Frank W. Abagnale

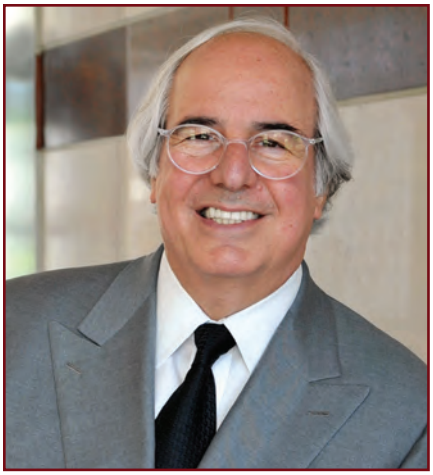
The Fraud Bulletin

Volume 15

Inside this Issue

1 The Evolution of Check Fraud
2 Positive Pay Lawsuit
3 Fraud In A Pocket . . . Mobile Phones
4 BEC Scams ***NEW!***
5 Corporate Imposter Fraud ***NEW!***
6 Cyber Crime – A Never-Ending Challenge
7 Check 21: The Hidden Liability
8 Court Cases: Holder In Due Course Check Fraud Scams
10 Laser Printing and Check Fraud
11 Positive Pay, ACH, and Secure Check Writing Software
12 Check Fraud Prevention – Best Practices
14 Check Security Features – Why They Matter
16 Abagnale SuperBusinessCheck
17 SAFEChecks
19 Supercheck
20 Embezzlement
22 Ransomware ***NEW!*** eChecks ***NEW!***
23 Identity Theft
24 Wire Transfer Fraud – An Explosion In Cyber Space ***NEW!***
25 Same Day ACH – Innovation in Payments ***NEW!*** ACH Fraud – On the Rise...

Frankly Speaking . . .



As I survey the financial fraud landscape today, I am amazed at technology and the interconnectedness of fraud – email scams lead to fraudulent wire transfers; hand-held mobile card readers capture debit and credit card information from cards inside the wallets of innocent victims as they walk down a street; mobile banking fraudsters deposit physical paper checks and then cash the same checks at check cashing stores; and cyber criminals divert vendor payments via fraudulent "change of remittance address" correspondence sent to unsuspecting victim organizations by email or by replicated letterhead.

Digital developments over the past two decades have brought the world tremendous advances. But, it has also allowed fraudsters both domestic and foreign to perpetrate financial fraud schemes worldwide. Truly, the world is more interconnected today than ever before.

Real-Time Payments

In order to speed up payment processes, new financial systems are being developed in the United States. Known as Real-time Payments (RTP), these new financial structures will allow consumers and businesses to send and receive payments almost instantly from their accounts at financial institutions. The systems follow guidelines established by the Federal Reserve's *Faster Payments Task Force* and the Consumer Financial Protection Bureau[1,2].

The goal of RTP is to facilitate nearly instant, 24/7/365, interbank electronic fund transfers that can be processed through computers, tablets, smart phones, digital wallets, etc., with access to the Web.[3] The new RTP systems are being developed primarily by The Clearing House (TCH) and the National Automated Clearinghouse Association (NACHA). Real-time payment methods already exist in about 40 other countries.

Because new innovations invite new fraud schemes, the Fed created the *Secure Payments Task Force*. It coordinates with the *Faster Payments Task Force* to ensure that any new or modified payments infrastructure is secure. The Fed's approach makes sense, because as I have said for over 40 years, the punishment for fraud and the recovery of stolen funds are so rare, prevention is the only viable course of action.

Payment Fraud at an All-time High

Payment fraud is now at an all-time high, according to the Association for Financial Professionals (AFP). In 2016, over 75% of companies experienced some kind of payment fraud attempt, up from 62% in 2014.[4] The attempts hit all payment avenues – checks, wire transfers, ACH debits and credits, and credit cards.

Amazingly, the latest AFP survey indicated that companies are actually reducing the number of internal controls that could help prevent payment fraud. Perhaps these two phenomena go hand-in-hand – the reduction of controls and the rise in fraud.

Old-school check fraud still remains the payment fraud leader, even as total check usage is dropping and other more sophisticated payment fraud methods are occurring at lightening speed. Check fraud is a "crime of opportunity" and criminals typically seek out an unsuspecting soft target.

According to the most recent Payments Fraud and Control Survey conducted by the Association for Financial Professionals (AFP), 74% of organizations experienced check fraud attempts in 2016. This is a reversal of the downward trend in check fraud since 2010. Criminals are reverting back to check fraud because checks continue to be the payment method most often used by organizations, and are often considered an easier target than other payment fraud methods.

In addition, new technology is equipping fraudsters with an expanded toolset with which to commit check fraud – notably, mobile phones via Mobile Remote Deposit Capture (mRDC), and the internet via Business Email Compromise (BEC) scams. In fact, 32% of the losses created by BEC scams involved the use of checks. I designed the **SuperBusinessCheck, SAFEChecks** and the **Supercheck** to help organizations and individuals protect themselves against check fraud losses. **(See Pages 16-19.)**

Ransomware

Ransomware is malware that locks down computers and mobile devices or encrypts their electronic files. The data is inaccessible until a ransom is paid. Any organization can be targeted, as proven by the May 2017 WannaCry cyber attack that crippled well over 300,000 computers in more than 150 countries. Preventing ransom attacks requires continual vigilance, beginning with installing computer and software security updates. Educating employees in safe email and Internet protocols is essential because the weakest link in every organization's cyber defenses is its employees. Almost every security breach can be traced back to a human making a judgment error or not following security protocols. **(See Page 22.)**

AARP

Some of my most rewarding work has been partnering with AARP's *Fraud Watch Network*. For the last three years, I have served as their ambassador. It is distressing to see those who should be among the most respected and cared for in our society – the elderly – become some of the most susceptible victims of fraud.

Recently, I had the honor to testify before the United States Senate regarding fraud committed against our seniors. According to the Government Accountability Office, financial fraud targeting older Americans is a growing scourge that costs seniors an estimated $2.9 billion annually. This estimate is probably low because many seniors are too embarrassed to admit that they have been defrauded and don't report it. The number of calls to the Senate Aging Committee's Fraud Hotline more than doubled in 2016 – hard evidence that fraudsters target the elderly.[5]

While law enforcement, consumer protection agencies, and financial institutions play important roles in identifying and thwarting elder fraud, alert citizens are still the first and best line of defense. The goal of the *Fraud Watch Network* is to arm Americans with the knowledge and tools they need to spot fraud and avoid scams.

This Fraud Bulletin was created to help individuals, families, and organizations learn to protect themselves. I hope you find it useful. I have written three books, *The Art of the Steal, The Real U Guide to Identity Theft* and *Stealing Your Life*, which cover numerous scams and solutions in detail. **(See Page 24.)** Fraud prevention is everyone's business!

Frank W. Abagnale

www.abagnale.com

1 https://fedpaymentsimprovement.org/wp-content/uploads/path-to-faster-payments.pdf

2 https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-guiding-principles-for-faster-payment-networks/

3 https://www2.deloitte.com/content/dam/Deloitte/us/Documents/strategy/us-cons-real-time-payments.pdf

4 2017 Payment Fraud and Control Survey conducted by the Association for Financial Professionals (AFP)

5 https://www.aging.senate.gov/press-releases/senate-aging-committee-announces-top-scams-targeting-nations-seniors-in-2016

The Evolution of Check Fraud

Picture by The Colonial Williamsburg Foundation

Origins of Check Fraud Legal Doctrine

The first lawsuit related to check fraud occurred over 250 years ago in London, with the famous case of Price v. Neal. This case set the legal precedent regarding the use of checks in the U.S. banking system. In Price v. Neal, the judge's ruling was not that different from how the law is often applied today – in favor of the bank.

In 1762, Benjamin Sutton had an agreement with John Price whereby Sutton would periodically prepare "bills of exchange" (precursors to checks) for monies owed him by Price. Edward Neal had obtained two of these bills of exchange that supposedly were signed by Mr. Sutton. Neal cashed them, receiving the money for one bill from Mr. Price, and money for the second from Mr. Price's bank.

Unbeknownst to Price, Sutton and Neal, Sutton's signature on the bills of exchange had been forged by a Mr. Lee. Mr. Price brought suit against Neal for the return of the payments. The jury and court ruled in favor of Price and his bank. Mr. Lee was later hung for his crime.

Check Fraud and the Evolution of Security Methods

Negotiable instruments have been altered and counterfeited since the 1700s. Methods have included signature and endorsement forgeries, check "washing," counterfeit checks printed on uncontrolled, blank check stock, and altered payee names and dollar amounts. As criminals found ways to scam check issuers, financial institutions developed specific ways to identify and stop fraudulent checks.

Over 30 years ago banks developed *Positive Pay*, an automated check-matching system now available at most banks. With Positive Pay, a company sends to its bank a list of the checks it has issued, itemizing the date, dollar amount, and check number. As checks are processed by the bank to be paid, they are compared against the list provided by the company. If there is a discrepancy in the numbers, the check is set aside as an "exception item" until the company confirms or rejects the check.

Criminals then began altering the Payee Name on checks, or replacing the original check with a counterfeit check. The fraudulent check had the identical account number, check number and dollar amount, but with a new payee name. This avoided Positive Pay detection because the bank's software only matched numbers.

As check fraud losses from altered payee names surged, banks created Payee Positive Pay, which compares the numbers and the Payee name on the check to the list of issued checks provided by the company.

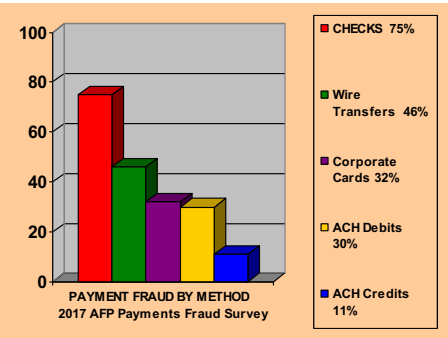
The criminals then began beating Payee Positive Pay by adding a fraudulent Payee name two lines above the original name, once again evading detection by Payee Positive Pay. Currently, there is only one known solution to this problem – special check writing software which eliminates the space for an added Payee name. **(See Page 11.)**

Another variation on Positive Pay is Reverse Positive Pay. In a Reverse Positive Pay system, the bank sends to the customer a list of checks that have been submitted to the bank for payment. The customer compares the information from the checks at the bank to its records. If a bad check is presented to the bank, it is not paid and the customer is not defrauded.

The Struggle to Defeat Check Fraud Continues

All types and sizes of organizations are targeted by check fraud criminals, and those that are successfully defrauded once are often targeted repeatedly. Some organizations reported being hit with check fraud over 15 times in 2016.

Today, check fraud accounts for 75% of all payment fraud attempts. (Other payment fraud methods include wire transfers, corporate credit/debit cards, and ACH debits and credits). This is an upward trend from last year, and reverses a downward trend that had been occurring since 2010.



Checks are the payment method most frequently targeted by fraudsters because checks continue to be the payment *method* most often used by organizations, and because checks are an easy target for fraudsters. Blank check stock can easily be obtained by criminals, as well as routing and account numbers, and fraudulent checks are then printed with relative ease. Poor quality check stock can be altered, and this also accounts for a good portion of fraud losses.

There were several reasons listed for check fraud losses in the 2017 AFP Survey, all of which were within an organization's control: 23% of check fraud losses were due to not using Positive Pay, and another 18% were due to clerical errors. Internal fraud, poor reconciliation, and stolen check stock each accounted for another 15%. Another 13% had gaps in online security control and/or criminal account takeover that contributed to check fraud losses.

In the 2014 AFP Survey, more than half of check fraud attempts involved altered payee names, and 37% were altered dollar amounts. Such alterations may have been prevented by using high security checks. **(See Pages 16-19.)**

New technology is now equipping criminals with an ever-increasing set of tools they can use to commit check fraud. The most prominent are mobile phones using Mobile Remote Deposit Capture (mRDC), and the internet using Business Email Compromise (BEC) scams. A third of the losses created by BEC scams involved the use of checks. Electronic checks, or eChecks, are on the rise, and is a new source of fraud. **(See Page 22.)**

Uniform Commercial Code

The legal basis for liability in check fraud losses is found in the Uniform Commercial Code (UCC), which was revised in 2002. The UCC now places responsibility for check fraud losses on both the bank and its customers. Responsibility for check issuers and paying banks falls under the term "ordinary care." Ordinary care requires account holders to follow "reasonable commercial standards" prevailing in their area and for their industry or business.

For example, in the AFP 2017 Payments Fraud and Control Survey, 87% of larger organizations use Positive Pay or Reverse Positive Pay. A bank can argue that a commercial account holder not using Positive Pay is not exercising "ordinary care" and could be held liable for fraud losses. **(See "Cincinnati Insurance" on Page 2.)**

Uniform Commercial Code, continued

Under Sections 3-403(a) and 4-401(a), a bank can charge items against a customer's account only if they are "properly payable" and the check is signed with an authorized signature. If a signature is forged, the account holder may still be liable if one of the following exceptions applies:

First, if account holders' own failures contributed to a forged or altered check, they may be restricted from seeking restitution from the bank. Section 4-406 requires customers to reconcile their bank statements within a reasonable time and report unauthorized checks immediately. Typically, this means reconciling bank statements as soon as the bank makes the statement available, and always within 30 days.

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.

The internal controls used by a company when issuing checks will be questioned to determine negligence. Since banks are not required to physically examine every check, companies may be held liable for all or a substantial portion of a loss, even if the bank did not review the signature on the fraudulent check.

Holder In Due Course

Holder in Due Course (HIDC), a powerful part of the Uniform Commercial Code, can adversely impact an organization's liability for check fraud. Losses from Holder In Due Course claims, mainly stemming from claims brought by check cashing companies, are rising rapidly. Half of companies hit with an HIDC claim pay the full face value of the check or more.

Under HIDC, a company can be held liable for counterfeit items that look "genuine," or are virtually identical to its checks. **(See Page 9, Robert J. Triffin v. Somerset Valley Bank and Hauser Contracting Co.)** If a genuine-looking counterfeit check was caught by the bank, even on Positive Pay, the issuer can still be held liable. HIDC trumps Positive Pay. **This is the reason to use a controlled check stock.**

Placing a stop payment on a check does not end the issuer's liability to pay the check. Again, Holder In Due Course trumps stop payments and Positive Pay. **(See Page 8, Robert J. Triffin v. Cigna Insurance.)**

"Prevention" Applies To Everyone

It is impossible for organizations to be completely protected against fraud, but there is much they can do to limit their exposure.

Companies that successfully thwart check fraud attempts have multiple techniques and layers of controls. These controls, in order by frequency of use are: Positive Pay, Segregation of accounts, Payee Positive Pay, and "Post no checks" restrictions on depository accounts. Most companies use checks with varying degrees of security features although astonishingly, some still use uncontrolled blank check stock. **(See Page 13, Controlled Check Stock.)**

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 most organizations still issue checks, financial professionals must use a number of tools and strategies to protect their organizations. The Federal Reserve requires 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

www.quimbee.com/cases/price-v-neal
2017 AFP Payments Fraud and Control Survey
2016 Federal Reserve Payments Study
2016 AFP Electronic Payments Survey
Is It Time to Write Off Checks? npr.org
Return of the eCheck Scam. www.qgiv.com/blog
Counterfeit Cashier's Checks Continue To Flood The Banking System. problembanklist.com

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 from the prior 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/articles.

Fraud in a Pocket...Mobile Phones

Mobile fraud is skyrocketing through the cyber sphere. Traditional PC attack techniques are expanding to mobile channels, and malicious activity on mobile phones is growing much more quickly than it did on PCs. Malicious code infects almost 12 million mobile devices at any given time. Protect your mobile device from malware by updating to the latest operating system and using mobile security apps. Trustworthy apps will have many users and many reviews written in correct English.

Mobile Banking Fraud

There are currently over one billion mobile banking customers and that number is expected to increase to two billion in the next few years. As expected, mobile banking fraud has risen at the same time. Many malicious mobile banking apps are fake versions of official mobile banking apps. These fake 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.

Mobile remote check deposit, called Mobile Remote Deposit Capture (mRDC), has become one of the most desirable mobile banking applications. Almost all banks now offer or plan to offer mRDC. According to Guardian Analytics, 72% of all mobile banking fraud last year included mRDC. The American Bankers Association indicates that 50% of small banks, 90% of mid-size banks, and 100% of all major banks have reported mRDC fraud, with a corresponding 400% rise in losses.

There appears to be two primary mRDC schemes. One is the "sweetheart" scam, where fraudsters develop an online romantic relationship, gain access to the victim's checking account and use it to remotely deposit fraudulent checks, and then use various means to quickly get the money out of the account. Another major scam is where fraudsters mimic an online payday lender and convince applicants to unwittingly deposit fraudulent checks via mRDC as part of the loan approval process and then remit the money back to the lender.

There are various practical ways to prevent these and other mobile banking scams: Take note of unusual login activity, such as multiple daily logins, or logins from multiple locations, and unusual endorsements. Financial institutions can also help prevent scams by noting unusual requests to obtain an mRDC account and unusual deposit patterns.

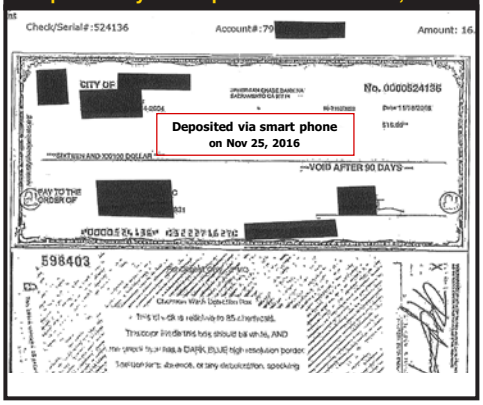
Although making mobile payments is still viewed with suspicion because of security concerns, the Federal Reserve Board predicts that almost half of all mobile users will adopt mobile banking in one capacity or another. It will behoove all mobile phone users and financial institutions alike to be alert and vigilant toward fraud prevention.

Mobile Deposits & Double Debits

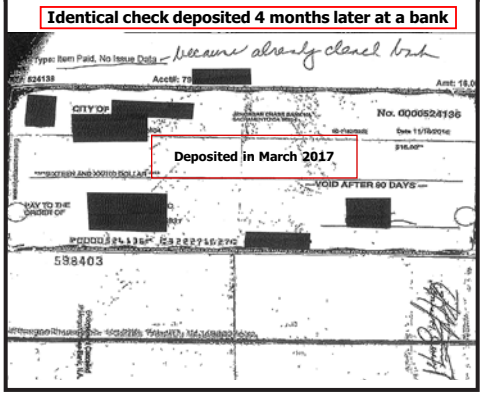
Cases of double-depositing checks with the use of mRDC are growing. The legal basis for Remote Deposit Capture is Check 21. Check 21 has a rule ("Warranty") that specifically prohibits a check or its image from being presented for payment more than once, and provides a powerful recovery remedy if it occurs.

Example: Mary receives a check and deposits the check (its electronic image) via her mobile phone app. She still has the physical check, which she 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 Mary made when the electronic image was deposited.

Deposited by smart phone November 25, 2016



Same check deposited later at a bank . . .



Remedy: Under Check 21, the first presentment of the check (via mRDC) 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

There are additional variations of fraud via mRDC, and they may trigger Holder In Due Course (HIDC) rules. **(See HIDC on Pages 2, 8, 9.)** Example: 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 smart phone. 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 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 the original check even though you have it in your position. Require 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 7.)**

Remember: for mobile fraud prevention, the best defense is to use common sense.

Resources

Guardian Analytics
American Bankers Association
Juniper Research
IBM Software, "Mobile Malware Adapting PC Threat Techniques"
Kount, 2016 Mobile Payments & Fraud Report

BEC Scams

The Business Email Compromise (BEC) scam is a sophisticated email scam in which the attacker assumes the role of the boss, a supervisor, a customer, or a vendor. The purpose is to trick an employee at the victim organization into believing it is a legitimate communication. The email requests funds be sent to an account that is actually controlled by the scammer. The most frequently impersonated people are the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO). BEC scams have been reported in all 50 states and in 131 countries.

According to FBI statistics released in May 2017, BEC scam losses worldwide between October 2013 and December 2016 were **$5.3 Billion**.[1] There were 40,203 incidents adversely impacting 22,292 U.S. victims and 2,053 non-U.S. victims (some hit more than once). While fraudulently transferred funds have been sent to 103 countries, the primary destinations are Asian banks located in China and Hong Kong, followed by banks in Europe.

To put these numbers in perspective, worldwide losses in the 15 months from October 2013 and December 2014 totaled **$214 Million**, with 1,198 U.S. victims and 938 non-U.S. victims. In the following 24 months, from January 2015 through December 2016, losses increased by **$5.1 Billion**, or 2,370%.[2]

Given the number of attacks and losses borne by American companies, it is statistically undeniable that America is the primary target of cyber criminals. Because there are no risks or repercussions to these criminals, scamming and hacking is here to stay. If you can be hacked, you will be hacked, and that fact is not going away.

Common BEC Scam Strategies

- Spoofing legitimate email addresses, using one similar to the targeted business.
- Sending fraudulent e-mails impersonating an executive who supposedly is traveling or im a meeting so the request likely can't be confirmed.
- Stressing urgency, requesting that the funds transfer be done ASAP.
- Using a phrase like, "Sent from my iPad" instead of a corporate email signature. This trick excuses poor grammar and misspellings and helps reinforce a sense of urgency.

1 https://www.ic3.gov/media/2017/170504.aspx

2 https://www.ic3.gov/media/2017/170504.aspx#fn3

Basic Scam Scenarios:

Businesses Working with Foreign Suppliers

A business that has a longstanding relationship with a foreign supplier receives a request from the supplier to wire future invoice payments to a new bank account controlled by a fraudster. The request may be made via telephone, facsimile, or a spoofed e-mail.

Executives Receiving or Initiating a Request for a Wire Transfer

The e-mail accounts of high-level business executives are compromised. A request for a wire transfer from the compromised e-mail account is sent to an employee within the company who is responsible for processing these requests.

Business Executive and Attorney Impersonation

Victims report being contacted by fraudsters who often identify themselves as lawyers or representatives of law firms. They claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims are pressured by the fraudster to act quickly or confidentially in handling the transfer of funds.

If you can be hacked, you will be hacked, and that fact is not going away.

W-2 Data Theft

Fraudulent requests for all employees' W-2s or personal employee information are sent to the human resources department, bookkeeping, or treasury. Victims have fallen for this new scenario even after they were able to successfully avoid the traditional BEC money transfer scam. This data theft BEC scam first appeared just prior to the 2016 tax season.

Remittance Diversion

Cyber criminals infiltrate a company's computer system and access its customer receivable database. They send a change-of-bank/change-of remittance notification to a few high-value customers. The fraudulent notices include instructions to remit payment to a new PO Box or to a new bank account the scammer controls.

Scammers access the company's supplier payable database and change the internal remittance instructions. Payments to the supplier go to the PO Box or bank account the scammer controls. The bank is not responsible for losses these kinds of diversions. However, if the payment was made by check, the bank can help recover the funds from the bank of first deposit after receiving an affidavit of forged endorsement from the victim.

Real Estate Sales Transactions

This scam targets all participants in real estate transactions, including buyers, sellers, agents, and lawyers. The FBI saw a 480% increase in the number of complaints in 2016 filed by title insurance companies that were the primary target of this BEC scam. BEC perpetrators submit a fraudulent request for a change in payment type (from check to wire transfer), or a change from one account number to a different account controlled by the scammer. The scammers are somehow able to monitor the real estate proceedings, and time the change request just before closing.

Escrow Company's Email is Hacked

A title insurance company emailed a preliminary title report to an escrow agent. The report included the title company's bank wiring instructions. The escrow agent's email system had been hacked, allowing the fraudster to open the title officer's email attachment and alter the title company's bank information. When the transaction closed, the escrow agent wired funds according to the altered instructions she had received. The funds went to the hacker and were not recovered. The investigation that followed revealed the title company's original email and attachment were intact; the escrow company suffered a significant loss.

These examples may justify buying cyber-crime insurance.

Selecting Their Victims

While it is not known how BEC scammers select their victims, social media is one obvious method. When companies post events that key executives will be attending, the scammers know when that executive will be out of the office.

Social media tools such as LinkedIn can be used to identify individuals responsible for financial transactions within a business. Scammers learn the procedures or protocols for funds transfers by hacking into the targeted company's computer system and observing communications among and between key individuals, as well as with their bank.

Corporate Impostor Fraud

Corporate Impostor Fraud: Imitating a Legitimate Business

Corporate Impostor Fraud is the unlawful use of a company's name and information to obtain money, goods, or services.

In a case first reported in March 2017, a Lithuanian man stole $100 million from two US-based multinational technology companies. He registered a company in Latvia which bore the same name as an Asian-based computer hardware manufacturer. He opened accounts in its name at several banks using fraudulent documentation. He then set up fake email accounts, and sent phishing emails to agents of the victim companies that regularly conducted multimillion-dollar transactions with the Asian company.

He gave instructions directing payments for legitimate goods and services be sent to the accounts he had opened. He then had the money wired to different bank accounts around the world, including banks in Latvia, Cyprus, Slovakia, Lithuania, Hungary and Hong Kong. To deceive the banks and appear legitimate, he created bogus invoices, contracts, and letters. The scam lasted for two years.

Small Companies at Risk

Smaller companies are frequently targeted because they have fewer legal and financial resources and defenses than large corporations. This includes family-owned businesses with strong credit ratings. Such companies are easily identified through credit reporting agencies that sell business credit reports that can be sorted based on financial strength. Owners and officers' names are often included in credit reports.

Corporate impostors also access State governments' files on businesses for owner and officer information. Using that data, they can submit fraudulent updated owner and officer and new address and P.O. Box to the State and credit reporting agencies to divert correspondence to themselves. Then, the impostors take out loans, corporate credit cards, lease office space and fill it with computers and other office equipment that can easily be sold, etc.

Resources

2017 AFP Payments Fraud and Control Survey

Guardian Analytics

Dun & Bradstreet

FBI Public Service Announcement, Business Email Compromise, 6/14/2016

What Is A BEC Scam? fraudwatchinternational.com

Prevention Strategies

There are numerous solutions for preventing BEC scams and Corporate Impostor Fraud. The overarching theme is awareness through education, proper payment protocols, and continual vigilance. Here are some effective prevention strategies:

- Organizations should monitor its own information with credit reporting agencies and state record databases.
- Educate employees at all levels about BEC scams, starting with executives. Get executive buy-in that instructs mid and lower-level employees to confirm all urgent payment requests. Warn employees to be wary of any request that requires doing something outside of normal channels or standard procedures.
- Use dual controls (two computers, two passwords) when originating and releasing wire transfers or ACH payments. Always release funds using a "clean" computer that is used **only** to connect to the bank. To ensure there are no viruses, that computer should **never** be used for email or web searches.
- All changes of remittance address, bank wiring, or ACH instructions received from vendors must be verified. CALL to confirm any change of payment instructions. Use the contact information on file. Never respond by email or call the phone number on the document that requested the change.
- Banks should verify any bank or account number change on outgoing repetitive wires by calling their clients using a trusted phone number. A bank in Texas implemented this protocol. In the first year, it stopped a BEC scam wire for $900,000 going to China and another wire for $1,400,000 to Eastern Europe. All banks have protocols to authenticate wire transfers. They should have protocols to monitor their customers' bank changes on repetitive outbound wires.
- To prevent check fraud losses, use Positive Pay with Payee Name Match. If extracting and formatting the check issue file is a challenge, SAFEChecks has a solution. Call (800) 755-2265.
- Use a controlled, high security checks with at least 10 security features. **(See Pages 16-19.)** More security features help thwart more criminals. **Frank Abagnale designed SAFEChecks and the Abagnale SuperBusinessCheck, which have never been replicated or used in a check fraud scam in over 20 years.**

Hacked VoIP Phone Systems

Very few organizations know that VoIP phone systems are vulnerable to hacking. In a recent Los Angeles case, a company with a VoIP phone system was hacked. Its bank has a policy of calling to confirm all foreign-bound wires and also re-confirming a change-of-bank on repetitive wires. The hackers observed that when the company sent a wire, the bank called back to confirm the wire. Because of the VoIP phone system, they were able to listen in on conversations between the company and its bank.

When the hackers accessed the company's online banking system[3] to request a wire be sent to a foreign supplier, they changed the bank information. The bank called to confirm the wire and to question the bank change. The hackers had re-programmed the VoIP phone system to re-route the in-bound call from the bank to an accomplice. The accomplice confirmed the wire but was unable to give adequate responses to the change-of-bank questions because they had never heard them.

After getting unsatisfactory responses about the bank change, the banker hung up and called the company again. The call was again re-routed; the wire was again confirmed, and the banker was again given inadequate responses to the bank change. The banker hung up and called the company's CFO on his cell phone. The CFO had been in the office all morning. He stated that the wire was not authorized and that the company had not received any calls from the bank.

An in-depth security inspection of the company's computer system revealed the hacking intrusion. The bank's policy of verifying bank changes on repetitive wires prevented the company from suffering a significant loss. Because banks are not responsible for a customers' computer security, they have no liability for losses from this type of cyber-attack.

Companies that send wires to foreign suppliers are wise to buy cyber-crime insurance, preferably from their existing commercial insurance provider to reduce finger pointing if there is a loss.

3 Many financial institutions use tokens with a code that changes every 60 seconds. If the hacker can capture enough data points, the equation creating the code can be determined and a legitimate online access code can be created.

Cyber Crime – A Never-Ending Challenge

Although statistics regarding cyber crime have worsened in recent years, the underlying fundamentals remain the same. The criminal community includes large syndicates, individual small-time players, and everything in between. Individuals and institutions of every size and industry have been victims. Even though cyber criminals are increasingly more inventive, sophisticated, and malicious, many of their attacks are "low tech" and could have been prevented by implementing simple controls and better educating employees regarding cyber crime prevention.

The battle against cyber crime will never end, and governments, organizations and individuals must be continually vigilant. This includes devoting time and resources to thwarting cyber criminals' attempts at fraud.

New Twists on Cyber Crime

Many organizations are still relying on defenses that are out of date. It's important to update those protections. Also, different industries and types of organizations face different cyber threats and should align their protections appropriately against these evolving threats.

In the latest data on cyber crime, 75% of attempts came from an outsider, while 25% came from internal sources. While the media is rife with headlines of data breaches in large organizations, 61% of data breaches actually happened in organizations with fewer than 1000 employees, showing that small companies are also at risk.

Hacking and malware are the primary methods used to infiltrate an organization's computer system. Hacking was evident 62% of the time, and 81% of hacking breaches were accomplished because of weak or stolen passwords.

Malware was included in 51% of the attacks. 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. In 66% of the attacks, malware was installed because email recipients opened an infected attachment.

Almost 90% of data breaches fall into one of nine broad schemes: insider abuse, cyber-espionage, web-application attacks, crimeware, point-of-sale intrusions, denial-of-service, payment card skimmers, physical theft or loss, and miscellaneous errors. Some schemes are more prevalent in certain industries than in others, and organizations should structure their defenses accordingly. In addition, some attacks are common but do not cause great harm, while other attacks are infrequent but can be financially deadly. Describing the many methods criminals use to infiltrate computer systems and mobile devices is beyond the scope of this Bulletin. Please review the excellent articles and links listed at the bottom of this page in **Resources** and they will provide you with this information.

Preventing Unauthorized Wire Transfers

Wire transfer fraud has increased dramatically, from 5% of payment fraud attempts in 2010 to 46% today. Protections include using dual controls to initiate a request for a wire transfer, and using a clean, "dedicated" computer to release the funds. Because online threats are ubiquitous and insidious, assume that your computers now being used for email and web searches are already infected. Use the details on wire transfer fraud and the specific remedies to prevent it as discussed in depth on **Page 24**.

Companies / Organizations

- Review the latest reports from Verizon, Symantec, and other reputable organizations that do in-depth cyber crime research, and implement their recommendations.
- 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.
- Perform thorough background checks on new employees.
- 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, smart phones, 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 smart phone, 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 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, social media, IM, and websites they visit on their computers and cell phones. See PhoneSheriff, Qustodio, etc.

Resources

2010-2017 Verizon Data Breach Investigations Report
2006-2017 Symantec Internet Security Threat Reports
2014-2016 WhiteHat Website Security Statistics Report
2009-2013 CSI Computer Crime and Security Survey
PC Magazine (pcmag.com)
CNET Networks (cnet.com)
https://www.fbi.gov/investigate/cyber

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 16-19)** 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.

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.

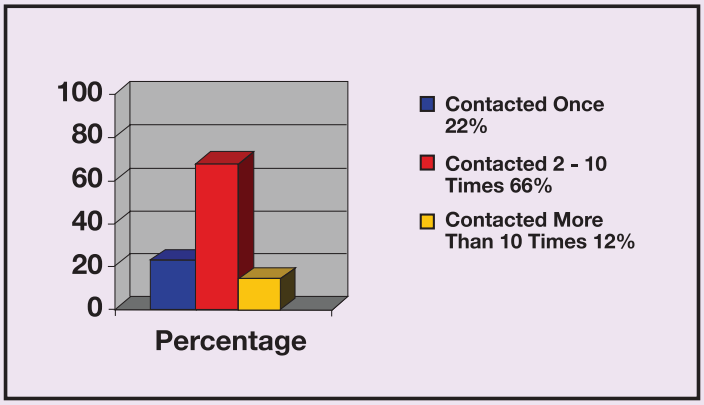
Holder in Due Course trumps stop payments and Positive Pay exceptions. Further, an HIDC can assign, sell, give, or otherwise transfer its rights to another party, who assumes the same legal rights as the original Holder.

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 HIDC claims. This is up from 37 percent in the 2009 survey, indicating a growing and serious concern.

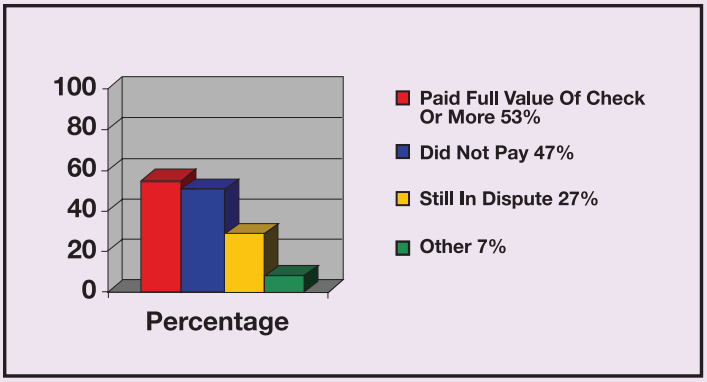
Prudent companies use controlled high security checks to protect themselves from some HIDC claims.

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

Frequency of HIDC Claims



Actions Taken in Response to Holder in Due Course Claims



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 Workers' 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.

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.

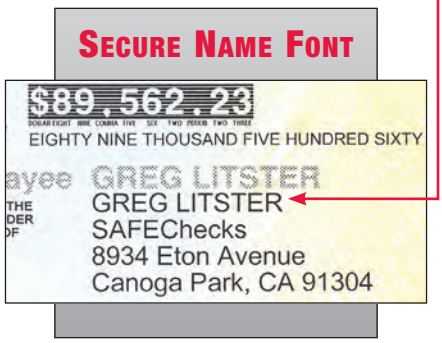
Checks will absorb moisture over time; this reduces the effectiveness of toner anchorage. Use checks within 18 months of production.

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 16-19.**

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 9, Robert J. Triffin v. Somerset Valley Bank and Hauser Contracting Company.** **SAFEChecks sells 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

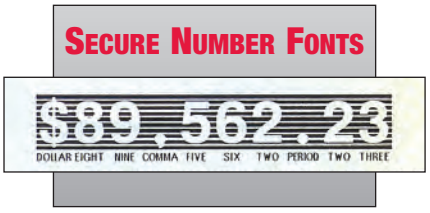
printed above the payee name is another way to prevent added payee names. Forgers add a new payee name two lines above the original payee name. To prevent additions, insert a string of asterisks above the original payee name. Asterisks can be pre-printed on the checks by the check vendor. Do not use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



Check Printing Controls

Because a company has more exposure to check fraud 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.

Positive Pay, ACH, and Secure Check Writing Software

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 16-19.**

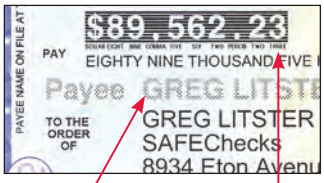
Caution: Some companies have the mistaken notion that if they use Positive Pay they do not need to use high security checks.

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 10 and 13.)** 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 10 and 13).

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.

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 16 through 19 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 11 and 12).**

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 10).**

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 10 -11)** 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.

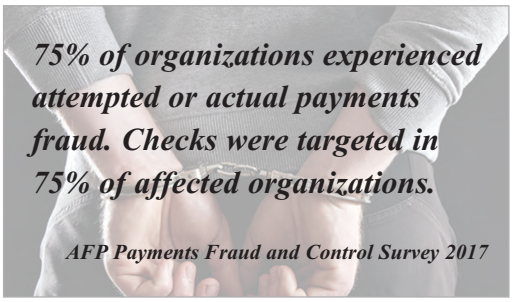
Repeater Rule

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 left with no legal defense against their bank



iStock Photos

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 9.)**

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, or in the catalogs 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.

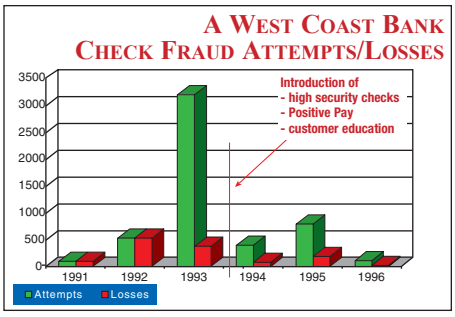
Wire Transfers

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.

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.

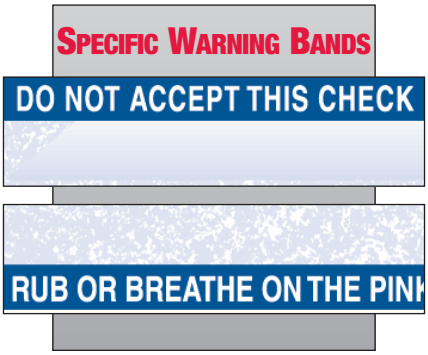
Controlled Paper
is manufactured with many built-in security features, such as a true watermark, visible and invisible (UV light-sensitive) fibers, and multi-chemical sensitivity. To keep the paper out of the hands of forgers, the paper manufacturers have written agreements that restrict the paper's 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 16-19.**

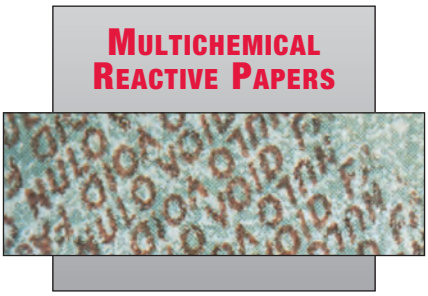
Fourdrinier Watermarks
are faint designs pressed into the paper while it is being manufactured, and are also known as "true" watermarks. When held to the light, these watermarks are easily visible from either side of the paper for instant authentication. Copiers and scanners are not capable of replicating 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 9, Pomerantz Staffing Services.**

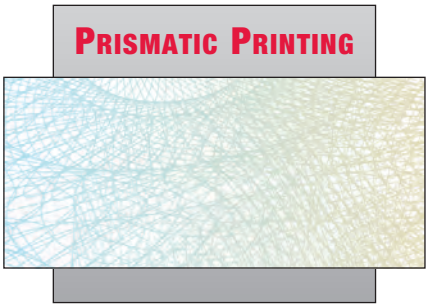


Multi-chemical Reactive Papers
produce a stain or speckles or the word "VOID" when activated with ink eradicator-class chemicals, making it extremely difficult to chemically alter a check without detection.

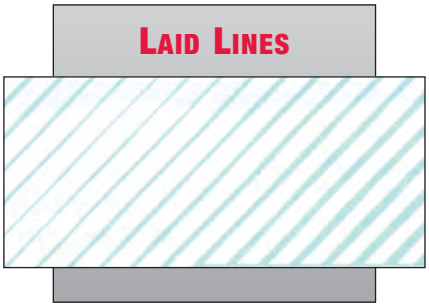


Checks should be reactive to at least 15 chemicals.

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.

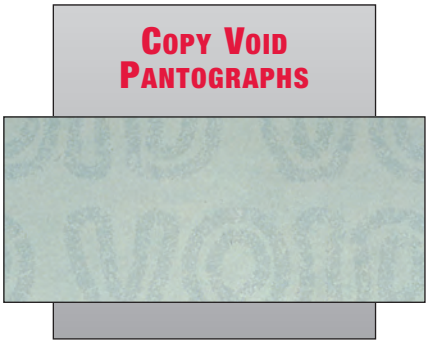
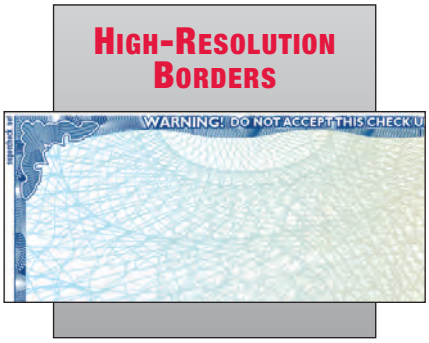


Image Survivable Secure Seal Barcode

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 10 and 11.**

High-Resolution Borders

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

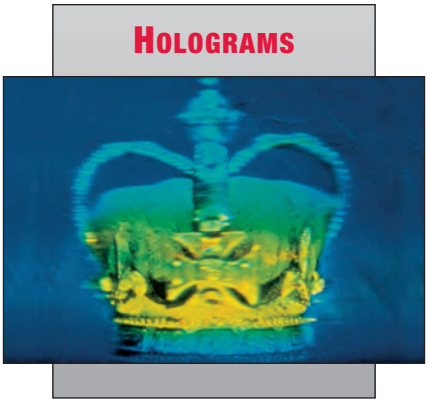


Ultraviolet Light-Sensitive Ink and Fibers

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

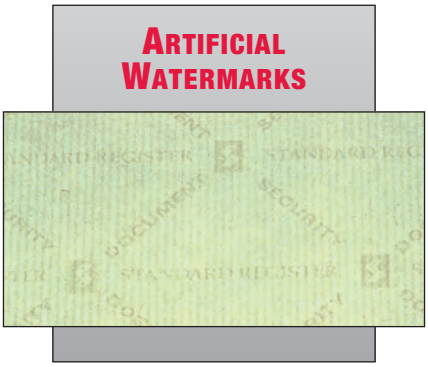
Holograms

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.



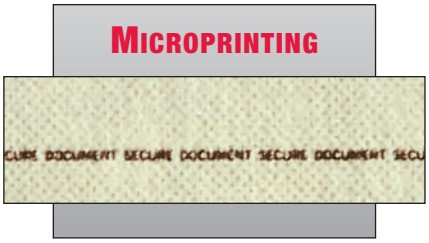
Artificial Watermarks

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 9),** and establish the basis for an indemnity claim under Check 21's Indemnity Provision. **(See Page 7.)** 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 16-19.)**

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

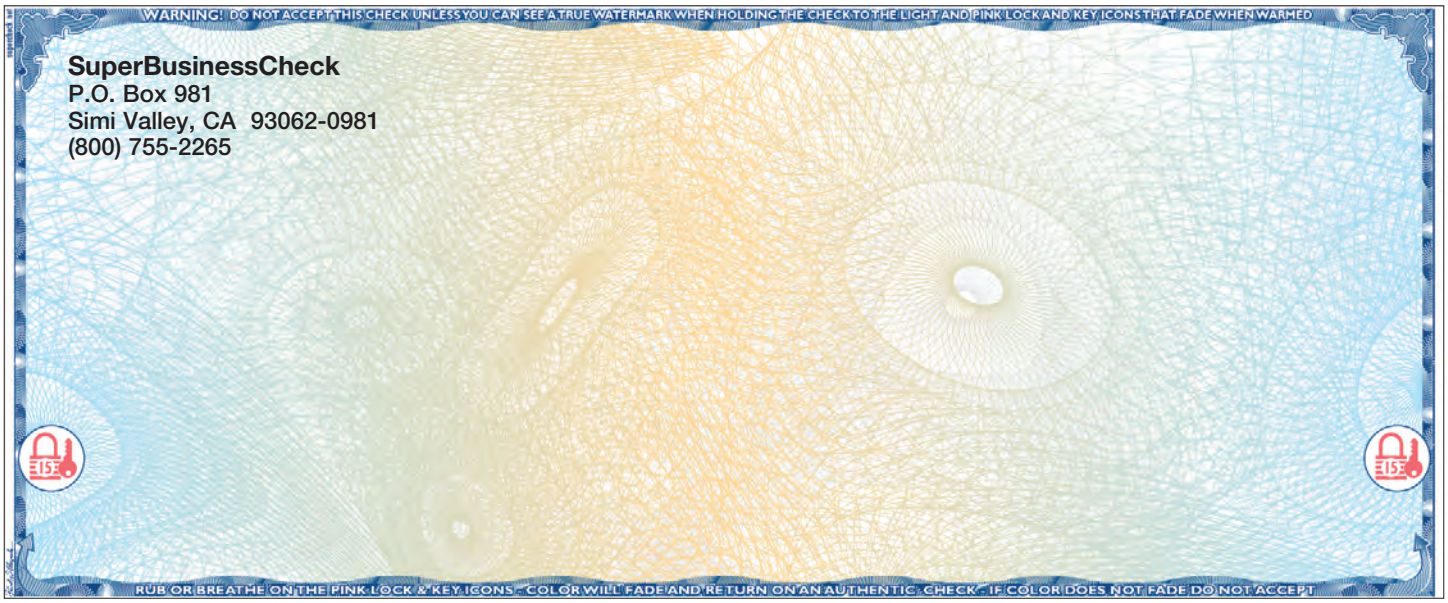
- Controlled Paper Stock
- Toner Anchorage
- Chemical Sensitivity
- Copy Void Pantograph
- Chemical Reactive Ink
- Fluorescent Ink
- Fluorescent Fibers
- Microprinting

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



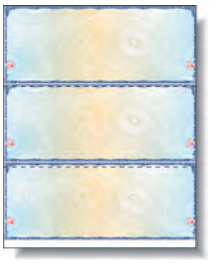
Available Styles

Laser - Top

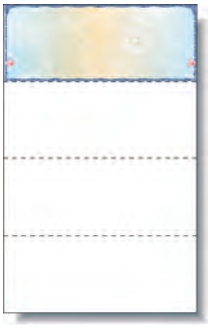
Laser - Middle

Laser - Bottom

Laser 3-On-a-Sheet



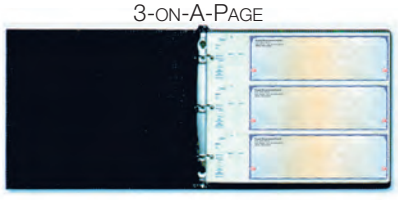
Legal Laser - Top



Legal Laser - Second Panel

Pressure Seal Checks Also Available

3-on-A-Page

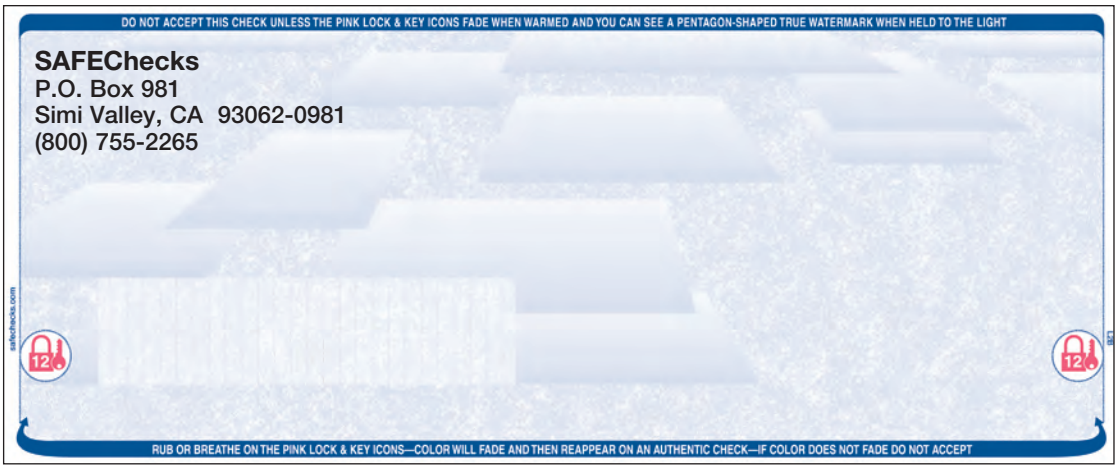


Secure Ordering Procedures

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
Sequenced Inventory Control Numbers
Microprinting
Laid Lines

Available Styles

Laser - Top

Laser - Middle

Laser - Bottom

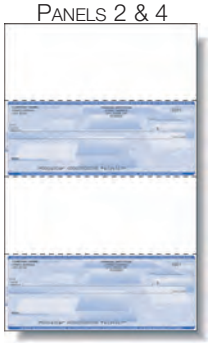
Continuous - 1 part

Continuous - 2 part

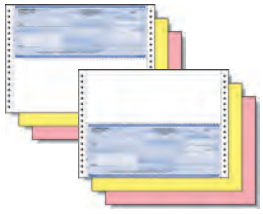
Legal Laser - Top

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 11, 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

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

SAFE Checks®

Download a price list at SAFEChecks.com
8934 Eton Avenue (800) 755-2265
Canoga Park, CA 91304 Fax (800) 615-2265

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

Text to be printed above signature lines

☐ Check this box for two signature lines

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

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

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

LASER CHECKS

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

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

☐ **8½ X 11 SAFE Checks®**
- ☐ Top Check ☐ Blue ☐ Green ☐ Red ☐ Plum
- ☐ Middle Check ☐ Blue ☐ Green
- ☐ Bottom Check ☐ Blue ☐ Green

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

→ **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: _____

THREE-ON-A-PAGE HANDWRITTEN CHECKS

- ☐ **Single Stub (General Check) Frank Abagnale's SuperBusinessCheck**
- ☐ **Duplicate**
- ☐ **Three-on-a-Page Binder**

SAFE Checks® SECURE ORDERING PROCEDURES

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

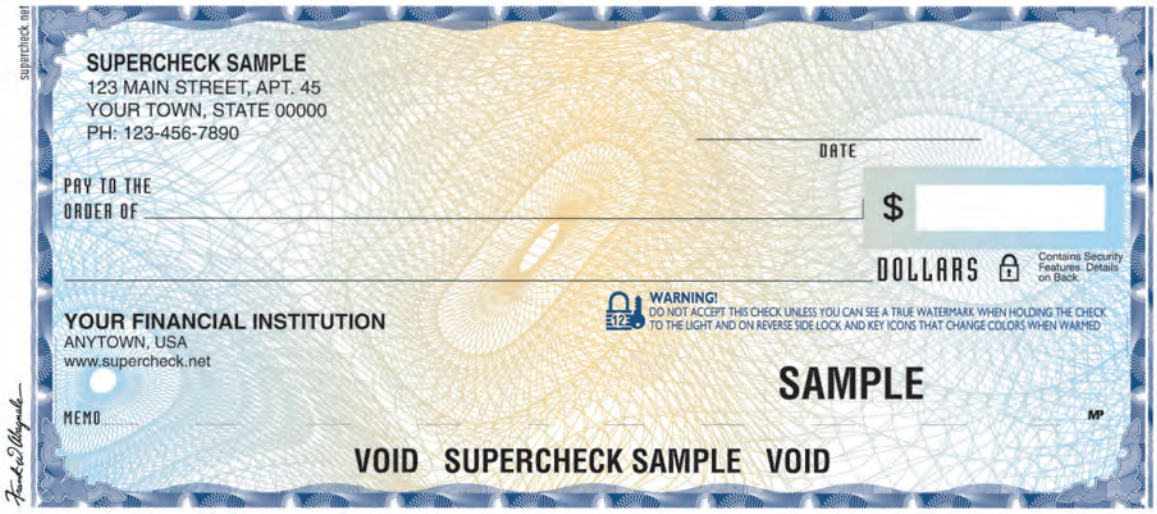
Download a price list from SAFEChecks.com
Call (800) 755-2265 for assistance in completing form or to answer any questions.

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

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

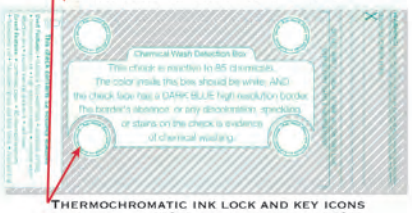
Controlled Paper Stock
Fourdrinier (True) Watermark
Thermochromatic Ink
Chemical Sensitivity
Explicit Warning Bands
Prismatic Printing
Chemical Wash Detection Box
High-Resolution Border
Laid Lines
Fluorescent Fibers
Fluorescent Ink
Microprinting

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:

1. Completed ORDER FORM
2. VOIDED CHECK (indicate any changes on the face)
3. VOIDED DEPOSIT SLIP

Please mail to:

SAFEChecks
P.O. Box 981
Simi Valley, CA 93062-0981

Delivery Times:

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 - $31.95 per box of 120
Duplicate - $34.95 per box of 120
Shipping/Handling - $5.80 per box

PAYMENT OPTIONS:

_____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

Preventing Embezzlement

A 46-year-old bookkeeper embezzled $155,460 from a nursing center in Kansas. When she was caught, it was found she'd also stolen from several other employers as well. Her job as a bookkeeper was a violation of her parole on previous fraud charges...

- A woman who worked as a bookkeeper in Maryland stole over $1.3 million from four different non-profit organizations. She took money that was intended to provide services for disadvantaged children and homeless families.
- The controller at a manufacturer in Cincinnati stole $8.7 million over 11 years through fraudulent checks.
- The controller of a Connecticut hedge fund embezzled more than $9 million over 9 years by transferring money from his employer to accounts he controlled.
- A Texas bakery executive and his wife stole almost $17 million over 15 years through paying personal expenses with company checks.
- A hospital payroll director stole $480,000 over three years by 'paying' salaries and vacation time to terminated employees.

Embezzlement has damaged countless organizations of every type and size. Some have gone out of business due to losses. Those that do survive often experience layoffs, cutbacks and salary freezes. A typical organization loses 5% of annual revenue to fraud. The victims are not only the organizations themselves, but their suppliers, vendors, and families.

Organizations of different sizes have different fraud risks. Corruption is more prevalent in larger organizations, while check tampering, skimming, payroll, and cash larceny schemes are twice as common in small organizations.

Fraud Loss Statistics

According to the Association of Certified Fraud Examiners (ACFE) "Report to the Nations" 2016, the worldwide median loss for embezzlement cases was $150,000, with 23% of cases causing losses of $1 million or more.

In the 2016 Hiscox Embezzlement Study of the United States, particularly those cases occurring in companies with fewer than 500 employees (which represents 69% of all Federal cases reviewed), the average loss was $807,443. The median loss was $294,354. There were projected losses in excess of $500,000 in 36% of cases involved, and 20% of losses involved $1 million or more.

Given that embezzlement is so pervasive, one must 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?

Only about 5% of perpetrators had previously been convicted of a fraud-related offense, so background checks are ineffective in preventing this type of crime. Embezzlers were most likely to hold bookkeeping or finance positions. While regular employees embezzled most frequently, the greatest losses came from managers and executives. In some studies, females embezzled more often than males. In other studies, males were the more frequent perpetrators; however, males always caused the greatest losses.

The perpetrator's level of authority was strongly linked to the size of the fraud. In the cases studied by ACFE, the median loss in the schemes committed by an owner/executive was $703,000. This was more than four times higher than the median loss caused by managers ($173,000) and nearly 11 times higher than the loss caused by employees ($65,000).

The majority of embezzlers were in their early 40s, but the greatest losses came from those aged 60 and above. In some studies, about 40% had been at the job one to five years, and over 50% had been there more than five years.

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 almost 30% of the cases, and in over 40% of the small business cases. In other instances, controls were in place but were overlooked or were overridden by upper management.

An overlooked but vital factor is the tone set by executives, especially in cases over $1 million. Management tone contributing to fraud includes unethical "wheeler-dealer" 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.

Various motivating factors included financial difficulties, shopping addiction, substance abuse, an entitlement attitude, and a desire to support a significant other.

In past studies, 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.

2016 Hiscox Embezzlement Study

Detecting Embezzlement

Embezzlers 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 financial difficulties and/or family problems, and having an unusually close association with a vendor or customer. They also included an overt sense of entitlement, excessive control issues, unwillingness to share duties or take vacations, addiction problems, and irritability or defensiveness. At least one of these red flags was present in almost 80% of the cases.

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. Almost 40% of all cases were detected by receiving a tip, higher than any other detection method, including audits. Organizations that had a tip hotline had an almost 50% rate of discovery. Employees provided more than half of all tips that led to the discovery of fraud.

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

Having anti-fraud controls in place – and following them – directly led to quicker detection of embezzlement schemes and lowered fraud losses. Companies without these controls experienced losses 45% higher than those with the controls. Anonymous "Tip Hotlines" with a cash reward significantly decreased the duration and cost of a fraud scheme.

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 can be an effective deterrent. They provide a psychological benefit: potential embezzlers believe that they will be caught.

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.

Education is a significant element in 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.

> ***"If you make it easy for people to steal from you, they will."***
>
> ***— Frank W. Abagnale***

Using your bank's Lockbox service is the best and most cost-effective way to prevent embezzlement via diverted deposits.

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 Business Fraud

Embezzlement is a significant threat to small businesses. These companies usually have fewer antifraud controls than larger companies, and therefore are more vulnerable to fraud. The median loss suffered by small organizations was the same as that of large organizations, but it inflicted greater damage on the small organizations which had fewer resources to defend themselves.

Of cases that were active in the US federal court system in 2015, 80% had fewer than 100 employees. Smaller organizations with a tight-knit employee base are particularly vulnerable precisely because employees are trusted and empowered. Check tampering, skimming, payroll, and cash larceny schemes were twice as common in small organizations as in larger organizations. Most small-business fraud victims did not recover any of their losses.

Resources

Association of Certified Fraud Examiners "Report to the Nations" (2010 – 2016)

Hiscox Embezzlement Study (2016)

Marquet International "Marquet Report on Embezzlement" (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

A checklist for establishing an effective fraud prevention program:

1. Is ongoing anti-fraud training provided to all employees?
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?
6. Does internal auditing have the 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 appropriately?

Ransomware – The Pirates are Back

Mimicking pirates plundering on the high seas, cyber pirates today use malware attacks as a new money-making scheme. Healthcare providers, municipalities, transportation companies, banks, manufacturers, churches and other non-profits worldwide have been hit by attacks demanding a ransom. The malware locks down the computer and mobile devices, or encrypts the files. The files can't be accessed unless the ransom is paid.

Many times, the ransom note appearing on the victim's screen has a digital clock ticking down the minutes and seconds from 72 hours. When the timer expires, the ransom demand doubles. If the ransom is not paid after a week the files are deleted forever. The threat should not be taken lightly.

In the recent WannaCry attack in May 2017, cyber criminals exploited a vulnerability in the Windows operating system that allowed the cyber pirate to take over more than 300,000 computers worldwide. Within days of the initial attack, unrelated third-party hackers began altering the malware's original code to make the virus more difficult to kill. The ransom demand was $300, payable in BitCoins. Microsoft's XP operating system, which Microsoft stopped supporting in 2014 but is still widely used around the world, was very vulnerable and was hit particularly hard.

Within two days of the attack, Microsoft took the unprecedented step of issuing a fix for Windows XP and Windows 8 machines. The following webpage address provides links to all the Microsoft patches for various systems: http://bgr.com/2017/05/16/wannacry-ransomware-how-to-stop-wanna-cry-windows-patch/. Microsoft also added updates to Windows Defender in an attempt to stop the malware from spreading further.

Pay the Ransom?

According to a survey by Trend Micro, the average ransom demand is around $722 per computer, although that is changing. Cyber security expert Brian Krebs writes that ransomware attacks are becoming more targeted and the ransom demands more expensive. Many security experts strongly recommend against paying the ransom. They argue that sending money to cyber criminals reinforces bad behavior and proves that ransomware works; they suggest there is no guarantee the decryption key will be sent. Notwithstanding, Trend Micro found the majority of organizations that got infected paid the ransom.

Before paying a ransom, victims should find out if a solution has already been found. Krebs recommends victims visit the "Crypto-Sheriff" page at www.NoMoreRansom.org, a site backed by security firms and cybersecurity organizations in 22 countries. NoMoreRansom claims it saved over 6,000 victims of ransomware more than $2 million in its first six months of operation after launching on July 25, 2016.

Recommendations

1. Install computer and software updates, especially anti-virus software. Update at least weekly.
2. Educate employees about safe email practices such as:
   - Don't click on embedded links unless the true source of the email can be validated;
   - Only open attachments you're expecting;
   - Scan attached files with antivirus software before opening;
   - Don't open unsolicited e-mail;
   - If you open spam, don't click links to unsubscribe unless the sender is a trusted vendor;
   - Never forward messages, which reveal coworkers' and colleagues' e-mail addresses;
   - Create a generic e-mail account for newsletter subscriptions.

eCheck Fraud – It's Already Happening

eChecks is a new technology designed to move money quickly and efficiently. The concept is simple: Send money to the intended recipient by email. The email includes a link to a file that contains a check image payable to the recipient, and an access code to open the file and download and print the check. The check image can be downloaded only once for printing.

The flaw is the recipient's ability to print the eCheck as a high resolution PDF, which can be reprinted and cashed multiple times. Every check appears genuine. Fraudsters have already exploited this flaw.

A company in the West with hundreds of small vendors in 40 states switched to eChecks. Over a few months the company issued about 9,000 eChecks, and soon had over $17,000 in check fraud losses!

More than 50 of the eCheck recipients downloaded and saved the check images as high resolution PDFs. Then, they printed and cashed or deposited those duplicate checks, getting paid multiple times on the same check. Over 300 duplicate eChecks hit the company's bank account.

Banks have used software to detect duplicate checks for decades. The process is based upon check numbers and dollar amounts. In this case, the bank could not identify many of the duplicate eChecks because about 10 percent of the total eChecks issued had a check number that was not readable or captured by the bank's Character Recognition (OCR) software.

As the duplicate eChecks were discovered by the company and presented to the bank, the bank began reimbursing the company. However, as the dollar losses grew, the bank told the company it should have been using Positive Pay, even though the bank had never before mentioned Positive Pay. The bank refused to reimburse the company for additional losses. (Positive Pay will work with eChecks, but would be difficult because of the high percentage of unreadable check numbers, each of which would have become a Positive Pay exception item.)

One of the company's vendors had its email system hacked. The hacker intercepted the eCheck email, and downloaded and printed the $2500 check image. The hacker then cashed the check at a check cashing store after forging the endorsement. The company has filed an affidavit of forged endorsement with its bank and expects to recover the $2500 from the bank of first deposit; however, this does not spare them the harassment of dealing with the fraud.

eCheck users should be mindful of their legal liability for duplicate checks under UCC § 3-302, Holder In Due Course. If a check looks "genuine," the drawer can be held liable for the face value of the check, even if the check is counterfeit. **(See Page 9, Robert Triffin v. Somerset Valley Bank and Hauser Contracting Co.)** Because every eCheck can be printed/saved as a PDF that appears "genuine," eCheck users are strongly encouraged to buy check fraud insurance.

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 16-19.**

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

Wire Transfer Fraud – An Explosion In Cyber Space

Wire transfer fraud has increased dramatically, from 5% of payment fraud attempts in 2010 to 46% today. Wire transfers were the second most-often targeted payment method in 2016, and the dramatic increase in wire fraud coincides directly with the rise in Business Email Compromise (BEC) scams. Sixty percent of organizations that experienced actual payments fraud via BEC scams did so via wire transfers. Fraudulent transfers have been sent to 103 countries, with the majority going to banks in China and Hong Kong.

After compromising an account, fraudsters submit wire requests through online and mobile banking channels as well as through offline channels such as a call center, fax, or through a branch of a financial institution.

While wire transfers themselves are often for large dollar amounts, the losses associated with a fraudulent wire go well beyond that. Additional costs incurred by victimized companies and financial institutions include investigation, remediation, litigation, brand erosion, fines, and loss of customer base.

Behavior-based solutions employed by financial institutions have proven effective at detecting fraud. Although fraudsters can mimic the computer, location, IP address of an originator, they cannot mimic all aspects of normal behavior that is used by organizations and personnel. At some point during the process of originating a wire, the fraudster will do something that is unusual or suspicious when compared to the victim's normal behavior. Anomaly detection solutions used at financial institutions are very effective in catching and stopping fraudulent attempts.

On the part of organizations, having dual controls in initiating a wire transfer is important. In addition, unauthorized wire releases can be prevented in four straightforward steps:

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. 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.

2) Require two different computers and users/passwords to send money out of the organization's 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) Request the organization's bank to update its Electronic Funds Transfer (EFT) agreement to reflect these revised, two-computer initiation-release procedures.

4) Implement all additional controls and technologies recommended by the organization's bank. Failure to implement the controls the bank recommends may result in the organization being liable for any cyber losses.

RESOURCES

Guardian Analytics – "Dissecting Wire Fraud: How it Happens, and How to Prevent It"

2017 AFP Payments Fraud and Control Survey

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 microcut 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.

Same Day ACH – Innovation in Payments

Prior to September 23, 2016, most ACH payments were settled (became available to the recipient) on the next business day. However, many businesses and consumers could benefit from same-day processing and availability. In May 2015, the voting membership of the National Automated Clearinghouse Association (NACHA) approved an amendment to their Operating Rules that made payment processing faster. The rule change phases in over three years; Phase 1 became effective September 23, 2016.

Phase 1 of Same Day ACH, as the rule is called, requires all receiving financial institutions (RDFIs) to have the capability to process transactions on the same day they're received. It enables ACH Originators (ODFIs) that want same-day processing the option to send same-day ACH transactions to accounts at any receiving financial institution (RDFI).

The Rule includes a modest "Same Day Fee" of 5.2 cents paid by the ODFI on each Same Day ACH transaction so that RDFIs can recover their costs for enabling and supporting Same Day ACH through a new ACH Network. It does not affect existing ACH schedules and capabilities.

Originating financial institutions (ODFIs) can now submit files of same-day ACH payments through two new clearing windows provided by the ACH Operators:

- A morning submission deadline at 10:30 AM ET, with settlement occurring at 1:00 PM.
- An afternoon submission deadline at 2:45 PM ET, with settlement occurring at 5:00 PM.

Virtually all types of ACH payments, including both credits and debits, will be eligible for same-day processing. Only high-value transactions above $25,000 and international transactions (IATs) will not be eligible. Eligible transactions account for approximately 99 percent of the current ACH Network volume.

Phase 2 is effective September 15, 2017. It enables same-day processing of virtually any ACH payment; this benefits consumers paying items like mortgage and credit card payments.

The last phase, Phase 3, becomes effective March 16, 2018. On that date RDFIs are mandated to make funds available from Same Day ACH credits (such as payroll Direct Deposits) to their depositors by 5:00 PM at the RDFI's local time. Financial institutions may make funds available earlier than 5:00 PM, just not later.

Resources

NACHA.ORG: Same Day ACH

ACH Fraud Is On The Rise

The Automated Clearing House (ACH) and its "ACH Network" serve as the backbone for electronic payments between individuals and organizations in America. Last year, the ACH Network processed over 25 billion transactions valued at $43 trillion. These transactions included services such as payroll direct deposit and direct bill payment.

ACH transactions are primarily generated through files sent from organizations to their banks to be processed through the ACH Network, a payment vehicle which is more secure than other payment methods. In fact, the ACH Network is one of the safest payment systems in the world. However, the Association for Financial Professionals 2017 Payments Fraud and Control (AFP) Survey reported a recent rise of ACH debit fraud attempts—from 25 percent in 2014 to 30 percent today. This figure is the highest ever reported and could be an indication of some new type of fraud effort. ACH credit fraud has held steady at 11%. Of those reporting ACH fraud attempts, 84% experienced between one and five ACH fraud incidents in 2016.

While there are several ways a criminal can commit ACH fraud, they all have one element in common: gullibility or complicity on the part of someone along the ACH "highway." Fraudsters only need two pieces of information, plus an entry point onto the highway, to commit ACH fraud: A checking account number and a bank routing number. The easiest way for criminals to obtain bank account information is by stealing checks out of the mail. This method can be thwarted by taking your mail to the Post Office or by giving it directly to a USPS mail carrier.

Another source of bank account information is a dishonest employee working in a company's Accounts Receivable department with access to images of all the checks received by the company. This threat is difficult to thwart because the account information is part of the check image. However, this threat might be prevented by using your bank's lockbox service.

Returning Unauthorized ACH Debits

The timeframe for a business to return an unauthorized ACH debit is 24 hours; for a consumer it is 60 days. Most ACH fraud losses can be avoided by adopting and adhering to the "best practices" listed below. For example, in the AFP survey, of the companies reporting ACH fraud losses nearly 33% said they did not return the unauthorized ACH debit in a timely fashion; 29% indicated a gap in their online security; and another 24% did not use ACH debit blocks or filters.

Best Practices

- Use an ACH filter or block on every bank account. An ACH block stops all ACH debits from paying against your account. An ACH filter allows pre-authorized ACH debits to pass through the block; all other ACH debits are blocked.
- Monitor your accounts daily, and always in the morning. Every bank has a cut-off time; don't miss it.
- 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.
- Know the person with whom you are dealing– fraud happens by incorrectly assuming an unknown party is legitimate.

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

- Not reconciling accounts on a timely basis and reporting unauthorized transactions
- Not using appropriate ACH blocks or ACH filters when suggested by the bank
- Not returning suspect ACH items on time
- Not using ACH positive pay when recommended by the bank

Resources

2017 NACHA - The Electronic Payments Association
2017 AFP Payments Fraud and Control Survey

Frank W. Abagnale

Frank W. Abagnale is one of the world's most respected authorities on the subjects of forgery, embezzlement and secure documents. For over 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 over 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.

SAFE*Checks*®

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. SAFEChecks 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, their 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, they know the various methods criminals use to commit payment fraud. SAFEChecks 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.

SAFE*Checks*®

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