T5
lawlibrary.rutgers.edu/courts/appellate/a4000-95.opn.html

An analysis of court cases can be downloaded from www.safechecks.com. Click on Fraud Prevention Tips, then Holder in Due Course.

ROBERT J. TRIFFIN v. SOMERSET VALLEY BANK AND HAUSER CONTRACTING CO.

You May Be Held Liable 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 the ADP checks used by Hauser Contracting Co.

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."

Robert 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

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.

Robert 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.

CHECK FRAUD SCAM — IT CAN HAPPEN TO ANYONE

Greenberg, Trager & Herbst, LLP v. HSBC Bank, USA 17 N.Y.3d 565 (2011)

In a landmark decision, the New York Court of Appeals upheld that the depositor of a counterfeit check is responsible for risk of loss "until the settlement becomes final. Statements concerning 'clearing' of a check and funds availability are irrelevant."

A New York City law firm (Greenberg) received an email requesting legal services from a potential client in Hong Kong. As part of the transaction, the client requested that the law firm accept a check for $197,750, deduct $10,000 for its fee, and wire the balance to another firm in Hong Kong. (This should have been the first clue that this was a scam.) The law firm deposited the check, which appeared to be drawn on a Citibank account, into its account at HSBC Bank.

The next business day, HSBC provisionally credited the firm for $197,750, per federal funds availability regulations. A day later, the law firm called HSBC, asking if the check had "cleared" the account. Being told that it had, the firm wired $187,750 to the other firm in Hong Kong as instructed. The check ultimately proved to be counterfeit, and HSBC charged back $197,750 to the Greenberg account.

Greenberg sued Citibank for "failing to discover that the check was counterfeit" and sued HSBC for "negligent misrepresentation" for stating that the check had cleared when in fact it had been returned to HSBC, re-routed to a different Citibank processing center, and then returned again as counterfeit to HSBC.

The New York Supreme Court issued summary judgment for both banks and dismissed all of Greenberg's claims. Upon appeal, the Court of Appeals upheld the first court's decision. Citing the Uniform Commercial Code, Citibank had no obligation to detect fraud for Greenberg because Greenberg was not Citibank's client. Its only obligation was to pay the check, return it, or send written notice that it had been dishonored. It had returned the check within the prescribed deadline.

Both claims against HSBC were also dismissed. The bank's contract specifically stated that clients may not pursue claims based on a bank employee's oral representations. The Court also held that the term "a check has cleared" is ambiguous and not definitive that final settlement had occurred.

Furthermore, the Court rejected Greenberg's argument that both banks should have had procedures in place that would have prevented the fraud. The Court ruled that the law firm itself was in the best position to prevent fraud, and had a responsibility to know its client.

This scam was a text-book-case scenario, and while it is shocking that a law firm could be taken in by such a classic scam, it should serve as a warning that anyone can be deceived. Vigilance and intelligence must be used when accepting a check. Do not accept a check for more than the amount due and then wire out the difference. Visit ***www.safechecks.com*** for additional fraud prevention tips.

ACH Fraud – Small But Growing....

ACH stands for Automated Clearing House, and the "ACH Network" serves as the infrastructure for electronic payments between individuals and organizations. The ACH Network accommodates and moves both debit and credit transactions. Last year, the ACH Network handled over 21 billion transactions such as Direct Deposit and Direct Payment.

Even though the ACH Network is one of the safest payment systems in the world, ACH fraud has almost tripled, from 12% in 2010 to 35% today

The ACH Network began as a system for moving recurring transactions between parties who knew and trusted each other, but has evolved into a system of transient and often one-time transactions between unfamiliar groups and individuals. This evolution, combined with the growing sophistication of swindlers, has made ACH fraud hard to detect and prevent.

There are many ways a criminal may commit ACH fraud, but they all have one element in common: gullibility on the part of someone along the ACH "highway."

Fraudsters only need two pieces of information to commit ACH fraud: a checking account number and a bank routing number. Criminals typically obtain bank account information by sending a phishing email that tricks a victim into disclosing the required information, or that installs malicious software on the victim's computer, allowing criminals to access the desired information.

Other infiltration methods used by criminals are infected flash drives, or social networking sites where malware is embedded in a document, video, or photo, and is downloaded onto victims' computers when they click on that item.

The newest strategy for fraudsters is pretending to be part of established organizations, well-known social networking sites, and government entities, deceiving the victims and allowing fraudsters to plant malware that eventually leads to account takeovers.

The ACH Network itself is not the focus of the fraud. The focus is to simply gain fraudulent access to that network. Most ACH fraud could have been prevented if "best practices" had been followed by organizations or individuals. Some of these practices include:

- Know the person with whom you are dealing – fraud happens by incorrectly assuming an unknown party is legitimate
- Utilize your bank's fraud detection and prevention resources such as ACH Filters, Blocks, Transaction Review, UPIC codes, etc.
- Monitor your accounts daily
- Segregate accounts for better control, e.g. collections, vs. disbursements, high volume vs. low volume, paper vs. electronic, etc.
- Use encrypted email for confidential information
- Mask account numbers and tax ID numbers in correspondence
- Collect bank tokens and change passwords when an employee leaves the company and contact your bank to remove them as a signer or authorized user of ACH origination services.

The bank is not always responsible for ACH fraud losses. Some reasons why an organization or individual is responsible for ACH losses include:

- Not reconciling accounts on a timely basis
- Not using appropriate ACH blocks or ACH filters
- Not returning suspect ACH items on time
- Not using ACH positive pay.

ACH fraud can often be thwarted by using caution and prudence.

CINCINNATI INSURANCE COMPANY v. WACHOVIA BANK

Wachovia Bank Wins Lawsuit Over Customer That Refused Positive Pay

Schultz Foods Company issued a check for $153,856 to Amerada Hess Corporation. Thieves stole the check out of the mail, changed the name of the payee, and convinced the new bogus payee (an unwitting accomplice) to endorse the check and deposit it into his bank.

His bank presented the check for payment to Schultz Foods' bank, Wachovia Bank, and Wachovia charged $153,856 against Schultz Foods' account. Before Schultz Foods discovered the fraud, the funds had been wired out, and the money disappeared.

When the fraud was discovered, Schultz Foods reported the altered check to Wachovia and demanded its account be re-credited. Wachovia refused, citing that Schultz Foods had been offered the chance to implement "Positive Pay" after three previous check fraud incidents, but had declined. Instead, Shultz Foods had purchased a check fraud insurance policy from Cincinnati Insurance Co. Positive Pay, however, would have prevented this loss.

Schultz Foods made a $153,856 claim under its policy with Cincinnati, who paid the claim and filed suit against Wachovia to recover its loss.

Cincinnati contended that the altered check was not "properly payable" and Wachovia was liable for the loss. However, the Wachovia deposit agreement signed by Schultz Foods contained a list of precautions that a customer should take to protect their account. The Agreement included a conditional release of Wachovia's liability: "You agree that if you fail to implement … products or services [that are designed to deter check fraud], … you will be precluded from asserting any claims against Wachovia for paying any unauthorized, altered, counterfeit or other fraudulent item …."

Wachovia had not required Schultz Foods to absorb any losses because of the incidents, even though Schultz Foods never implemented Positive Pay. Cincinnati argued that Schultz Foods "had an expectation that Wachovia would reimburse Schultz Foods' account" for unauthorized charges if Schultz Foods took precautions such as closing its account. However, that expectation was contrary to Wachovia's deposit agreement, which contained an anti-waiver provision, allowing it to waive enforcement of the terms of the Agreement.

Even though Wachovia voluntarily shielded Schultz Foods from past check fraud losses, its deposit agreement protected it from liability.

The Court agreed with Wachovia's argument that the deposit agreement between Wachovia and Schultz Foods required Schultz Foods either to implement Positive Pay or to assume responsibility for any fraud losses caused by its failure to implement Positive Pay.

For the complete court case and commentary, visit www.safechecks.com/fraudprevention.

Software: Positive Pay, ACH, and Secure Check Writing

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 most banks to businesses and organizations. It helps stop most (not all) counterfeit and altered checks.

Positive Pay requires a check issue file (information about the issued checks) to be sent to the bank before the checks are released. There are two primary obstacles to using Positive Pay. First is a company's inability to format the check issue file correctly and securely transmit it to the bank.

Second, some accounting software will truncate part of a long Payee name when it generates the Payee Positive Pay file. This creates a mis-match between what is written on the check and what is recorded in the file, producing a false positive alert "exception item." Repairing the Positive Pay file and dealing with these exception items can be costly and time-consuming.

SAFEChecks has software that eliminates these problems. The software creates the Positive Pay file automatically as the checks are being printed. It writes the checks, creates the check register, and formats the Positive Pay file all from the "stream of data," eliminating truncation errors and significantly reducing false positive errors and exception items.

In addition, the software can be customized to include another internal security control where checks can be reviewed and approved prior to printing. It can also be customized to automatically transmit the Positive Pay file to the bank.

SAFEChecks' secure software is invaluable in helping "tech-challenged" organizations use Positive Pay.

The software produces a Secure Name and Number Font to prevent alterations **(See Page 10)**, and also imprints a unique, encrypted, image-survivable "secure seal" barcode on the front of each check. The barcode is an effective technological weapon in the fight against check fraud. It contains all the information found on a check, including the maker (drawer), payee name, check number, dollar amount, issue date, and the X,Y coordinates of each piece of data. It is an on-board Payee Positive Pay file for that check, and can eliminate the need to transmit it to the bank if the bank has the barcode decryption software.

The decryption software reads the check using Optical Character Recognition (OCR), and the barcode data is compared to the printed data on the check. If the two don't match, the check becomes a suspect item. High-level encryption prevents the barcode from being altered or decrypted by other software.

The barcode creates an audit trail, including who printed the check, and the date and time the check was printed.

When Positive Pay is used with high security checks, such as the **Abagnale SuperBusinessCheck** or **SAFEChecks** fraud losses can be cut dramatically. **See Pages 14 – 15.**

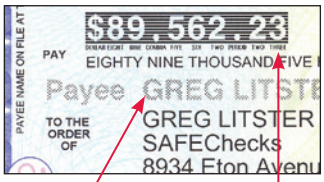
Caution: Some companies have the mistaken notion that if they use Positive Pay they do not need to use high security checks.

This is a serious misconception. Positive Pay and Payee Positive Pay are not foolproof! Consider this analogy: Using Positive Pay is like catching a thief standing in your house, 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.

The check writing software can print checks for multiple divisions, multiple accounts, and multiple banks in a single run, using "blank" check stock **(See Pages 5 and 10.)** This eliminates the need to switch check stock between check runs. Its secure signature control feature allows up to five levels of signature combinations.

The software also has an ACH module that can make payments electronically, with the remittance detail printed or emailed. The system can automatically switch between printing checks and making ACH payments in the same run.

ChequeGuard Secure Seal Barcode



Secure Name Font
Secure Number Font

The barcode, Secure Name Font and Secure Number Font are great visual deterrents to would-be criminals, discouraging them from attempting alterations (See Pages 4 and 10).

High security checks and Positive Pay are critical companions in effective check fraud prevention strategy.

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

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.

Laser Printing and Check Fraud

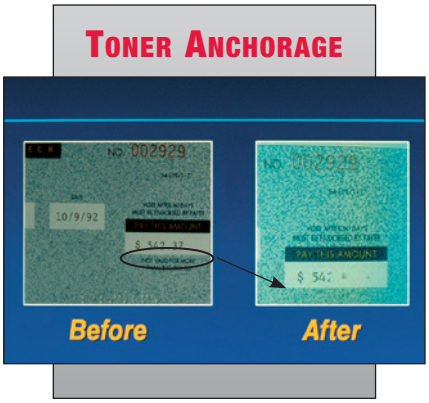
Most organizations and companies print checks on a laser printer. This technology is highly efficient, but proper controls must be in place or laser printing can invite disaster.

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.

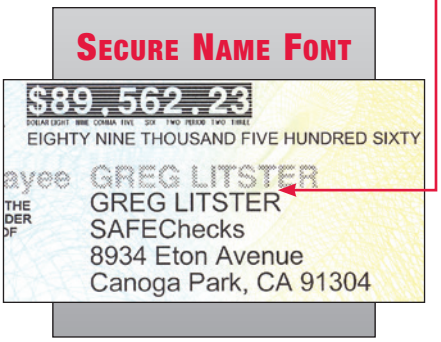


Blank Check Stock

that is not customized for each customer should be avoided. Check stock that is sold completely blank to multiple companies is "uncontrolled check stock." If a printer or computer company is selling you entirely blank checks, they are likely selling the identical blank 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. **See Pages 14 – 15.**

Secure Name Fonts

help prevent added or altered payee names. In many cases, adding to or 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 to print the payee name. This makes it extremely difficult to remove or change the Payee name without leaving evidence. **It also eliminates the spacing for an added payee.**



Uncontrolled Check Stock

Recent court cases have shown that using blank, uncontrolled check stock can contribute to check fraud losses. Companies can be held liable for the resulting losses if the bogus checks look "genuine." **See Page 7, Robert J. Triffin v. Somerset Valley Bank and Hauser Contracting Company.** **SAFEChecks sells only controlled check stock.**

Sequenced Inventory Control Numbers

should be printed 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 and tracking each sheet discourages internal fraud and maintains compliance with auditors.

String of Asterisks

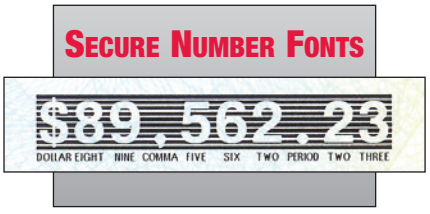
printed above the payee name is another way to prevent added payee names. Forgers add a new payee name two lines above the original payee name. To prevent additions, insert a string of asterisks above the original payee name. Asterisks can be pre-printed on the checks by the check vendor. Do not use asterisks when using Payee Positive Pay. They cause false positives.

Image Survivable Barcode "Secure Seal" Technology

is a 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, issue date, etc. 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 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.



Protect Passwords

Passwords should be 8+ characters and should include a captal letter and a character (e.g: !@#$%&). An email address makes an excellent password. Because a company has more exposure from dishonest employees than from a hacker, two people should be required to print checks, add new vendors, and add or change employees and pay rates.

Check 21: The Hidden Liability

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 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).

This second Warranty is a powerful protection against "double-dipping" – someone depositing a check via their phone and then cashing the same check elsewhere. If this deception is not caught and both deposits clear the maker's account, the bank of first deposit can be held liable for the loss.

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.

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." 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."

Remote Deposit Capture

Remote Deposit Capture is a service that allows a business or individual to scan, image and transmit to its bank the checks it normally would deposit. While the technology is convenient, you must understand your risk. Under the law, an organization or individual 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 to file a claim 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 or company, as allowed under Check 21's Indemnity Provision. This assumes that their bank has a Sight Review threshold such that the original check would have been 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 safechecks.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 14 – 17)** 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 **SafeChecks.com** and **Supercheck.net** 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.

Visit www.FraudTips.net for information.

Check Security Features

In response to the alarming growth of check fraud, the check printing industry developed many new security features. The best features are illustrated here. While nothing is 100% fraudproof, 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 them first being customized. Ask your check printer for their written policy about blank check stock. If there is none, the check stock most likely is not controlled. **See Page 14 – 17.**

Fourdrinier Watermarks

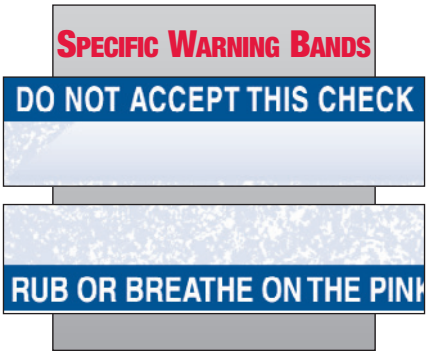
are faint designs pressed into the paper while it is being manufactured, and are also known as "true" watermarks. When held to the light, these watermarks are easily visible from either side of the paper for instant authentication. Copiers and scanners are not capable of replicating dual-tone Fourdrinier (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. Checks with thermo ink should have properly worded warning bands.

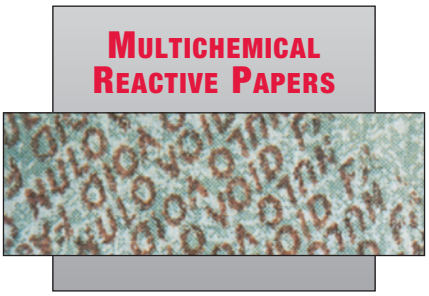
Specific Warning Bands

are printed messages that call specific 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. A properly worded warning band may protect a company from some Holder In Due Course claims. **See Page 7, Pomerantz Staffing Services.**



Multi-chemical Reactive Papers

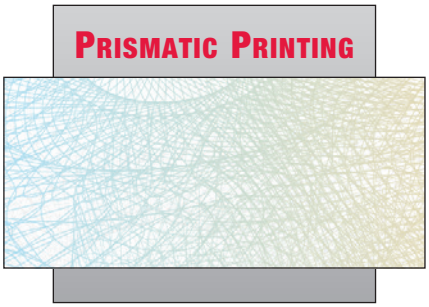
produce a stain or speckles or the word "VOID" when activated with ink eradicator-class chemicals, making it extremely difficult to chemically alter a check without detection.



Checks should be reactive to at least 15 chemicals.

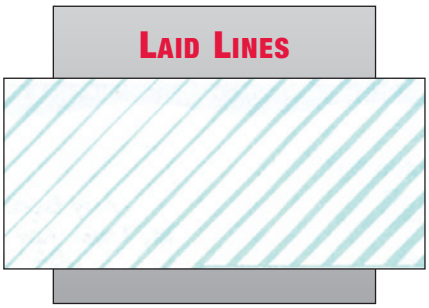
Prismatic Printing

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



Laid Lines

are parallel lines on the back of checks. They should be of varying widths and unevenly spaced. Laid lines make it difficult to physically "cut and paste" dollar amounts and payee names without detection.



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 and so is not foolproof.

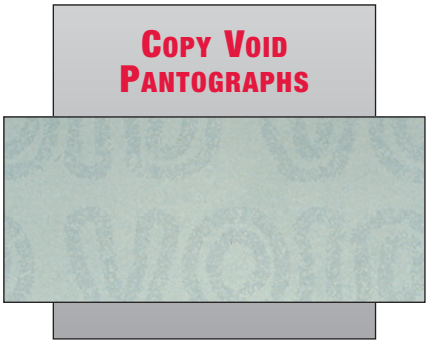


Image Survivable Secure Seal Barcode

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 Pages 9 and 10.**

High-Resolution Borders

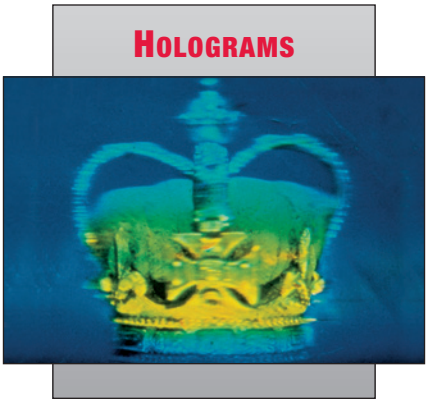
are intricately designed borders that are difficult to duplicate. They are ideal for covert security as the design distorts when copied.

Ultraviolet Light-Sensitive Ink and Fibers

can be seen under ultraviolet light (black light) and serve as a useful authentication tool.

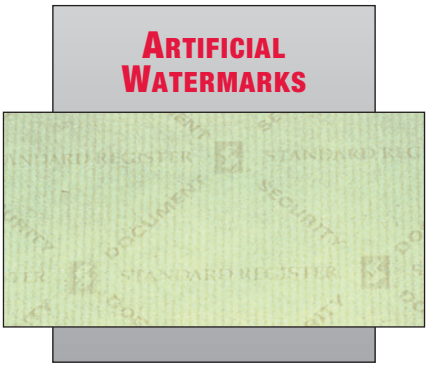
Holograms

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.

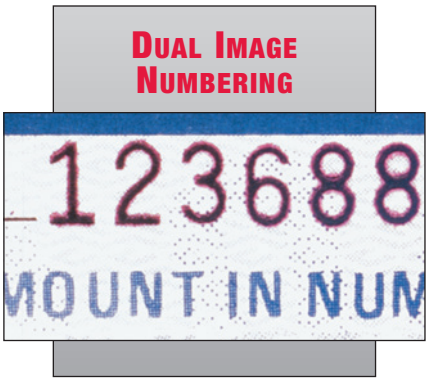


Microprinting

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 many check fraud attempts by making it more difficult for a criminal to alter or replicate an original check. They help thwart some Holder in Due Course claims **(See Page 6)**, and establish the basis for an indemnity claim under Check 21's Indemnity Provision. **(See Page 11.)** High-security checks should have at least ten (10) safety features, the most important being that the check is a "controlled" stock. This means the check is never sold or made available entirely blank. Forgers can make authentic-looking checks using original blank checks, a scanner and Adobe Illustrator. An organization may be held liable for these fraudulent checks.

Other "best" features are a dual-tone true watermark, UV ink, thermochromatic ink (accompanied by a properly worded warning band), and toner anchorage. Frank Abagnale designed the **SuperBusinessCheck**, **SAFEChecks** and the **Supercheck** to help individuals and organizations have access to high security checks at reasonable prices. **(See Pages 14 – 17.)**

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 tightly controlled, true-watermarked 28 pound security paper. For your protection, the SuperBusinessCheck is never sold completely blank without first being customized for a 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
- Toner Anchorage
- Chemical Sensitivity
- Copy Void Pantograph
- Chemical Reactive Ink
- Fluorescent Ink
- Fluorescent Fibers
- Microprinting

OVERT SECURITY FEATURES

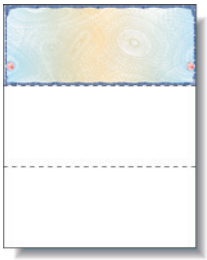
- Thermochromatic Ink
- Fourdrinier (True) Watermark
- High-Resolution Border
- Prismatic Printing
- Explicit Warning Bands
- Chemical Wash Detection Box
- Sequenced Inventory Control Numbers
- Laid Lines

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

Frank W. Abagnale

Available Styles

Laser - Top

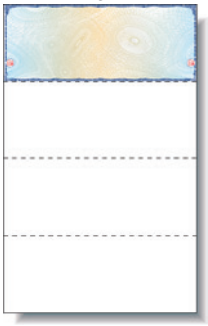


Laser - Middle

Laser - Bottom

Laser 3-On-a-Sheet

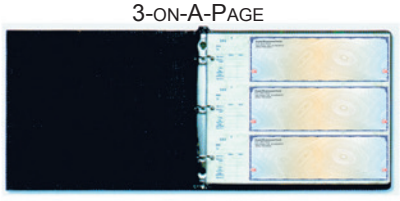
Legal Laser - Top



Legal Laser - Second Panel

Pressure Seal Checks Also Available

3-on-A-Page

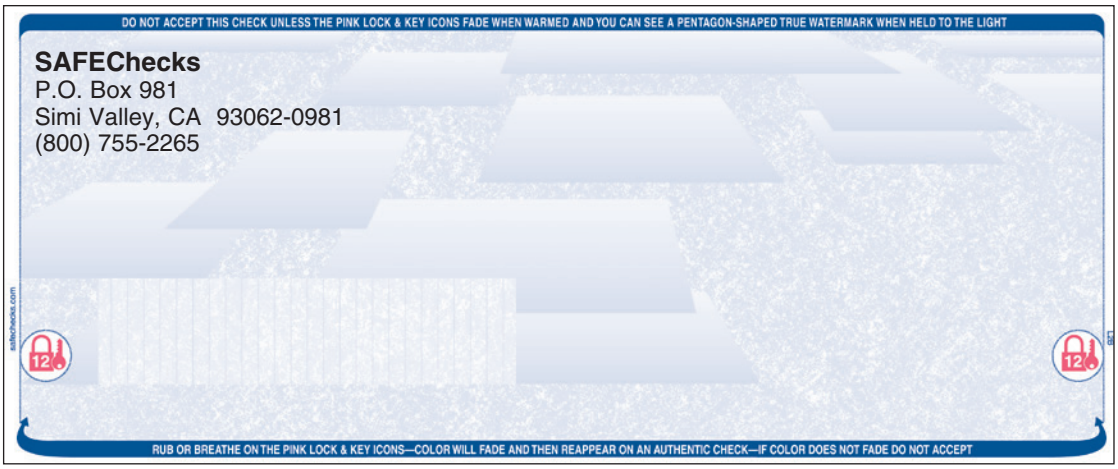


Secure Ordering Procedures

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 independently. Our Secure Ordering Procedures are in place for your protection, and are unparalleled in the check printing industry.

SAFEChecks

The SAFECheck was designed by Frank Abagnale with 12 security features, and is virtually impossible to replicate or alter without leaving evidence. SAFEChecks are printed on tightly controlled, true-watermarked, 28 pound security paper. To prevent unauthorized use, SAFEChecks are never sold completely blank without first being customized for each specific customer.



12 Safety Features

Covert Security Features

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

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 12.**
Sequenced Inventory Control Numbers
Microprinting
Laid Lines

Available Styles

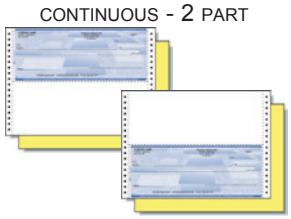
Laser - Top

Laser - Middle

Laser - Bottom

Continuous - 1 part

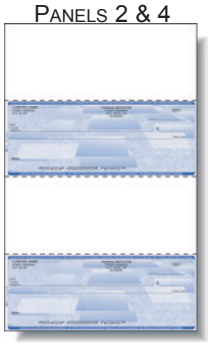
Continuous - 2 part



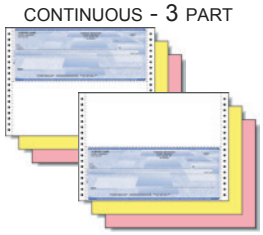
Legal Laser - Top

Legal Laser - Second Panel

Legal Laser - Panels 2 & 4



Continuous - 3 part



Pressure Seal Checks Also Available

SAFEChecks also offers secure laser check writing software (See Page 9, MICR toner cartridges, and envelopes. Call (800) 755-2265.

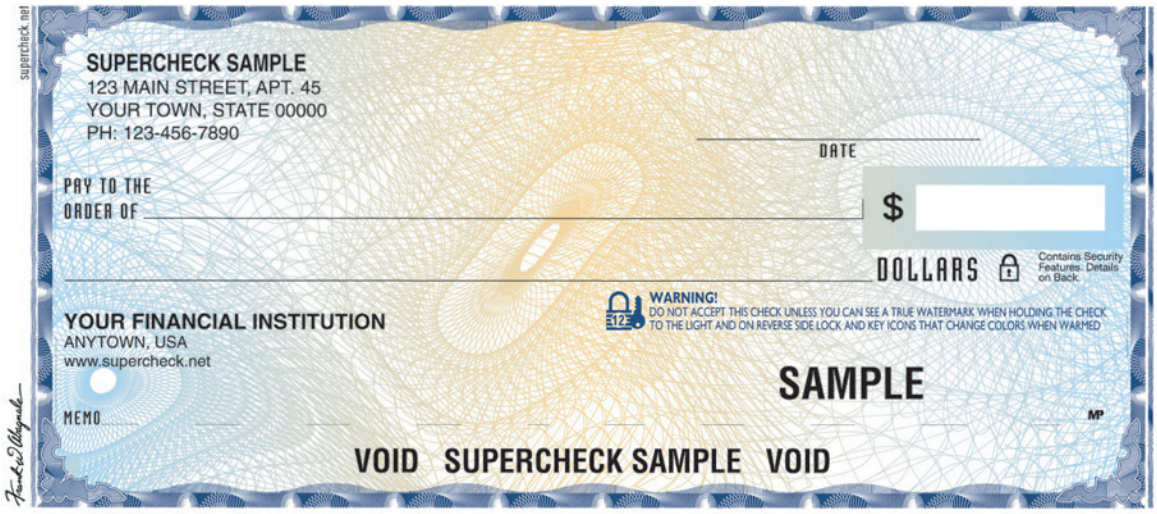
NOT USING POSITIVE PAY?
You should! Talk to your banker ASAP.
Visit
PositivePay.net
safechecks.com

MORE FRAUD PREVENTION TIPS
Visit
SAFEChecks.com
FraudTips.net
Supercheck.net

ABAGNALE SUPERCHECK

The Supercheck is a high security personal check designed by Frank Abagnale to help individuals 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

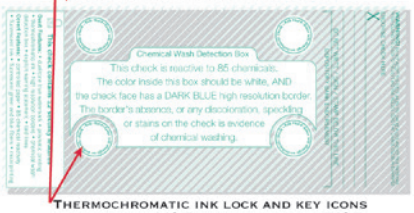
Controlled Paper Stock
Fourdrinier (True) Watermark
Thermochromatic Ink
Chemical Sensitivity
Explicit Warning Bands
Prismatic Printing
Chemical Wash Detection Box
High-Resolution Border
Laid Lines
Fluorescent Fibers
Fluorescent Ink
Microprinting

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 OR DOWNLOAD IT FROM WWW.SAFECHECKS.COM

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 2. VOIDED CHECK (indicate any changes on the face) 3. VOIDED DEPOSIT SLIP	SAFEChecks P.O. Box 981 Simi Valley, CA 93062-0981	Allow 3 weeks for delivery. Expedited service is available. Call (800) 755-2265 ext 3304

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

Single - $29.95 per box of 150
Duplicate - $32.95 per box of 150
Shipping/Handling - $4.50 per box

PAYMENT OPTIONS:

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

_____Bill my credit card: _____MasterCard _____Visa

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)

Credit Card Account Number / Expiration Date Security Code

Cardholder Name

Authorized Signature

Billing address of credit card if different from address on checks

PLEASE PHOTOCOPY THIS FORM OR DOWNLOAD FILLABLE FORM AT WWW.SAFECHECKS.COM

SAFEChecks®

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 _____ ☐ Web ☐ Other _____

CUSTOMER NAME, ADDRESS AND PHONE NUMBER

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

Phone ( )

Please MAIL a VOIDED ORIGINAL CHECK with this completed order form. We will call you to confirm receipt.

BANK NAME AND ADDRESS

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

Please ship to:

Attention:

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

Check Starting Number	Quantity	☐ 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
Text to be printed above signature lines			

☐ 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 SAFEChecks®**
- ☐ Top Check ☐ Blue ☐ Green ☐ Red ☐ Plum
- ☐ Middle Check ☐ Blue ☐ Green
- ☐ Bottom Check ☐ Blue ☐ Green

☐ **8½ X 14 SAFEChecks®**
- ☐ Top Check ☐ Blue ☐ Green ☐ Red
- ☐ Check in 2nd Panel ☐ Blue ☐ Green
- ☐ Check in 2nd & 4th Panels ☐ Blue

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: _____

SAFEChecks® 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**
- ☐ **Duplicate**
- ☐ **Three-on-a-Page Binder**

Download a price list from SAFEChecks.com
Call (800) 755-2265 for assistance in completing form or to answer any questions.

Prepared by: _____
Phone Number: _____
Fax Number: _____
Email: _____
Date: _____

Embezzlement: Preventing the Inside Job

A blizzard in Missouri kept the bookkeeper of a small construction company home, so the founder/CEO picked up the mail. She found a letter from the IRS threatening to seize the assets of the business for failure to pay taxes. She was shocked, since the longtime bookkeeper had supposedly kept the taxes and other bills paid. The CEO immediately contacted the FBI and the IRS, and the investigation revealed that the bookkeeper had embezzled almost $400,000 over the course of six years. The CEO worked out payment deals with the company's vendors and the IRS, and the business survived.

Other organizations have not been so fortunate. Many have gone out of business due to embezzlement losses. Organizations that do survive often experience layoffs, cutbacks and salary freezes for an extended period of time. The victims are not only the organizations themselves, but their suppliers, vendors, and families.

Two reputable organizations have extensively researched embezzlement, and their reports should be carefully studied: *The Marquet Report On Embezzlement* by Marquet International, and *A Report To The Nations* by the Association of Certified Fraud Examiners (ACFE). Additional important Resources are listed on Page 19.

The financial services industry, especially credit unions, and government entities are most likely to experience embezzlement. However, organizations of every type and size have been negatively impacted by this crime. Estimates show that a typical organization loses 5% of annual revenues to fraud.

The Marquet Report analyzed hundreds of cases involving losses of $100,000 or more. Hundreds of cases fell below that threshold or were not reported. The average loss of those that were analyzed was $1.1 million, with a median loss of about $325,000.

According to the ACFE Report, 58% of victimized organizations had not recovered any of their losses, and only 14% had made a full recovery.

Given that embezzlement is so pervasive, it is imperative to understand why and how it occurs, and how to defend against it. Early detection and prevention strategies are key to controlling losses.

Who are the Perpetrators?

Embezzlers are most likely to hold bookkeeping or finance positions. While regular employees embezzled most frequently, the greatest losses came from managers and executives. Females embezzled more often than males, but males caused almost triple the losses.

Position	Female Losses	Male Losses
Employee	$50,000	$75,000
Manager	$150,000	$200,000
Executive	$300,000	$700,000

The majority of embezzlers were in their early 40s, but the greatest losses came from those aged 60 and above. About 40% had been at the job one to five years, and over 50% had been there more than five years. The vast majority of embezzlers had no prior criminal history, so background checks were ineffective in preventing this type of crime.

Why Embezzlement Occurs

Workplace conditions are a major predictor of fraud. Internal fraud occurs when the "fraud triangle" is present – motive, opportunity, and rationalization – and effective fraud prevention controls are not in place. In fact, there were no internal controls to prevent embezzlement in over 30% of cases, and in over 40% in small businesses.

An overlooked but vital factor is the tone set by upper management, especially in cases over $1 million. Management tone contributing to fraud includes unethical attitudes and behavior, overriding established safeguards, and pressuring employees to meet unrealistic goals. Employees who feel unfairly treated sometimes believe they can get "justice" by embezzling.

While there were various motivating factors, the two overwhelming factors motivating embezzlement are a desire to obtain and/or maintain a more lavish lifestyle than what they otherwise could afford, and a gambling addiction. Those two motivations were often intertwined. In the cases where gambling addiction was the primary motivator, all but three occurred in states where casinos and/or Indian gaming facilities were permitted.

Other motivations were an entitlement attitude, financial difficulties, shopping addiction, substance abuse, and to support a significant other.

Detecting Embezzlement

Fraudsters exhibit many behavioral red flags that can help management detect fraud. Managers who ignore these red flags do so at the company's peril. These include displaying a more lavish lifestyle than what their legitimate income would suggest, having an overt sense of entitlement, having financial difficulties and/or family problems, excessive control issues, unwillingness to share duties or take vacations, addiction problems, and irritability or defensiveness.

Managers, employees and auditors should be educated on these common behaviors to help spot fraudulent activity. Anonymous tips are one of the most important means to detect fraud. Over 40% of all cases were detected by a tip — more than twice the rate of any other detection method, including audits. Employees provided nearly half of all tips that led to the discovery of fraud.

Most tips are given anonymously via hotlines. If a hotline does not exist, tips most likely will not be given. Tip hotlines should be designed to receive tips from both internal and external sources, and should allow anonymity, confidentiality, and include a reward. Tip hotline reporting programs should be publicized to employees, as well as outsiders. Although employees are the most frequent source of fraud tips, customers, vendors, and even competitors have also provided valuable information.

Management review and internal audits are the next most common forms of detection. One of the least effective methods of detecting fraud was through external audits of financial statements. In fact, more fraud was discovered by accident than by external audits! While external audits are important, they should not be solely relied upon to detect embezzlement.

Strategies For Preventing Embezzlement

Using your bank's Lockbox service is the best and most cost-effective way to prevent embezzlement via diverted deposits. Anonymous "Tip Hotlines" with a cash reward significantly decrease the duration and cost of a fraud scheme. Add surprise audits, employee education, and support programs to achieve the greatest decrease in losses. Companies without these controls experience losses 45% higher than those with the controls.

Education is part of an effective fraud prevention program. Organizations with anti-fraud training programs for employees, managers, and executives have fewer losses and shorter durations of fraudulent schemes than those without these programs. Training should include what constitutes fraud, how it hurts everyone in the company, and how to report questionable activities. (Tip Hotline)

Employee support programs that help employees struggling with gambling or drug addictions, mental or emotional health, and family or financial problems will reduce losses.

Surprise audits' most important benefit is psychological: Potential embezzlers believe that they will be caught, which has a strong deterrent effect.

Additional internal controls include a separation and rotation of duties, proactive data monitoring and analysis, mandatory vacations, written protocols for issuing and reconciling checks, proper documentation of payments and receipts, and independent verification of all new vendors and any change of remittance or banking information for existing vendors.

Certain schemes are more prevalent based upon the industry or department. Organizations need to consider the specific fraud risks they face when deciding which controls to implement.

The Internal Revenue Service requires embezzlers to report embezzled funds as income in their annual tax filing; compliance is rare. Failure to report embezzled funds as income can result in tax evasion charges. The threat of the IRS should be well-publicized to deter would-be embezzlers.

Small Businesses Fraud

Embezzlement is a significant threat to small businesses. The smallest organizations consistently suffer the largest relative losses. These companies usually have fewer anti-fraud controls than larger companies, and therefore are more vulnerable to fraud.

Resources

Marquet International "Marquet Report on Embezzlement" (2010 – 2014)

Association of Certified Fraud Examiners "Report to the Nations" (2010 – 2014)

"Effective Solutions for Combating Employee Theft –Implementing and Managing a Fraud Hotline" by Donald L. Mullinax, ACFE 2004

"Enemies Within" by Joseph Wells, ACFE 2001

http://topics.law.cornell.edu/wex/embezzlement

Focus on Prevention to Limit Fraud Losses

This checklist can help organizations establish an effective fraud prevention program.

1. Is ongoing anti-fraud training provided to all employees of the organization?
2. Is an effective fraud reporting mechanism (tip hotline) in place?
3. Is the management climate/tone at the top one of honesty and integrity?
4. Are fraud risk assessments performed to identify and mitigate the company's vulnerabilities to internal and external fraud?
5. Are strong anti-fraud controls in place and operating effectively? (See Resources, above)
6. Does the internal audit department have adequate resources and authority to operate effectively and without undue influence from senior management?
7. Does the hiring policy include thorough fraud prevention controls?
8. Are employee support programs in place to assist employees struggling with addictions, mental/emotional health, family or financial problems?
9. Are employees allowed to speak freely about pressures, providing management the opportunity to alleviate such pressures before they become acute?

Small Business – Fraud Prevention

Small businesses (fewer than 100 employees) are victimized by embezzlement more frequently than larger organizations and suffer disproportionately larger losses. They are far less able to absorb these losses, and many have gone bankrupt or were severely crippled because of embezzlement.

Small businesses typically have fewer human and financial resources than large companies, which means they have fewer and less-effective anti-fraud controls in place, making them more vulnerable to fraud. A internal lack of controls was the most frequently cited factor in 45% of embezzlement cases in small organizations.

Although some controls require significant resources, other anti-fraud measures can be implemented for a minor cost and could significantly increase the ability to prevent and detect fraud. These controls include a separation of financial duties, a code of conduct, anti-fraud training programs, and formal management review of controls and processes. Also, check tampering in small businesses is three times more likely than in large organizations, and in some cases can be thwarted with high security checks. **See Pages 4, 5, 14 – 17.**

Identity Theft – It Can Happen To You

Identity theft is motivated by financial rewards, the easiness of the crime, and the small chance of being caught. Here are several suggestions to reduce your risk of ID theft:

Social Security Number

1. Guard your Social Security number vigilantly.

2. Do not print your Social Security Number on your checks.

3. Review your Social Security Earnings and Benefits Statement annually and look for employers you didn't work for.

4. Monitor your credit report. After applying for anything that requires a credit report, request that your SSN on the application be truncated or removed, and that your original credit report be shredded after a decision is made.

Internet / Computers

5. Make sure your computer is protected with Internet security software that is updated regularly.

6. Do not download anything from the Internet that you did not solicit.

7. Shop only on secure websites.

8. Avoid using a debit card when shopping online.

9. Use a strong password.

10. When possible, choose to have a second-level password.

11. Never leave your laptop where you wouldn't leave your baby….

12. Before donating your computer or cell phone to a recycling center, completely wipe out all confidential information. This requires special software.

Credit Cards

13. Shred anything with personal information on it. Use a crosscut or microcut shredder.

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 out, be aware of how salespeople or waiters handle your card.

16. Promptly examine the charges on credit card statements. Keep track of the billing cycles.

17. Minimize the number of credit cards you own.

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

19. Shred the cards on unused credit card accounts. If you close an 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 14 – 16**.

22. Do not mail checks from home.

23. When writing manual checks, use the uni-ball® 207 gel pen.

24. Use a strong PIN and protect it.

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.

28. Add your name to the Name Deletion List of the Direct Marketing Association.

29. Subscribe to a credit monitoring service to alert you "in real time" if your credit history is being requested.

30. Avoid ATMs that are not connected to a bank or a reputable business.

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, both sides of each card.

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.

If It Happens to You:

Even though you may take every possible precaution, identity theft can still happen to you. If it does:

- 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: 1-888-766-0008 www.equifax.com
- Experian: 1-888-397-3742 www.experian.com
- TransUnion: 1-800-680-7289 www.transunion.com
- Federal Trade Commission: 1-877-438-4338 www.consumer.ftc.gov
- Privacy Guard: 1-800-374-8273 www.privacyguard.com
- Privacy Rights Clearinghouse: www.privacyrights.org
- Fight Identity Theft: www.fightidentitytheft.com
- Identity Theft Resource Center: 1-888-400-5530 www.idtheftcenter.org
- National White Collar Crime Center: 1-800-221-4424 www.nw3c.org
- Social Security Administration 1-800-269-0271 http://oig.ssa.gov
- U.S. Postal Service: 1-877-876-2455 postalinspectors.uspis.gov

Corporate Identity Theft

Corporate identity theft is the unauthorized use of a company's name and information by criminals in order to illegally obtain money, goods, or services. Because the Internet has made it easy to re-create a non-existent business that looks legitimate, no organization is immune from the threat of corporate identity theft.

Targeting businesses can be much more profitable for fraudsters than personal identity theft. Dun & Bradstreet has reported cases of corporate identity theft in at least 22 states, and predicts this crime will spread across the country. Some losses have reached a half-million dollars before the crime was discovered.

There are two major types of Corporate Identity Theft. The first involves hacking, when criminals defraud a company's clients or vendors. These schemes are detailed on the inside front cover of this Bulletin.

In the second type of Corporate Identity Theft, fraudsters target and imitate a legitimate business. Criminals open new bank accounts and obtain loans and credit cards in the name of the business, often using the compromised identity of business owners or officers.

When banks or other commercial lenders evaluate a business, they look for evidence that the company is who its officers say it is, and that it has the legal and financial capacity to conduct its business. This evidence is called "Proof of Right," and can include financial statements, business addresses and telephone numbers, government licenses, credit history, etc. Each Proof of Right that can be verified increases the appearance of a company's legitimacy.

Thieves can create fraudulent Proofs of Right of targeted businesses by gaining access to state government records of legitimate businesses, and then altering company information, such as the registered agents' names and addresses. They use falsified financial statements to lease offices, furniture and equipment to create the illusion of a successful business. They obtain bank loans and retailer lines of credit to purchases items that can readily be sold for cash. Often, this leaves the unwitting victimized business awash in debt and legal fees defending itself against creditors.

Criminals tend to target smaller and midsize businesses with strong credit ratings that are easily identified through credit rating agencies. Because business credit reports are intended to promote and enable "buying and selling," and help managers make risk assessment decisions, business credit reports are readily available to virtually anyone.

Smaller businesses with strong credit ratings are tempting targets for criminals. Fraudsters select smaller companies because they often erect fewer legal and financial defenses than large corporations. Family-owned businesses, churches, and even inactive companies have been targeted. Some state governments are now actively working to help better protect government controlled and regulated business data.

The biggest challenge is alerting and educating organizations about this new type of crime, and motivating them actively self-monitor. Defensive strategies include using better passwords, dual-authentication controls, and checking their legal filings regularly. Businesses should verify atypical large purchases from current clients and unusual purchases from new clients.

Businesses that have been duped are understandably reluctant to make their deception public. A balance must be found between making it easy to do business with legitimate companies, and protecting those companies from criminal activity. Better partnering between the private and public sectors is needed to successfully fight this crime.

Resources

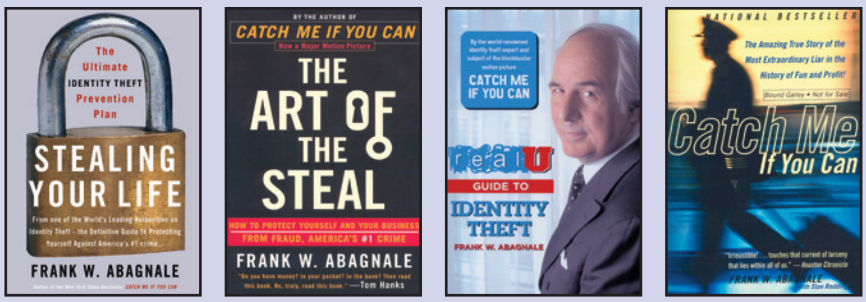
Dun & Bradstreet, Bloomberg BusinessWeek, The Council of State Governments

Examples of Corporate Identity Theft

California: A seafood company received a $500,000 order for goods. After completing a credit check, the company shipped the order and billed the customer. The customer responded that it had not placed or received the order. Later, it was discovered that the customer's credit information and a different shipping address had been supplied by a fraudster. By that time, both the goods and the thief had vanished.

Colorado: Criminals altered a company's registration information on file with the state. After changing the registration information, the criminals used the altered corporate identity to make online applications for credit from various retailers, including Home Depot, Office Depot, Apple and Dell.

Florida: An aviation company had been dissolved by its owners. The company was reinstated by corporate identity thieves. The thieves applied for a $140,000 federal fuel tax credit, which was delivered as a check. The scammers and the money disappeared. The original owners were completely unaware until the IRS knocked on their door.



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

Shredding Documents

Shred anything with your personal information on it before throwing it away. It is best to use a crosscut or a microcut shredder. A crosscut shredder will cut the paper into tiny squares. A micro-cut shredder will turn the papers into confetti. Paper that has been shredded with a straight shredder can be pieced back together, and criminals will have your personal information. Crosscut and microcut shredders can be found at most major office supply stores.

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 almost 40 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 almost 40 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.

SAFEChecks®

The Check Fraud Prevention Specialists

SAFE*Checks*® originated in 1994 as a division of a Southern California business bank battling an epidemic of check fraud. Over a three-year period, altered and counterfeit checks increased from $90,000 to over $3,000,000. Many of these checks were perfect replicas of its clients' authentic checks.

To stem this epidemic, Greg Litster, then Senior Vice President and head of the bank's Financial Services Division, retained fraud consultant Frank Abagnale, the world's foremost authority on check fraud prevention. At the bank's request, Mr. Abagnale designed **SAFE***Checks* – America's first truly affordable high security check designed for organizations of any size, including small and medium-sized companies. The bank strongly encouraged its clients to use these new checks, and over the next three years, check fraud attempts fell to $126,000, a drop of 95%.

Mr. Litster acquired the **SAFE***Checks* operation from the bank in 1996, and is its President and CEO. **SAFE***Checks* has continued to be a pioneer in check fraud prevention, and has clients of every type and size throughout the United States and Canada. Because of **SAFE***Checks'* extensive security features and unique Secure Ordering Procedures, our checks have never been replicated, nor has a check manufactured by **SAFE***Checks* ever been used in a check fraud scam.

SAFE*Checks* offers high security business and personal checks, and secure check writing software that includes Positive Pay and ACH functionality. In addition, Mr. Litster provides fraud prevention educational seminars, consulting services, and expert witness services.

SAFE*Checks* ***"The Check Fraud Prevention Specialists"*** understands the serious nature and magnitude of check fraud. Because of SAFEChecks' unique foundation in banking, we know the various methods criminals use to commit payment fraud. **SAFE***Checks* has designed specific protocols and security features to thwart these fraud attempts. While no product, policy, or program can provide 100% protection, **SAFE***Checks* helps organizations and individuals build the strongest possible defense against check fraud.

SAFEChecks®

The Check Fraud Prevention Specialists

(800) 755-2265

safechecks.com

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