Don't Cash That Check: BBB Study Shows How Fake Check Scams Bait Consumers

BBB International Investigations Initiative

BBB Chicago bbbinfo@chicago.bbb.org
BBB Dallas info@nctx.bbb.org
BBB Omaha info@bbbinc.org
BBB San Francisco info@bbbemail.org
BBB St. Louis bbb@stlouisbbb.org

BBB International Investigations Specialist

C. Steven Baker stbaker@bbbinc.org

Issued: September 2018

Better Business Bureau®

If someone calls and asks for money, you might be skeptical. But what if the person sends you a check in advance, you cash the check, and your bank tells you that money is in your account? Sounds like a safe deal, especially if it is a cashier's check, which is as good as gold. Right? Wrong. Here's what crooks know, but you may not: even when a check is credited to your account, it does not mean the check is good. A week or so later, if the check bounces, the bank will want the money back. And you, not the fraudsters, will be on the hook for the funds.

It happens to tens of thousands of people every year. "Buyers" send a check for more than the full price to sellers of cars or other items on Craigslist and other online classifieds sites. "Employers" send a check to "new hires" to buy supplies needed to do the job from home. Sweepstakes or lottery "winners" are given a check to pay taxes so the award can be delivered.

All of these are scams involving counterfeit checks which are often altered versions of business checks from real companies.

Fake check fraud is a huge problem, with complaints to government agencies and consumer advocacy groups doubling over the last three years. Millions of fake checks worth billions of dollars circulate every year.

"Fake check fraud is an exploding epidemic," says Elaine Dodd, Executive Vice President of the Oklahoma Bankers Association. "More education and enforcement to stem this problem are clearly needed."
This study by Better Business Bureau (BBB) details the wide variety of frauds that employ fake checks.

Here are two things BBB wants you to know and tell your friends about fake check fraud

1. Having the funds credited to a bank account does not mean the cashed check is valid.
   Federal banking rules require that when someone deposits a check into an account, the bank must make the funds available right away – within a day or two. But the bank also has the right to recover the money from the account holder if the check is counterfeit. It is only when the check works its way back to the bank that supposedly issued the check that it is discovered to be counterfeit.

2. Cashier's checks and postal money orders can be forged. A cashier's check is a check guaranteed by a bank, drawn on the bank's own funds and signed by a cashier. Cashier's checks are treated as guaranteed funds because the bank itself, rather than the individual account holder, is responsible for paying the amount of the check. Cashier's checks are commonly required for real estate and brokerage transactions. If a person deposits a cashier's check, the person's bank must credit the account by at least $5000 the next day. The same holds true for postal money orders.

What are fake checks?

Fake checks are simply counterfeited checks, usually copies of business checks from real companies. Three different types of financial documents are commonly involved in fake check frauds: **regular checks, cashier's checks, and money orders.** Some appear to be created in the U.S. and Canada, but many are shipped in from overseas and then sent to victims.

- The regular **fake check** purports to be from a business, and usually contains a real account and routing number. These are not handwritten, and they look quite professional. The name of the business will appear on the check, and they often include a phone number as well.
- **Fake Cashier's checks** look like they are from a bank or financial institution. A genuine cashier's check is a check guaranteed by a bank, drawn on the bank's own funds and signed by a cashier. Cashier's checks are treated as guaranteed funds because the bank itself, rather than an individual, is responsible for paying the check amount. These are commonly required for real estate and brokerage transactions.
  Most financial institutions have seen counterfeit cashier's checks using their information. **The Office of Comptroller of the Currency** has issued an alert about fake cashier's checks.
- **Money orders** are issued by banks and the United States Postal Service. These are effectively a cash substitute. Money orders can be cashed at a bank and postal money orders at a post office. They are printed on special paper with watermarks to make them difficult to counterfeit. **The Postal Service has issued an alert** on how to detect a fake money order or a money order scam.

Fake checks are used in a variety of frauds such as mystery shopper or nanny "jobs", as well as prize and sweepstakes scams. What the scams have in common is that victims have to send money to the fraudsters. After depositing the check, victims are asked to quickly wire money or buy gift cards that eventually make their way to the fraudsters before the checks bounce.

Regardless of the format, the checks usually look professional and convincing. Fraudsters have been known to obtain the names and account information of legitimate businesses by fishing inside mailboxes with sticky tape or even stealing entire mailboxes off the street, hoping to find business checks inside. Crooks then scan and Photoshop checks.

High quality check stock is easy to obtain. Fraudsters often replace the phone number on the check with a number they can answer if someone calls the "business" to see if the check is legitimate. To test the actual validity of

Details in this example are fictitious

ELEMENTS OF A FAKE CHECK

Is the company name or address misspelled?

Does the check number match the check number included in the line at the bottom of the check?

Is the check stock flimsy or suspicious?

Does the check have the correct routing number at the bottom for the bank it is supposedly drawn on? Consumers can google routing numbers now.

Is the check missing the special ink for the MICR code at the bottom?

If the check is for lottery winnings, why is it written from a company and not the state lottery commission?

a check, consumers should not call a phone number printed on the check but should instead look up the telephone number for the supposed source of the check and call directly to see if it is real.

Relevant check laws

Under both Canadian and U.S. federal banking laws, when someone deposits a check, the bank generally must make funds available in day or two, although there are exceptions. For cashier's checks, a bank must make the funds available within 24 hours if the check is for less than $5,000. In practice, banks usually credit accounts right away. If the check is suspicious, however, they may put a hold on it.

Crediting the account does not mean that the check is valid. If the check is written on an account from another bank, and most fake checks are, the check must go from the bank where it is deposited through a clearinghouse, normally operated by the Federal Reserve Board, then back to the bank which has the account the check is written on. Only then can anyone in the banking system establish whether the check is legitimate. Although this system is now more likely to be automated, it can still take two weeks or more before anyone can determine if the check is valid – whether it was actually signed and issued by the bank or business that has its name on the check.

Who are fake check fraud victims?

Young people. Fake check frauds affect victims of all ages and income levels. However, the Federal Trade Commission's Consumer Sentinel complaint database shows that the biggest age range for victims are those between 20 and 29 years old, at 21 percent of the total. By contrast, less than 10 percent of the victims were 70 or older.

FAKE CHECK VICTIMS

From Consumer Sentinel 2015-2017

Age Range	No. of Victims
13 - 17	583
18 - 19	1578
20 - 29	8977
30 - 39	7449
40 - 49	6724
50 - 59	7703
60 - 69	5783
70 - 79	2506
80 +	1087

The results are consistent with the findings of BBB in its study **Cracking the Invulnerability Illusion**, which found

that millennials are most likely to be victims of fraud.

Small businesses. Check frauds affect not only individual consumers, but small businesses as well. The American Bankers Association survey for 2016 found that bank losses from small business accounts increased to 22 percent for fake check fraud, up from 14 percent from two years before.

Lawyers. Some sizable law firms have lost hundreds of thousands of dollars to collection fraud. The attorney deposits a fake check from the client's "debtor", deducts their legal fee and use a bank-to-bank wire transfer to send the remaining money to the supposed client. It is the rare lawyer who has not come into contact with this fraud. Fraudsters may even do careful research on the lawyer or law firm to make the solicitation appear as legitimate as possible.

Banks. Those depositing fake checks are responsible for losses when the checks are found to be counterfeit. Banks can take funds from victims' bank accounts or take collection action if they do not have enough to cover the losses. When victims don't have the money to cover fraudulent deposits, banks may end up absorbing the losses. FDIC insurance does not cover losses due to theft or fraud.

If a check is fraudulent, the company that has its name on the check is not liable as long as it has no knowledge of the fraud.

The person who deposited the fake check is responsible for returning money to the bank that made the money available to the depositor. This is explained in the Deposit Account Agreement people sign when they open a bank account. Of course, victims have a right to sue those who defrauded them, but fraudsters are often difficult to find.

Stories from victims of fake check fraud

A St. Louis college student, Isayas, was looking for a part time job online, and found an offer to hire him as a

mystery shopper. He took the job, and received a very professional-looking letter outlining his tasks.

Isayas got a cashier's check in the mail written on a credit union in California for $1,987.22. He deposited the check in his bank, and the following day the money was credited to his bank account. He was told to go to McDonald's, Subway or Starbucks, have a meal, and complete an evaluation form. Then he was to go to WalMart and send money twice to addresses in Seattle and Tacoma, Washington. He withdrew cash from his account and sent $885 to the two addresses specified, filled out the evaluation form, and sent it back.

Then the bank informed him that the check was no good and wanted the money returned. His family helped him to set up a payment plan with his bank. They then reported the fraud to the police and to BBB.

Kathy, from the Chicago suburbs, was contacted on LinkedIn by someone impersonating a competitor of her employer. Kathy had heard very good things about this company, so she was excited. The person she was dealing with used the name of the real head of HR at the company. In addition, the email she got looked very professional, and the email address looked like it was from the company.

Kathy interviewed over a chat feature and was offered a job. She was told that she would need to buy office supplies, a laptop, a printer, and other items needed for the work.

The impersonator emailed several checks to Kathy so she could buy these items from the "company's vendor" in Huntington, West Virginia. Kathy printed the checks and deposited them into her bank. Kathy says she waited until her bank told her the checks had cleared, and then sent several payments to the "vendor" through Western Union. She sent about $2,000 in all.

After that Kathy's bank completely froze her account – for three months. The checks did not have the correct routing number for the company for which she believed she was working Kathy reached out and tried to contact the real company, but never heard back.

Kathy reported this to the police and BBB. She never received the supplies she had sent money for, and never heard any more about the supposed job. Kathy was surprised by the level of detail the crooks were able to provide, and urges people to be extra cautious, especially if a check is involved. She advises people to never take a job found online without meeting the employer in person.

Pam is a 71 year old retired nurse near Dallas, Texas. In May 2018 she received a phone call from "Mike Lowry" telling her she had won $2.5 million in the Mega Millions lottery. Pam thought about how useful the money could be. She hoped to pay off bills and help some neighbors that were short of money.

She received a check in the mail for $5,000, and was told that she needed to send part of that money to pay for expenses for her winnings.

She deposited the check, and the bank credited her checking account. Pam first bought a $2,500 money order, as directed, and mailed it to an address in St. Petersburg, Florida. She also went to Western Union and sent another $1,300 to the same person at the same address.

Several days later, the bank notified her that the check she had deposited was invalid and she needed to pay the bank back. Because she did not have the money, the bank took her Social Security check for partial repayment, and told her it would continue to take her social security checks.

Because Pam's only source of income was social security, this hit her hard. She was unable to make her car payments, and even had to go to a food bank because she could not afford groceries. Her church helped her with her rent so she would not be evicted.

Since then she has received other calls claiming she has won a lottery. When she does she gives them a piece of her mind and hangs up.

Auri, a college student in Oakland, got an email about a job at her college email address. The school often sends along job postings, so this was not unusual. This one was a very-professional looking offer by "Pepsico" to hire her to have her car wrapped with an advertisement for Mountain Dew, promising they would pay her $250 per week to drive it around. Auri took the job in order to get more money to pay her tuition.

Auri received a check in the mail for $4,850. She was told to deposit $4,000 into the bank account of the "car specialist." She deposited the check and was able to withdraw $3,500 the next day, which she then deposited into the account as she had been instructed.

She was able to withdraw another $500 the next day, and she suggested that she could just pay the car wrapping company the cash when the car was wrapped. She got a text message back saying she should go to WalMart and buy a $500 iTunes gift card.

This made no sense to Auri. When she asked why she should buy a gift card, she did not get a straight answer. She realized that this might be a fraud, and called the police and BBB. The bank account she had deposited money into was already closed with the money gone.

Auri's bank wanted the $3,500 back, and she did not have enough in her account to pay it. She arranged a payment plan with the bank, and is still paying off her losses.

She urges others not to trust emails, even if they seem to come from your college, and to do research before getting involved in an online employment offer.

Connor is a college student in Kansas. He saw an ad online offering to pay people monthly if they would have their car wrapped with a beer brand logo. Connor texted the number and received full instructions by text message.

He received a check in the mail for $1,950. Connor went

to Walmart to cash the check. They wouldn't cash it, so he took a photo of the check and deposited it in his account using an app. The bank initially credited his account.

The scammers asked Connor to send money by Western Union to the company that would wrap the car. He refused, because he had heard of fraud involving money sent that way. He offered to pay cash to the company when they arrived to wrap his car. After a few days, Connor's bank withdrew the money from his account.

The scammer got angry when Connor told him that the bank said the check was no good. When Connor told him he was going to file a report with BBB, the scammer threatened to report Connor to the FBI.

Connor was fortunate that he didn't lose any money, but wants others to watch out for this type of fraud.

Common Frauds that employ fake checks

For fraudsters, the possibilities are almost endless in how they exploit people's erroneous belief that having the money credited to a checking account means the check is good.

Mystery Shopper Check Scams

The most common frauds that employ fake checks are mystery or secret shopper frauds. Police and other agencies across the U.S. and Canada routinely issue warnings about this fraud.

Those operating this fraud contact victims, often by mail, offering jobs as mystery shoppers and enclosing fake checks. After receiving a mystery shopping check in the mail, victims are directed to deposit the check into their own checking account, then to mystery shop a retail location, often Walmart. Consumers are told to wire part of the money from the check they received, write up a report on their experience at the store, and keep the "remainder" as their pay. For example, if the fake check is for the sum of $2,500, the victim may be directed to send $2,100 and keep the "remainder" as pay. But the checks are fake, and the victim is simply sending his or her own money to the crooks.

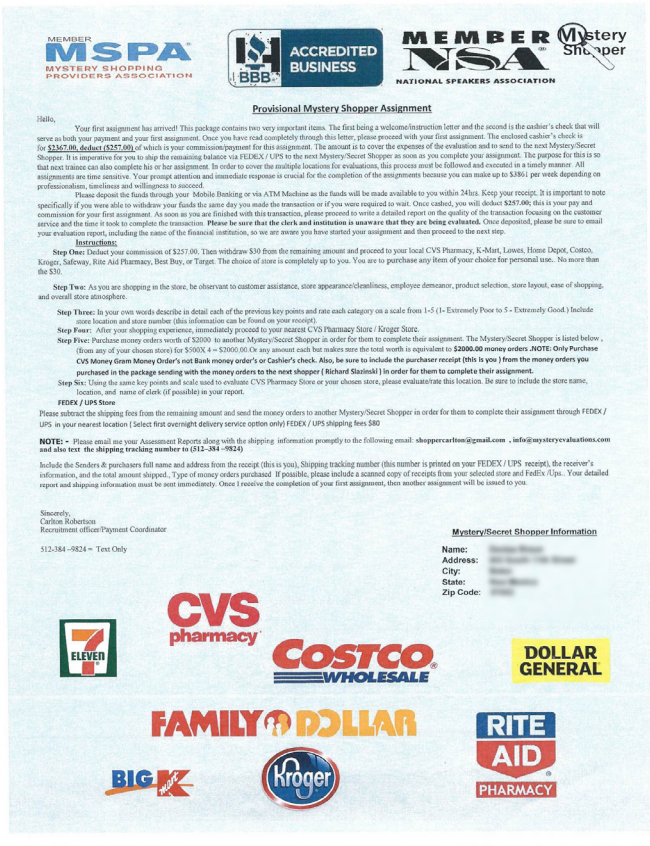
Walmart says it never hires mystery shoppers and that it trains employees about common scams such as fake check fraud, even rewarding employees for spotting and stopping fraud transactions.

In more recent variations of the fraud, scammers mail fake checks and ask people to visit drug stores or other retailers. They ask "shoppers" to buy gift cards, take a photo of the numbers on the back of the card and send the photo back to the fraudsters before completing a report about the shopping experience. After being supplied with the gift card number, fraudsters sell the cards through underground marketplaces.

There is a real mystery shopping industry, but checks typically aren't sent in advance to shoppers. Businesses may hire people to visit a retail location, make a small purchase and report back. This allows businesses to assess customer service, cleanliness and other aspects of a business location. Most of those engaged in this business are part-time workers who are paid after work is completed.

This industry is organized through the Mystery Shopper Providers Association (MSPA). The MSPA is regularly contacted by victims of these frauds; Sarah Saar, the group's executive director, says that it hears from as many as five to 10 victims daily. In addition, the fraudsters often impersonate the MSPA or its members.

Here is one mailing MSPA received from a victim. In addition to falsely displaying the MSPA logo at the top of the letter, the "company" also falsely claims to be a BBB Accredited business. The letter notes that a cashier's check for $2,367 is enclosed. The recipient is directed to keep



MEMBER MSPA MYSTERY SHOPPING PROVIDERS ASSOCIATION

ACCREDITED BUSINESS BBB

MEMBER NSA NATIONAL SPEAKERS ASSOCIATION

Mystery Shopper

Provisional Mystery Shopper Assignment

Hello,

Your first assignment has arrived! This package contains two very important items. The first being a welcome/instruction letter and the second is the cashier's check that will serve as both your payment and your first assignment. Once you have read completely through this letter, please proceed with your first assignment. The enclosed cashier's check is for $2367.00, deduct ($257.00) of which is your commission/payment for this assignment. The amount is to cover the expenses of the evaluation and to send to the next Mystery/Secret Shopper. It is imparative for you to ship the remaining balance via FEDEX / UPS to the next Mystery/Secret Shopper as soon as you complete your assignment. The purpose for this is so that next trainee can also complete his or her assignment. In order to cover the multiple locations for evaluations, this process must be followed and executed in a timely manner. All assignments are time sensitive. Your prompt attention and immediate response is crucial for the completion of the assignments because you can make up to $3861 per week depending on professionalism, timeliness and willingness to succeed.

Please deposit the funds through your Mobile Banking or via ATM Machine as the funds will be made available to you within 24hrs. Keep your receipt. It is important to note specifically if you were able to withdraw your funds the same day you made the transaction or if you were required to wait. Once cashed, you will deduct $257.00; this is your pay and commission for your first assignment. As soon as you are finished with this transaction, please proceed to write a detailed report on the quality of the transaction focusing on the customer service and the time it took to complete the transaction. **Please be sure that the clerk and institution is unaware that they are being evaluated.** Once deposited, please be sure to email your evaluation report, including the name of the financial institution, so we are aware you have started your assignment and then proceed to the next step.

Instructions:

Step One: Deduct your commission of $257.00. Then withdraw $30 from the remaining amount and proceed to your local CVS Pharmacy, K-Mart, Lowes, Home Depot, Costco, Kroger, Safeway, Rite Aid Pharmacy, Best Buy, or Target. The choice of store is completely up to you. You are to purchase any item of your choice for personal use.. No more than the $30.

Step Two: As you are shopping in the store, be observant to customer assistance, store appearance/cleanliness, employee demeanor, product selection, store layout, ease of shopping, and overall store atmosphere.

Step Three: In your own words describe in detail each of the previous key points and rate each category on a scale from 1-5 (1= Extremely Poor to 5 - Extremely Good.) Include store location and store number (this information can be found on your receipt)

Step Four: After your shopping experience, immediately proceed to your nearest CVS Pharmacy Store / Kroger Store.

Step Five: Purchase money orders worth of $2000 to another Mystery/Secret Shopper in order for them to complete their assignment. The Mystery/Secret Shopper is listed below , (from any of your chosen store) for $500X 4 = $2000.00 Or any amount each but makes sure the total worth is equivalent to **$2000.00 money orders .NOTE: Only Purchase CVS Money Gram Money Order's not Bank money order's or Cashier's check. Also, be sure to include the purchaser receipt (this is you) from the money orders you purchased in the package sending with the money orders to the next shopper (Richard Slazinski) in order for them to complete their assignment.**

Step Six: Using the same key points and scale used to evaluate CVS Pharmacy Store or your chosen store, please evaluate/rate this location. Be sure to include the store name, location, and name of clerk (if possible) in your report.

FEDEX / UPS Store

Please subtract the shipping fees from the remaining amount and send the money orders to another Mystery/Secret Shopper in order for them to complete their assignment through FEDEX / UPS in your nearest location (Select first overnight delivery service option only) FEDEX / UPS shipping fees $80

NOTE: - Please email me your Assessment Reports along with the shipping information promptly to the following email: **shoppercarlton@gmail.com , info@mysteryevaluations.com and also text the shipping tracking number to (512–384 –9824)**

Include the Senders & purchasers full name and address from the receipt (this is you), Shipping tracking number (this number is printed on your FEDEX / UPS receipt), the receiver's information, and the total amount shipped., Type of money orders purchased If possible, please include a scanned copy of receipts from your selected store and FedEx /Ups.. Your detailed report and shipping information must be sent immediately. Once I receive the completion of your first assignment, then another assignment will be issued to you.

Sincerely,
Carlton Robertson
Recruitment officer/Payment Coordinator

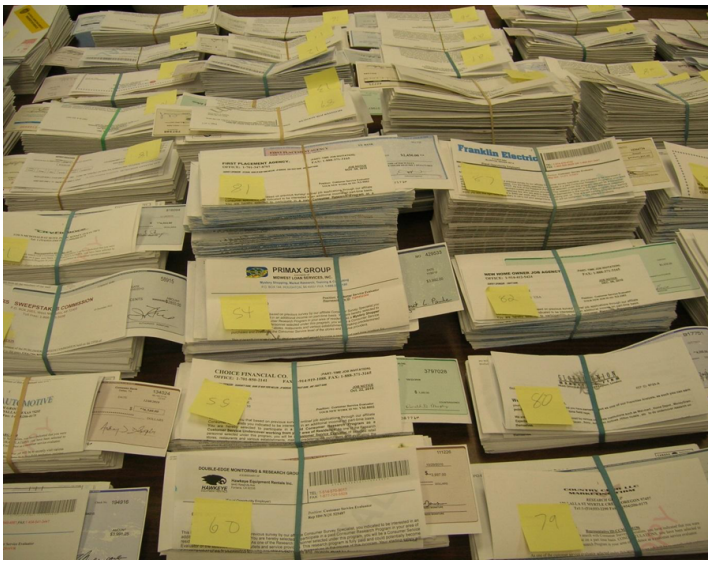
512-384 –9824 = Text Only

Mystery/Secret Shopper Information

Name:
Address:
City:
State:
Zip Code:

7-ELEVEN CVS pharmacy COSTCO WHOLESALE DOLLAR GENERAL FAMILY DOLLAR RITE AID PHARMACY BIG K Kroger

$257 as pay for the work, and go to a local retailer such as CVS, Kmart, Lowes, Home Depot, Costco, Kroger, Safeway, Rite Aid, Best Buy or Target to make a small purchase for $30 or less. The recipient was then to go to CVS to buy four $500 MoneyGram money orders and ship them by FEDEX. The recipient was instructed not to tell store employees about the mystery shopper job.
Here is a batch of mystery shopper scam letters the U.S. Postal Inspection Service seized before they could enter the U.S. mail.



Here is the FTC warning about this type of fraud.

Check overpayment scams

Fake check frauds appear to have originated with this type of fraud, and there continue to be large numbers of complaints about it. **The FTC issued its first warning** about fake checks in 2004, and it was about this type of fraud. In overpayment scams, fraudsters contact people who are selling cars, boats, and other items over Craigslist or other websites and offer to buy them. They claim that a third party owes them money, and this third party will send a check to pay for the item. The victim gets a legitimate looking check that is for more than the sale price. The fraudsters ask that the victim send them the difference through Western Union or MoneyGram. There is no real buyer -- it is just a fraud to get the victim to wire money.

Fraudsters can review Craigslist posts from anywhere in the world, so it is an easy way for them to find potential victims. Craigslist has fairly prominent warnings about frauds, even stating directly: "**Don't accept cashier/ certified checks or money orders** - banks cash fakes, then hold you responsible."

Another variation of this fraud involves a seller who requests that the buyer send a check to a supposed third party that will ship the car or other item. Victims do not realize that they are sending money to the original fraudster or a co-conspirator.

Fraudsters often engage in a variety of scams. For example, Christopher Nduka, a Nigerian man living in Toronto, **was indicted** for operating check overpayment frauds, mystery shopper fraud, as well as sweepstakes scams. He sent mail to victims from Canada, and collected the victim funds in the Toronto area.

Law firm collection scams

Lawyers are often contacted by someone in a different country, usually by email, from someone who claims that a U.S-based business owes them money. The lawyer is assured that if they collect this money they will receive a fee. The law firm reaches out to the "debtor," which sends a fake check to the law firm, supposedly to pay the debt. The law firm deposits it, and the "client" directs them to deduct their fee and do a bank to bank wire transfer to send the remainder to this supposed client.

Other variations on this fraud may involve a supposed divorce settlement. Both the **American Bar Association** and the **California Bar** have issued warnings about this type of fake check fraud. Note that the sums involved in these lawyer-centered frauds may be far larger than those in mystery shopper or other fake check frauds.

Jim Grogan, the deputy administrator and chief counsel for the Illinois Attorney Registration and Disciplinary Commission (ARDC), says that fake checks continue to be a big problem for lawyers. In fact, twice in the last three months they have been alerted to fake checks that supposedly are from the ARDC itself.

The case of **Emmanuel Ekhator** may help illustrate the

scope of this problem. Ekhator was living in the Toronto area. He was part of a ring conducting this type of fraud, one that targeted lawyers in both the U.S. and Canada, claiming money was owed from a real estate transaction, tort claim, or divorce settlement. Law firms received checks supposedly from well-established financial firms. But the phone number on the checks was a number that went to a co-conspirator, Yvette Mathurin, who "verified" that the check was legitimate. Victims wired the money to bank accounts in Asia. Ultimately, this fraud raked in more than $70 million.

Ekhator was successfully extradited from Nigeria, pleaded guilty in the Middle District of Pennsylvania and

was sentenced to serve 100 months in federal prison. He also had to forfeit properties in Canada and the contents of Nigerian bank accounts and pay $11 million in restitution.

One of Ekhator's co-conspirators, Yvette Mathurin of Canada, had a guilty plea accepted on May 29, 2018. She has not yet been sentenced. Another, Kingsley Osagie, **pleaded guilty and was sentenced** to 57 months in federal prison.

A Nigerian living in Canada also was successfully prosecuted in the Middle District of Pennsylvania. Henry Okpalefe was convicted after a bench trial. He and his co conspirators stole over $23 million from law firms across the U.S. He and his co-conspirators had victims wire money to Asian bank accounts. The fraud operated in Canada, Nigeria, Japan and South Korea. He has not yet been sentenced.

Car wrap scams

BBB receives many complaints from victims who are approached via email or social media to "shrink wrap" their cars with advertisements for energy drinks, beer, or other products in exchange for a monthly payment, often around $200 per month. Fraudsters tell victims that companies are happy to pay for this type of advertising. **The FTC has issued a warning about car wrap scams.**

Victims receive a counterfeit check, which they are told to deposit, and then to send money through Western Union or MoneyGram to the company that will supposedly wrap their cars. But the check is counterfeit, and by the time victims realize it, they have lost the money they sent by wire.

Energy drink company Red Bull reports it has reached out to the FBI about this problem. The company's website posts a warning about this and other types of fraud using its name, stating "Red Bull does not do such advertising at all and never asks third parties to brand their private cars."

There are several businesses that really do pay people to place ads on their cars. Greg Star, one of the owners of **carvertise.com** in Delaware, pays Uber, Lyft and other drivers to wrap their cars for hospitals, colleges or businesses like Buffalo Wild Wings. Carvertise typically pays drivers $100 per month for periods of time between two and twelve months.

Star says that they never send people checks, instead sending drivers to the locations where they have their cars wrapped with an ad. Carvertise itself pays the company that wraps the cars. He also says that scammers have begun impersonating his business and that they hear from victims once or twice a week. He says this has been a growing problem that involves victims who are may be vulnerable.

Nanny or caregiver scams

Fraudsters often advertise "jobs" for nannies, babysitters, caregivers for the elderly or disabled, housekeepers or tutors on Craigslist, at Care.com or at other job web sites. Those who are "hired" are told that they need to buy a wheelchair or other equipment for job purposes. Victims receive and deposit the fake check, and then wire money to a supposed third party to get the equipment needed for the job. But there is no real job, and those who respond lose their own money.

The FTC has both a **consumer warning** and a short **video** explaining caregiver frauds and how to avoid them.

Care.com is one of the largest forums for caregivers, operating in 20 countries with a membership of more than 28 million people. They regularly hear about these frauds trying to operate on their system, almost all of which involve fake checks. This company appears to be making efforts to prevent fraud through its services, and the complaints they receive have dropped by the "high double digits." Care.com warns its client base about frauds and how to avoid them. Both potential employees and employers have to create a profile to take part. The company closely examines the "digital fingerprint" of those joining their service. For example, they try to see if the IP address of the computer matches the location claimed in the profile.

Care.com reports that all new members receive an email that directly explains how frauds work and how to avoid them. They repeat this by sending monthly emails to all

their clients repeating these fraud warnings. Care.com also has a **safety center** on its site with more tips and resources for their clients.

Sweepstakes and lotteries

This type of fraud was addressed in a June 2018 **Better Business Bureau study** on prize and sweepstakes fraud. This is the third most common type of fake check reported to BBB Scam Tracker (after "fake check fraud" and "employment").

Victims typically get a letter in the mail announcing that they have won the Publishers Clearing House lottery or another major sweepstakes or lottery. The letter tells them that they have won a large sum of money, and need to call a phone number to confirm their winnings. The fraudster explains that money is needed for taxes or other costs before they receive their winnings. They are told a check is enclosed with the letter to cover those costs. The victim need only deposit the check and send the money by Western Union or MoneyGram to a third party to pay these expenses and then receive their prize. But there is no prize, and of course the check is fake. Here is the **FTC warning on prize frauds**.

The U.S. Postal Inspection Service reported stopping and seizing over a million pieces of sweepstakes mail last year, with counterfeit checks that had a face value of $62 billion. USPIS issued this statement:

> Foreign lotteries are illegal in the U.S. These lottery solicitations are almost always criminal scams designed to dupe victims into sending money to the scammers. Using the legal process, Inspection Service screeners interdict illegal lottery mailings and protect victims from criminal misuse of the mail. In FY 2017, interdictions removed 1,083,903 illegal lottery solicitation letters detailing 4,723 different scams. Often these letters contain counterfeit checks or money orders. Inspection Service screeners interdicted solicitations containing counterfeit checks with a face value of approximately $62 billion. Approximately 963 Canadian telephone numbers used in the illegal lottery scam letters were terminated as a result of these interdictions.

Small business fraud

An American Bankers Association survey found in 22 percent of the cases, banks lose money because of fake checks where the victim is a small business.

Fraudsters may use fake checks to "pay" in advance for goods and shipping costs. For example, one banker related that one of their customers sold paintings online. They received a fake check, but did not ship the paintings right away, learning later that the check they received was counterfeit.

Other complaints describe how businesses received checks made out for more than the amount owed for services provided and then were asked to send back the overage. These frauds often target photographers, sending checks and then asking that part of the proceeds be sent along to another party supposedly involved in the wedding or other event.

A recent BBB survey of frauds affecting small business identified fake checks among the top five scams that put small businesses at risk.

Other types of fraud

The frauds discussed here are not exhaustive. BBB Scam Tracker also receives a significant number of reports of fake checks employed by frauds offering loans, government grants, and even in tech support frauds. In any transaction where a check is involved, consumers need to remember that money credited to a bank account does not mean the check is good.

Why does this fraud work?

The public writes far fewer personal checks than in the past, thanks to alternatives such as debit and credit cards and online bill payment services. With the decline of personal checks comes a decline in knowledge about how banks process checks. Just as a lack of knowledge can create a target-rich environment for frauds, more robust consumer education about checks and their processing may help prevent such check fraud.

Victims believe that they are protected because they think they have been provided with money in advance of the actions they are being requested to take. By reinforcing this belief, scammers build trust and alleviate concerns that the deal might be a fraud. And once consumers confirm that there is money in their account, they are far more willing to proceed.

Who is behind fake check scams?

Nigerians and nationals of other West African countries appear to be deeply involved in fake check frauds, though others are likely involved. Every prosecution of fraud involving fake checks that BBB is aware of, where the victims respond by sending money, has involved Nigerian fraudsters. Nigeria is the most populous country in Africa, and it has an educated population, but many of its citizens have few job prospects. Moreover, Nigerians have migrated to countries around the world.

The presence of fraud is an issue of concern in Nigeria, and the country's Economic and Financial Crime Commission (EFCC) not only actively works to prosecute frauds in Nigeria, but also cooperates with law enforcement around the world.

Several steps are required to make this fraud work. Someone must create the checks or receive them in the U.S. or Canada. Then they must be mailed to potential victims. Finally, someone must collect the money sent by fraud victims. These steps may be undertaken by fraudsters in the U.S., but also may be the work of money mules or other co-conspirators physically in the U.S or Canada. In short, those engaging in this fraud are very organized, and may have a variety of conspirators that make them successful.

This suggests that there could be organized crime groups operating worldwide to conduct fraud. The same groups, or even individual fraudsters, usually engage in a variety of frauds.

For example, a June 2018 indictment in Memphis, Tennessee involved business email compromise fraud diverting money from real estate closings. But it also charges that the African defendants, nationals of Nigeria and Ghana, **were also involved in** "various romance scams, fraudulent-check scams, gold-buying scams, advance-fee scams, and credit card scams."

Many of these fake checks are shipped to the U.S. and Canada, often from Nigeria and elsewhere in West Africa. A 2010 International Mass Marketing Group study, **"Mass-Marketing Fraud: A Threat Assessment,"** found:

> Law enforcement intelligence indicates that fraud perpetrators routinely send counterfeit financial instruments through myriad countries and alternate their routes and shipment methods to circumvent law enforcement and customs investigations. Recent investigations by Nigerian authorities have resulted in the arrest of check-carrying couriers preparing to board flights to South Africa, the United Arab Emirates, the United Kingdom, and the United States, and in the seizure of bulk packages of checks destined for reshippers in France, Italy, and Spain.

As noted, law enforcement makes serious efforts to keep fake checks from entering the country. But some are being created in the U.S. and Canada, and interdiction does not catch all of them.

How do crooks get money?

Finding a way to get money back from fake check victims is integral to making these frauds successful. The FTC reports that the most common way of obtaining the money from the victims is by wire transfer. Most of the wire transfers are sent through Western Union and MoneyGram, which are by far the biggest players in this money-sending market, each having outlets around the world.

Recent cases against both companies by the FTC and Justice Department alleged that they were aware of large fraud problems, that fraudsters themselves had become agents of each company, and that both failed to take effective action. MoneyGram settled with the **FTC** in 2009, paying $18 million in restitution, and resolved a case with **DOJ** in 2012. Moneygram denied allegations that it knew about the fraud. Western Union entered a **joint settlement** with the FTC and DOJ in 2017 and agreed to pay $581 million.

The fraud was effective because wiring money is like sending cash – as soon as the money is picked up, it's gone. Victims have no ability to get their money back as they might have had if they used a credit card. Both companies have since significantly improved their procedures for handling money transfers, and have made real efforts to keep fraud out of their systems.

For frauds involving larger sums, such as those in which lawyers are the victims, fraudsters may request the money be sent by bank-to-bank wire transfer. These transfers can be difficult to reverse.

Fraudsters are shifting to having victims buy gift cards, especially Apple iTunes cards. They often ask victims to buy the cards, scratch-off to reveal the security code on the back, take a picture of those numbers, and text or email that photo. With these numbers the fraudsters can quickly cash out the gift cards. There is apparently a large worldwide underground market trading in gift cards.

No legitimate business asks for payment by Western Union, MoneyGram, or by gift cards. Requests for payment through these avenues are one of the hallmarks of fraud.

CARD CRACKING

A related form of counterfeit check fraud is known as "card cracking." Like other fake check frauds, this fraud takes advantage of the fact that money is credited to accounts and can be withdrawn before the check bounces.

These fraudsters recruit young people on social media sites, enticing them with offers to make money from home. Those who respond, usually students, are asked to provide their full bank account information, including security questions, PINs for ATMs, and a range of other personal information. These are used as "mule" accounts by the fraudsters.

The fraudsters deposit fake checks into the mule accounts, wait until the account is credited, and then withdraw cash from the account by using ATM machines. They may pay the mule part of the proceeds. Mules are told that if anyone asks about the activity involving their accounts, they should simply say that their ATM card was stolen. They are falsely led to believe that they will not be responsible

In reality, these mules are co-conspirators who may be prosecuted. At the very least, they ruin their own credit.

Cumulative losses for this type of fraud can be large. The **American Bankers Association reports** that just between July and August 2014, banks experienced more than $18 million in card cracking attempts.

The same tactics can be employed to launder money for other types of fraud. There is no apparent connection between card cracking fraudsters and the other fake check fraudsters discussed in this report. Those involved in cracking have been successfully prosecuted in (at least) **North Carolina**, **Virginia**, and in enforcement efforts in **Manhattan**. In addition, two crackdowns have been announced by the Manhattan DA. **First crackdown**, **second crackdown.** The FTC has also **warned** about this fraud.

Money mules

Fraudsters often seek people to help collect money. The fraudsters know that the traditional method law enforcement officials employ in investigating is to follow the money. Thus, when money is initially collected and forwarded by someone who is not directly involved in the fraud, it becomes much more difficult to find those actually responsible. Those providing this assistance are known as "mules," and they may or may not know that there is fraud involved. Sometimes mules get a part of the proceeds.

Mules may get involved in several ways. Some may respond to a job offer online which they believe to be legitimate that involves transferring money. Another favorite tactic to obtain free help is for the fraudsters to use romance fraud victims to help them. **A recent BBB Report on romance frauds** explains that those running these frauds meet victims online, "groom" them for an extended period, and then claim an emergency to get the victim to send money. But victims are useful even if they have no money to send. Victims are often provided with plausible reasons why their romantic interest/fraudster needs some help. Romance fraud victims provide the help, not realizing that they are assisting in a fraud. If mules, even romance fraud victims, come to realize that they are doing something illegal, the fraudsters sometimes threaten them, either to end the "relationship" or to turn them in to law enforcement.

Mules also may be involved in printing and mailing checks.

How large is the fake check problem?

Frauds employing fake checks are growing rapidly and cost billions of dollars. The number of complaints received by the Federal Trade Commission's (FTC) Consumer Sentinel database (Sentinel) and the Internet Fraud Complaint Center (IC3) more than doubled between 2014 and 2017, rising from 12,781 to 29,513. The National Consumers League (NCL), which also receives complaints from fraud victims at **fraud.org**, found that fake checks complaints in 2017 were up 12 percent and were the second most common type of complaint over all (after goods ordered online but never delivered). Fake checks were involved in 7 percent of all complaints filed with BBB Scam Tracker.

The Postal Inspection Service reports stopping fake checks with a face value of $62 billion from entering the United States in fiscal year 2017. Postal Inspectors also intercepted 13,724 counterfeit postal money orders, and 550 non-counterfeit postal money orders, with a total face value of $14,157,204.

During 2016, total check frauds cost banks $789 million, a 25 percent increase from two years before. Efforts by banks stopped $7.8 billion in losses to victims in 2016.

Because checks flow through a national system, one would expect records to be kept on how many of them bounce after being deposited. The Federal Reserve, which handles the clearing process between banks for most checks, does not maintain figures on losses. This makes it difficult to determine the amount of money victims lose (or that fraudsters make) from fake check frauds. The best data available are complaints about fake checks and the amounts banks lose to counterfeit check frauds.

FAKE CHECK COMPLAINTS AND LOSSES BY AGENCY AND BY YEAR

Year	Complaints Reported to FTC	Loss $ Reported to FTC	Complaints Reported To IC3	Loss $ Reported To IC3	Complaints to Canadian Agencies	Loss of Canadian $ Reported to Canadian Agencies
2015	17,923	$17,817,271	6,188	$9,547,192	508	$2,002,000
2016	20,954	$20,136,112	5,503	$15,935,970	1,876	$7,083,000
2017	24,437	$25,073,672	5,076	$12,770,164	1,024	$3,611,000
TOTALS	**63,134**	**$63,027,055**	**16,767**	**$38,253,326**	**3,408**	**$12,696,000**

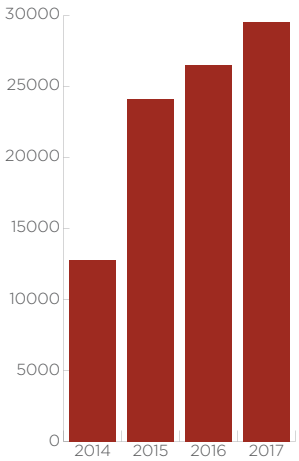
Complaints

There are two databases of consumer fraud complaints in the U.S.: Consumer Sentinel and IC3. Sentinel contains complaints made directly to the FTC but also gets downloads of complaints originally made to BBB, the NCL, the Postal Inspection Service, Western Union, MoneyGram, Publishers Clearing House, many State Attorneys General and other sources. Local police generally do not contribute the complaints they receive. Sentinel is available online to thousands of state and local enforcement agencies. Hosted by the FBI, IC3 is similarly available to many enforcement agencies.

BBB's Scam Tracker system has received 5,820 complaints involving fake checks between 2015 (when the program began) and the end of 2017. After complaints filed as "fake checks," BBB found fake check frauds were also included in reports about employment frauds, sweepstakes fraud, and smaller numbers in areas such as bogus grants, tech support, online purchase fraud, and rental frauds.

Fake checks rank as the 6th most common fraud reported to Sentinel in 2017. Losses averaged $1,008. Most victims were contacted by mail, and the most common method of transferring money to the fraudsters was by wire transfer (typically Western Union or MoneyGram).

FTC and IC3 numbers from January through May, 2018, suggest that the trend line is unlikely to change. Curiously, complaints to the Canadian Anti-Fraud Centre (CAFC) dropped somewhat over this period.



Fake Check Complaints Reported to FTC & IC3, 2014-2017

In 2009, there was a coordinated effort by law enforcement and private partners to concentrate on fake check fraud, with both consumer education and enforcement efforts brought to bear. The **fakechecks.org** web site was constructed during this period. Complaints in Sentinel dropped dramatically after these efforts before they started climbing sharply in the last four years.

These complaint numbers understate the actual extent of the fraud. As the FTC has found in fraud surveys it has conducted, the vast majority of fraud victims never report it. In fact, the FTC has found that less than 10 percent of fraud victims ever report to BBB or law enforcement.

The number of victims who file a report that goes to Sentinel or IC3 may be even lower. A **fraud survey released by the FTC** in 2013 covered frauds that had occurred in 2011, and it asked specifically about counterfeit check fraud. The survey found that roughly 400,000 people in the U.S. had been victims of a fraud involving a counterfeit check in 2011. The Sentinel system received 33,359 counterfeit check complaints in 2011; suggesting that Sentinel only got complaints from 1 in 17 of the actual victims. Presuming this ratio is constant, this suggests that there may have been over 500,000 victims of a counterfeit check in 2017.

Banking Losses

The banking system has experienced an increase in fake check fraud. The American Bankers Association (ABA) recently completed a survey, "2017 Deposit Account Fraud Survey Report." (2017 ABA survey). Results were extrapolated from U.S. banks of various sizes for the whole industry for 2016. These studies are done every two years, providing a baseline for trends.

The 2017 ABA survey looked at losses to the banks, rather than losses to consumers. In many cases victims of fake check fraud don't have funds in their accounts to cover money lost in fake check frauds. Banks sometimes absorb these losses.

All banks that responded to the survey had customers who experienced check fraud, and nearly half of the banks had themselves lost money to check fraud. Counterfeit checks were the main type of check fraud that banks experienced, but it also included check "cracking" schemes.

The survey for 2016 saw the first increase in check fraud losses since 2008. During 2016, check frauds cost the banks $789 million, an increase of more than 25 percent from the $615 million reported losses in 2014. Average losses for check fraud were $1,195 in 2016, up from $1,087 in 2014. These losses also include losses from counterfeit money orders. With the average check at $1200, banks could have been on the hook for funds for 65,750 checks.

As noted elsewhere in this study, most front-line employees at banks, such as tellers, are familiar with fake check fraud and make efforts to identify unusual situations, warn victims, and try to stop the fraud. Banks reported in the ABA survey that they conduct training for their staffs

on fake check and other types of fraud, and many also engage in efforts to educate the public.

The banks collectively have had some significant success with these efforts. The ABA survey found that they stopped $7.8 billion in losses to victims in 2016, although we do not know how many victims – or checks -- were involved. But if the average fake checks was for $1,200 that would suggest that 6.5 million checks were stopped by the banks.

The ABA survey also found that more than ten percent of the time funds were obtained over the counter (from a teller). But 74 percent of the time the money was spent at a point of sale (e.g. where a debit card was used to buy something, such as a gift card, or to withdraw cash to send to a fraud).

How can we prevent and avoid fake check scams?

What banks do to help prevent fraud

While check fraud activity such as handwritten counterfeit check writing and "kiting" have decreased in recent years, banks continue to address fraud involving fake checks.

So how do banks help victims? BBB talked to two banks that make special efforts to combat the use of fake checks used by fraudsters. Both do training for their tellers on how to detect and stop the fake checks.

One of the most direct and helpful ways banks can help their customers is simply to remind them that crediting the money to their account does not mean the check has cleared and is legitimate.

There are two opportunities for bank tellers to become involved in identifying a fake check – when it is deposited and when the victim wants to withdraw the cash.

Check Fraud Red Flags for Banks

- **Out-of-state business accounts**. Tellers can determine a lot from the check itself. The check amount tends to be in the range of $1,200 to $2,000 and may be missing a company address or phone number. If an individual wants to deposit a check for over $1,000, tellers at one bank give a printed brochure to the client.
- **"Micr" code, or MICR line.** AARP describes that code this way: "The bottom of every real check has a series of digits in an unusual font, representing the bank routing number, the account number and the check number, generally in that order. That special font is known as MICR, which stands for magnetic ink character recognition. These numbers can be read by specialized check-sorting machines. Real magnetic ink looks and feels dull to the touch. Fake MICR numbers are often shiny. Though the lack of the MICR code is a sure sign that the check is fake, new technology and ink allows crooks to even copy this code."
- **Unusual circumstances.** Is it an elderly customer that rarely makes deposits? Is a deposit of this size very abnormal activity for the customer?
- **Customer questions.** If the customer asks when the money will be available or if the check cleared, that is a strong sign to tellers that a fraud may be involved, since fraudsters are anxious to have victims send the money before the check is discovered to be fraudulent. And when customers have deposited a check and ask to withdraw it in cash, simply asking nicely what the customer may do with the money may produce a response indicating that someone thinks they have won a lottery or sweepstakes. Most people are willing to engage, especially when it is clear that the teller is honestly trying to help. For example, the teller may ask why, if someone has won a lottery, the check is from a tire company.
- **Large deposits.** Many banks also allow check deposits through mobile devices such as apps that take a photo. These systems typically have a dollar amount limit on the size of the check that can deposited. Banks can also check the IP address of the depositor to see if it matches that of their customers.

Of course, victims may deposit the check with an ATM or banking app, but banks say that is not common. If banks suspect that a fake check is involved they do not have to credit the customer's account. Banks can accept the deposit, but send the customer a letter saying that they are holding it and won't process it pending an investigation.

One chain of banks in Texas gives its employees an award for discovering and stopping a fraudulent transaction. It has also set up partnerships with the local police, adult protective services and BBB. The bank has developed a speaker's bureau that goes out and talks to local community groups and retirement centers.

When tellers at these banks spot suspicious transactions they can call the local police, delaying the completion of the transaction by claiming their computers are down, and the police arrive quickly. Often the police are able to spot a fraud victim and stop the fraud. In other cases where the fraudster, or a runner, comes to the bank (such as in a card cracking situation) they can be arrested. This bank reports 50 or 60 arrests in the previous year.

In addition, banks file Suspicious Activity Reports (SARs) with the Treasury Department's Financial Crimes Enforcement Network (FinCen). They can report fake checks or other types of fraud. These reports can be reviewed by bank regulatory agencies and law enforcement, but are not public.

Companies like Advanced Fraud Solutions provide a service that allows banks to quickly determine if a check is a fake. With this service, a bank can tell if other fake checks have been reported on that business or account. Advanced Fraud Solutions compiles fake checks alerts from financial institutions, adding about 150,000 new alerts monthly. They report users have experienced a 70 percent reduction in fake check fraud.

Advanced Fraud Solutions says that nearly every financial institution in the U.S. has had its checks counterfeited, typically as bogus cashier's checks.

Law Enforcement

Law enforcement has done much work in finding and prosecuting fake check frauds, though significant challenges remain. Because mules are used so frequently, it is often hard to locate the actual actors behind the fraud or to recognize patterns. Moreover, many law enforcement agencies are not accustomed to dealing with fraud actors that are overseas, and they may be reluctant to try and extradite someone from another country. However, those involved in fake check frauds have been successfully extradited from Nigeria.

Because most of these checks go through the mail they are of special interest to the U.S. Postal Inspection Service, which has long been charged with enforcing federal mail fraud laws. Postal Inspectors are federal agents with guns and badges and are the equivalent of FBI agents. They are simply less well known.

In addition, the FBI, the Secret Service, Homeland Security Investigations, and other criminal investigative agencies are often involved in cases involving fake checks or other fraud affecting financial institutions.

In addition to the prosecutions outlined above, other recent efforts include;

- In July 2018, a Nigerian man was **sentenced to prison** in Louisville for his role in a sweepstakes fraud. He sent mailings to victims telling them that they had won a sweepstakes or lottery, and included a fake check for various "costs." The money victims sent went directly to him in Louisville.
- In August 2018, a man was **indicted in Pittsburgh** for his role in a mystery shopper fraud. He sent counterfeit postal money orders to victims and received the money from those victims. He is alleged to have been working with Nigerians in this fraud.
- In January 2018 five people were **arrested in Dallas** for international fake check fraud. The indictment charged that the defendants were involved in mystery shoppers fraud, and in addition to counterfeit checks they also employed counterfeit money orders.
- In February 2017 three Nigerians that had been living in South Africa were extradited to Mississippi and **convicted by a jury** of frauds including romance scams, reshipping scams, fraudulent check scams, and work-at-home scams, as well as bank, financial, and credit card account takeovers.

Such prosecutions are in addition to the consumer education efforts undertaken by many enforcement agencies.

What to do if you have deposited a fake check into your account

- Notify your bank or the bank that appears to have issued the check.
- File a complaint:
  - **Better Business Bureau**
  - **The Federal Trade Commission** (FTC), or call 877-FTC-Help
  - **The Internet Crime Complaint Center**, or IC3
  - **The U.S. Postal Inspection Service**
  - **Western Union**, 1-800-448-1492
  - **MoneyGram**, 1-800-926-9400
  - **Green Dot**, 1-866-795-7597
  - **Canadian Anti Fraud Centre**, toll-free from the US at 1-888-495-8501
- Victims who are seniors or other vulnerable adults may be able to obtain help through Adult Protective Services, which has offices in every state and many counties. Find a local office at **www.elderjustice.gov.**

Resources

- **BBB's Scam Tracker** allows you to report scams and see if others in your area have reported similar frauds.
- The Office of the Comptroller of the Currency has **helpful explanations** for many of the common questions that arise with fake checks.
- The American Bankers Association has **resources for consumers.**
- Publishers Clearing House helps you **check if you have won their sweepstakes, or complain about sweepstakes scams.**

Recommendations

- Organizations such as BBB and regulatory agencies should do more to provide fake check fraud prevention education.
- With wide-scale use of money mules and others to assist in frauds, it would be useful for law enforcement agencies to work collaboratively to both identify these individuals and to take action to ensure that they end these activities. Prosecuting them criminally may not be necessary, especially if they were not knowing participants in fraud, but administrative or civil actions could be taken simply to ensure that these activities cease.
- Investigative agencies may need more resources to effectively prosecute fake checks and other widespread frauds.
- Continued law enforcement coordination and training with enforcement counterparts in Nigeria and elsewhere remain important and should be strengthened.
- Banks and financial institutions might consider more collective efforts to educate their customer base about fake check frauds.
- Retailers should ensure continued training in identifying and alerting customers to potential fraud surrounding gift card purchases.

By Steve Baker, BBB International Investigations Specialist