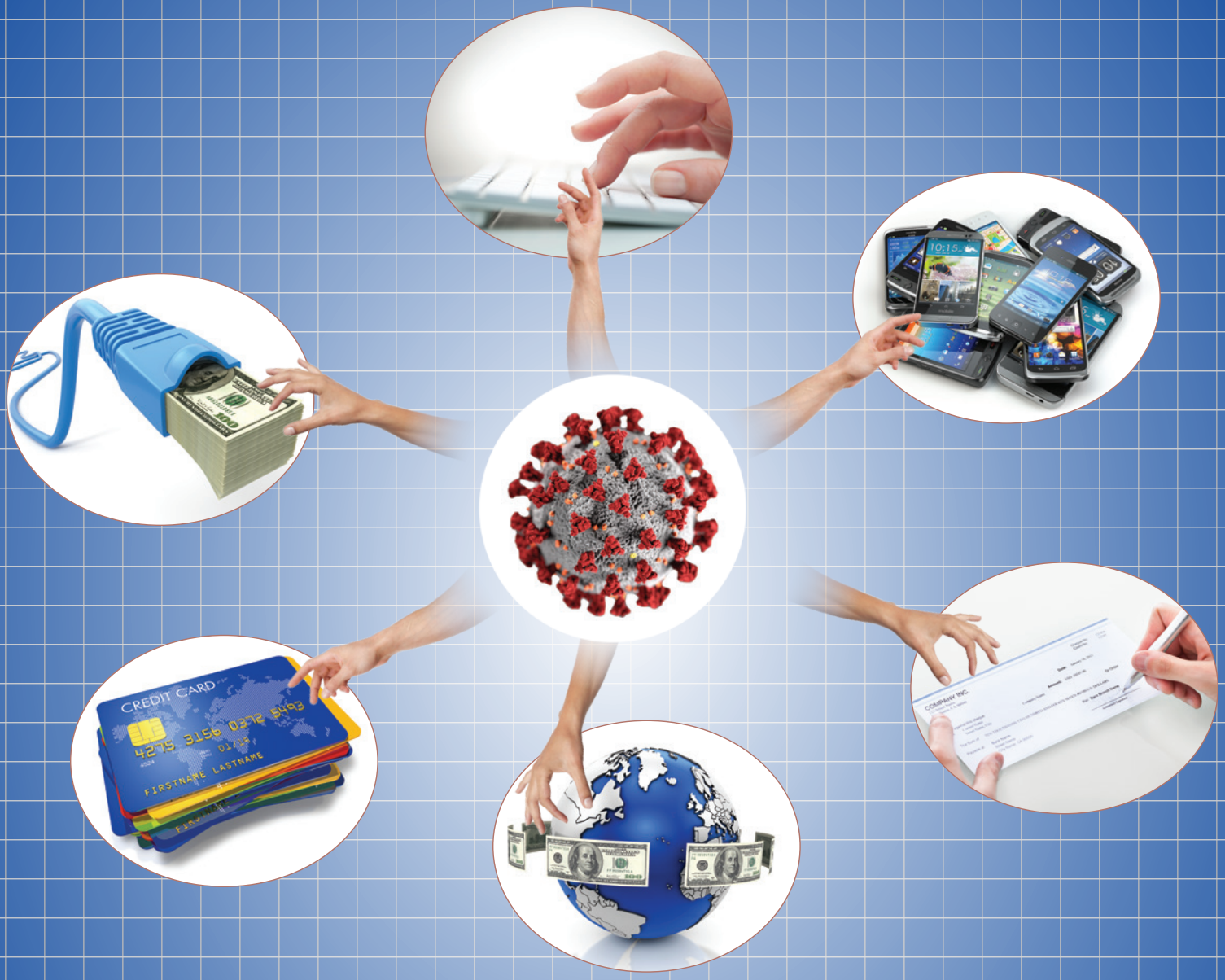
Frank W. Abagnale

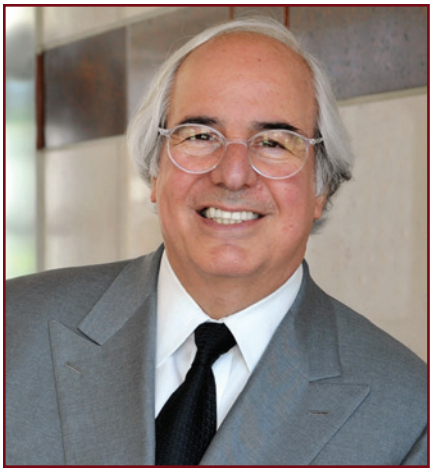
VOLUME 16

THE FRAUD BULLETIN



INSIDE THIS ISSUE

Frankly Speaking . . .



As the world emerges from the global pandemic, the meteoric rise in fraud attempts has been staggering. In 2020, consumers filed 400,000 complaints, stating their identities were stolen and used to claim government benefits. That is up from 13,000 complaints in 2019, a 2900% increase.

The Federal government sent $872 billion in unemployment insurance aid to the states during the pandemic. At least $163 billion was paid improperly, with a significant portion attributed to fraud.

In addition, cybercrime rose by over 300%. As internet use suddenly seemed to fill every virtual corner because of COVID-19 lockdowns, scammers quickly adapted and devised new methods to defraud individuals and organizations.

I am often asked what I believe is coming in the world of cybercrime. Cybercrime has historically been about stealing money and/or data. However, I believe cybercrime is becoming an overtly malicious crime. Fraudsters are motivated by greed and money, but what has startled me since the pandemic began is how many scams seem to be driven by sheer malice. Inflicting emotional or physical harm or creating social disruption is the objective, not money.

These crimes are easy to perpetrate because of the treasure trove of information people post on social media. There are endless apps and online means to find personal information, pictures, and travels, which fraudsters use to target future victims.

RED FLAGS

No matter how sophisticated or amateur a scam is, there are always two red flags. The first red flag is the scammer will ask for money, and it must be sent immediately! That's a huge red flag!

The second red flag is that the scammer will ask for personal information – social security number, date of birth, bank account number, credit card number, mother's maiden name. Even in romance scams that may last for months, the scammer will ask for information. Remember, you never met the scammer, and you didn't solicit the email or text. Before parting with money or data, you absolutely must know the true intensions of whomever is at the other end of that device.

PASSWORDS

I always make the statement that passwords are for treehouses! Passwords were invented in 1964 when I was 16 years old, before I did any of the things I did. Today, I'm 74 and we're still using passwords! How is that possible? Over 63% of network intrusions result from compromised user passwords, including the Colonial Pipeline. Nearly 81% of hack-related breaches involve weak or stolen passwords; 579 password attacks occur every second, or 18 billion attempted hacks a year. America's three largest banks spend over $100 million yearly resetting passwords in their call centers, an average of $70 per call.

EDUCATION

How can these issues and problems be resolved? My philosophy is based on three concepts: Prevention, Verification, and Education. For over 40 years, I have stressed education. Scams and technologies always evolve, so education will always be the single most effective crime-fighting tool. Regardless of security protocols and procedures, human beings will ultimately be implementing those processes, and people are always the weakest link in any defense system. People must learn how scams work, and recognize the red flags to avoid the loss of money or reputation. Scam Me If You Can (Page 29), is helpful.

ETHICS

What I did in my youth was unethical, immoral, and illegal, so I speak from experience.

Today's society has become extremely unethical. In the 1940s and 50s and for centuries before, people were taught right and wrong by their parents, grandparents, churches, and schools. Everyone was expected to do the right thing. The media in those bygone days would often include a moral code into the dramas and films that were produced, where the good guy who did the right thing, won.

In contrast, today's youth are engulfed by corruption on screens big and small, often shared with peers and communities. This environment teaches them it's okay to lie a little, to cheat a little, to steal – just don't get caught. Sadly, "ethics" is not taught in schools; teachers would be accused of teaching "morality."

I have spoken to thousands of students over the years and encouraged them to stand up for what is right. I challenge business and community leaders to do likewise; to live and display good ethics and be examples of honesty and fairness.

AARP

Every day in America, 10,000 Americans turn 65 years old. Some of my most rewarding work has been partnering as an Ambassador with AARP's Fraud Watch Network to help educate senior citizens to avoid becoming victims of fraud. It is distressing that those who should be the most respected and cared for in our society have become among the most victimized.

Senior scams are perpetrated by family members, alleged friends, advisers, health care providers, and strangers. While law enforcement and protection agencies play important roles in thwarting elder fraud, alert citizens are seniors' best line of defense.

20TH ANNIVERSARY

The year 2022 marks the 20th anniversary of the Steven Spielberg film, Catch Me If You Can, which became a Tony-award winning musical. Both the film and the musical are loosely based on the book, which was only semi-biographical. However, I'm gratified to see it portrayed how this amazing country, the United States of America, gave me a second chance. I have worked with the FBI for almost 50 years, and I accept no pay for this work.

The year 2022 is also SAFEChecks' 25th anniversary. I design their checks, and I'm proud to say that in 25 years, SAFEChecks has never had one of their checks replicated.

This Fraud Bulletin was created to help individuals and organizations protect themselves. I hope you find it useful and inspiring. Preventing fraud is everyone's business!

Frank W. Abagnale

www.abagnale.com

Greg Litster, Robin Johnson, Elaine Litster - Editors

Payments At The Speed Of Light

Ever-faster payments have been the Holy Grail sought by those engaged in commerce almost since the exchange of goods and services for money began. Modern technology and the internet took this exchange process into an entirely new realm, and it is believed that the first e-commerce transaction occurred in 1994 with the most ubiquitous of foods: ordering pizza online.

The Federal Reserve Banks indicated a new direction in payments as early as 2012, stating a desire to "improve the speed and efficiency of the U.S. payment system from end-to-end over the next decade while maintaining a high level of safety and accessibility." In September 2013, the Federal Reserve released its "Public Consultation Paper" in which it discussed the deficiencies and opportunities it saw in the U.S. payments system, and five general outcomes it desired for improvement. The Federal Reserve overtly sought extensive input and insights from a deep and broad range of stakeholders on how to create solutions for those deficiencies, to fully harness those opportunities, and to achieve those outcomes.

In January 2015, the Strategies for Improving the U.S. Payment System document was released, and the more-refined five desired outcomes for enhancing the payments system were outlined and discussed in depth. These outcomes were Speed, Security, Efficiency, International accessibility, and Collaboration. Five Strategies were also outlined and discussed in depth for achieving these outcomes. These Strategies included 1) actively engaging with stakeholders, 2) identifying methods for creating "safe, ubiquitous, faster payments," 3) reducing fraud, 4) increasing efficiency, 5) enhancing Federal Reserve Bank payments, settlement, and risk-management services.

The Faster Payments Task Force and the Secure Payments Task Force were established, again with a deep and broad set of stakeholders making up each Task Force. They issued their findings in the U.S. Path to Faster Payments Report, Part 1 in January 2017, and their Call to Action in the second report in July 2017.

Findings included the benefits of speed, availability, efficiency, security, interoperability, and global competitiveness. The Call to Action established an Effectiveness Criteria and called for setting rules and standards around items such as security and ubiquity, creating an infrastructure that includes interoperability, and building sustainability and evolution into the entire ongoing process.

Current examples of faster payments include Zelle, Venmo, PayPal, and Same Day ACH. A milestone occurred in May 2015 when the National Automated Clearinghouse Association (NACHA) voted to allow "same day" ACH payment settlements. This significant change was phased in over time, beginning September 23, 2016. The most recent

development in Same Day ACH was raising the limit of a transaction to $1 million in March 2022.

Faster payments are similar to but are not the same as payments made instantaneously, or in "real time." A primary organization leading the charge for instant payments is The Clearing House.

The Clearing House is a banking association and payments company owned by the country's largest banks. It was founded before the Civil War, in 1853. It has developed an entirely new platform, or "rail," for payments called Real-Time Payments, or RTP. As the name implies, transactions done over the RTP platform happen within seconds. All federally insured U.S. depository institutions are eligible to use RTP for "payments innovation," and institutions of all sizes are joining this payments revolution. As RTP grows, it adds more innovations such as Secure Token Exchange and the ability to include PDF or XML documents.

The Federal Reserve Banks are also creating a platform for instant payments with its FedNow Service. Due to be released in 2023, it is designed to be a flexible, neutral platform that can handle many types of instant payments.

While this may seem redundant to The Clearing House's RTP platform, it is "consistent with the Federal Reserve's historical role of providing payment services alongside private-sector providers." The FedNow Service will give additional options to the marketplace for processing instant payments, and the redundancy actually helps create resiliency within the entire system.

A crucial component for the success of real time payments is the adoption of ISO 20022. ISO is the International Organization for Standardization, has members from countries around the world, and has created over 21,000 standards for business, government, and society in general. ISO 20022 is a standardized language for payments that can be used globally between financial institutions, their market infrastructures, and their clients and customers. Electronic payments frequently need remittance information, what one would previously have found on the stub of a check. ISO 20022 helps transmit this information. A common language increases efficiency, reduces costs, and may help fight fraud.

New technology is always accompanied by new fraud. We will continue to watch and report on how fraud develops around instant payments and how it can be thwarted.

Resources

FedPaymentsImprovement.org
ISO20022.com
NACHA.ORG: Same Day ACH
PaymentsJournal.com
SWIFT.com
SquareUp.com
TheClearingHouse.org

QR codes are the latest avenue being exploited by cyber criminals to separate you from your money. Read the latest fbi announcements and precautions on the fbi internet cyber complaint center (ic3), ic3.Gov.

BEC, VEC…What the Heck?

The Business Email Compromise (BEC) scam is an email scam in which the attacker pretends to be a boss, customer, or vendor and tricks an employee into sending funds to a bank account controlled by the scammer. Email Account Compromise (EAC) are attacks on personal accounts. BEC/EAC scams have been reported in all 50 states and in dozens of countries. BEC scams may have begun as unsophisticated and sometimes poorly written emails with simple instructions to send an urgent wire or buy a (fake) gift card, but they have now evolved into sophisticated cyberwizardry, manipulating virtual meeting platforms to hack emails, spoofing business leaders' credentials to initiate fraudulent wire transfers, and quickly moving money into cryptocurrency wallets, dispersing it across the world in a matter of minutes.

The FBI Internet Crime Report 2021 reveals almost **$2.4 billion** in losses this year from BEC/EAC. That amount is projected to grow to **$6.9 billion** in losses by 2025. To put this in perspective, less than 10 years ago there were BEC losses of "only" **$226** million reported.

In 2021, there were almost 20,000 BEC/EAC complaints filed with the FBI Internet Crime Complaint Center (IC3), and more than half of all organizations surveyed by the Association for Financial Professionals in its 2021 report were victims of BEC fraud. Fraudsters target the United States significantly more than any other country.

Selecting Their Victims

While it is not known how BEC scammers select their victims, social media is one obvious method that aids them in honing their schemes. When companies post events that key executives will be attending, the scammers know when those executives will be out of the office, and can imitate them in a scam. 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

Common BEC Scam Strategies

- Spoofing legitimate email addresses by using one similar to the targeted business, sometimes changing only one letter, or turning an "m" into an "r" and an "n" which is difficult to detect.
- Sending fraudulent e-mails impersonating an executive who supposedly is traveling or is "in a meeting" so the request 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.

Vendor Email Compromise

While BEC scams were reported in 2017, VEC scams emerged later and are close cousins. The variation occurs when the fraudster, after hacking into the victim organization's system, looks for customers of the victim that owe it large dollar amounts. The fraudsters study how invoices are designed and delivered, and other standard

behavior between the victim and its customers. At an apropos moment, they target the customers with genuine-looking but fake invoices that instruct them to send payments to a "change-of-bank" or "updated" bank account that is actually controlled by the fraudsters. Because the invoice and the requesting email or letter look genuine, the customers often fall for the scam.

Prevention Strategies

There are numerous, effective solutions for preventing BEC, VEC, and EAC scams. The overarching theme is awareness through education, proper payment protocols, and continual vigilance.

- Organizations should monitor their own information with credit reporting agencies and state record databases.
- Educate employees at all levels about BEC, VEC, and EAC scams. Executives must instruct and authorize 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, and/or that is secretive.
- Verbally confirm ALL changes of remittance address, bank wiring, or ACH instructions received from vendors. CALL to confirm any change of payment instructions, using the contact information on file. Never use the email, phone number, or address listed 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.
- 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 24-27.) More security features help thwart criminals. Frank Abagnale designed the Abagnale Premier, the Abagnale SuperBusinessCheck and Supercheck, and SAFEChecks. These products have never been replicated and used in a check fraud scam in over 25 years.

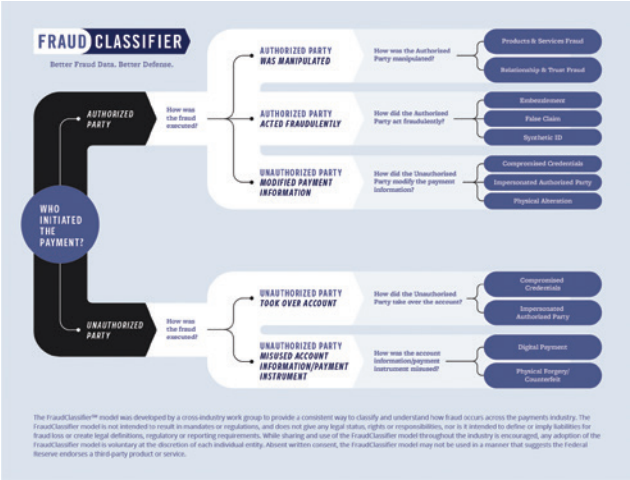
Resources

FBI Internet Crime Report 2021
2022 AFP Payments Fraud and Control Survey

Tech Support Fraud

Was a "minor" scam that is now exploding. It includes a fraudster offering to give customer service, security, or technical support, but is actually defrauding people. Many victims report being told to make wire transfers to overseas accounts or to purchase large amounts of prepaid cards. There was a 137% increase in this crime between 2020 and 2021, and we presume this correlate with increased online use due to pandemic lockdowns. Tech support fraudsters typically impersonate well-known tech companies, offering to fix non-existent technology issues or renew fraudulent software or security subscriptions. However, in 2021, the FBI's Internet Crime Complaint Center (IC3) received many more complaints reporting the impersonation of customer support from companies such as financial institutions or utilities.

FBI Internet Crime Report 2021



New Fraud Classification Model

One of the challenges in fighting payment fraud has been the ever-increasing avenues, methods, and mechanisms by which it occurs. As technologies have evolved, mushroomed, and become globalized, so has payment fraud. Having a common language and a comprehensive, consistent, and coherent understanding of fraud's mechanisms can aid in creating more effective defenses against it. To that end, the Federal Reserve collaborated with a large and diverse group of stakeholders from the payments and fraud prevention industries, forming the Fraud Definitions Work Group (FDWG), and together they created the FraudClassifier℠ model. This innovative model can be used to more effectively analyze payment fraud and to create structures and processes for thwarting its effects.

As explained by FDWG, there were "inconsistencies in the classification and reporting of ACH, wire, and check fraud data from study to study, and a significant lag between the reporting period and when study results become available. As a result, the industry has a limited capacity to identify and track payments fraud trends on a timely basis….if you do not know where fraud is occurring, you cannot effectively address it." The FraudClassifier℠ model aids in identifying and tracking payment fraud trends. The model is not regulatory in nature, nor does it hold legal status. Its usage is completely voluntary. The Federal Reserve and the FDWG believe its adoption and usage will significantly strengthen organizations' ability to thwart payment fraud.

RESOURCES

FedPaymentsImprovement.org

ACH and Its Evil Twin…Debits and Credits Fraud

The ACH Network is one of the safest payment systems in the world, and in 2021 it processed over 29 billion payments valued at $72.6 trillion. Same Day ACH payment volume surged almost 74%, growth fueled by pandemic lockdowns.

Despite its strong safety record, when looking at the attacks on different payment methods, ACH Debits were targeted 37% of the time in 2020, making them the second most popular payment method targeted. ACH Credits were targeted 24% of the time. The limit on Same Day ACH was raised to $1 million in March 2022, so organizations must be especially cautious and add strong safety controls around ACH transactions, looking for any unusual activity.

NACHA is strengthening its Rules to help combat fraud, requiring Third-Party Senders to conduct Risk Assessments, and requiring validation of checking account numbers the first time they are used for an ACH payment.

There is one common element in ACH fraud: gullibility or complicity on the part of someone on the ACH "highway." Fraudsters only need a checking account number, a bank routing number, and an entry into the ACH system in order to commit fraud. An easy way for criminals to obtain bank account information is to steal checks out of the mail. Thwart this by taking 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 with access to images of 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 a bank's lockbox service.

Returning Unauthorized ACH Debits

Businesses must return unauthorized ACH debits within 24 hours; for a consumer, it is 60 days. Most ACH fraud losses can be avoided by following the "best practices" listed below. In a prior AFP survey, of those reporting 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. These practices may have thwarted the fraud.

Best Practices

- Implement multiple-authentication requirements.
- Process all ACH transactions on a secure, encrypted computer
- Use an ACH filter or block on every bank account.
- Monitor your accounts daily, and always in the morning.
- Segregate accounts for better control.
- Mask account numbers and tax ID numbers in correspondence.
- Know the person with whom you are dealing– fraud happens by incorrectly assuming an unknown party is legitimate.
- Financial institutions can place limits on new accounts, which can be higher risk for fraud, and look for unusual activity.

Resources

NACHA - The Electronic Payments Association
2022 AFP Payments Fraud and Control Survey

Wire Fraud - Still Lurking

The owner of a small escrow company received an e-mail that a UPS package she had been sent was lost and urged her to open the attached notice. When she opened the attached file, nothing happened, so she forwarded it to her assistant, who also tried to open it. The alleged "notice" contained a keystroke logger virus that captured the passwords used on both the owner's and the assistant's computers. After the passwords were captured, the fraudsters sent 26 wire transfers totaling $465,000 to 20 people around the world.

Wire transfer fraud increased dramatically between 2010 and 2017, surging from 5% to 48% of payment fraud attempts. However, it is now declining, and in 2022 was only 32% of payment fraud attempts. This signals that companies are detecting and thwarting wire transfer fraud. However, it continues to be closely linked to BEC scams, with 41% of BEC scams using wires as a fraud strategy. The costs associated with a fraudulent wire go well beyond dollars. Other costs include investigation, remediation, litigation, brand erosion, fines, and loss of customer confidence.

Behavior-based solutions used by financial institutions can detecting fraud. Although fraudsters can mimic many aspects of a computer, they cannot mimic all aspects of normal human behavior. At some point, 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.

To prevent wire transfer fraud, having dual controls in initiating a wire transfer is crucial. In addition, unauthorized wire releases can be prevented in four steps:

1) Purchase a new computer that is dedicated to connecting to the bank, and nothing else, ever.

2) Require at least two different computers and usernames and passwords to wire money out of an account. Anyone can initiate a wire with an everyday computers, but require that all transfers be released using only the dedicated banking computer. Use different usernames 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.

RESOURCES

Guardian Analytics – "Dissecting Wire Fraud: How it Happens, and How to Prevent It"
2010 – 2022 AFP Payments Fraud and Control Surveys

Cyber Crime - Its Meteoric Rise During Covid-19

As the world shut down in early 2020, SAFEChecks anticipated– accurately – that cybercrime would explode, shattering every previous record as businesses and daily life moved online. We attended hours of webinars and conferences on cybercrime by outstanding fraud prevention organizations such as Arkose Labs, Artic Wolf, NICE Actimize, Guardian Analytics, Advanced Fraud Solutions, The Paypers, KrebsOnSecurity, American Banker, Pink Collar Crime expert Kelly Paxton, and FBI's Internet Crime Complaint Center (IC3).

Summarizing "best practices" from this avalanche of information is a bit like seeing the doctor for a checkup and being told to "eat your veggies and exercise…." Cybercrime statistics and fraudsters tactics may change, but the basics in preventing and thwarting it are largely the same.

The cybercriminal community includes players both large and small, and they are now joined by millions of "bots," giving new meaning to the word "hybrid." Individuals from every walk of life and groups of every size and industry have been victims.

Although cyber criminals are increasingly inventive, many attacks are "low tech" and can be prevented with standard controls, and by thoroughly educating employees on cybercrime prevention. **Human error was at the root of almost all successful cyber attacks.**

The Stats

- Statistics regarding cybercrime are staggering, as opportunities for fraud proliferated during the pandemic and the rise in fraud shows no signs of stopping. There were almost 850,000 internet crime complaints in 2021 compared to 300,000 in 2017, with $6.9 billion in losses compared to $1.4 billion. Cybercrime continues to rise, and fraudsters are more proficient, causing greater losses per attack.
- Phishing touched the greatest number of victims, with almost 324,000 attacks reported in 2021 alone, a 34% increase from 2020. Only five years ago – 2017 – phishing attacks were a paltry 25,344. Phishing is almost entirely preventable if one knows what to look for. Dollar losses were headed by BEC/EAC scams, at almost $2.4 billion.

Innovations in Cybercrime

An "innovation" in cybercrime is the "registration attack," when companies are flooded with fake new account registrations. These "fakers" spew spam, phish users, and hoard offers meant for real customers. This threatens any business. Detecting and eliminating fake registrations is difficult, as fraudsters have many ways of hiding amongst legitimate users. In 2021, registration attacks increased 70% over 2020, reaching 43,000 attacks in one week.

Another attack is "credential stuffing." Fraudsters acquire lists of stolen credentials (usernames and passwords) and test them against other websites' login pages. It is a low-cost scheme to take over accounts, steal assets and data, and launder money. A business does not have to be breached to suffer from credential stuffing. Credential stuffing accounts for about a third of all attacks, double from the last 12 months.

Most attacks are financially motivated, and most criminals are part of organized crime. The battle against cybercrime will end only when cybercrime ends, which appears to be never. So everyone must be vigilant, devoting time and resources to understand and protect against cyber-attacks.

Suggestions from the Top

- Review the latest reports from the FBI and reputable fraud prevention groups, and implement their recommendations. We recommend the 2021 State of Fraud report by Arkose, and especially the 2021 Verizon Data Breach Investigations Report. It is packed with vital data, and is highly entertaining.
- Use a Risk Assessment to determine the most likely threats facing your organization based on industry, type, and size.
- Educate employees at all levels on in-depth "internet hygiene," especially how to avoid phishing.
- Use multi-factor or biometric authentication.
- Install a system that can detect attacks and stop them in real-time.
- When working remotely, use a Virtual Private Network (VPN). This provides a secure digital pathway for data.
- Securely backup data in an area separate from the data source. Test your ability to access the data in a complete failure. Have two people with full authority to recover all data.
- Patch all software and keep it up-to date with the latest version. This reduces vulnerability to attacks.
- Create an incident response policy and plan.
- Implement security policies and safeguards that restrict unauthorized access to sensitive data.
- Regularly review innovations in software designed to protect computers and mobile devices, and upgrade as needed.
- Establish policies and install software that limits the sites users may access; use caution on unknown websites.
- Educate in-house developers about secure development.
- When people discontinue their employment, immediately disconnect their access to the company's network, shutdown remote connections, and collect their cell phones and other devices issued by the company. Delete their passwords.

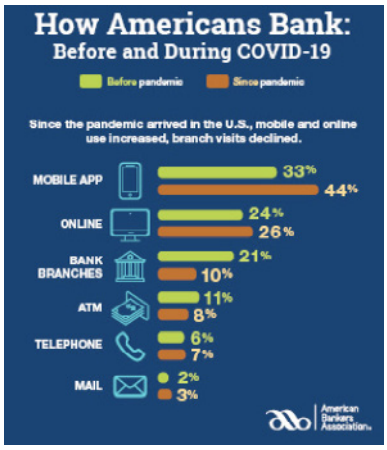
Resources

Advanced Fraud Solutions
American Banker
Arkose Labs
Artic Wolf
FBI's Internet Crime Complaint Center (IC3)
KellyPaxton.com
KrebsOnSecurity
NICE Actimize/Guardian Analytics
SecurityBoulevard.com
The Paypers
Verizon 2021 Data Breach Investigations Report

Mobile Banking "Going Rogue"

As world shut down in early 2020, new mobile banking enrollments jumped 200%. Not only did enrollment surge, mobile banking app usage jumped as well, with a peak increase of 145% in April 2020. As of 2020, 1.9 billion people worldwide used online banking services. It is predicted to reach 2.5 billion by 2024. In addition, in 2021 less than half of mobile banking users indicated they would go back to only in-person banking. The world of mobile banking is here to stay. The FBI predicted a surge in mobile fraud. As Frank Abagnale observes, fraudsters follow the headlines.

Scammers have many chances for mobile fraud, as almost 80% of smartphone owners used their phones last year to make an online purchase. Even more accessed their bank accounts from their phones. Mobile security apps are highly sought-after apps, to help prevent fraud.



There are many ways fraudsters can compromise phones and bank accounts. One common method mimics the ancient Greeks and their Trojan Horse. Malicious apps, known as banking trojans, are disguised as games or tools. Once downloaded, they stay inactive until the user opens a legitimate banking app. Then it displays a fake version of that banking app's login page. After the consumer enters their information into the false login page, the trojan captures the information. The consumer is usually unaware their information has been stolen.

Similarly, scammers make malicious apps that look like a real bank's app. Confused customers download these malicious apps. When they try to log in, the app shows an error message and asks for permission to acquire and bypass the security codes sent to the consumer. There are thousands of fake apps on major app stores. This scheme is a fast-growing method of mobile fraud.

Smishing is another type of mobile fraud, combining texting and phishing. It occurs when people respond to messages they get from unknown numbers. The links in the messages connect to malicious websites, or download malware. Victims then give personal information to cybercriminals.

Follow these precautions:

- Download apps ONLY from valid sources
- Use two-factor, multifactor, or biometric authentication
- Create unique, strong passwords
- Know where personal info is stored
- Do not click links in text messages or emails appearing to come from a financial institution
- Do not give passcodes over the phone – banks will not ask for this.

Mobile Deposits & Double Debits

Cases of double-depositing checks through mRDC are growing. A Check 21 Warranty specifically prohibits a check or its image from being presented for payment twice.

Example: Mary deposits a check via her bank's mobile phone app. She later cashes the physical check at a check-cashing store. The store deposits Mary's original physical check. When it hits the drawer's bank account, it breaches the Warranty made when the check was deposited remotely. **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 other variations of fraud via mRDC. **(See HIDC, Page 16.)**

Example: John Doe picks up a check made payable to "John Doe," then leaves and deposits the check remotely. He comes back and returns the check, asking that it be replaced with a check made payable to John Doe OR Jane Doe. The issuer gives him a new check payable to John Doe or Jane Doe. They don't 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. The issuer of the check can be held liable for both checks. Why? The second check was cashed at the bank, and the first check was deposited remotely. While banks often cooperate to stop this fraudulent activity, John Doe's bank is an HIDC and is not required to return the funds.

To prevent mRDC fraud, if a check leaves your possession and is later returned for a substitute, put a Stop Payment on the original check even though you have it in your possession. 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 19.)**

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

RESOURCES

The Many Faces of Mobile Malware –Biocatch
Massive Mobile Banking Fraud –OneSpan
ACFE Insights
Fidelity National Information Services (FIS)
Statista.com
American Bankers Association

SHREDDING DOCUMENTS

Shred anything with your personal information on it before thrwoing it away. it is best to use a crosscut or microcut shreddder.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 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.

Ransomware – The Pirates Persevere

Mimicking pirates plundering on the high seas, cyber pirates today use malware attacks as a lucrative money-making scheme. Ransomware attacks were first seen around 2005 and have proliferated around the world despite global collaboration between numerous governments to stop these modern-day pirates. Ransomware can infect a computer through insecure and fraudulent websites, software downloads, and malicious attachments. The malware locks down the computer and mobile devices, or it encrypts the files. The files can't be accessed unless the ransom is paid. Organizations of all types and sizes, as well as individuals, are at risk. Ransomware pirates are serious criminals, and their threats should not be taken lightly.

WannaCry, CryptoLocker, and Petya were all different forms of ransomware that caused internet infrastructure shutdowns around the world, including those of government agencies and financial institutions. Current ransomware threats include Gandcrab, SamSam, Zeppelin, and REvil. They are dangerous malware with the ability to destroy corporate systems.

In 2018, the U.S. Government established the Cybersecurity and Infrastructure Security Agency. It includes significant information on ransomware as well as a Cyber Security Evaluation Tool (CSET®). The CSET® was updated in June 2021 to include a Ransomware Readiness Assessment Tool (RRA). See Resources below.

Pay the Ransom?

Many security experts, and the FBI, strongly recommend against paying the ransom. They point out there is no guarantee the decryption key will be sent after the ransom is paid, and in some instances the key is sent, but it deletes the data, so the payee loses anyway. They argue that cyber piracy is a business model. If no one paid the pirates, then the model would collapse. Notwithstanding, TrendMicro found that most infected organizations paid the ransom.

Before paying a ransom, victims should find out if a solution has already been found. Brian Krebs of KrebsOnSecurity recommends victims visit the "Crypto-Sheriff" page at www.NoMoreRansom.org, a site backed by security firms and cybersecurity organizations in numerous 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 and anti-malware 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

See Resources below for important recommendations.

Resources

Cybersecurity and Infrastructure Security Agency (CISA)
https://www.cisa.gov/stopransomware

KrebsOnSecurity
https://krebsonsecurity.com

MicroTrend
https://www.trendmicro.com/vinfo/us/security/definition/ransomware

NoMoreRansom.org

Imposter Fraud Hits Companies

Impostor Fraud Hits Companies

Corporate Impostor Fraud is the unauthorized use of a company's name and information to obtain money, goods, or services, and was first reported in March 2017. It is now a global threat. Its name is a misnomer, as all organizations are victims, not just corporations. Smaller companies are frequently targeted because they have fewer legal and financial resources, and fewer defenses than large corporations. This includes family-owned businesses with strong credit ratings.

Criminals steal the federal tax ID number, the employer identification number (EIN), and other core pieces of information, to open lines of credit for purchasing items illegally, and to file illegal tax returns.

There are two common schemes. First, criminals make illegal changes in your business registration information and conduct business in your organization's name. They may also reopen a business that was closed. Next, they may "mirror" the address of a well-known organization, creating an address that is similar, such as using a different suite number, which allows illegal purchases to be sent to new address.

Prevention Strategies

- Prevention and protection against Corporate Identity Theft includes education at all levels of an organization, proper payment protocols, and continual vigilance:
- • Organizations should monitor their information with credit reporting agencies and state record databases.
- Educate employees at all levels about Corporate ID scams.
- All changes of remittance address, bank wiring, or ACH instructions received from vendors must be verified.
- CALL a known number to confirm any change of payment instructions. Use the contact information on file, never by responding by email or calling 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 numberzby email or call the phone number.

Resources

CPO Magazine, October 2019
2017 AFP Payments Fraud and Control Survey
Guardian Analytics
Dun & Bradstreet

The Inside Job – Stopping Embezzlers

As Frank Abagnale famously said, "If you make it easy for people to steal from you, they will." Most crimes are crimes of opportunity, and in most embezzlement cases, basic controls would have prevented or substantially reduced the losses. Each year for the last several years, embezzlement records have surpassed the previous season's "blockbuster year." Given the disarray caused by the global pandemic and its aftermath, an upward spiral of internal fraud will most likely continue for years to come.

Real Life Examples

- A credit union teller who was also a vault supervisor embezzled more than $1.1 million by depositing fraudulent checks into personal, family, and friends' checking accounts, and by falsifying the credit union's account reconciliations and general ledger history.
- Over the course of eight years, a Yale University administrator bought millions of dollars' worth of computer equipment, sold it on the black market, and pocketed the revenues, costing Yale over $40 million. She was caught through an anonymous tip.
- Two sisters working as "lunch ladies" embezzled almost $500,000 from two school cafeterias over five years. Officials found inconsistencies in how cash was handled and asked police to investigate.
- The chief fiscal officer of a state agency wrote checks to herself using the agency's bank account and with the help of her son who also worked there, created bogus invoices from vendors. During a seven-year period the CFO and her son embezzled over $1 million from the organization.

Who are the Targets?

Every type and size of organization has suffered from embezzlement, with size making almost no difference in probability of being a victim. Although the methods of internal fraud may differ, small companies are just as likely to be a target as large companies; however, the highest median loss was found in companies with the fewest employees.

Likewise, every type of industry has had its share of embezzlement, although, as might be predicted, the greatest number of cases were found in the banking and financial services sector.

Global losses can be measured in trillions of dollars. This has resulted in layoffs, cutbacks, salary freezes, and even bankruptcy. The casualties are also non-monetary, including severe emotional distress and damaged reputations. Organizations are not the only victims – business partners, suppliers, vendors, customers, clients, and families also suffer. The 2022 Association of Certified Fraud Examiners (ACFE) "Report to the Nations" found that typical losses from "occupational fraud"(including asset misappropriation, corruption, and financial statement fraud) in the United States were almost $650,000, and that 54% of victim organizations recovered none of their losses. Almost all cases included multiple methods of fraud.

The Psychology of Embezzlement

Internal fraud occurs when the "fraud triangle" is present – motive, opportunity, and rationalization. Workplace conditions are a major predictor of fraud, and usually reveal overconfidence on the part of owners and managers, and a lack of effective fraud prevention controls. In almost 30% of cases there were no internal controls to prevent embezzlement, and the number rose to over 40% of small business cases. In 20% of cases, 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. An unethical management tone contributing to fraud includes "wheeler-dealer" attitudes and behavior such as overriding established safeguards, "bending the rules," and pressuring employees to meet unrealistic goals.

There have been six common behavioral "red flags" in every internal fraud study conducted by ACFE since 2008. The 2022 ACFE study identified two more. In 85% of cases, fraudsters displayed at least one of these red flags. Managers, employees, and auditors should be educated on these common behaviors to help spot fraudulent activity. Those who ignore these red flags do so at the company's peril. These red flags include:

- Living beyond one's means
- Financial difficulties
- Being unusually close to a vendor/customer
- Control issues – unwilling to share duties or take vacations
- Unusual irritability, suspiciousness, or defensiveness
- Bullying or intimidation
- Divorce/Family problems
- A "wheeler-dealer" attitude; shrewd/unscrupulous behavior

Other motivating factors include a shopping addiction, substance abuse, an attitude of entitlement, a desire to support a romantic relationship, and a gambling addiction. 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. Also, employees who feel unfairly treated sometimes believe they can get "justice" by embezzling.

Who embezzles?

Embezzlers were most likely to hold accounting or upper management positions. Although studies vary whether males or females embezzle more often, males have always caused the greatest losses.

The perpetrator's level of authority was strongly linked to the size of the fraud and the longest duration of the schemes. In the cases studied by ACFE 2022, the median loss in the schemes committed by an owner/executive was $337,000 and lasted 18 months. This was higher and longer than median losses caused by managers ($125,000; 16 months) and regular employees ($60,000; 8 months).

The majority of embezzlers are typically in their early 30s to mid-40s, but the greatest losses by far come from those aged 60 and above. In some studies, about 40% had been at the organization for one to five years, and over 50% had been there more than five years. Almost 58% of the schemes involved more than one person, and the more people involved, the greater the median loss.

Only about 6% of perpetrators had previously been convicted of a fraud-related offense, so background checks, while important for other reasons, are ineffective in preventing embezzlement.

Methods of Embezzlement

Organizations of different sizes and industries have different fraud risks. For example, corruption is more prevalent in larger organizations, while check and payment tampering schemes are more common in small organizations. Review Resources (below) to determine your organization's and industry's risks.

Detecting Embezzlement

Most embezzlement schemes are long-term, with a majority lasting more than a year, and a few lasting decades. Anonymous tips are by far one of the most successful means to detect fraud. 42% of all cases were detected by a tip, 3 times higher than any other detection method, including audits. Organizations without tip hotlines had almost twice as many median losses as those with a tip hotline.

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 well-publicized to employees, as well as to outsiders. Employees provided more than half of all tips that led to the discovery of fraud. Customers, vendors, and even competitors have also provided valuable tips on fraud. Hotlines should include a variety of methods – telephone, email, online forms, and hard copy forms that can be mailed in. Also, many tips were reported informally to managers or associates at all levels. Therefore, everyone in an organization should be educated on how to handle allegations of fraud.

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 relied on to detect embezzlement.

Strategies for Preventing Embezzlement

Having anti-fraud controls in place – and following them – directly lead to quicker detection of embezzlement schemes and lowered fraud losses. Companies without these controls experienced almost twice as many losses as those with controls.

In addition to the hotlines, management reviews, and internal audits mentioned above, organizations can reduce losses by establishing employee support programs that help employees struggling with gambling or drug addictions, mental or emotional health, and family or financial problems. Surprise audits can also 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. Using your bank's Lockbox service is the best and most cost-effective way to prevent embezzlement via diverted deposits. Organizations need to consider the specific fraud risks they face when deciding which controls to implement, as some schemes are more prevalent based upon the industry or department..

Education is a vital 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.

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. Since most losses will not be recovered, it is advisable to obtain appropriate "crime and fidelity coverage" for fraud losses.

If You Suspect Embezzlement

DO:

- Create a small internal team to confidentially investigate.
- Bring in outside help as needed to add objectivity and deal with complex situations.
- Take thorough notes on the various steps in the investigation.
- Examine pertinent records.
- Restrict access to bank accounts, credit cards, etc. by those who are under suspicion.
- Find witnesses.
- Correct internal controls that allowed fraud to occur.
- Praise honesty.

DON'T:

- Rush to judgment or confrontation.
- Conduct group interviews.
- Interview an employee alone.
- Interfere with law enforcement.

Resources

ACFE Report to the Nations (2010 – 2022)

Hiscox Embezzlement Study (2016 – 2018)

Marquet Report, Embezzlement (2010 – 2013)

When "Yes" is a Big Red Flag

These are some of the characteristics that may influence employees to commit internal fraud.

Financial Statement Frauds

- Is management compensation tied closely to company value?
- Is management dominated by a single person or a small group?
- Does management display a significant disregard for regulations or controls?
- Has management restricted the auditor's access to documents or personnel?
- Has management set unrealistic financial goals?
- Does management have any past history of illegal conduct?

Asset Misappropriations

- Is an employee obviously dissatisfied?
- Does that employee have a past history of dishonesty or illegal conduct?
- Does that employee have known financial pressures?
- Has that employee's lifestyle or behavior changed significantly?

Occupational Fraud Prevention Checklist

The most cost-effective way to limit fraud losses is to prevent fraud from occurring. This checklist will help organizations test the effectiveness of their fraud prevention program.

1. Is ongoing anti-fraud training provided to all employees of the organization?
2. Is an effective fraud reporting mechanism 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 the internal audit department have adequate resources and authority to operate effectively and without undue influence from senior management?
7. Does the hiring policy include thorough fraud prevention controls?
8. Are employee support programs in place to assist employees struggling with addictions, mental/emotional health, family or financial problems?
9. Are employees allowed to speak freely about pressures, providing management the opportunity to alleviate such pressures before they become acute?

Identity Theft - "Is That Really 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 24-27.**

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: www.dmachoice.org

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

Laser Printing's Impact on 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 enable fraud attempts and fraud losses.

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.

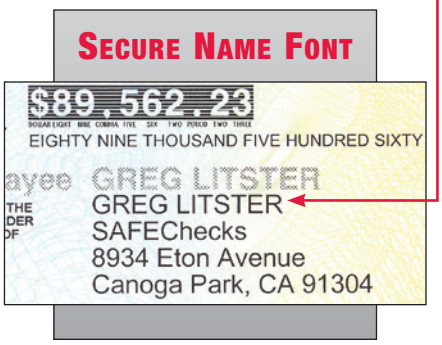
Blank Check Stock

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 24-27.**

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. **See Page 28.**

It also eliminates the spacing for an added payee.



Uncontrolled Check Stock

Multiple 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 17, 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

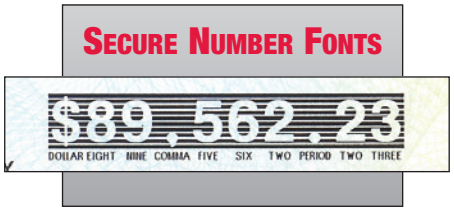
printed above the payee name is another way to prevent added payee names. Forgers add a new payee name two lines above the original payee name. To prevent additions, insert a string of asterisks above the original payee name. Asterisks can be pre-printed on the checks by the check vendor. Do not use 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. **See Page 28.**

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. **See Page 28.**



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.

Check Fraud - Still Holding Strong

Picture by The Colonial Williamsburg Foundation

Origins of Check Fraud Legal Doctrine

To paraphrase Mark Twain, the death of the paper check has been greatly exaggerated, multiple times. One prediction of its demise came in 1975; however, by 1979, 86% of companies still paid with paper checks. In 2013, another prediction arose that checks would be extinct by 2026. Yet, at the time of this writing in 2022, even after the global pandemic sent so many transactions online, 42% of companies still use paper checks. The paper check is still going strong, along with its evil twin, check fraud.

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.

Almost 40 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 28.)**

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. As pointed out by Advanced Fraud Solutions, counterfeit checks are created en masse by criminals on high-quality but uncontrolled check stock using up-to-date printing technology. These fraudulent checks include legitimate names and addresses of banks, verifiable routing and account numbers, and are almost identical to genuine checks. "Front line" controls are imperative. SAFEChecks' unique Secure Ordering Procedures **(See Page 25, 26)** are one of the most effective controls for preventing criminals from acquiring legitimate high security check stock with which they commit fraud.

Today, check fraud accounts for 66% of all payment fraud attempts (other attempts target wires, ACH, and credit/debit cards.) While this is a large drop from the high of 94% in 2008, it represents significant fraud losses. While financial institutions absorb many dollars losses, everyone suffers from the time, mental, and emotional costs of fraud.

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 many fraud losses..

There are several reasons for check fraud losses, most of which are within an organization's control: not using Positive Pay or Payee Positive Pay, not checking Positive Pay exception items in a timely manner, delinquent reconciliation of checking statements, clerical errors, and internal fraud such as stolen check stock. Gaps in online security and account takeovers by cyber criminals also contribute to check fraud losses.

In addition, many fraud losses are due to altered payee name and dollar amounts which could have been prevented with the use of properly made high security checks **(See Pages 24-27).**

Social engineering, vast cyber technology, and the ubiquity of internet use due to the global pandemic has equipped criminals with an ever-increasing set of tools they can use to commit check fraud. Some of these are Mobile Remote Deposit Capture (mRDC) **(See Page 6)**, Business Email Compromise (BEC) scams (**See Page 2)**, and electronic checks, or eChecks, which are a relatively new source of fraud. **(See Page 13.)**

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 due to the flood of check fraud. 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 2021 Payments Fraud and Control Survey, 85% of 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 Page14.)**

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 17, 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 supersedes stop payments and Positive Pay. **(See Page 16, 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 include Positive Pay, Payee Positive Pay, segregation of accounts, separation of duties, daily reconciliation, and "Post no checks" restrictions on depository accounts. Most companies use checks with varying degrees of security features although astonishingly, many still use uncontrolled blank check stock. **(See Page 21, Controlled Check Stock.)**

Everyone has a responsibility to help prevent check fraud. Financial institutions still list check fraud as one of their top threats, and view a lack of customer awareness as one of their biggest challenges in fraud prevention.

Given that many 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
2017–2022 AFP Payments Fraud and Control Survey
The Changing Landscape of Check Fraud, Advance Business Solutions, 2021
The Death of the Paper Check, Business Insider, March 2013
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

eChecks: The Devil Is In The Details

eChecks is a 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 began exploiting this flaw upon release of the technology.

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 hampered 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 17, 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.

Introducing the "Abagnale Premier" Check

OVERT FEATURES

"Signature" Dual-tone True Watermarked Paper
Thermochromatic Ink
High-Resolution Border
Prismatic Printing
Explicit Warning Bands
Chemical Wash Detection Box
Sequenced Inventory
Control Numbers
Laid Lines

I designed this unique 6-color check in 2013 for my own personal use. I've decided to share this design exclusively through SAFEChecks.

The Premier is ideal for Cashier's Checks, Warrants, and every type of business.

Contact SAFEChecks for ordering information:
(800) 755-2265 • gina@safechecks.com

COVERT FEATURES

Controlled Paper Stock
SecurLaser PLUS
Toner Anchorage
Chemical Sensitivity
Copy Void Pantograph
Chemical Reactive Ink
Invisible Fluorescent Ink
Invisible Fluorescent Fibers
Chemically Resilient Fibers
Microprinting

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 (now Wells Fargo), 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.

Introducing "Signature" paper . . .

In early 2021, Greg Litster, president of SAFEChecks, called to share with me his concern about the rapid consolidation taking place in the paper industry and the impact it might have on their customers. He asked for my help in developing an entirely new, highly secure paper for checks and other negotiable and secure documents that would be proprietary to SAFEChecks.

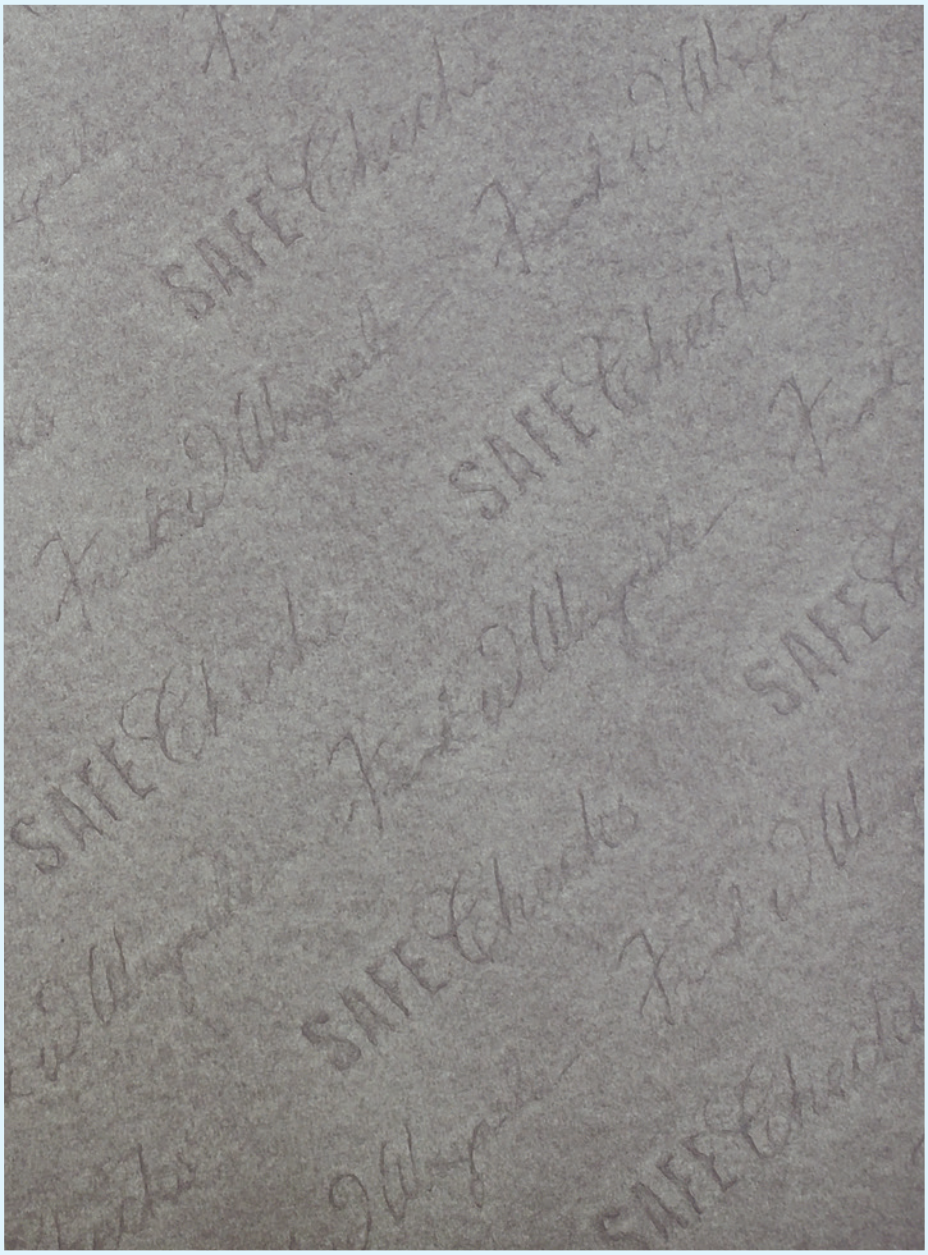
I agreed to help.

After a year in development, I am pleased to announce the "Signature" paper is now available.

This 28-pound paper is the most secure of any paper I know of, excluding currency. Features include a customized dual-tone true watermark of my signature and the SAFEChecks logo/signature. The paper contains three different colors of invisible, ultraviolet light-sensitive fibers, and is manufactured with toner anchorage on both sides.

Signature paper is reactive to over 85 chemicals, and when touched or washed in chemicals, the paper reacts with black speckling and spots that are imbedded into the fibers of the paper and cannot be washed out by continued soaking.

Signature paper is manufactured in a very sustainable way. The paper mill's main energy source—biogas—is transported in a dedicated, 8-mile pipeline from an nearby landfill to fulfill 93% of the mill's thermal energy needs instead of using traditional combustible fuels.



Biogas is mainly carbon dioxide and methane that comes from decomposing landfill organic waste that is captured to prevent its release into the air. When methane burns to produce steam for papermaking, it becomes carbon dioxide, which is 21 times less harmful to the atmosphere than methane.

Available exclusively through SAFEChecks and its distributors, Signature paper is completely controlled and is virtually impossible to replicate.

Court Cases

Holder In Due Course

Holder in Due Course, a powerful part of the Uniform Commercial Code (UCC), 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 supersedes 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.

Many payment fraud losses experienced by organizations of all sizes are a result of payouts to check cashers (bank and non-bank) from HIDC claims. Prudent companies use controlled, high security checks to protect themselves from some HIDC claims. The Abagnale Premier, the Abagnale SuperBusinessCheck, and SAFEChecks are controlled, high security checks.

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

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

ROBERT J. TRIFFIN v. CIGNA INSURANCE

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

Sun's 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

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, as did Somerset Valley Bank, the bank on which the checks were drawn. 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 totaling $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 the facsimile stamp used to "sign" the checks. (See Facsimile Signatures, Page 18).

One might question how Triffin was able to assert HIDC status when he knew the checks were fraudulent to begin with. This is answered by the transferability rules found in the UCC. As stated earlier, a Holder can transfer his or her rights to a new Holder, who then holds all of the same rights as the original Holder. Although Mr. Triffin knew about the fraud after the fact, he did not participate in creating or cashing the fraudulent checks, and therefore was not a party to the fraud. Because he was not a party to the fraud, the original Holder's rights passed to him, and he legally claimed HIDC status.

Because the counterfeit checks and the authentic checks looked identical, the lower court ruled for Triffin.

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

Hauser appealed, asserting that the fraudulent checks were not negotiable instruments because they were not produced and distributed by ADP, and because he did not authorize them to be signed. However, the Federal Appellate Court responded that authorization and negotiability are two separate issues, and because the checks met all of the requirements for negotiability described in Article 3 of the UCC, they were indeed negotiable instruments. The Court ruled against Hauser, holding him liable for the $8800.

In doing so, the Court also cited another key element found in the HIDC rules – the validity of the signature. Under the UCC, a signature is presumed to be valid unless the defendant specifically denies the validity of that signature. Beyond specifically denying the validity of the signature, the defendant must provide concrete evidence to support that denial, bring forth specific facts to disprove the authenticity of signature, and demonstrate that the signature was unauthorized and/or forged. Hauser's declarations during the trial were only general assertions regarding the invalidity of the signatures, and those declarations were deemed "self-interested and conclusory" by the judges. Hauser's weak arguments did not prevail against the power of Holder in Due Course.

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. The **Abagnale Premier**, the **Abagnale SuperBusinessCheck**, and **SAFEChecks** 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 **Abagnale Premier**, the **Abagnale SuperBusinessCheck**, and **SAFEChecks** are properly designed high security checks.

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

Visit www.SAFEChecks.com for an in-depth article, Holder In Due Course and Check Fraud, written by Frank Abagnale and Greg Litster. Click on Fraud Education, Holder In Due Course..

CHECK FRAUD SCAMS - EVEN SMART PEOPLE CAN BE FOOLED

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.

Safeguarding Facsimile Signature Devices

Many banks' Deposit Agreements place the burden of responsibility on its customers for non-authorized use of their facsimile signature devices. Multiple court cases have upheld these agreements, affirming it is up to the customers to safeguard their own devices used to automatically sign checks.

One common example of such an Agreement states, "If your items are signed with the use of any facsimile signature or other non-manual form of signature, you acknowledge that the use of such signature is solely for your benefit and convenience. You accept sole responsibility for maintaining security over any device for affixing such signature. Such signature will be effective as your signature regardless of whether the person affixing the signature was authorized to do so. Owner agrees to indemnify and hold us harmless from all losses resulting from our honoring an item in any instance in which the item ***bears or purports to bear*** a facsimile signature resembling a facsimile signature on file with us, regardless by whom or by what means the actual or purported signature was affixed to the item."

That phrase – "bears or purports to bear" – saved NationsBank (now Bank of America) $4 million in losses from checks signed with unauthorized facsimile signatures. Florida Power and Light (FPL), a customer of NationsBank, used a facsimile machine to sign most of its corporate checks, nearly 20,000 each month. Unfortunately, 27 fake checks were cashed, totaling $4,387,057. They bore exact replicas of the facsimile signature and used actual serial numbers from real FPL checks that had been voided or canceled. The fake checks appeared authentic, the signatures were identical to the signature card, and therefore were paid "in good faith." Because the fraud was discovered after the 24-hour recission period, FPL's account was not credited for the loss.

FPL's insurance company, Arkwright Mutual, reimbursed the company, and sued NationsBank for damages, claiming the checks were not "properly payable" because nothing in the contracts between the two had authorized NationsBank to pay checks with forged facsimile signatures. NationsBank disputed this, pointing out that FPL had agreed to a provision in its Deposit Agreement that said, "If your items are signed using any facsimile signature or non-manual form of signature, you acknowledge that it is solely for your benefit and convenience. You accept sole responsibility for maintaining security over any device affixing the signature. Such signature will be effective as your signature regardless of whether the person affixing it was authorized to do so."

The Courts have ruled similarly in additional cases where there were clear and unambiguous facsimile signature agreements. Banks are advised to have clearly worded facsimile signature agreements, and clients are advised to carefully review their Bank agreements, especially when using a non-manual method of signing checks.

RESOURCES

https://www.bankersonline.com/qa/facsimile-signatures
Arkwright Mutual Ins. Co. v. NationsBank, N.A. (South)
Original Case No. 96-2969-CIV-GOLD; (SD Fla. 1999)
Appeal Case 2000 WL 679165,41; Rep.2d 726 (11th Circuit 2000).
Spear Insurance Co. v. Bank of America, N.A., 40 UCC Rep Serv 2d 807 (IL 2000).

Timely Bank Account Reconciliation is Essential

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

The UCC requires an account holder to exercise "reasonable promptness" in examining monthly statements and reporting unauthorized signatures or alterations. "Reasonable promptness" is considered 30 days, with a one-year outside limit for reporting discrepancies or errors "without regard to care or lack of care of either the customer or the bank."

UCC 4-103 allows for contractual amendments of the UCC rules, provided the bank does not try to disclaim its own negligence.

MANY BANKS HAVE SHORTENED THE ONE-YEAR TIMEFRAME FOR REPORTING DISCREPANCIES.

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

In court, the bank moved for summary judgment based on the signature card agreements on the two accounts, which each stipulated that the bank be notified within 14 days after it sent the statements or made them available for review. The bank argued that these specific provisions completely invalidated Borowski's claims. Borowski acknowledged that he had not reviewed the statements because his fiancée intercepted them and then lied to cover their receipt. However, he argued that the bank was negligent in the handling of his accounts.

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

As admonished by the Georgia Government Finance Officers Association, a timely reconciliation of bank accounts is "a critical control activity to determine if processes are working as intended….Bank reconciliations can also identify errors or fraudulent transactions…. Bank reconciliations will identify items that are not clearing the bank. This allows staff to follow up with employees and vendors to resolve remittance address or other issues."

RESOURCES

Borowski v. Firstar Bank Milwaukee, NA 579NM2d 247,
35 UCC Rep.2d 221 (Wis. Ct. App. 1998)
https://ggfoa.org/press-releases/importance-of-timely-bank-reconciliations

The Under-used Warranties of Check 21

Because check imaging has become so ubiquitous, many do not know the history and power of Check 21, and its Warranties and Indemnity provision. The 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, individual, or other entity to convert and truncate paper checks. It is voluntary. Any entity 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 Capture (RDC) 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. This includes checks deposited via mobile phone, known as mRDC. 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 safechecks.com.
2) Make large dollar payments electronically.
3) Use high security checks with 10 or more safety features. The checks should include a true watermark, thermochromatic ink and 16+ chemical sensitivity. The **Abagnale Supercheck**, the **Abagnale Premier**, the **Abagnale SuperBusinessCheck**, and **SAFEChecks** **(See Pages 24– 27)** have these and many additional security features, providing prudent individuals and organizations the strongest defense possible against check fraud. Visit SAFEChecks.com to request a free sample.
4) Avoid using laser checks that can be purchased by multiple people entirely blank because that stock is uncontrolled and aids fraudsters.
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 SAFEChecks.com, Fraud Education for more information.

Stopping Check Fraud - Beyond 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 24 through 27 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 25 and 28).**

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 one of the best technologies developed in decades to counter the problem of altered, forged, 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 28).**

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 11 & 28)** or insert a row of asterisks above the payee name. To help prevent altered payees, use high security checks like the **Abagnale Premier**, the **Abagnale 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 Pages 20 and 22-23.**

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 11 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 and One-Year Rules

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 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 16.)**

iStock Photos

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 24 and 25.**

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.

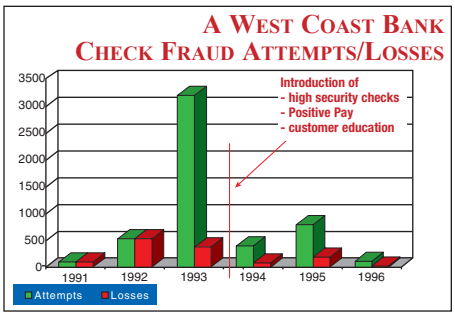
Wire Transfers

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.

Why Check Security Features Matter

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 Pages 24-27.**

Fourdrinier Watermarks

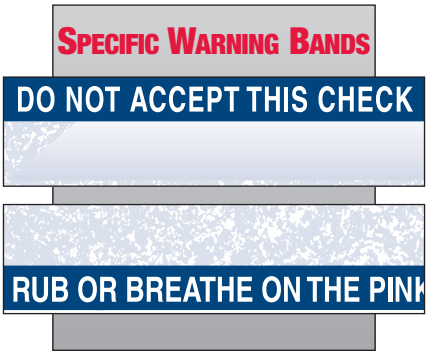
are faint designs pressed into the paper while it is being manufactured, and are also known as "true" watermarks. When held to the light, these watermarks are easily visible from either side of the paper for instant authentication. Copiers and scanners are not capable of replicating dual-tone Fourdrinier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

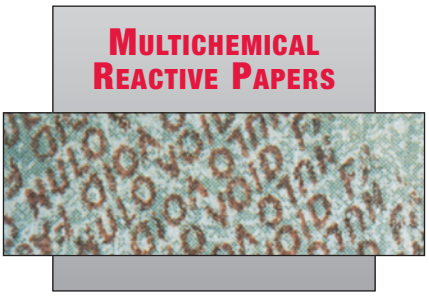
Specific Warning Bands

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 17, Pomerantz Staffing Services.**



Multi-chemical Reactive Papers

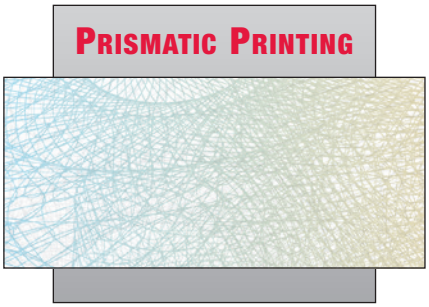
produce a stain or speckles or the word "VOID" when activated with ink eradicator-class chemicals, making it extremely difficult to chemically alter a check without detection.



Checks should be reactive to at least 15 chemicals.

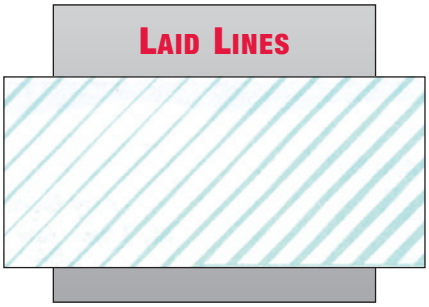
Prismatic Printing

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.

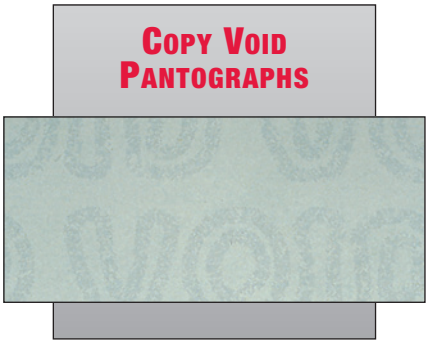


Image Survivable Secure Seal Barcode

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 11 and 28

High-Resolution Borders

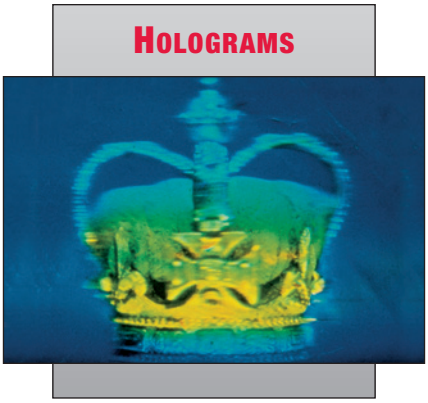
are intricately designed borders that are difficult to duplicate. They are ideal for covert security as the design distorts when copied.

Ultraviolet Light-Sensitive Ink and Fibers

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

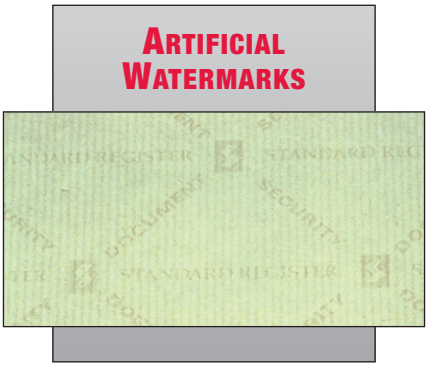
Holograms

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.

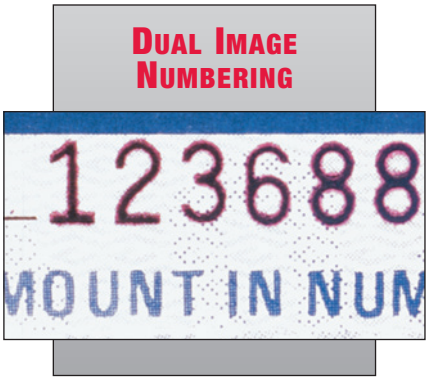


Microprinting

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 16),** and establish the basis for an indemnity claim under Check 21's Indemnity Provision. **(See Page 19.)** 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, thermo-chromatic ink (accompanied by a properly worded warning band), and toner anchorage. Frank Abagnale designed the **Abagnale Premier**, the **Abagnale SuperBusinessCheck**, and **SAFEChecks** for organizations, and the Abagnale Supercheck for individuals, so they have access to top security checks at reasonable prices.
(See Pages 24-27.)

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

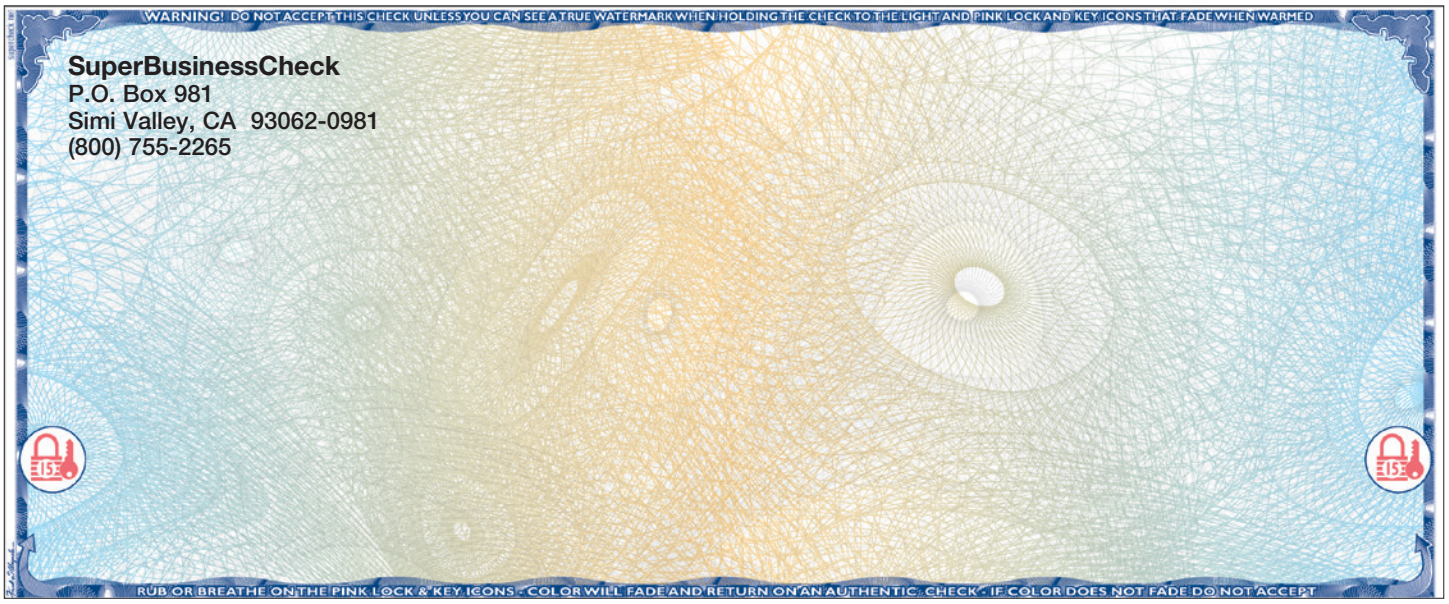
Controlled Paper Stock
Toner Anchorage
Chemical Sensitivity
Copy Void Pantograph
Chemical Reactive Ink
Fluorescent Ink
Fluorescent Fibers
Microprinting

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

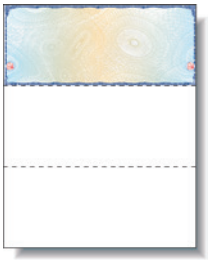
"After years of designing checks for Fortune 500 companies and major banks, I designed the Supercheck, the SuperBusinessCheck and SAFEChecks to help individuals, medium and small businesses, and organizations protect their checking accounts."

Frank W. Abagnale



Available Styles

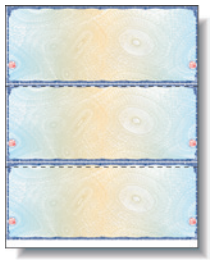
Laser - Top



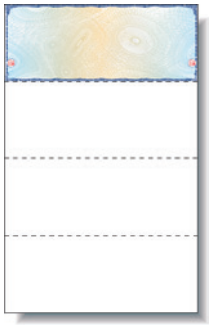
Laser - Middle

Laser - Bottom

Laser 3-On-a-Sheet



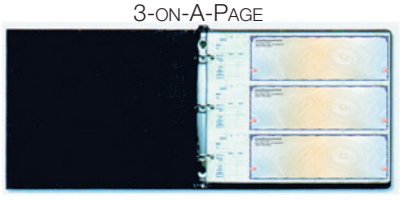
Legal Laser - Top



Legal Laser - Second Panel

Pressure Seal Checks Also Available

3-on-A-Page

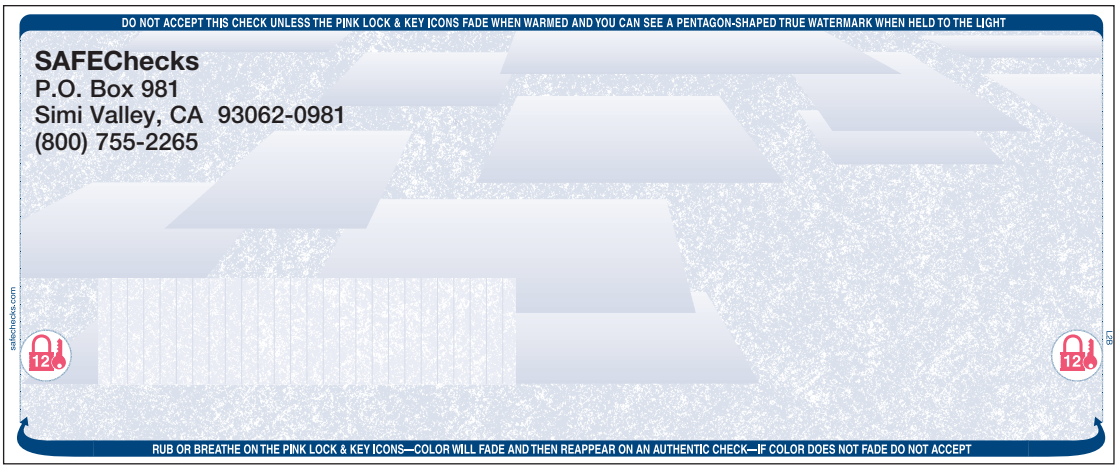


Secure Ordering Procedures

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

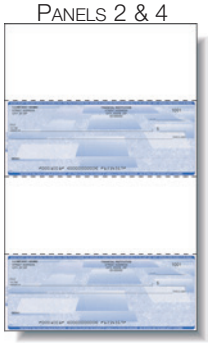
Continuous - 1 part

Continuous - 2 part

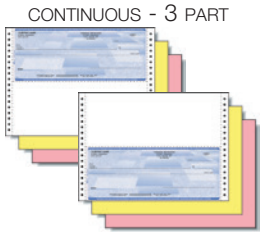
Legal Laser - Top

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 28, 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

4680 E. Los Angeles Ave., Suite L (800) 755-2265
Simi Valley, CA 93063 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
☐ **Duplicate** ☐ Blue ☐ Green
☐ **Triplicate** ☐ Blue ☐ Green ☐ Red

Check: ☐ **Top** ☐ **Bottom**

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.

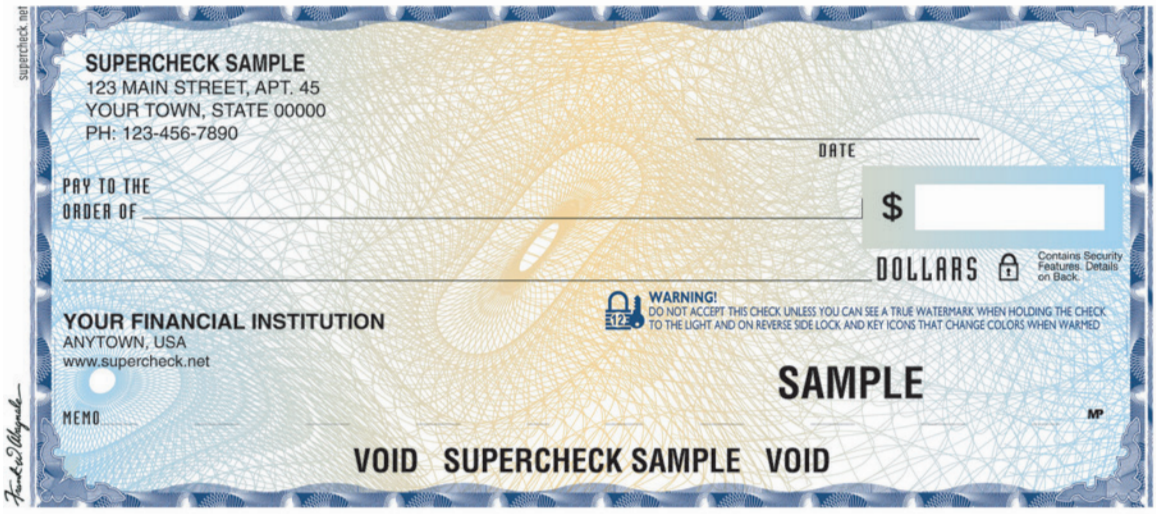
Also order online at SAFEChecks.com
Call (800) 755-2265 for assistance in completing form or to answer any questions.

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

Front View of the SuperCheck

Figure 1

Back View Under Normal Light and Temperature

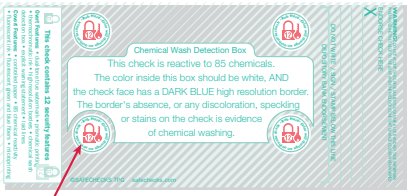


Figure 2

Back View Under Ultraviolet Light

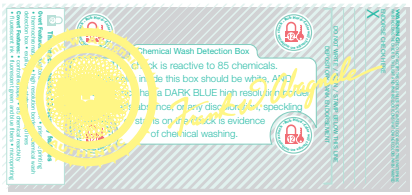


Figure 3

Back View of Check Above 90° F

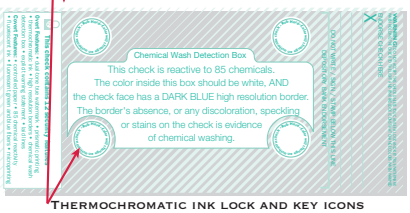


Figure 4

Thermochromatic ink lock and key icons fade away at 90° F and reappear at 78° F.

PLEASE PHOTOCOPY THIS FORM OR DOWNLOAD IT FROM WWW.SAFECHECKS.COM

CHECK ORDER FORM AND INFORMATION

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

We need all three (3) items below to complete your order:	Please mail to:	Delivery Times:
1. Completed ORDER FORM	SAFEChecks	Allow 3 weeks for delivery.
2. VOIDED CHECK (indicate any changes on the face)	4680 E. Los Angeles Ave., Suite L Simi Valley, CA 993063	Expedited service is available. Call (800) 755-2265
3. VOIDED DEPOSIT SLIP		

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

Email Address _____ Alternate phone where you can be reached

Please mail checks to the:

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

____ Financial institution _____
Branch Address City State Zip

____ Other _____
(Address must be on file with bank)

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

Single - $30.95 per box of 100
Duplicate - $30.95 per box of 100
Shipping/Handling - $7.95 per box

PAYMENT OPTIONS:

_____Check or Money Order enclosed (made payable to SAFEChecks)

_____Bill my credit card: _____MasterCard _____Visa

Credit Card Account Number / Expiration Date _____ Security Code

Cardholder Name

Authorized Signature

Billing address of credit card if different from address on checks

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 mismatch 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 Pages 23-24)**, 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 Premier,** the **Abagnale SuperBusinessCheck** or **SAFEChecks,** fraud losses can be cut dramatically. **See Pages 24-27.**

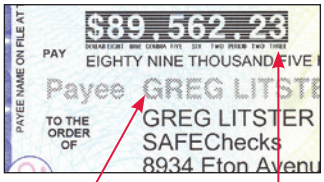
Caution: Some companies have the mistaken notion that if they use Positive Pay they do not need to use high security checks.

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 Page 28).

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.

Securing Our Seniors

The FBI Elder Fraud estimates that scams aimed at the elderly create $3 billion in losses each year. Senior citizens are typically trusting, and have financial assets such as a home and savings, making them prime targets for scammers. Common scams include romance, lottery, home repair, and sweepstakes schemes conducted directly by phone, email, or regular mail, and indirectly through TV and radio ads. Sometimes the fraudsters are relatives or caregivers. Victims are often too ashamed to ask for help or admit they have been targeted. They worry that family members will doubt their ability to manage their finances and will put constraints on their independence. When senior citizens do report a crime, they are sometimes not able to remember all the details requested by the police.

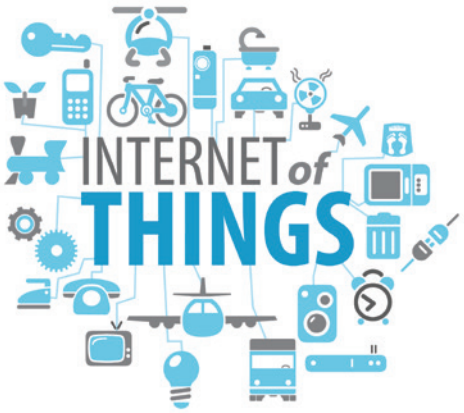
SENIORS CAN PROTECT THEMSELVES:

- Learn about scams and how to recognize them
- Research the proposed offer through reputable sources
- Avoid making financial decisions while being pressured
- Use caution with unsolicited phone calls or letters asking for money
- Do not give money or goods (jewelry, etc.) to unverified entities
- Update security software on computers (firewalls, anti-virus, etc.)
- Never open an unexpected email attachment
- Be wary of email attachments forwarded to you

Internet of Things (IoT)

The Internet of Things (IoT) is the "nickname" given to physical devices, or groups of objects, which have sensors or software enabling them to "talk" with other such objects. These include "smart" appliances, doorbells, thermostats, etc. Contrary to what some might think, these items do not have to be directly connected to the "public" internet in order to connect and communicate with each other.

Convenience appears to be a key factor in the adoption of IoT devices. Other benefits may include energy savings, with lights and other devises being automatically turned off.



The spread of IoT is causing alarm amongst privacy and security experts, as these devices usually are not able to include basic security measures like firewalls or encryption systems. Various groups are addressing these security concerns, such as the Things Security Foundation (IoTSF) which focuses on education and the creation of "best practices," Mozilla's "Project Things" which is devising an IoT system intentionally focused on security, privacy, and interoperability, and various large IT companies who are focused on IoT security solutions.

The Human Side of Fraud

As Frank Abagnale consistently teaches, the weakest link in any fraud prevention defense will be the people of an organization. This is because all security protocols and procedures will ultimately be created, established, and enacted by human beings. At the end of many highly technical cybercrime and other fraud prevention seminars, where a multitude of advanced and sometimes newly-invented fraud prevention technologies have been presented, the instructors will often conclude by saying that, of course, the human side of fraud is ultimately the determining factor in aiding or in thwarting fraud. For example, most, if not all, investigations into cyber security breaches eventually reveal that an employee, in a moment of forgetfulness or simple disregard, clicked on a link, downloaded an attachment, or otherwise broke an established fraud prevention protocol, creating a fissure in the dike of protection, opening the floodgates of fraud that swamped their organization.

On the other side of the spectrum, one of the key predictors of internal fraud such as embezzlement is a company's culture, and most importantly, the "tone" set at the top by the leaders of the organization. If leaders display "slips" of integrity and a lack of human decency, that tone ripples throughout the company, often with disastrous effects.

In addition to preventing fraud, the human side of enterprise is core to the success of an organization. What were once considered "soft skills" – empathy, collaboration, a sense of belonging, finding meaning at work – are now considered "power skills." They proved essential in surviving the pandemic's assault on organizations, and for thriving as the world reopens and the pandemic recedes.

Frank W. Abagnale

Frank W. Abagnale is one of the world's most respected authorities on the subjects of forgery, embezzlement and secure documents. For almost 50 years he has lectured to and consulted with hundreds of financial institutions, corporations and government agencies around the world.

Mr. Abagnale has been associated with the Federal Bureau of Investigation for almost 50 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. *Catch Me If You Can* also became a Tony-award winning Broadway musical and is now performed in various venues across the county.

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

SAFEChecks®
The Check Fraud Prevention Specialists

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

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

Mr. Litster acquired the **SAFE***Checks* operation from the bank in 1996, and is its President and CEO. **SAFE***Checks* has continued to be a pioneer and leader 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 successfully replicated and 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. He has served on several national and international check fraud and embezzlement cases. Mr. Litster has written numerous articles for publications such as AFP Exchange, American Payroll Association, American Land Title Association, and Sheshunoff's Corporate Cash Management Manual.

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

SAFEChecks®
The Check Fraud Prevention Specialists

(800) 755-2265

safechecks.com

4680 E. Los Angeles Ave., Suite L
Simi Valley, CA 93063
(800) 755-2265
Fax (800) 615-2265
www.safechecks.com
info@safechecks.com