YOUR COMPLETE *Guide to* CHECK FRAUD

How to Identify Different Types of Check Fraud

Before It Harms Your Bank

STAN JASLAR

TABLE OF CONTENTS

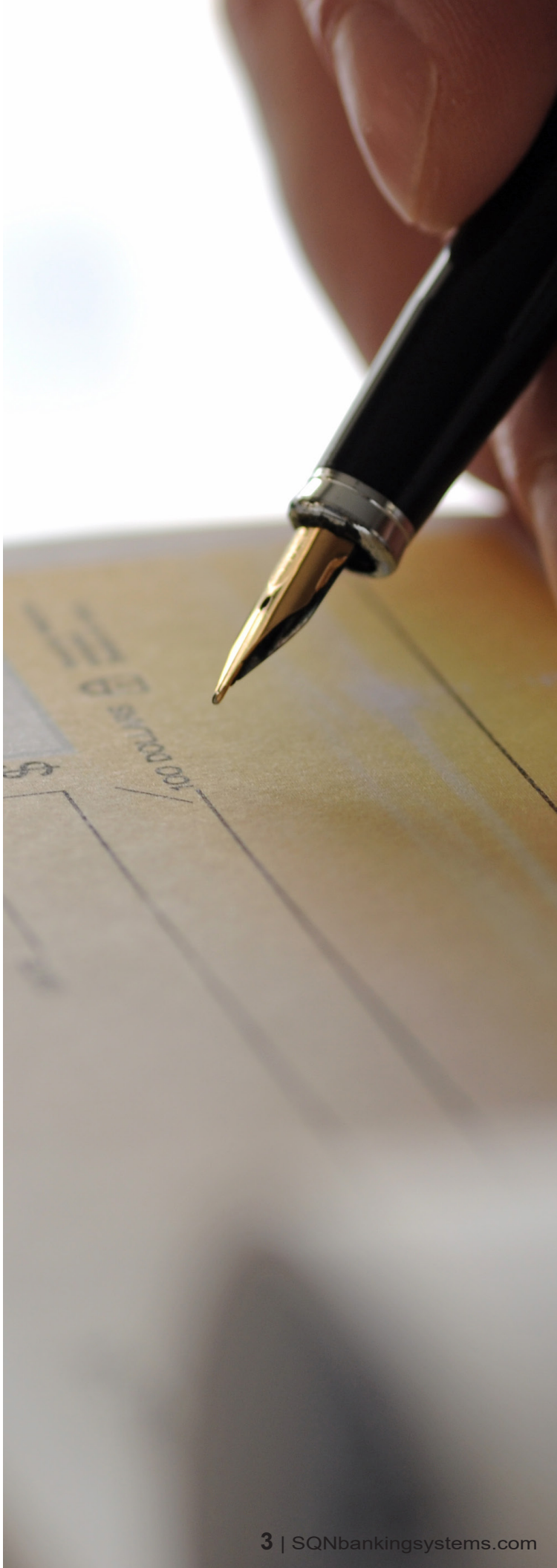
INTRODUCTION

Check fraud is incredibly widespread. In fact, because there are so many different types of check fraud, no one has the exact numbers on how many people are affected or how much money is lost each year.

The rise of the digital age has not eliminated check fraud. In many ways, it's made scam artists even savvier with their schemes. To protect your bank from check fraud, you need a fraud protection partner who can provide you with the products and services your financial institution needs. At SQN Banking Systems, we offer a suite of products, solutions, and services to help financial institutions fight fraud.

This eBook will help financial institutions understand the most common scams involving business checks, personal checks, cashier's checks, and money orders — and then determining ways to prevent them.

Keep reading to find out more about check fraud and how to educate your customers so that they don't fall victim to these scams — which ultimately helps you avoid holding the loss.



WHAT IS CHECK FRAUD?

A 2016 global fraud study indicates that the typical organization loses 5% of its revenue every year due to fraud. The biggest culprit in these losses is asset misappropriation, and in that category, check tampering and billing schemes accounted for the biggest threats. Banks and other financial institutions face a heightened risk of these losses, and you need tools in place to protect yourself.

Check fraud refers to any efforts to obtain money illegally using paper or digital checks. This can include someone writing a bad check on their own account, forging a check in someone else's name, or drafting a completely fake check. But it can also include countless other types of fraud using checks.

In one form or another, checks have existed since ancient times, and as trade spread from the Middle East through Europe in the middle ages and into the colonial era, checks became even more popular. Initially, checks were designed to save traveling merchants from the risks and inconveniences associated with carrying large bags of cash. However, fraud followed right on the coattails of the invention of checks, and in fact, the development of modern checks was largely based around trying to minimize check fraud.

Ways Check Fraud is Committed

Scam artists are always on the lookout to find new ways to commit check fraud. They forge signatures, alter ink on stolen checks, steal checking account information to print checks for fraud, and dabble with a range of other techniques. Check fraud can also overlap with identity theft, and it includes scams based around fake money orders and cashier's checks.

Customers, merchants, and financial institutions all bear the costs associated with counterfeit checks and other types of check fraud. Annually, scam artists draft millions of fraudulent checks for billions of dollars. To protect your financial institution, you should understand both the indirect and direct costs of counterfeit checks and how to protect your business.

Depending on the situation, the extent of the fraud, and the amounts involved, check fraud can constitute a misdemeanor or a felony. The exact penalties vary and may include bank fees, closed accounts, or damage to consumer credit ratings as well as criminal penalties such as fines and imprisonment.

Tools are available to detect fraud. For example, if the signature on the check doesn't match the signature in your database, if the check font or other stock details aren't right, if the numbers are out of order, or if the information on the check is suspicious in any other way, check fraud software flags the check for manual review. At that point, bank staff can step in and verify whether the check is real and decide which steps to take next.

CHECK FRAUD FAQ

Annually, the banking industry loses about $2 billion in fraud against deposit accounts, and over a third of these losses are related to check fraud. To protect your financial institution, your customers, and yourself from check fraud, you need to understand the essentials.

How Does Check Fraud Happen?

Check fraud can take several different forms:

- Stealing check blanks to use for fraud
- Using someone's account and routing number to create fake check blanks
- Taking a check written out to someone else, using chemicals to erase the ink, and writing it out to yourself
- Altering the amount on a check written out to you and cashing it
- Giving someone a bad check to pay for something and having them give you cash in return
- Signing checks that are not yours
- Endorsing and cashing a check that is not made out to you
- Writing checks from closed accounts
- Purposefully depositing a bad check into an account and withdrawing the funds

Is Check Fraud a Felony?

Depending on the situation, check fraud can be a felony or a misdemeanor, but in many cases, check fraud isn't detected or punished. Generally, the line between misdemeanor and felony depends on the amount of money involved in the fraud. Many states classify check fraud under $500 as a misdemeanor, and they consider fraud over that amount to be a felony.

What Are the Penalties for Check Fraud?

Generally, misdemeanor charges for check fraud can lead to criminal fines plus up to a year in jail. With felony charges, the fines can be thousands of dollars, and jail sentences may be over a year or even several years, depending on the extent of the crime and specific state laws.

Civil penalties for check fraud vary from state to state. In some cases, the victim may have the right to claim two or three times the amount of the check plus the victim's attorney fees. Some states outline a minimum civil penalty of $10 to $100, and others have a maximum penalty of $1,500.

How Can Check Fraud Be Prevented?

Educating your customers is a critical part of preventing check fraud. Reach out to your business customers and make sure they understand the importance of using checks with built-in security features that make the checks hard to copy or mimic. When possible, steer these customers toward electronic payments or direct deposit. Keep in mind, however, as you embrace other payment methods, you also must be vigilant about fraud in those areas as well.

Risks of Check Fraud

With individual clients, let them know about the risks of check fraud. Remind them not to put checks in their mailboxes or they might get stolen. Send out newsletters letting them know about popular check fraud schemes and how to avoid them. Advise them not to accept checks from people they don't know and never to give cash back to a stranger who writes them a check or gives them a money order.

What Happens When a Check Doesn't Clear?

Also, work hard to make sure your customers understand what happens when a check doesn't clear. In other words, they should understand that if they deposit a fraudulent check, some of the funds may be available right away, but once the check comes back as fraudulent, the credit gets reversed. At that point, the customer may experience returned payments and overdraft fees. To be on the safe side, your customers shouldn't draw funds on checks unless they are sure the check is not fraudulent.

Reducing Check Fraud

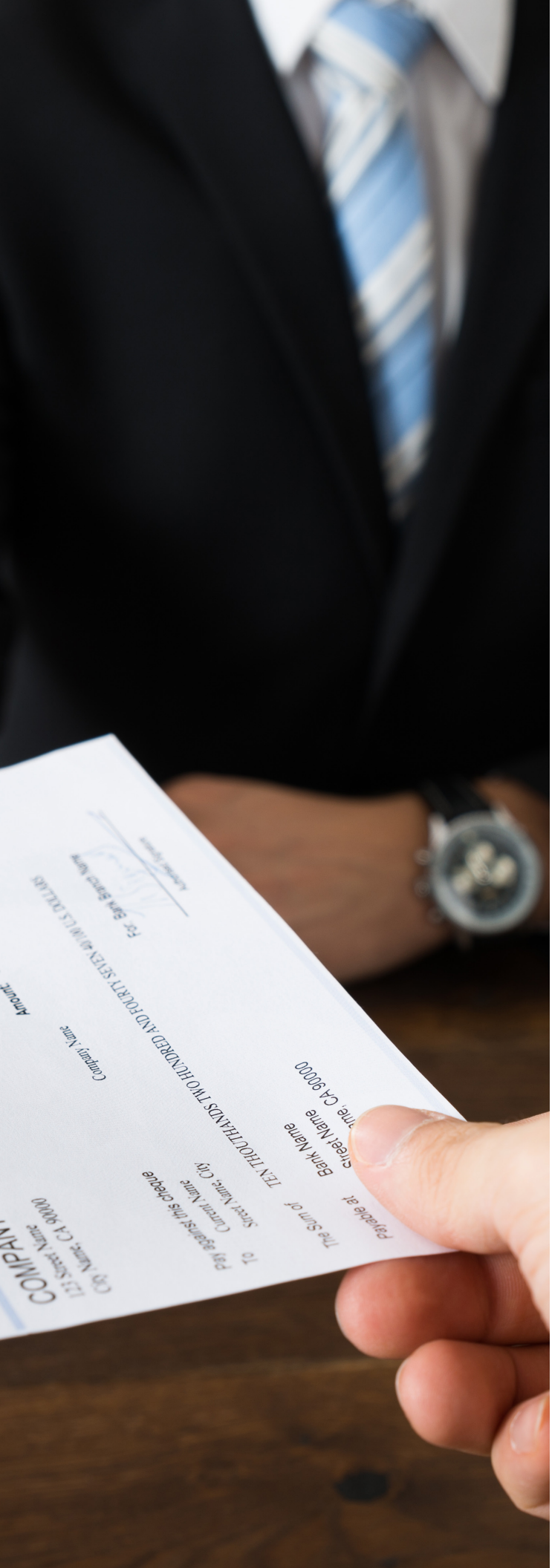
At the same time, you also need procedures and tools to reduce check fraud in your financial institution. Checking customers' identification and requiring a personal identification number (PIN) before allowing them to cash checks or make withdrawals on their accounts is essential. You may want to hold checks over a certain amount until the check clears. In some cases, this can be challenging because you need to balance customer satisfaction, bank security, and compliance with Regulation CC.

To be competitive with other financial institutions, you may need to credit checks relatively quickly, but you also need to make sure you don't end up holding a bad check and losing money. To help you strike the right balance, you need tools that can help you detect check fraud quickly and efficiently. Then, you can confidently credit other checks, without worrying about the risk of fraud.

How Do You Detect Check Fraud?

To detect check fraud, you need analyze the information, signature, and other details on checks and flag checks with issues that may indicate potential fraud. At that point, your Analysts can manually review the check and decide which actions to take.

Additionally, you may want to invest in special software that allows business customers to print a barcode on each of their checks. The barcode contains all the details on the check, including payee and amount. When you accept the check for processing, your system reads the barcode and ensures all the details match. If the barcode is missing or the check has been altered, the system picks that up immediately.



Who Pays for Check Fraud?

If a bank customer deposits a check that doesn't clear due to fraud, insufficient funds, or any other reason, the customer is responsible for any payments that have been drawn against that check and any fees that ensue as a result of those payments. At that point, the customer may try to recoup their losses from the person or business that issued the check.

In some cases, customers may leave an account overdrawn after depositing a fraudulent check, and then, the bank may end up paying for the losses. If someone comes into the bank and uses a check to make a fraudulent withdrawal from an account that is not theirs, the bank is typically liable for the fraud. Similarly, if a bank cashes a check that was created fraudulently, the bank is also responsible for covering those funds.

How is Check Fraud Investigated?

Banks and businesses often do their own investigations to figure out the truth behind check fraud. Depending on the extent of the fraud, local law enforcement agencies may handle the investigation, and in large cities, police departments often have their own financial fraud departments. Often, federal agencies such as the FBI, the Financial Crimes Enforcement Network (Fin Cen), or the financial crimes task force of the United States Secret Service handle fraud investigations.

What is Cashier Check Fraud?

Cashier check fraud uses cashier checks to commit fraud. A popular variation of this fraud involves the thief giving the victim a fake cashier's check and then asking the victim to give some cash in exchange for the cashier's check. When the victim tries to deposit the cashier's check, they find out it's fraudulent. By that time, they can't recoup their cash because the thief is gone.

HISTORY OF CHECK FRAUD

As long as there have been checks, there has been check fraud. Fraudsters have forged checks, impersonated account holders to cash checks, stolen checks, tricked people into giving them checks, and committed countless other types of fraud. Banks have been fighting check fraud for hundreds of years, and the struggle continues.

To get a sense of the types of fraud that may have taken place through the years, review this brief history of checks and check fraud.

The Origins of the Check

Humans started using financial tools similar to checks about 2,000 years ago. Ancient Romans used prescriptions, Ancient Indians used adeshas, and Ancient Persians used letters of credit. So, they didn't have to carry heavy bags of coins or risk being robbed, Arab traders invented the sakk, a paper document that allowed them to deposit money in a bank in one country and then withdraw the funds in another country.

As they dealt with Arab traders, Europeans were inspired to adopt these practices, and over the next few centuries, the modern check was born. In the 1500s, cashiers in the Dutch Republic accepted deposits for a fee, and they also paid out money to anyone with a note from the depositor. During the next few hundred years, this practice spread throughout Europe, but because the notes were all handwritten, fraud was rife. Many areas even banned this form of payment.

The First Modern Day Checks

In 1717, the modern check was born when the Bank of England began using pre-printed forms for these withdrawals. The forms were numbered and printed on check paper so that the bank could easily "check" for issues or inaccuracies. At that point, account holders had to go to the bank and have a cashier issue the check paper. Then, after they paid the check to someone, that person could return to the bank to retrieve the funds. This setup was expressly designed to minimize fraud.

The very young United States quickly followed suit and began using checks in 1784 at the Bank of New York. Arguably, the Commercial Bank of Scotland created the first personalized checks in 1811 by printing its customers' names on the side of the check. About 20 years later, the Bank of England began printing and binding check books for its customers. Again, by putting more information on the checks, the banks hoped to reduce fraudulent transactions.

Keep in mind that during this time period, paper money was not very popular. The United States didn't start printing paper notes until after the Civil War, and in the United Kingdom, generally only the upper-class elite used paper money until after the First World War. In this climate, checks helped to make business possible.

Fighting Check Fraud through Laws and Auditing

As checks became more popular, fraud increased. Governments created laws such as the Bills of Exchange Act 1882 in the United Kingdom and the Negotiable Instruments Act 1881 in India. At the same time, banks strived to create technologies to minimize bank fraud.

During this time, banks could only cash checks by sending porters to the other bank from where the funds had been drawn. Eventually, this process became too time consuming and inefficient, and bankers developed clearing houses so that they could cash their checks in a central location.

The clearing process took so long that it increased the risk of checks not being paid. In this era, when an account holder deposited a check, the teller stamped the deposit slip and made notes on when the funds would be available. Every morning, banks received returned checks from the Federal Reserve. Then, bank auditors looked for trends with the returned checks and the deposit slips, and they tried to identify kiting schemes.

The Invention of MICR

In 1959, Magnetic Ink Character Recognition (MICR) was patented and used on checks. This magnetic ink made automatic sorting possible and decreased the amount of time required for a check to clear. Over the next three or four decades, checks rose to their highest level of popularity.

This ink also created another layer of fraud protection — bankers could make sure that the check numbers were printed with this ink and that they matched the rest of the information on the check. Eventually, however, some thieves began buying MICR printers, making their scams even more effective.

Check Fraud in the Modern Day

After their peak in the 1990s, checks began to be replaced by electronic forms of payment. However, as of 2019, people still use checks. Roughly 15% of people use checks on a regular basis, and about 3% of people think checks are the best way to pay.

Many people now use electronic checks, and the implementation of the Check Clearing Act for the 21st Century decreased processing time by allowing banks to use substitute checks rather than paper checks.

TOP 6 MOST FAMOUS CHECK FRAUD SCAMS

Some check fraud scams were extensive, resulting in millions of dollars stolen. The following check fraud scams were some of the most infamous in the last few years.

1. Big Losses in Texas

Between 2004 and 2006, Texas entrepreneur Jeff Woodward engineered a check kiting scheme between four bank accounts for his motorsports and car dealership businesses. Every day, Woodard or his associates deposited bad checks in one or more accounts and drew money from other accounts.

Woodward signed about half of the checks and instructed his employees to sign the other half. Ultimately, the checks were for a total $114 million, which led to $1.6 million in losses for the banks. Woodard was sentenced to four years in federal prison, five years of supervised release, and was ordered to pay $2.5 million in restitution.

2. Hot Checks in Cleveland

In Cleveland, three young women ran a check kiting scheme for $165,000, which led to $120,000 in losses for banks. The women convinced other people to open new checking accounts. Then, they deposited bad or counterfeit checks into the accounts and withdrew large amounts of cash at a local casino before the banks realized the checks were bad.

Ultimately, the women deposited checks on 31 different occasions before getting caught. Their case was investigated by the FBI with help from the Ohio Casino Control Commission and prosecuted by the Assistant U.S. Attorneys.

3. Trouble from the Inside

Often, fraud starts inside of financial institutions. In one case, a financial advisor who had been with Vanguard for 23 years stole passwords and wrote checks from inactive or dead account holders. Generally, these abandoned investment accounts are turned over to state treasurers for distribution to next of kin or the original account holders, but Scott Capps wrote checks from these accounts to his brother-in-law and other co-conspirators.

In 2013, he actually doubled his income with these fraudulent checks and used the money to invest in real estate. After discovering the issue, Vanguard covered all the customer losses and brought charges against the perpetrators.

4. Fraud at the Top

Even chief executive officers of major corporations can put banks at risk with kiting schemes. In 2008, the CEO of Synergy Brands, Inc. wrote over $1.3 billion in bad checks through Signature Bank, Capital One Bank, and several Canadian banks. The checks were sent to Canadian companies that wrote checks in corresponding amounts to other companies also controlled by him.

While the scheme was active, the bad checks artificially inflated Synergy's account balances, and the CEO and his co-conspirators booked millions of dollars in fake accounts receivables and revenue. At the same time, they also inflated values for the company's filings with the Security and Exchange Commission (SEC). When the kiting scheme eventually fell to the ground, Synergy went bankrupt, losing investors a lot of money in the process, and the banks lost over $26 million dollars.

5. Shopping and Stealing Locally

In Sacramento County, George Pappadopoulos wrote approximately $195,345 in bad checks. He primarily wrote these checks to 38 small businesses in the Sacramento area, hitting many of them more than once. The ensuing losses were so significant that one business was forced to lay off employees. The Papadopoulos family was already well known for crime in the area, as his parents were convicted of insurance fraud for burning down their house in the 1990s.

For this scam, Papadopoulos received 20 years and four months in federal prison and was ordered to pay restitution to the victims. The judge lengthened his sentence due to a prior conviction for battery in 1993.

6. From Nigeria to Florida with "Love"

A scam artist from Nigeria reached out to an 80-year old woman in Florida. He strung along the woman romantically and convinced her to give him money. Then, he drew her into a check fraud scandal. Scam artists often target elderly or widowed people and leverage love to draw them into the scam.

Essentially, he contacted businesses and requested services. Then, he sent the victims a fake check for over the amount of the services, and he asked them to send the change to his agent in Florida (the 80-year old woman).

When police found the woman, she had $10,000 in cash and cashier's checks. She claimed that she had only received and sent money to the Nigerian man and that she hadn't personally taken any funds. One victim lost $4,300, but ultimately, they were able to recoup everything but $218 in fees.

101 FACTS ABOUT CHECK FRAUD

Scam artists use all kinds of tricks to get money from their victims, and checks are at the heart of a lot of scams. These facts will help financial institutions know what to look for; when you're educated about the scams and have the proper prevention tools in place, check fraud is less likely to occur. Check out this list of 101 facts about check fraud.

1. Check fraud refers to any type of fraud that relies on paper checks to steal money from individuals or businesses.
2. Check fraud is the second most common type of bank fraud, after debit card fraud.
3. Although check use is down overall, the Federal Trade Commission has received more complaints about check fraud in the last three years.
4. Banks can hold checks for three days, but just because a bank releases a hold doesn't mean the check has cleared yet.
5. If you receive an email about a potential check scam, you can forward the email to the FTC at spam@uce.gov.
6. Check fraud accounts for 35% of bank fraud.
7. Banks noticed and stopped about $5.9 billion in check fraud in 2016.
8. Banks suffered from $789 million in check fraud in 2016.
9. In 2016, check fraud had its first increase since 2008, surging by 28 percent.
10. Approximately 1.2 million bad checks go through the check processing system every day.
11. In 1995, Americans wrote $51 million in bad checks every day.
12. Annually, about 500 million checks are forged every year.
13. Forged checks lead to about $10 billion in total annual losses.
14. The Z-method refers to looking over a check from the top left corner to the top right corner, through the body of the check down to the bottom left corner, and over to the bottom right corner.
15. In the decade between 2003 and 2012, checks were replaced by debit cards and ACH as the most popular payment methods for transactions around the world.
16. Although check use is declining, businesses still use checks for 51% of B2B transactions.
17. Even the government has reduced use of paper checks, by issuing Social Security payments, unemployment benefits, and most tax refunds as direct deposits.
18. On average, businesses incur costs of $4 to $20 for every check they write.

19. Paying by check is more susceptible to fraud than any other kind of payment.
20. Over two thirds of businesses (71%) reported dealing with fraudulent checks in the last year.
21. Of the businesses that received bad checks, 44% reported dealing with one to five incidents.
22. About 22% of businesses dealt with bad checks six to 10 times.
23. Every year, half a million Americans fall victim to fake check scams
24. In one popular scam, thieves convince victims that they have been selected to become a secret shopper. They are instructed to review a money wiring service. They receive a check, and they are supposed to deposit the check and wire the funds to a certain recipient. However, after they wire the funds, the check bounces, and the victim has lost all that money.
25. Often, scam artists invent an excuse for giving someone a check written over the amount. Then, they convince the victim to give them change for the extra amount. Ultimately, however, the check is no good, and the victim loses the funds they paid out.
26. When victims deposit fraudulent checks into their accounts, they may end up writing personal checks against that amount. Then, when the fraudulent check turns out to be worthless, they may face fees and penalties for the bad checks they wrote.
27. Because of that, sometimes the victims of check fraud end up being accused of fraud as well.
28. In most cases, when you deposit a check into your account, you are personally liable if the check is bad and you spend money against it.
29. Banks are not liable for most bad checks.
30. The bank may be liable, if its employees allow a thief to cash forged checks against your account.
31. However, if the bank can establish that the customer was negligent in how they kept their checkbook or account information, the bank may be able to shift liability for forged checks to the customer.
32. On average people who fall victim to these check fraud scams lose about $2,400.
33. Check washing is when criminals use chemicals to erase the ink on a check, and then, they rewrite the check to another party for a different amount.
34. Sometimes, check washing is called chemical alteration.
35. Between 2007 and 2009, two ringleaders worked with 950 people to steal $1.4 million in fraudulent checks from New York banks, arguably one of the nation’s biggest check fraud schemes of all time.
36. When an account holder purposefully writes a bad check from their own account, that is called paperhanging.
37. Check kiting is when an account holder writes a bad check from one account and deposits it in another account to make the second account look as if it has a positive balance.

38. As float time has decreased, kiting has become less common.
39. If you write a check a couple days before you have the funds and hope that the check doesn't hit your account, that is called floating a check.
40. Businesses watch customers who frequently write checks over the amount because they get concerned that the customers may be writing bad checks to take advantage of the float time.
41. Forging a check refers to faking the account holder's signature.
42. Counterfeiting a check is when a thief prints a check with the victim's name and account number, and then, writes it out to themselves or uses it to buy items.
43. When someone opens a checking account in another person's name, that is identity theft.
44. Some scam artists offer victims a money order in exchange for a check, but then, after the scammer takes the money from the check, the money order turns out to be fake.
45. Magnetic ink character recognition (MICR) is a special type of magnetic ink that is often used on checks to streamline processing and reduce fraud.
46. If an account holder doesn't have enough funds in their bank account to cover a check, their bank may accept the check or return it.
47. When banks accept checks that make an account become negative, they charge an overdraft or insufficient funds (NSF) fee.
48. On average NSF fees are about $35.
49. If a bank returns a check, they assess a bounced check fee.
50. Merchants may also charge customers fees for writing bad checks. Generally, when someone writes a check to a business, they agree that the business can add an additional fee if the check is returned.
51. ChexSystems track people who have written bad checks or refused to pay banking fees.
52. Over 80% of banks use ChexSystems to assess the creditworthiness of new account holders.
53. ChexSystems keeps most reports for about five years.
54. Consumers receive a score ranging from 100 to 899, with higher scores being the best.
55. Organizations lose an average of 5% of their revenues to different type of fraud every year.
56. While large corporations are likely to lose money through corruption, small organizations are more likely to face losses due to check tampering, skimming, and payroll fraud.
57. Fraudsters only need an account and routing number to commit check fraud.
58. The account and routing number is clearly printed on every single paper check, making it relatively easy to access.

59. Robbing a national bank or any member of the FDIC became a federal crime in 1934.
60. Usually, writing a bad check for over $500 is a felony.
61. Bad checks under that amount are usually a misdemeanor.
62. If you're caught writing a bad check in Los Angeles, you may have to go to personal finance classes through the bad check restitution program.
63. As a general rule of thumb, you have up to a year to notice a forged check on your account, and the bank may accept liability during that time.
64. If there are multiple forged checks, you usually need to report that within a month, but the rules vary from bank to bank.
65. In January 2019, a couple of thieves printed fake checks using information from two accounts based in North Dakota, and they wrote checks for $48,500 in Alabama and $32,600 in New Jersey.
66. The CEO of Synergy was convicted in a $1 billion check kiting scheme.
67. The defendant wrote $1.3 billion in checks and the bank lost $26 million before uncovering the scheme.
68. The punishment for this check kiting scheme was 30 years in prison.
69. In Cleveland, three women wrote approximately $165,000 in fraudulent checks, and they were able to withdraw $120,000 before getting caught.
70. Although these women didn't try to steal as much as the CEO, they were able to reap a higher portion of their fraudulent checks than he was.
71. They convinced co-conspirators to open bank accounts. Then, they deposited fake checks into the accounts and made large cash withdrawals at a local casino.
72. By the time, the banks realized the checks were fraudulent, the accounts were overdrawn, and the banks were left holding the empty bag.
73. For attempting to kite $1.3 million in bad checks, Texas entrepreneur Jeff Woodard received 30 years in prison, a million dollar fine, and five years of supervised release.
74. In the past, banks took manual measures to detect check kiting schemes.
75. After receiving piles of returned checks from the Federal Reserve, bank auditors went through the ledgers to see if daily deposits differed from daily balances. Then, they analyzed account activity and deposit slips, and if they noticed a potential history of check kiting, they closed the account.
76. Check 21 refers to the Check Clearing for the 21st Century Act.
77. In 2003, this law gave banks the right to create electronic copies of consumer checks.
78. This process is called check truncation because it truncates (shortens) the information on the check so that it can be processed more quickly and doesn't have to be physically transported to another bank.

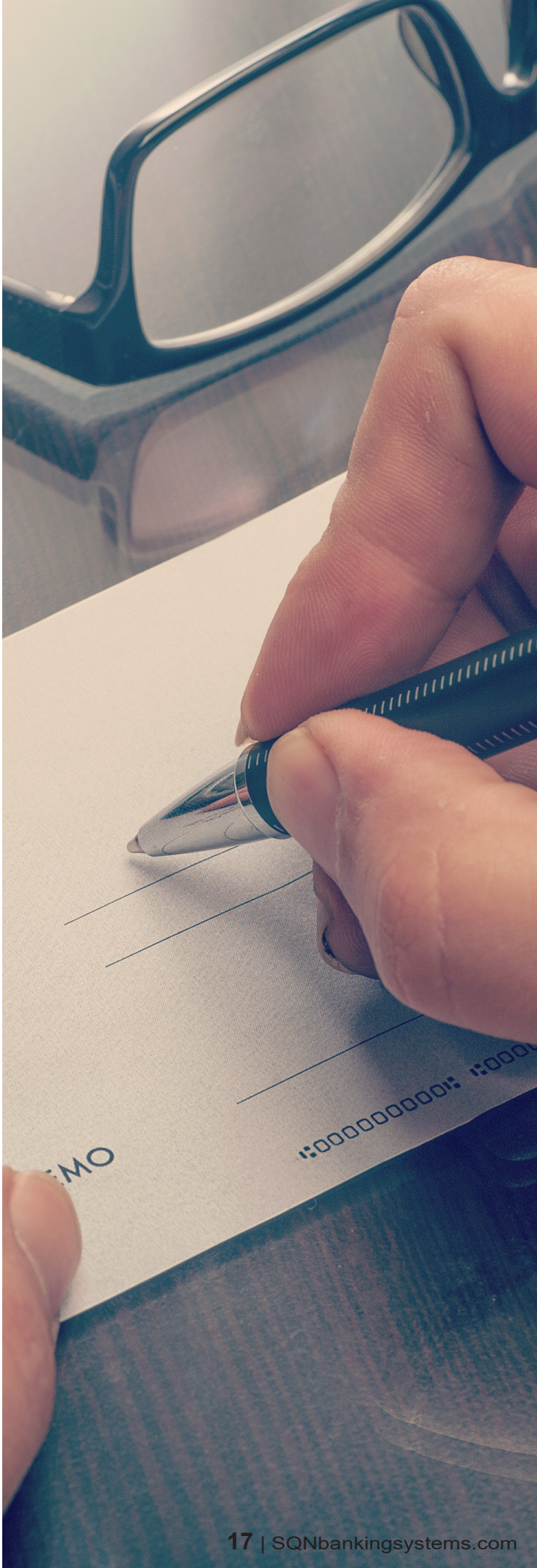
79. Some speculate that ancient Romans used checks as far back as the 4th century.
80. Arguably, checks were first used in the western world in the 1500s in Holland.
81. On the Silk Route, Muslim traders used checks because they were more practical than carrying around bags of metal coins.
82. Europeans picked up the tradition from Muslim traders during the Crusades.
83. People deposited their funds with Dutch cashiers for safe keeping. Then, they issued written orders or notes that the cashiers should pay some of their debts or bills. This practice was one of the first uses of paper checks.
84. Due to being handwritten, early checks were highly susceptible to fraud.
85. Many European cities banned checks, and banks often required both parties (the check writer and the recipient) to be present to cash a check.
86. In the colonies, people first began using checks in 1681 nearly 100 years before the formation of the United States.
87. In the United States, checks are older than paper money.
88. The nation didn't begin printing paper notes until after the Civil War.
89. In the mid-1700s, British banker Lawrence Childs began printing numbers on these paper notes as a way to "check" on their authenticity.
90. Then, this usage of the word check entered the English language.
91. At this point, the word check came to mean "examine the accuracy of something," but over the next few hundred years, it evolved to refer to a paper check.
92. Prior to that, the word check was mostly only used in relation to putting the king into check while playing Chess.
93. In the United Kingdom, paper money didn't become popular until after World War I. By that time, checks had been in use in the country for over 200 years.
94. Although checks were numbered for decades, banks didn't start using account numbers until well into the 20th century, after computers entered the world of finance in the 1960s.
95. Banks present checks they have received to the Federal Reserve System or to a private clearing house. Then, that third-party handles the process of presenting the checks to the bank that owns the account attached to those checks.
96. In 2003, the Federal Reserve cleared paper checks at 45 locations.
97. Now, the Fed clears most checks electronically and only has one location for clearing paper checks.

98. The concept of a clearing house started when two messengers with checks with different banks, bumped into each other at a London coffee shop and decided to exchange the checks there, rather than continuing onto the bank in person.

99. Fifteen percent of Americans use checks regularly, and the number is expected to stay consistent through 2020.

100. Three percent of people think checks are the best way to pay.

101. However, even those people use cash more often than checks.



TYPES OF CHECK FRAUD

Fraudsters use a variety of different types of check fraud to steal money from people and businesses. These are some of the most common types of check fraud that may impact your financial institution or your customers.

Paperhanging

Paperhanging refers to situations where account holders purposefully write bad checks on their accounts. In some cases, the account holder may have opened the account just to write bad checks. Remind your business clients that they may not want to accept starter checks or checks under a certain number from their customers — a lot of check fraud is related to brand new accounts. Other paperhanging fraud includes people purposely writing checks from closed accounts — knowing full well that the funds are not there to cover the check.

Additionally, the check writer may have an established account, but they write a check that exceeds their balance. They may do this with intent to overdraw the account before they leave the country, they may be trying to take advantage of the float time, or they may simply be mistaken about their available balance.

Check Kiting

Check kiting involves two different accounts. The same person may own both accounts, or they may work with another account holder. Essentially, they write a check from one account to another account. This check creates the illusion of a balance in the second bank account. Then, they may withdraw cash and run, or they may repeatedly kite checks between the accounts to take advantage of the float time.

For example, imagine someone writes a $500 check from Bank A and deposits it in Bank B. Then, they withdraw $500 from Bank B. By the time, Bank B realizes the check from Bank A is no good, the check writer has disappeared.

Check Floating

Check floating is any situation where someone writes a bad check to take advantage of the float time. Sometimes, account holders float a check to buy an extra day or two before payday. In other cases, they run a more elaborate scheme that is a variation on the scam explained above.

Say someone writes a check from Bank A to Bank B for $500. Then, they withdraw $500 cash from Bank B. The next day, they write a check from Bank B to Bank A. This check brings Bank A's balance up to $500, and as a result, the original check clears. The check writer continues this pattern for a few days or weeks, and eventually, they deposit their paycheck to cover the check, and they stop kiting.

Although the above scenario didn't result in any losses, these patterns are a strong indicator that an account holder may be likely to overdraw their account or make other serious errors. Therefore, financial institutions should have tools in place to identify these types of patterns.

Check Forgery

Check forgery is when someone forges their name on a check. They may take someone else's check and forge their signature. Then, they may deposit the check in their own account or use it to buy goods or services at a business.

In other cases, thieves may forge the endorsement. For instance, if a check is written out to Bob Smith, a thief can forge Bob Smith's signature on the endorsement line, and then they deposit or cash the check by finding someone who is willing to accept an endorsed check. Other times, the forger may actually pretend to be Bob Smith and cash the check at his bank.

Check Theft

Check theft typically involves forgery. Basically, someone steals a paper check and forges the signature. In some cases, the fraudster may steal an account number and print and use checks from that account. When the thief prints checks, that is usually called counterfeiting.

Identity Check Theft

With this type of check fraud, the thief steals personal details from someone. Then, they open a bank account in that person's name, and they write bad checks from the account. By the time the bank closes the account, the fraudster is gone, the bank gets stuck with the bad checks, and the identity theft victim has to deal with the repercussions of compromised information.

Account Takeover

This is similar to identity theft, but in this case, the scam artist takes over another person's account. They may gain access through the online account or even by going into a branch and pretending to be the actual account holder. At that point, they may draft fake checks from the account, use the check for a kiting scheme, or explore other possibilities.

Chemical Alteration

Also called washing, chemical alteration is when some uses chemicals to wash away the information printed on a check. Then, they populate the check with new information. They may write the check out to themselves or another entity, or they may change the amount.

Fake Paycheck Scams

In a fake paycheck scam, the scam artist reaches out to the victim and offers them a job. Often, the position is to be a secret shopper or test out a wire transfer service. Then, the scam artist sends a paycheck to the victim and gives the victim instructions. Generally, the victim needs to test out a wire transfer service by sending money to someone else. The paycheck was large enough to cover the wire plus some payment. However, when the check bounces, the victim is left with nothing, and they've lost the wired funds.

Fraudulent Lottery Checks

In another variation of this scam, the scam artist tells someone they have won the lottery. They receive a check for their winnings, but they are instructed to send back some money to cover fees and taxes. By the time they realize the check is no good, the payment they issued for their fees and taxes is gone.

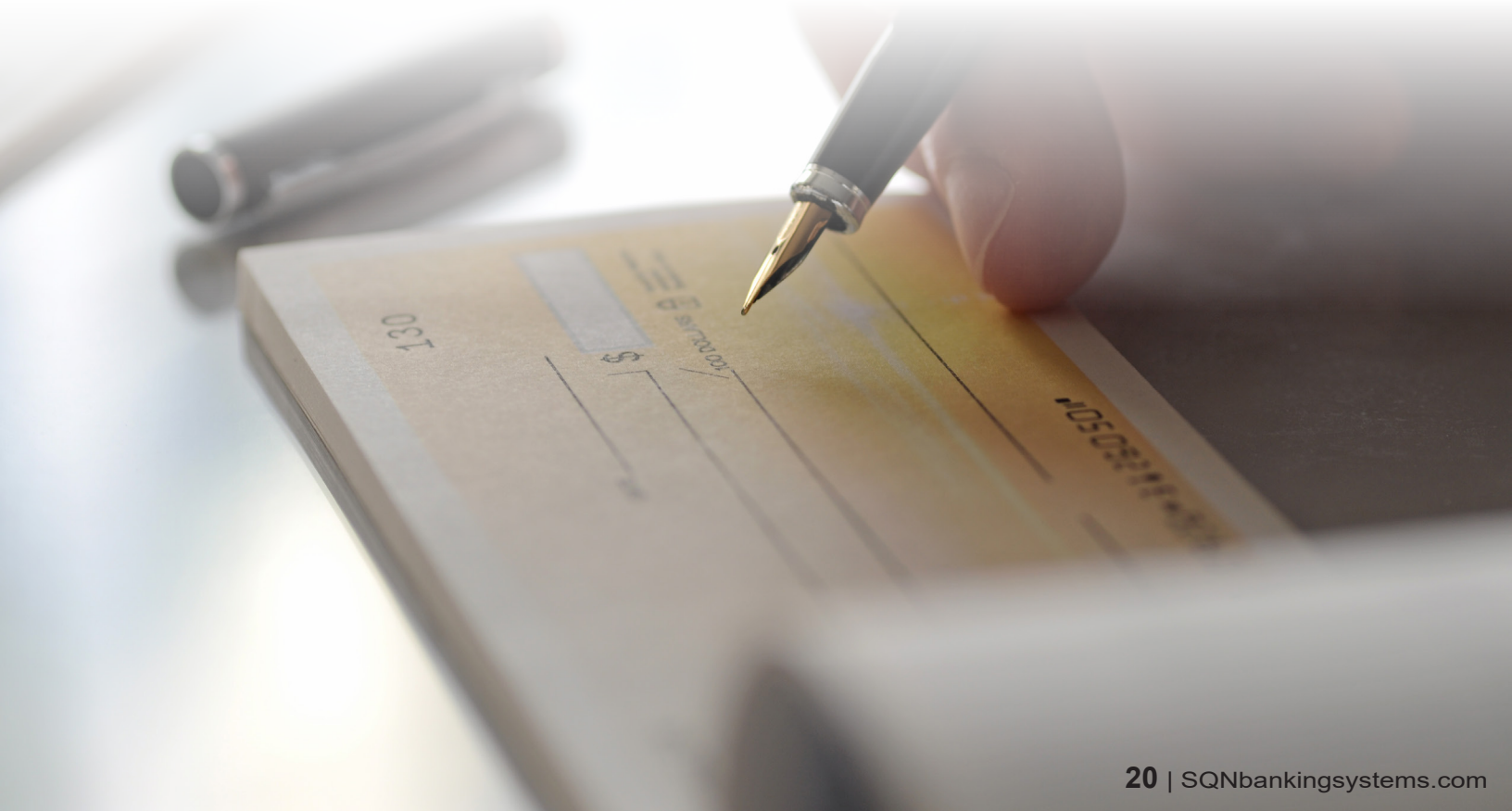
Bad Checks for Purchases

In yet another check fraud scam, the scam artist contacts someone who is selling something online. In some cases, they may even come to a garage sale or another in-person sale. Then, they ask if they can write a check over the purchase amount and get change.

To entice the victim to say yes, they might even offer to pay a bit more for the purchase. For instance, if the victim is selling a bike for $500, the scammer may offer a check for $800 if the seller will give them $200 in cash. The seller thinks they are making an extra $100 for being so accommodating, but in reality, the check is bad, and the seller is losing their bike and the $200 cash.

Money Order Fraud

This type of check fraud starts with a fake money order. The scam artist gives the victim a money order, and they ask for a check in return. They may use all kinds of excuses to convince the victim to make this trade. Again, however, when the victim deposits the funds into their bank account, they find out the money order isn't real, and they lose all the funds from their check.



CASHIER'S CHECK AND MONEY ORDER SCAMS

Savvy scam artists take advantage of the sense of security banking customers feel around cashier's checks and money orders, and they use fake money orders or cashier's checks to steal money from victims. In most cases, by the time your financial institution realizes the cashier's check or money order is fraudulent, your customer has likely spent the funds, putting their account in the red.

Your customer may end up suffering the loss, or they may just walk away, leaving your financial institution with a loss. Even if you can recoup some of the funds by pursuing collection activity, you still end up losing money your business needs to survive and thrive. To protect your financial institution and your customers, you should be aware of the main types of cashier check and money order fraud.

Anatomy of a Scam

Cashier's check and money order scams always tend to feature a few core elements:

1. The person issuing the payment refuses to use another type of payment method. They insist on a money order or a cashier's check.
2. The payment is more than the recipient needs or is entitled to receive.
3. The issuer requests the recipient to return some of the funds in cash, through a wire transfer, or with another secure method of payment.

Although these scams can be done with either cashier's checks or money orders, they tend to involve cashier's checks simply because cashier's checks have higher limits. Money orders are issued by post offices, grocery stores, and other entities, while cashier's checks are only issued by financial institutions. Money orders tend to be capped at about $700 to $1,000, but cashier's checks are often for up to $5,000 or more, allowing the scam artist to potentially receive a larger sum of money.

Types of Cashier's Check Scams

To lure in victims, scam artists use a variety of different lies. Some of the most popular scams that have emerged over the last few years include the following:

- **Check Overpayment:** With this scam, the thief contacts someone who is selling something over Craigslist, in a classified ad, or even at a rummage sale. They tell the seller that they can pay with a cashier's check or a money order, but the check is over the sale price. To entice the buyer to accept the fake money order, the scam artist might even offer to pay a bit extra. The victim gives the "buyer" the change in cash or potentially even wires change to them. By the time the fake money order or cashier's check is detected, the thief is long gone with the change and the for-sale item.

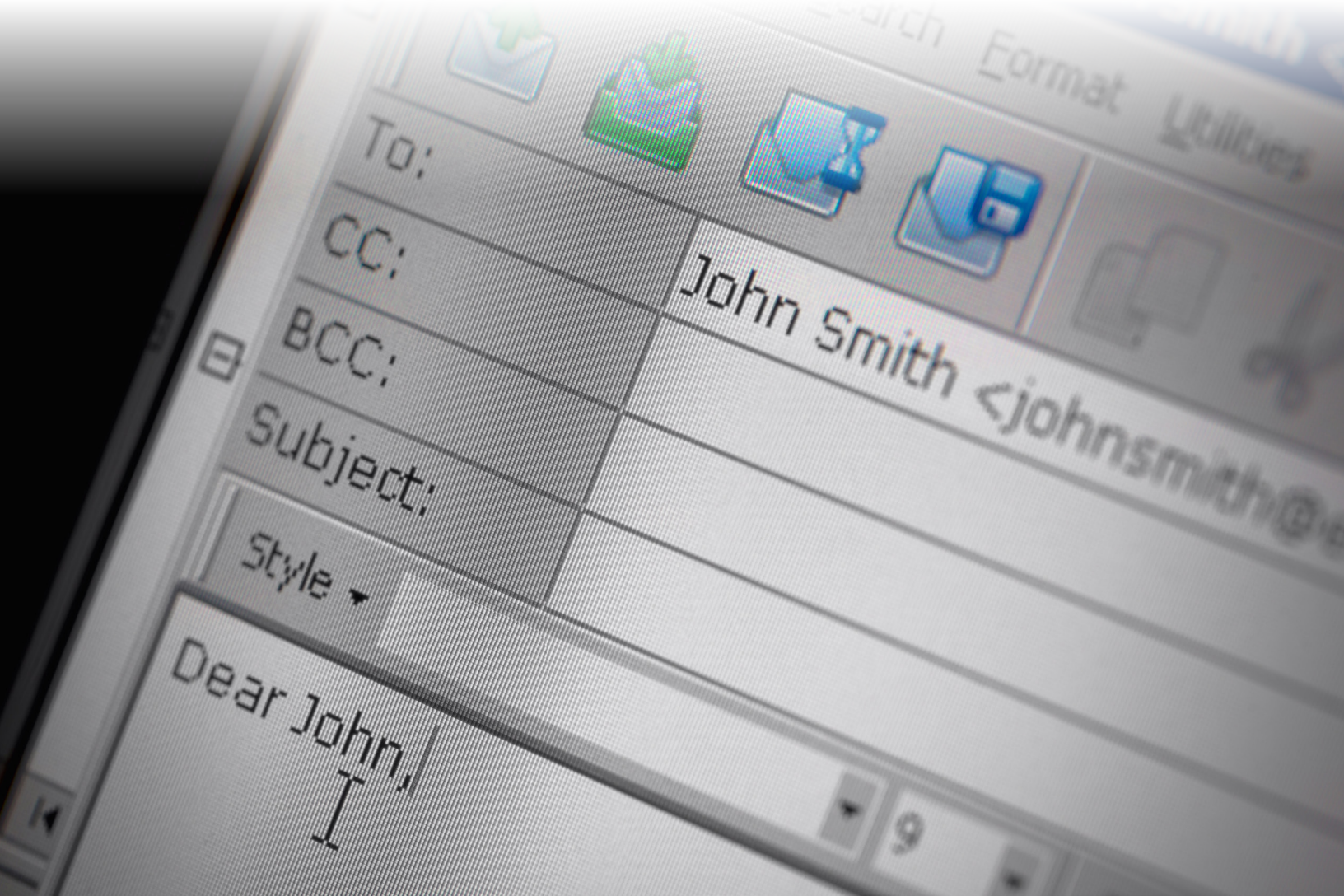
- **Secret Shopper:** This scam can take a few different forms, but usually, the scam involves offering a victim a job as a secret shopper who needs to review a wire transfer service. To help the "secret shopper" get started, the scam artist sends over a fraudulent cashier's check, and they direct the shopper to deposit the check, keep some of the money for their payment, and wire the rest of the funds to a recipient. After sending the funds, the secret shopper should review the service. Of course, however, the scammer is not really interested in a review. Once they receive the wired funds, they disappear, and eventually, the victim realizes they have been duped when the check doesn't clear.
- **Foreign Lottery:** The scam artists tells the victim that they have won a lottery. They can receive a giant cashier's check, but they have to pay a few taxes or processing fees. If the victim believes the lies, they deposit the fake check, they withdraw funds for the "taxes" or "fees" and then dispatch those amounts. They may even start spending their winnings. Then, the cashier's check proves to be fraudulent, the victim is left with an overdrawn bank account.
- **Foreign Wealth Scam:** Sometimes called the "Nigerian prince scam," this heist starts with an email or a social media message from a prince who's been rejected by their family, a scared diplomat, or another person who claims to be in danger in their current position. They need to escape, and they explain the reasons to their victim. First, however, they need to get some funds out of their country, and the victim is the only person who can help. Pretending to be a sympathetic character, the scam artist tells the victim that they will send a money order, and the victim should cash the money order and send some funds back in cash (usually through a wire transfer). In return for the favor, the victim gets to keep some of the money. Again, of course, the victim loses the funds they contribute when the bank realizes the cashier's check is a fake.
- **Money Mule:** Often cast as a check processing work-at-home job, this cashier's check scam can often be part of a larger money laundering operation. Basically, the victim gets a fake work-at-home job processing checks. They deposit the checks into their bank accounts, they send the cash to a recipient as instructed by their "boss", and they keep some money as payment. Sometimes with this scam, the scam artist starts with real cashier's checks, and then, after they establish trust with the victim, they issue a large fake cashier's check.

Reverse Money Order Scams

In some cases, these scams work in reverse. They don't rely on fake money orders or cashier's checks. Instead, they focus on convincing the victim to send a money order or a cashier's check to the scam artist. These scammers request money orders or cashier's checks because the funds are verified, and they don't have to worry about the victim issuing a stop payment as they can with personal checks

These money order scams take the following forms:

- **Stranded Friends or Loved Ones:** The scam artist pretends to be a friend or relative of the victim. They may hack the friend or relative's email or social media accounts and send messages from there; they may make up a fake email account or social media profile that appears to be from the relative; or they may even just call the victim and pretend to be their loved one. They say they are stranded in another country, and they need money to get home. Sometimes, they may even pretend to be kidnapped and request a ransom.
- **Romance Scams:** Often perpetuated on widowed people or other victims perceived to be emotionally vulnerable, this scam requires the scam artist to create an emotional connection with the victim. Often, they start by creating a fake social media or online dating profile, and they spend a lot of time messaging the victim. Once the victim is emotionally attached, the scam artist requests a money order or cashier's check. In some variations of this scam, the thief may obtain explicit photos from the victim, and then, they may blackmail them in exchange for not releasing the photos.
- **Debt Collection:** Pretending to be a debt collector or the Internal Revenue Service (IRS), the scam artist contacts the victim, threatens them about a fake debt, and requires them to send a cashier's check or a money order to them.



HOW TO PROTECT YOURSELF FROM FAKE CASHIER'S CHECKS AND MONEY ORDER SCAMS

When you run a financial institution, you inevitably hear about money order and cashier's checks scams, and eventually, some of your customers may fall prey to these scams.

Theoretically, your customers are responsible for losses related to fraudulent money orders and cashier's checks, but if they deposit a fake check and make withdrawals against that amount, they may not be able to bring their account back into the black when they realize the check is no good, and that puts you at risk of suffering a loss.

To protect your bank, credit union of other financial institution from fraudulent cashier's checks and money orders, you need to be vigilant.

Have Tellers Ask Questions When Customers Deposit Cashier's Checks

If one of your customers has become the unwitting victim of a scam, your tellers may be able to stop the issue from escalating simply by asking the right questions. Encourage tellers to ask the following questions when accepting deposits from customers, especially deposits of cashier's checks or money orders:

- Do you know the person who gave you this cashier's check or money order?
- Do you trust the person who gave you this cashier's check or money order?
- Have you met the individual in person, or do you only communicate electronically?
- If using electronic communication, do you notice a lot of issues with grammar or odd phrasing?
- Did the individual who gave you the cashier's check or money order request change in cash or from a wire transfer?

The wrong answers to those questions can be serious signs of fraud. Additionally, have your tellers remind customers that although funds from cashier's checks and money orders are available right away, that does not mean these deposits have cleared. Let your customers know how long it can take to figure out a money order is fraudulent and advise them that they may want to delay spending the funds until they are absolutely sure the deposit is valid.

Know the Signs of Fake Money Orders and Fraudulent Cashier's Checks

Your tellers should also be aware of telltale signs that a money order or cashier's check is fraudulent. With cashier's checks, they should look for the bank name and phone number. The absence of a name or phone number is a red flag, but in some cases, scam artists include a real bank's details. If your tellers are suspicious, they can contact the bank directly.

Additionally, most cashier's checks have the recipient's name professionally printed on the check. Handwritten names can be another sign of a fake.

Money orders are usually embedded with a classic security feature such as a watermark, color shifting ink, or heat-sensitive patches. Consider putting together a cheat sheet of the current security marks used by companies such as MoneyGram or Ben Franklin that issue money orders.

Use Real-Time Fraud Analysis Tools

In a lot of cases, your customers simply deposit funds into the automatic teller machine (ATM), and your tellers don't get a chance to talk with them personally. To protect your customers and your financial institution from fraud, you need fraud analysis tools that can look for potential fraud in real time.

You need tools that can find inconsistencies with ATM withdrawals and deposits and notice when transactions exceed a customer's usual spending profile. Ideally, these tools should alert you to the situation so that you can reach out to your customers as needed.

Check for Alerts from the Office of the Comptroller

A lot of scam artists use info from real banks, and the Office of the Comptroller of Currency publishes alerts on which bank's names are commonly being leveraged in scams. For instance, in March 2019, scam artists were using fake cashier's checks sporting the name of the First National Bank of Elmer, NJ, and in May 2019, thieves were issuing counterfeit cashier's checks from Farmers & Merchants National Bank in Nashville, IL.

Usually, scam artists choose to copy information from relatively small banks because they believe they are less likely to get detected by taking this route. Check regularly for updated information or sign up for alerts from the Department of the Treasury.

Educate Your Customers

Customer education can be one of your most effective lines of defense against fake money orders or cashier's checks. Consider using signs, direct mail pieces, inserts in mailed statements, and emails to tell your customers about the risk of scams.

Let customers know about the most common fraudulent cashier's checks and money order scams, and share the following tips so they can protect themselves:

- Be suspicious of offers from strangers — if it sounds too good to be true, it probably is.
- Don't accept international money orders.
- If someone wants to pay with a cashier's check or money order, consider asking for an alternative form of verified payment such as a wire transfer, an electronic funds transfer, or cash.
- If they insist on a cashier's check or money order, accompany them to the bank or store, and watch a professional issue the payment.

- Never accept cashier’s checks or money orders over the sale amount.
- Be wary of “buyers” who don’t seem interested in the product — they don’t ask questions or want to see it, but they offer to buy it quickly.
- Do not send cash or wire money to anyone (especially strangers) in return for a cashier’s check or money order.

If your customers follow that advice, you reduce your risk of exposure to scams involving fake money orders or cashier’s checks.

CHECK FRAUD DETECTION AND PREVENTION

Now that you understand the types of check fraud and the lengths these criminals will go to complete the scam, let's take a look at how to detect and prevent check fraud from happening.

A 2018 study conducted by American Bank and SourceMedia Research reveals that the majority of senior level executives from banks, credit unions, and other financial institutions report that they are more worried about fraud now than they were a year ago. They deal with multiple types of fraud, including check fraud. Account takeover alone accounts for over $5.1 billion losses per year.

90% of surveyed executives report that it takes over a day to deal with most cases of fraud and less than a quarter of respondents were able to clear up fraud incidents in less than a day. Fraud costs money, takes time, and can threaten a financial institution's reputation. Check fraud detection and prevention tools are absolutely essential to protect your financial institution. For best results, you need a multi-pronged strategy which involves the following elements:

Automated Check Image Analysis

Automated check image analysis uses powerful software to detect small alterations that may not be visible to the human eye alone. These tools look at fixed information on the check such as payer's details, signature line placement, font, layout, check size, and serial number. They can also look over the content of the check, scanning for signatures, stale or future dates, amounts, and MICR data.

When the software detects a problem, it flags the check for manual verification. At this point, your bankers can visually assess the check, look at the account, and decide on the next steps to take.

Secure Barcodes

Some banks offer their customers secure barcodes or seals to print on the checks. This technology largely takes the place of watermarks or special inks, and it works perfectly for business clients who print their own checks. Essentially, the software allows the account holder to generate a check with a special barcode or seal.

Then, when the bank receives the check for processing, the bank's software reads the seal or barcode and ensures that the encoded information matches the rest of the check. If a scam artist steals the business account and routing number and generates a fake check, the software notices the lack of a seal or barcode, and it flags the check as suspicious.

Ultraviolet Technology

To utilize UV fraud detection software, financial institutions have their customers print checks with special UV ink. Typically, they use the ink in sensitive areas such as the amount line, the signature, and the bank logo. Then, when the bank processes the check, it runs it under a UV-scanner which can detect if any of the UV ink has been altered or tampered. This type of technology is especially useful for fighting chemical alteration or check washing.

Signature Verification Tools

Signature verification tools allow you to collect and store your customers' signatures in a database. Then, special software scans the checks and other documents for discrepancies in the signature. When issues arise, the software displays the signature on the check next to the signature in the file, allowing your employees to make a manual comparison. These tools speed up processing times, without compromising bank security.

Transaction Analysis

Sometimes checks look perfect. The stock details are correct, the content is okay, and the signature is a match. But the customer may be kiting checks, drafting bad checks on a new account, or committing other types of check fraud. To uncover these issues, you need transaction analysis tools that can look for troublesome patterns or other potential red flags, such as out of range check or duplicate numbers.

Quality transaction fraud analysis tools look at on-us checks, but they also analyze ATM withdrawals, debit and credit card transactions, repetitive deposits, and spending amounts that don't fit with the customer's usual patterns. They can also help you monitor loan transactions, wire transfers, mobile banking, and a variety of other banking transactions.

Employee and Customer Education

On top of the above tools, you also need to train employees how to detect fraud, and you need internal safeguards in place to help prevent internal theft and fraud. Additionally, you need to educate your customers.

Consider sending newsletters or emails to individual and business customers to let them know about the lasted check fraud scams and how to avoid them. Also, hang infographics and posters in your branch locations to spread the word on check fraud. When your customers are savvy about fraud, your financial institution reaps the benefits.

HOW TO SPOT AN ALTERED CHECK

Thieves alter checks by changing the amount or the payee name. Then, they cash the check over the counter, deposit it into a new account and withdraw the funds before anyone detects anything or find other methods of getting the cash. To spot altered checks, keep the following tips in mind.

Look for Inconsistent Handwriting

When accepting checks for deposit over the counter, your tellers should look for handwriting inconsistencies. If they see differences between the amount and the payee name or other handwritten details on the check, they may want to investigate a bit more before accepting the check.

Check for Visible Signs of Alteration and Erasure

Your tellers should also look for visible signs of alteration when accepting checks for deposit. If they can see that the amount has been changed or if there are erasure marks underneath the payee name, they should follow the protocol you have laid out. Depending on the situation, you may want to put a hold on the check, reach out to the check issuer, or contact the bank from which the check is drawn.

Tell Customers Not to Leave Spaces

If your customers leave spaces when they write out checks, that can make their checks more susceptible to alteration. Ideally, they should fill up the check amount box and the line where they write out the check amount. Consider sending out samples of how to write out checks properly whenever your customers order a new box of checks.

Advise Customers to Keep Checks Safe

Checks need to be stolen before they can be altered, and to prevent that from happening, your customers need to keep their checks safe. They shouldn't leave checks unattended in desk drawers at work or in unlocked cars. Ideally, they shouldn't even put checks for bills into their mailboxes, as thieves are notorious for grabbing and altering checks from this vulnerable location.

Be Aware of Internal Risks for Corporate Clients

Check tampering often tends to affect corporate or business clients more than individuals. Make sure customers with business accounts are aware of the risk of internal fraud, and consider urging them to implement the following safeguards:

- Limit access to checks to certain employees.
- Have a clear chain of custody for checks from the time they are written until they are signed and dispatched.
- Keep vendor lists up to date to ensure no one is issuing checks to fake vendors.

- Destroy voided checks.
- Embrace built-in check security methods such as watermarks or security threads.
- Use electronic payment methods when possible.

Offer Positive Pay to Your Customers

Perfect for corporate customers, positive pay allows your customers to submit a list of the checks they issue every month or statement period. Then, special software automatically compares incoming checks with the amounts and payees specified by your customers. When aberrations pop up, the positive pay software alerts you so that you can manually review the check and reach out to your customer as needed.

Consider Using Security Seals

You may also want to offer business account holders the technology to print security seals on their checks. With SENTRY: Seal, your customers can print a seal or barcode onto their checks, which contains all the information (amount, payee name, date, etc.) from the check. When your financial institution accepts the check, SENTRY: Seal compares the information encoded into the seal or barcode with the details written on the check and notifies you of discrepancies.

Urge Account Holders to Report Stolen Checks

Let both your business and personal account holders know about the importance of reporting stolen checks. Then, whether they lose a few check blanks or a whole box of checks, you can issue a stop payment on all the checks in that series. Similarly, if your customers write out a check to someone who loses it, they should always be proactive about reporting the missing check so that no one finds it, alters it, and cashes it.

To encourage customers to make these reports, you may want to offer to stop a certain number of checks for free every year. That way, your customers don’t avoid making a report because they don’t want to pay the stop check fee.

Use Automated Check Image Analysis Tools

Unfortunately, even if your tellers are extremely well trained and have a keen eye for fraud, they are going to miss some altered checks. To minimize your losses, you should consider investing in check fraud analysis tools. Products such as SENTRY: Inspect and SENTRY: Content automatically look over the stock elements and content on on-us checks, and they detect minute issues that are not perceptible to the human eye alone. Then, these products present suspicious checks in a workflow application so that your employees can make a decision manually.

HOW TO SPOT A FORGED CHECK

Before cashing or accepting a check, your tellers should look it over using the Z-method. That means they should review the details on the check from the top left corner to the bottom right corner, looking for issues or errors with the check issuer, distorted images, incorrect dates, out-of-sequence check numbers, discrepancies between the written and numerical values, and the routing and account numbers at the base of the check. But, when they get to the signature, what should they look for? To spot forged checks, keep these tips in mind.

Ask for ID

When cashing a check for a customer, you should always ask for identification. Even if the records show that a customer comes to that branch often, your teller should still ask to see their ID. If you deposit the check and give the recipient cash but find out later that a stranger actually forged your customer's signature on the endorsement line, you will be responsible for the loss. Typically, by the time forged endorsements are found, the scam artist is long gone.

Look for the Criminal Tremor

The criminal tremor refers to the shaky writing of most forgeries. If you are depositing a check for a client and you see the hint of a tremor in the signature line, you may want to stop and take some extra steps to verify the check. In these cases, you usually won't be held liable for the check, but if it's a forgery, the owner of the account on which the check was drawn will probably issue a stop payment on the check. At that point, you will need to reverse the amount that has been credited to your customer's account. If that account falls negative and the customer can't rectify the situation, you may end up with a loss.

Be Cautious of Stamped Signatures on Personal Checks

Businesses have used stamped signatures for decades, but most personal checks are not signed with a stamp. If your customer is depositing a personal check, you may want to start by asking them if they were expecting the check. This simple question encourages customers to tell you if they received the check unexpectedly from a stranger online, and if so, you can dig deeper to help the customer figure out if the check is fraudulent.

On top of that, feel the signature. If it's been written with a pen, it should have some texture. In contrast, stamps are usually smooth. Then, look at the signature with a magnifying glass. With stamps, you usually see more ink on the edges than you do with a written signature. Additionally, most stamp ink appears to have a slightly purple hue. Written signatures tend to have tunnels or ridges running through the ink. You don't get that with stamps, autopens, or signing machines which may all be used in scams which involve forging a high number of checks.

Hold the Signature Up to the Light

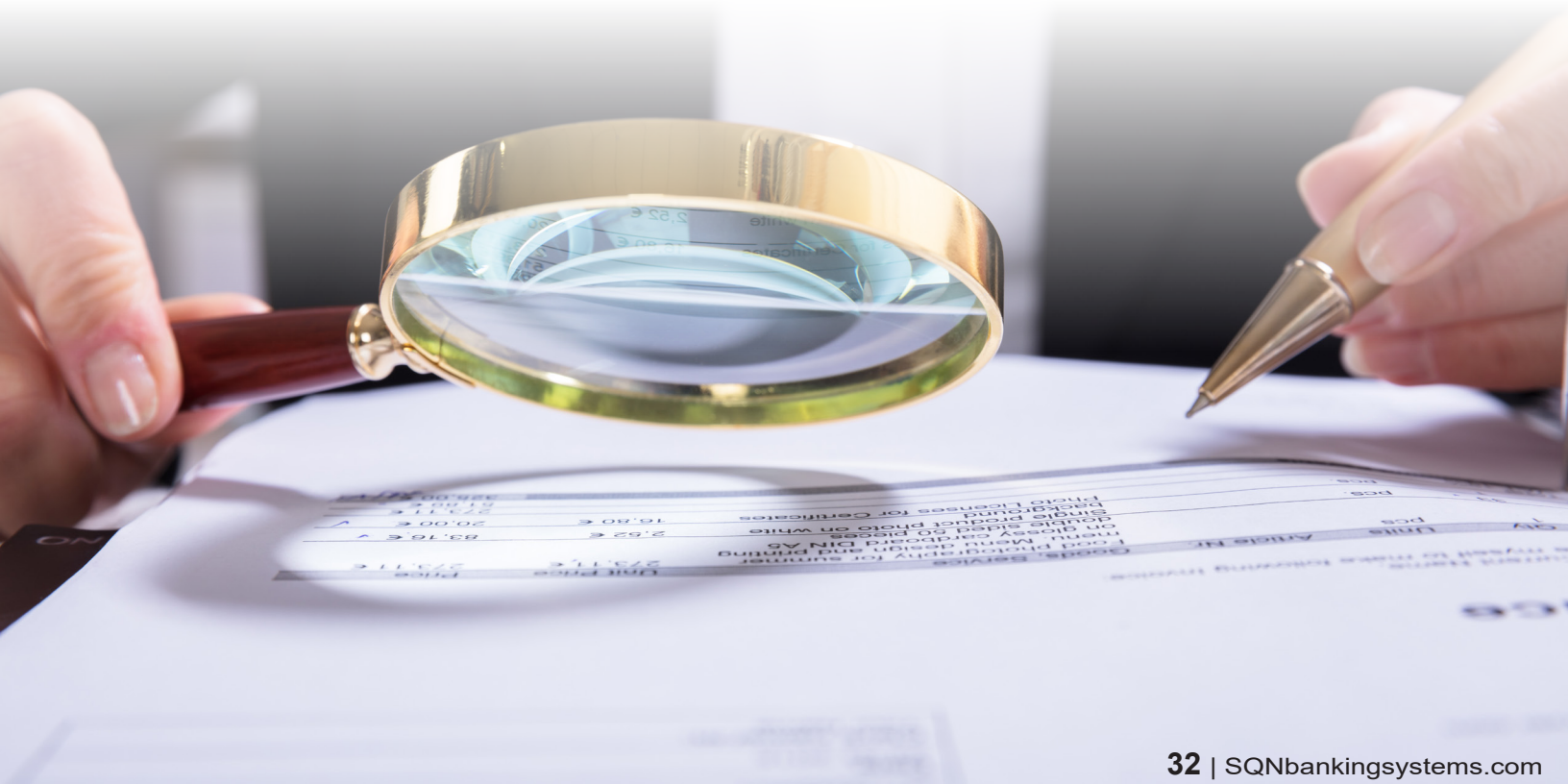
Looking at the signature in the light can also give you clues as to whether or not it's a forgery. Usually, very faint or equal amounts of pressure throughout the signature indicate that it's a fake. Typically, people write their own signatures very deliberately (which makes them not appear faint), and most people use a variety of different pressure levels when signing their name. For instance, they may put more pressure on downward strokes and less on the tails of letters.

Compare with the Signature on File

If the check has been written from your bank, you can compare the signature on the check to the signature on file. Tools such as SENTRY: SigTab make it easy to capture your customer's signatures and store them in a database where they can be found easily. As needed, you can simply pull up the signature and make sure it matches.

Invest in Signature Verification Tools

The above tips can help you spot forgeries in your financial institution, but you probably process a lot of checks electronically. To help with that process, consider investing in automated signature verification tools. SENTRY: SigCheck can identify fraudulent signatures on on-us checks. Then, the software can display the reference signature in the workflow so that your tellers can compare the signatures and decide whether or not to approve the check



WHAT ARE COUNTERFEIT CHECKS?

Counterfeit checks include any checks that have been created fraudulently with the purpose of stealing money from someone. This category can include fake cashier's checks, money orders, personal checks, and business checks. In some cases, all the information on the check is fake, but in other situations, scam artists create counterfeit checks using real account and routing numbers.

What Are the Signs of a Counterfeit Check?

Several different elements can indicate that a check is counterfeit. Some of the most common red flags include the following:

- Unusual check amounts — particularly, checks written for over the purchase price or over the amount needed by the depositor
- Often under $5,000 to avoid longer hold times
- Inaccurate account holder details such as fake business names or addresses
- Checks written for "cash" instead of to a payee name
- No bank logo or address on the check
- Faded bank logo, which can mean the check was copied from an original
- Fraudulent bank name or address, especially on cashier's checks
- Absence of security features such as watermarks or security threads
- Misspellings
- Shiny MICR numbers, whereas real MICR ink tends to look dull
- No routing number or routing numbers without nine digits
- Smooth edges on personal checks, indicating they were printed from a home computer
- Missing signatures
- Stains or gaps around signatures, which often means the signature was copied onto the check
- Up and down pen strokes associated with forged signatures

How Can Customers Protect Themselves Against Counterfeit Checks?

Your first line of defense in fighting fraud is to educate your customers. Let customers know about the most common scams involving counterfeit checks and give them tips on how to avoid these scams. You may want to create unique educational materials for your individual and business clients as they face slightly different risks. For example, individuals may be more likely to be targeted by thieves running a foreign lottery scam, while business customers may be more susceptible to internal fraud related to counterfeit checks.

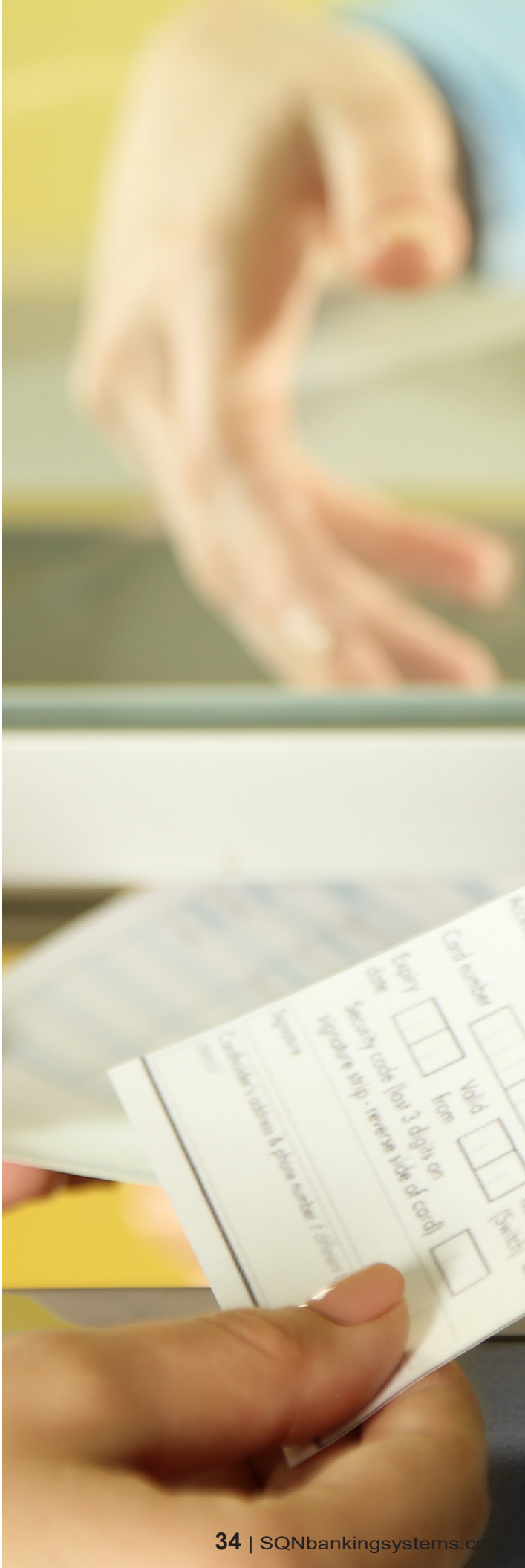
How Can You Protect Your Financial Institution from Counterfeit Checks?

Your tellers should be aware of the telltale signs of counterfeit checks. They should alert a manager or another appointed person when they suspect a customer is trying to deposit a counterfeit check, and when accepting large checks, they should ask customers if they know and trust the check writer.

Ideally, you should automate as much of this process as possible. The right products can scan on-us checks and look for issues with stock elements or check content, that is not perceptible to the human eye. When issues are detected, these tools display the suspicious check in a workflow application next to other details such as saved signatures that guide your staff as they manually decide if a check has a risk of being counterfeit or not.

Real-time fraud protection tools that look for aberrations in spending and deposit patterns can also be extremely useful, especially in the detection of counterfeit cashier's checks written for large amounts.

Unfortunately, financial institutions must make the funds available from deposits relatively quickly. Typically, funds drawn on U.S. Treasury checks, most government checks, cashier's checks, certified checks, and teller's checks must be available the next business day, and without fraud detection tools in place, that means the funds can be quickly spent before you find out whether or not the check is counterfeit.



CHECK FRAUD PENALTIES

Depending on several factors, fraud may be punished by the state or federal authorities, and because fraud varies so much, the punishments and penalties can also vary significantly. Here's a look at some of the most common penalties for check fraud.

Incarceration

For misdemeanor fraud, perpetrators may face up to a year in a local jail, and felonies may result in several years in jail. One man received 20 years in federal prison for felony check fraud related to writing $195,345 in bad checks to businesses in Sacramento County, but his sentence was increased due to prior convictions.

In other cases, perpetrators can face even longer sentences. For instance, a former Vanguard employee stole over $2 million by writing checks from inactive or dead account holders. His charges include mail fraud, money laundering, and falsifying tax returns, and although his has not been sentenced at the time of writing, his prison sentence may be up to 46 years.

Probation

In some cases, check fraud perpetrators are sentenced to probation. This may be on top of a jail sentence. Often, probation is used in lieu of a long jail sentence. For instance, when one man forged two $5,000 checks from his great grandfather's account, he received a 45-day sentence in the county jail followed by 13 months of probation.

During probation, perpetrators can walk free, but they have numerous restrictions on their freedom. Typically, they must meet with a parole officer at certain times. They may also have to submit to drug tests and of course, not commit any other crimes.

Fines

Like other check fraud penalties, fines also vary widely. Criminals may face hundreds or thousands of dollars in fines for misdemeanor fraud convictions, but for felonies, the fines may be $10,000 or more. For wire fraud, fines can be up to $250,000.

Edward Rostohar, the former CEO of CBS Employees Federal Credit Union, stole over $40 million from his employer over two decades. Because he was familiar with examiner auditor activities, he was able to avoid detection for over two decades. During that time, he made online payments to himself and forged another employee's signature on checks made out to himself. As of April 2019, he has not been sentenced yet, but his fine alone may be up to $1 million.

Restitution

To make amends to victims and to cover losses suffered by financial institutions, many check fraud perpetrators must pay restitution. Typically, restitution is close to the amount of losses suffered. In other cases, restitution may include additional amounts to cover the victim's legal expenses or as part of a civil penalty.

THE DANGERS OF FLOATING CHECKS

Floating a check may seem harmless; after all, check floaters may know they will have the money in their account within a couple of days. They may think that their actions can't hurt anything. Although that may be true in some cases, floating a check can be costly for consumers and dangerous for banks.

What is 'Floating a Check'?

Floating a check is when a customer takes advantage of the float to buy a bit of time on a bad check. For example, an account holder might write a check at the grocery store the day before payday. They give the check to the grocery store on Thursday. The grocery store deposits the check in its bank on Thursday evening, and by the time the grocery store's bank remits the check to the shopper's account, their direct deposit paycheck has already credited, ensuring they have enough funds to cover the check.

Customer Costs for Floating Checks

Ideally, accountholders should never spend money that isn't in their account. To continue with the above scenario, what happens if their paycheck doesn't get deposited for some reason? At that point, their bank may return the check from the grocery store and assess an insufficient funds fee on their account.

Typically, the grocery store presents the check to the bank again, sometimes adding an additional merchant fee, and if there still aren't funds in the account, the bank may return the check and assess another fee, drawing the account even further into the red. At this point, the customer has amassed two insufficient funds fees and a fee from the grocery store plus any additional fees for direct debits, automatic payments, or any other expenses that have hit their account.

In another scenario, the paycheck may get credited at the right time, but the account holder may begin to make floating a habit. Initially, they just need extra money the day before payday, but one week, they need the funds two days earlier, then three days, and so on. Eventually, they need the funds so soon that they decide to open another account and begin kiting checks back and forth. These activities can put banks at risk.

Risks to Financial Institutions for Floating Checks

Financial institutions can make some money by charging overdraft or insufficient funds fees on bad checks, but those relatively small amounts do little to mitigate a bank's overall risk. When dealing with overdrafts, banks incur communication costs for reaching out to customers, but even more significantly, they may be stuck with losses and potentially face legal fees as they try to recoup their funds.

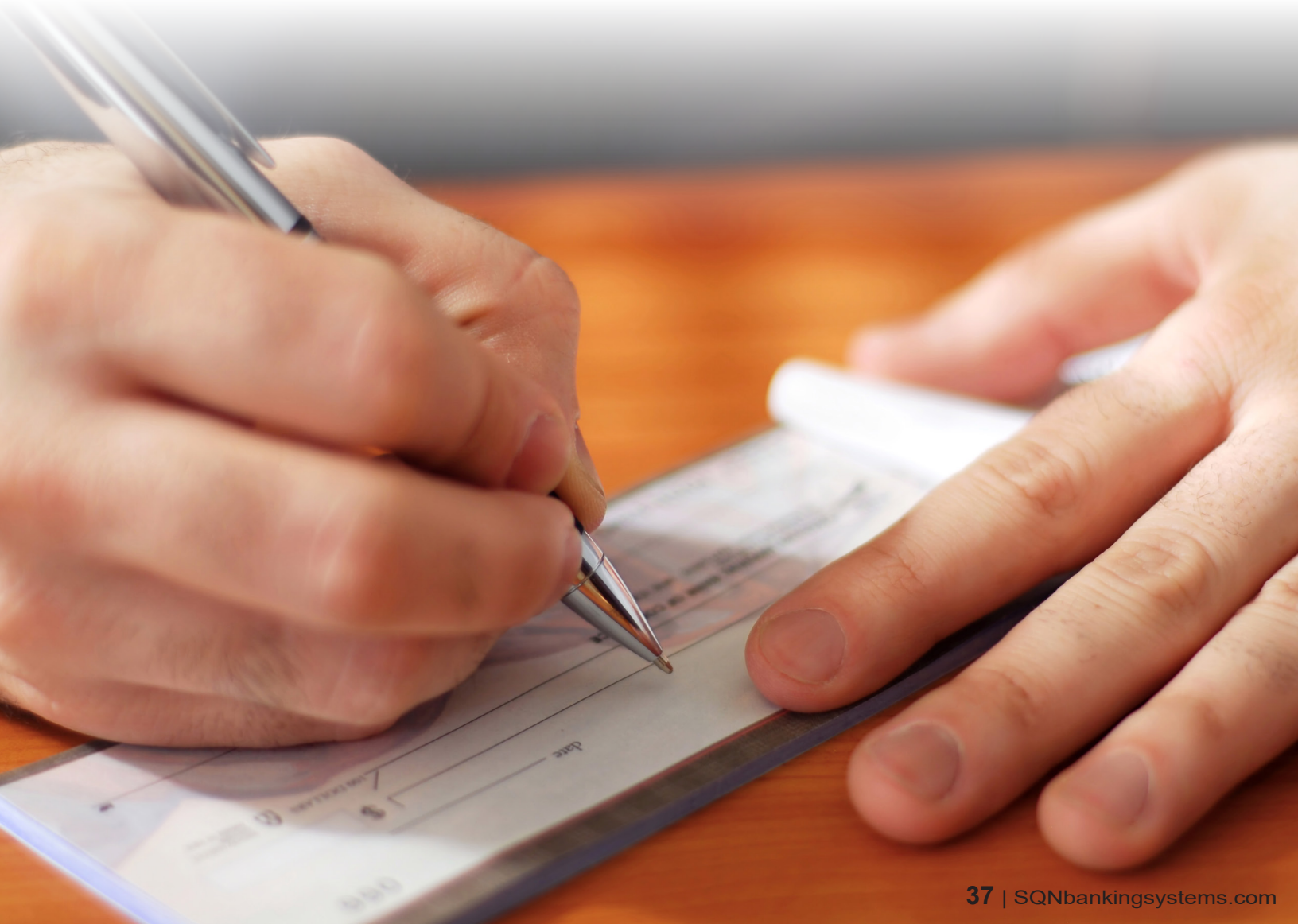
In some cases, banks have lost millions of dollars and threatened their solvency due to bad checks. For instance, a $911 million-asset bank in Kansas with $4.6 million in net income over six months lost $5 million due to an overdraft situation created by cashing third-party checks drawn on an account with insufficient funds. A $147.8 million-asset bank in New Jersey had a $2.1 million loss, and a $31 billion-asset financial group suffered a $9 million loss related to an undetected kiting scheme.

Small banks are hit disproportionally by these losses. Scammers may be wary of floating checks or performing other types of fraud at big banks because they know these financial institutions are more likely to have safeguards in place to detect fraud. Because of that, they often target small banks which may not have the capital available to recover from these types of losses.

How to Reduce Check Floats

To minimize the impact of check floating, educate your customers about the dangers of floating checks. Let them know how floating checks can cost them money, threaten their credit, and potentially even force you to close their account. To reduce the burden of fees on customers, some banks are offering overdraft forgiveness programs where customers don't face overdraft fees on items submitted the day before a direct deposit hits the account. When dabbling with programs like that, it's important to make sure you are offering a convenience to customers without encouraging them to float checks.

Beyond that, you need tools in place that can help you identify troubling patterns. Then, when an account holder is flagged, you can manually review their transactions, reach out to them with issues, and proactively close their account if needed.



CHECK FRAUD GLOSSARY

There are numerous words and terms associated with check fraud. To gain an understanding of the essential phrases, here's a check fraud glossary.

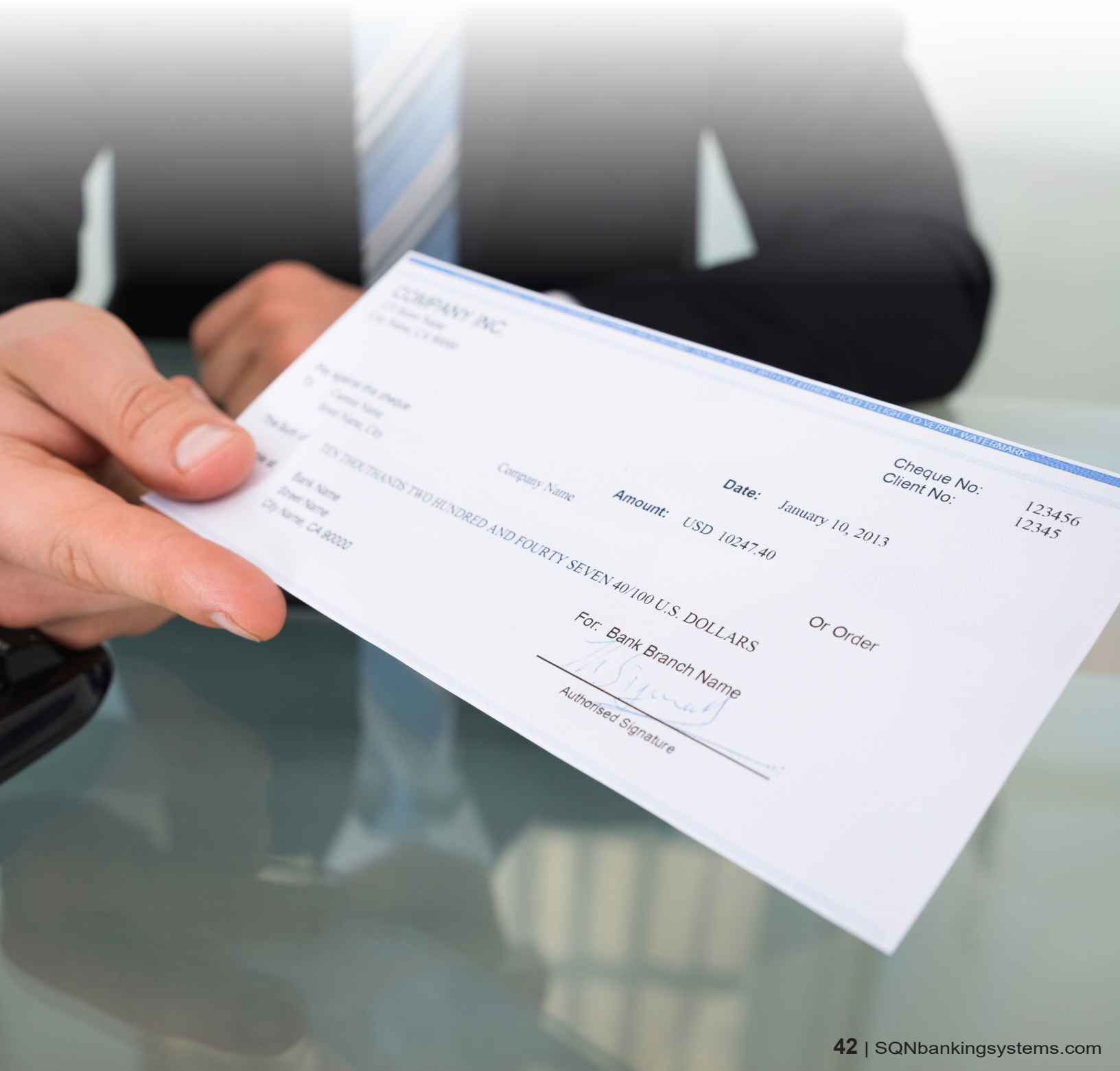
- **ACH Checks** — Electronic payments made through the Automatic Clearing House Network, including direct deposit and automatic bill payment.
- **Account Takeover** — Scam artists take over someone's checking account by faking their identity at a branch or accessing their online account. Then, they direct all correspondence to their own address and freely spend the money from the account, including writing fraudulent checks.
- **Automatic Clearing House (ACH) Network** — Run by the National Automated Clearing House Association, the ACH Network is a funds transfer system that helps financial institutions process transactions such as direct deposits, tax refunds, consumer bills, checks, and more. A financial institution takes all its ACH transactions and sends them to the Federal Reserve or a clearing house. Then, the ACH Network sorts the batch of transactions and sends the money to the financial institution of the intended recipient.
- **Bad Check** — A check written on an account that doesn't have sufficient funds to cover the amount. Account holders may write these checks purposefully or by mistake.
- **Billing Schemes** — A scam artist sends fake invoices to a company or individual and demands payment. Often, employees perpetrate billing schemes by drafting checks from their employer's business to a fictitious company, and they cover up the trail by creating fake profiles in their accounts payable database.
- **Bounced Check** — A bad check that is returned, or "bounced", by the bank back to the check recipient. At that point, the recipient can resubmit the check to the bank, or they can attempt to collect the funds from the check writer on their own.
- **Check 21** — Short for the Check Clearing for the 21st Century Act.
- **Check Alteration** — When scam artists alter the information on a check by changing the payee, the amount, or other details.
- **Check Clearing for the 21st Century Act** — Signed into law in 2004, the Check Clearing for the 21st Century Act sped up check processing time by allowing banks to use substitute checks to process checks electronically. Prior to the implementation of this law, banks had to physically transfer paper checks, and they also sent copies of cashed paper checks to their customers.
- **Check Content Analysis Tools** — Special software that analyzes the content on a check. Check content includes items added to the check such as amount, payee, and signatures.
- **Check Forgery** — Check forgery refers to any situation where someone forges a signature on a check.

- **Check Fraud** — Check fraud is any attempt to commit fraud using a check, including writing bad checks, forging checks, running billing schemes, and countless other fraud attempts.
- **Check Kiting** — Check kiting essentially uses bad checks as a form of credit. Typically involving two or more accounts, kiting schemes deposit bad checks in one account to make the account balance appear positive. Then, they may move money back and forth between the accounts to keep the balances artificially inflated. Sometimes, kiting schemes are used to buy a few days before payday. In other cases, they are elaborate frauds involving millions of dollars.
- **Check Overpayment Scams** — In these scams, the thief finds someone who is selling something. They provide a check for more than the amount of the sale price, and they request change. Then, they leave with the cash and the sale item, and when the victim deposits the check, they learn that it is counterfeit.
- **Check Stock Analysis Tools** — Special software that analyzes the stock information on a check such as account holder details, layout, font, and similar information.
- **Check Tampering** — Typically a type of internal fraud, check tampering is when employees tamper with the details on a check drawn on their employer's account. They may change the amount of a check written out to them, erase the payee's name and put in their own, or change other details.
- **Check Theft** — Check theft is any situation where someone steals a check. They may steal a check for alteration, or they may steal an entire check book to make purchases or write checks to themselves.
- **ChexSystems** — Owned by eFunds, a subsidiary of the Fidelity National Information Services, ChexSystems is a consumer credit reporting agency that focuses on consumer misuse of checking accounts. The agency tracks people who have a history of writing bad checks or bouncing checks and assigns them a rating of 100 to 899. Banks use ChexSystems to help them evaluate new customers.
- **Civil Penalties** — A civil penalty is a fine that check fraud perpetrators may be ordered to pay to provide restitution to their victims for the losses they caused.
- **Clearing House** — A place where checks and bills from member banks are exchanged. When a customer at Bank A deposits a check from Bank B, Bank A uses a clearing house to get the funds from Bank B.
- **Counterfeit Check** — A fake check, often used in a scam.
- **Digital Checks** — Electronic payment orders that work as a substitute for paper checks. Often with apps or special software, consumers can send digital checks to someone using just the recipient's email address.
- **eChecks** — An electronic alternative to a paper check.

- **Expedited Funds Availability Act** — Abbreviated as EFA or EFAA, the Expedited Funds Availability Act was signed into law in 1987. This act outlines how long banks can hold checks before making the funds available. Hold periods vary based on the amount of the check, the age or the account, and several exception categories such as frequent overdrafts or other issues.
- **Fair Credit Reporting Act (FCRA)** — Sometimes called the Consumer Credit Protection Act, the FCRA legislates how consumer reporting agencies, such as ChexSystems, must deal with consumer information to reduce inaccuracies or privacy breaches.
- **Federal Deposit Insurance Corporation** — Created by the 1933 Banking Act in the midst of the Great Depression, the FDIC insures deposits at member banks up to certain threshold.
- **Fines** — When someone is convicted of check fraud, they may face fines. Depending on the extent of the fraud, fines can range from a few hundred dollars to a million dollars in extreme cases.
- **Float** — The length of time between when a check is written and when the funds are taken from the account.
- **Forged Check** — A check with a forged signature or a forged endorsement.
- **Forged Maker Schemes** — When an employee forges an authorized signature on a business check and misappropriated the funds to themselves or a co-conspirator.
- **Forged Signature** — Falsely replicating the signature of an account holder or an authorized signer on a check.
- **Forged Endorsement** — When someone falsifies a check recipient's name on the endorsement line in order to illegally cash a check.
- **Hold** — When a bank holds deposited funds before making them available to the account holder.
- **Identity Theft Check Fraud** — When a fraudster steals someone's identity and opens an account in their name in an attempt to write bad checks or steal funds in other ways.
- **Insufficient Funds Fee (NSF)** — The fees banks charge when they receive a check from an account that has insufficient funds to cover the check.
- **Lottery Scam** — In the lottery scam, victims receive notification that they have won a lottery. They receive a check for their winnings and are instructed to pay taxes or fees. By the time, they realize the lottery check is bad, they have already dispatched the funds for the fees or taxes, and they lose that money.
- **Magnetic Ink Character Recognition (MICR)** — MICR is a special type of ink often used on checks or other documents. It is sensitive to magnetic fields and helps to facilitate electronic processing for checks in the middle of the 20th century.

- **Micro-Printing** — Check security feature that prints extremely small letters or other details onto a check. The microprint can't be seen by the human eye, but software can detect if the details are correct or not.
- **Money Order Fraud** — When perpetrators use money orders to commit fraud on victims.
- **NSF Check** — A bad check that creates an insufficient funds fee for a consumer.
- **Official Check Verification Tools** — Special tools that print secure seals or barcodes onto checks. When the checks are presented for payment, the bank uses special software to read the barcode and make sure the information on the check matches the info embedded in the barcode.
- **On-Us Checks** — A check presented to the check writer's bank.
- **Originating Depository Financial Institution (ODFI)** — The entity that initiates an ACH transfer.
- **Federal Reserve** — The central bank of the United States.
- **Overdraft** — When a bad check or draft draws an account over its available balance.
- **Overdraft Protection** — A product offered by many banks that ensures checks and debit transactions are not returned, even if the balance is insufficient to cover the draft. Typically, banks assess a fee for accepting these transactions.
- **Paper Checks** — A traditional paper check.
- **Paper Hanging** — Writing bad checks from closed accounts.
- **Positive Pay Software** — This check fraud protection tool allows business customers to provide a list of authorized checks to their bank. Then, when the bank receives a check written from that customer's account, special software makes sure the check has been authorized.
- **Real-Time Fraud Analysis Tools** — Software that analyzes checks, deposits, and other transactions in real time and alerts bankers of potentially fraudulent activity.
- **Receiving Depository Financial Institution (RDFI)** — The entity that receives the funds from a clearing house transaction.
- **Regulation CC** — The rules for the availability of funds and collection of checks.
- **Returned Check** — When a bank returns a check to the bank that submitted the payment. Also called an NSF check or a bounced check.
- **Restitution** — In some check fraud cases, thieves are required to pay restitution to their victims to replace the stolen funds.
- **Rubber Check** — Another name for a bounced check or an NSF check.
- **Stopped Payment** — If an account holder loses a check or changes their mind about a payment, they can issue a stop payment.

- **Ultraviolet Check Image Analysis** — Tools that look at ultraviolet ink used on checks to detect chemical alteration or other issues.
- **Washing** — Washing is when a thief washes the chemicals off a check to change its details.
- **Watermarks** — A faint design printed onto a traditional paper check and used to verify that the check is real.



CONCLUSION

Financial institutions need tools and protocols in place to spot fraudulent checks. Bank tellers need to be trained how to look out for check fraud, but ideally, you also need software that can automatically inspect on-us checks and look for aberrations that suggest forgeries, counterfeit checks, or alterations.

However, with every advancement in technology, scam artists adapt their techniques and find new ways to commit fraud. To protect your financial institution, you need a fraud protection partner that is nimble and flexible.

Knowledge and training are key to avoiding fraud, but you also need the right tools in place. At SQN Banking Systems, we help our clients automate fraud detection so that they can save time, reduce labor, and minimize fraud. Let us help you protect your reputation and your bottom line.

ABOUT

The acronym “SQN” stands for the Latin phrase “sine qua non.” The literal translation is “without which not,” meaning something indispensable or essential. In our business, we feel that fraud prevention, fraud protection and overcoming fraud loss is indispensable in the finance industry. Systems and workflows that provide protections and methods for prevention are essential in today’s high tech, and ever-changing business environment: signature verification, check fraud detection, mobile capture, and other verification systems.

SQN Banking Systems’ history began in 1983, when we revolutionized check fraud detection with the introduction of the first PC-based signature check verification system. Since then, needs have changed and SQN Banking Systems has changed with them. We have developed a comprehensive line of fraud protection software products crucial to overcoming the growing problem of fraud losses. And in an increasingly competitive banking world, we are helping our clients stay ahead of the curve with exceptionally efficient process improvement software. But we remain as committed to the high standards and innovative spirit when we built our first check verification software over three decades ago. We continue to further our fraud protection knowledge and methods to prevent against crimes as old as check fraud or as new as mobile fraud for the most secure transactions possible.

SQN Banking Systems delivers innovative check fraud solutions that serve a range of financial institutions from large, to mid-tier and community banks making them more competitive and more profitable. We offer on-premise applications and hosted solutions for fraud protection and signature verification. Browse our site to learn more about how SQN Banking Systems’ history and experience can assist your bank in detecting check, credit card and mobile fraud with our range of systems and services including image fraud analysis, signature verification, transaction fraud analysis, official check verification, mobile signature capture, safe deposit management and conversion services. Discover what each of these innovative programs can do for you, and how they can ultimately pay for themselves – often within six months.

SQN Banking Systems

888-744-7226

EAST COAST OFFICE

SQN Banking Systems

65 Indel Ave, PO Box 423

Rancocas, NJ 08073

WEST COAST OFFICE

SQN Banking Systems

22048 Sherman Way, Suite # 310

Canoga Park, CA 91303