JOB SCAMS

This BBB study finds job scams increased during pandemic and warns job seekers to verify employment offers to avoid illegal jobs, identity theft and fake checks

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 2021

SCAMMERS TARGET JOB SEEKERS

With millions unemployed in the United States and Canada, job scammers have a ready market of those looking for work. Not surprisingly, complaints and reported losses increased during the pandemic, and with more people currently wanting to work from home, the door is open to even more job scams. BBB reports that an estimated 14 million people are exposed to employment scams every year, with $2 billion in direct losses annually.

Job scams have long been a staple of scam operations. Once commonly found in the province of classified ads claiming people could work at home stuffing envelopes, assembling goods, or promises to provide jobs working for the Postal Service those scams are now far less common. A new generation of scammers advertise jobs on the web and social media, or reach out to those who have posted resumes on job boards. These changes increase the risks of identity theft. They also have resulted in a big increase in scams that involve reshipping goods purchased with stolen credit cards. Other common scams promise jobs but provide victims with counterfeit checks, asking them to send money to a supposed third party for equipment to perform the job.

This study examines how common these frauds are, who they are most likely to affect, how they operate and how to avoid them. Of particular concern is the risk of identity theft, jobs that require reshipping goods purchased with stolen credit cards or helping scammers in other ways, and scams that involve fake checks.

HOW BIG OF A PROBLEM ARE JOB SCAMS?

Job scams have been a growing problem for years. The 2020 BBB Employment Scams Report by BBB Institute for Marketplace Trust found that job scams were the riskiest of all the scams they tracked in both 2018 and 2019 and often affect those already in financial distress.

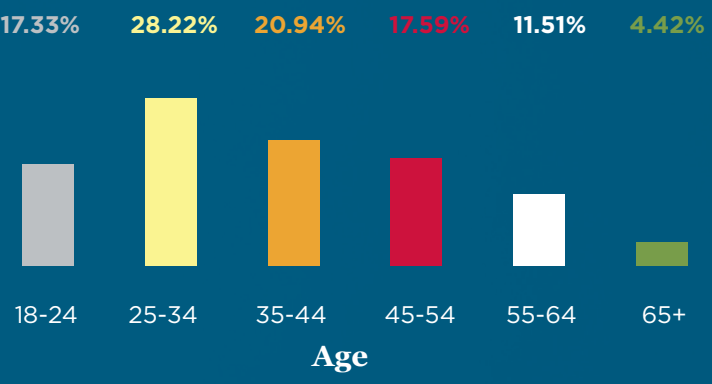
Losses reported to the FBI's Internet Crime Complaint Center (IC3) about employment scams were up 27% between 2018 and 2020. Complaints to Canada's Consumer Anti-Fraud Centre (CAFC) nearly doubled in 2020.

IC3	COMPLAINTS	LOSSES
2018	14,979	$45,487,120
2019	14,493	$42,612,705
2020	16,879	$62,314,015

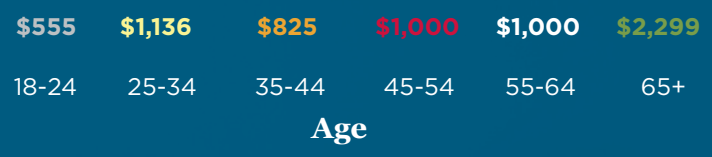
CAFC	COMPLAINTS	LOSSES
2018	1,949	$5,755,004
2019	2,414	$3,271,506
2020	4,429	$4,401,271
2021 (through June)	2,141	$2,385,017
2021 (projected)	4,282	$4,770,034

WHO DO JOB SCAMMERS TARGET?

Ages. The largest group of reports were from those 25-34, accounting for 28.2% of the BBB Scam Tracker reports, followed by those 35-44, with 21% of reports.



Median amounts lost. The overall median loss in reports to Scam Tracker was $1,000, though older reports lost more, with a median loss of $2,299 for those over 65.



Gender. Women accounted for 66.7% of complaints. It is possible that they were simply more likely to reach out and file a complaint. BBB is aware of no evidence that scammers are targeting women.

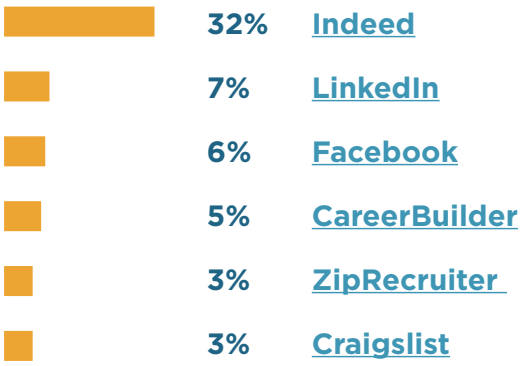
Employment status. 54% of victims were unemployed; 25% had full time jobs; 50% were looking for full time jobs; 28% flexible jobs; 10% part time; and 32% did the work but were never paid.

The BBB Institute report shared results from a survey of those who reported employment scams to BBB Scam Tracker between 2017 and March 2020.

ANATOMY OF AN EMPLOYMENT SCAM

Misusing online job sites. **Job seekers post resumes online, hoping they'll get noticed by potential employers. In its survey, the BBB Institute asked where people had seen the job advertised. Many responded "other" or said that they had received an email, but often they reported they had seen it on a job board. Here are the sites most commonly reported by survey respondents who listed a platform. All platforms have warnings on their sites about job scams.**

How scammers engaged with their targets - most reported online platforms



In April 2021, **Marie** was living in Orland Park, Illinois. Her former employer went out of business during the pandemic and she was looking for a new job. She posted her resume at PeoplePerHour.com, a job board for people seeking freelance jobs. She was contacted by Adam Tomasi at Alector Healthcare to do data entry and paid $37/hour. After an interview with the "company" on Skype messenger, she was told she had the job and needed to complete new hire and W-4 forms for payroll purposes. She was informed that she needed the newest iPhone which would require special programming, but she would get a discount and the cost would be reimbursed to her. She sent $400 through the Zelle payment app to a vendor provided by the company.

The next day, Marie was told that she also needed a special monitor and laptop, again payable through Zelle. She told them she would only use a credit card. They urged her to move as quickly as possible. Concerned, she said she called Tomasi on Skype and her suspicions grew when the profile picture on the screen showed a middle-aged white male but the voice on the call sounded to her like it was African. Tomasi told her he used his manager's photo.

Marie then tried to contact Alector Healthcare directly, but could not reach a live person. Tomasi told Marie that she would receive her iPhone on Monday. It never arrived. Marie learned that the scammers were using the name of the real head of HR at Alector Healthcare with a slightly different email address.

Conducting bogus interviews

Victims are often contacted by email or text message. Victims report that they have applied for several jobs online, and thus often believe that the contact is a result of those efforts. They then often have a cursory interview online. The BBB Institute report found that these were often done on Zoom, Skype, or Google Meet. But victims state that even when they do video conferences, they often do not see the face of a real person. Often the "employer" asks for a variety of personal information. One of the riskiest types of data to provide, of course, is bank account information, supposedly so that the scam employer can directly deposit the new employee's pay.

Impersonating legit employers

In the BBB Institute report, the largest number of victims believed that they were being hired by Amazon and Walmart.

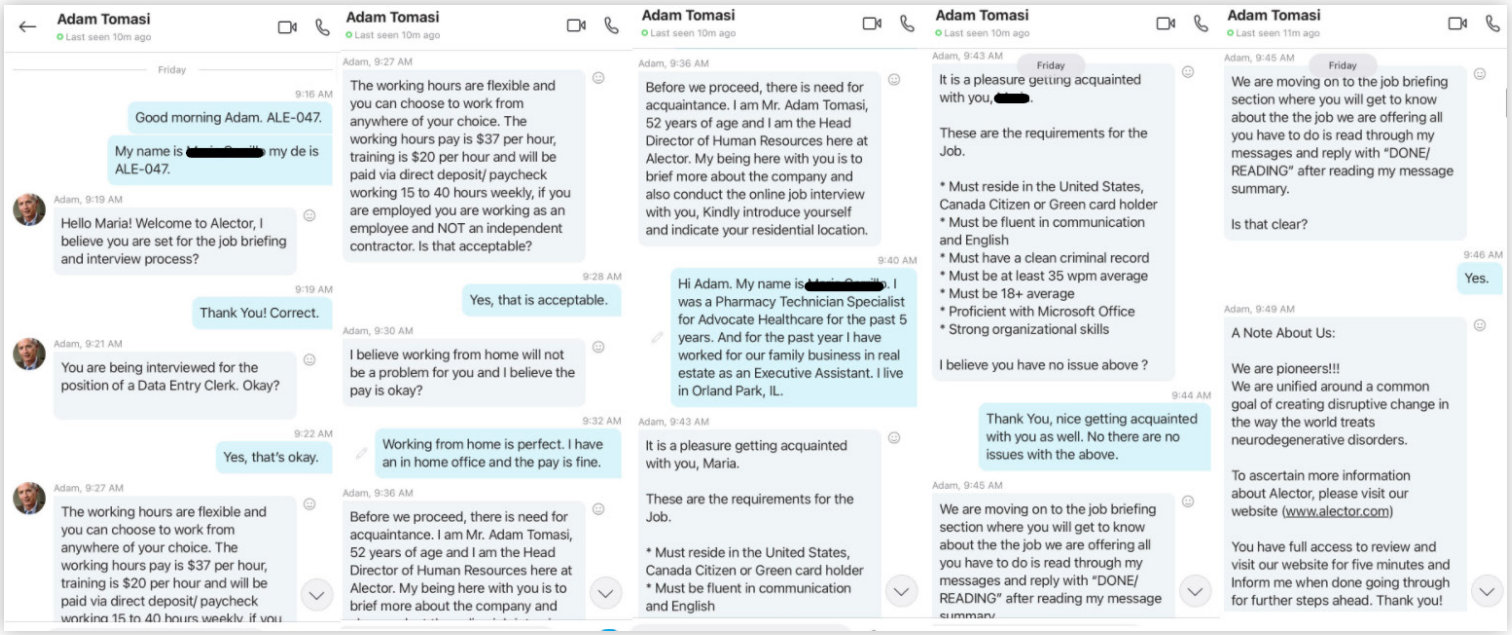
Amazon states that it posts all job opportunities at **Amazon jobs** and doesn't require anyone to purchase equipment or pay initiation fees. It has **warnings about job scams using its name.** The company states: "We take the fraudulent use of the Amazon brand very seriously. Any customer that receives a questionable email, call or text from a person impersonating an Amazon employee should report them to Amazon customer service. Amazon investigates these complaints and will take action, if warranted." It also has **advice on how to determine if someone claiming to be hiring for Amazon is legitimate.**

Walmart was the second most common employer victims believed they were dealing with, but almost all Walmart complaints involved mystery shopping scams. Walmart reports that all jobs it has available can be **checked out at its website** and advises the public to only trust emails that are from walmart.com; wal-mart.com, or samsclub.com.

Manyongbe lost her job in St. Louis during the pandemic and posted her resume on Indeed.com. She was contacted by phone and text message about a job doing remote monitoring, acting as an assistant and responding to phone calls and emails for Intuit. She interviewed for the job on Zoom, and the next day was told she was hired and would be paid $24 per hour. She provided her bank account information so that her pay could be deposited into her account.

She was also told that she needed a laptop and other equipment from a third party vendor to do the job, and that Intuit would give her the money to pay that by depositing money into her bank account. A check for $2400 was deposited into Manyongbe's account, and because the funds were credited as available, she believed that the check was valid.

The "employer" then had Manyongbe go to Home Depot to buy $2,400 in gift cards, scratch off the numbers on the back and provide them by text message. She was then supposed to hear from the vendor, which would send her the equipment she needed. When she did not hear from them, she became concerned. Then the bank informed her that the check deposited to her account was fraudulent and it took the $2,400 back. In addition, the scammers stole an additional $2,400 from her bank account. Manyongbe was unable to pay her rent and had to move in with her sister.



COMMON JOB SCAMS

There are a number of scams aimed at those seeking jobs, and the "jobs" offered by scammers include a wide variety of job titles and descriptions, ranging from personal assistant to data entry to distribution agent. No matter what the title and promised pay, these scams boil down to a few common job descriptions. Many job scams involve identity theft, reshipping schemes, and payments using fake checks.

Identity Theft

Scams operate to make money. In most cases, they deceive victims into sending money. But some scams concentrate on getting personal information from victims, which the scammers can then use to either steal from victims or to further their overall fraud efforts. This is a serious issue for those seeking jobs because, as the **FTC has noted,** resumes can be a "treasure trove for identity thieves." Many ID theft victims may not even know they are victims, and it is uncommon for identity theft complaints to be reported to BBB. The **FTC received 1.4 million complaints about ID theft in 2020**.

Online job frauds often concentrate on getting personally identifiable information (PII) from victims. The BBB Institute report found 34% shared driver's license numbers and 26% shared Social Security or Social Insurance numbers (in Canada). People posting resumes online should be careful not to include information such as social security numbers, their date of birth, or bank account information. The **FBI has warned** that victim's PII can be used for a variety of "nefarious purposes, including taking over victim's accounts, opening new financial accounts, or using the victims' identity for another deception scam, (such as obtaining fake driver's licenses or passports)."

In order to be paid for a job, most employers require bank account information in order to deposit an employee's pay. Job applicants should never provide this information before they are actually hired, and even then should take special care. Those being hired for jobs may want to consider setting up a second bank account simply to handle the pay from jobs where they have never met the employer in person.

This also highlights the importance of making sure you are dealing with a real employer. Many employers not only consult job boards but also post available jobs on their own web sites. Checking to see if the supposed employer is real, in advance, is of the utmost importance. Check **BBB.org** to find out if a potential employer is a legitimate business. Another option is to do an internet search of the supposed employer and the word "scam." This can help determine if the potential employer is actually a scammer or if a real business's name is being used for scam purposes.

Identity theft victims may not know right away if their identities have been compromised. It is a good idea for everyone to get a free copy of their credit reports regularly, and this is especially true for those who have posted their resumes online or that have been victims of job scams. Go to **annualcreditreport.com** to get them for free. **The Identity Theft Resource Center** also provides advice on protecting your identity during a job search.

RESHIPPING SCAMS WHERE VICTIMS HELP SCAMMERS

One of the most common job scams BBB sees are reshipping scams, and many of those who perform this work never get paid. Hundreds of millions of credit and debit card numbers have been stolen and are available to scammers worldwide. So what do fraudsters do with those numbers? Often stolen credit card numbers are used to buy high value items such as laptop computers or phones. Since most retailers will only ship those kinds of goods domestically, scammers enlist people to receive the ordered goods, repackage them and send them out of the country. Warnings about this type of fraud have been posted by the BBB, the U.S. Postal Inspection Service, the National Consumers League, and the FTC.

For example, romance scammer Olyinka Sunmola was a Nigerian living in South Africa, where he operated a romance fraud. He used stolen credit cards to order at least $1 million of laptops and other electronics which were shipped to his romance fraud victims. He then used pretexts to get those victims to send the goods to him in South Africa where he had a store that sold them.

But a large segment of reshipping schemes operate as job scams, "hiring" people to work from home reshipping goods. Many of the innocent people employed to do this work never get paid for their efforts, and may have their identities stolen or face law enforcement scrutiny.

65% of scam job offers reported to BBB Scam Tracker involve reshipping.

An education video released by the U.S. Postal Inspection Service states that "There are no legitimate jobs sending or receiving packages."

So how do reshipping scams work? An academic study took a close look at several of the criminal gangs involved in reshipping and how they operated. Conducted with the help of the FBI and the U.S. Postal Inspection Service, the study found that this fraud is often undertaken by organized crime gangs. Most of the goods are ultimately shipped to Moscow and its suburbs. The study estimated that the gangs they examined used 1.6 million cards, and accounted for annual losses at $1.8 billion.

Daniel, who lives in Dallas, was looking for a way to make some extra money in February 2021. He saw a job posted on Indeed.com for a distribution associate. He contacted Shanghai Pudong Ship, which listed an address in Bergen, New Jersey. He was to receive, process and forward packages. Daniel did a short interview over the phone and completed an application. An email asked for his bank account information so that his monthly paycheck of $2,200 could be directly deposited, along with $40 for every package he handled.

Thinking this was a bit odd, Daniel did some research and found a company website. He checked the address on Google Earth and it appeared to be a real business address. After accepting the job, Dan received credentials for the company website where he could upload photos and other information. He was asked to open boxes and take photos of the shipping label and packing list. He was instructed not to open the individual boxes within the packages. The prepaid pdf mailing labels he received for UPS, FedX, and the Postal Service had the recipient addresses already filled in.

Daniel began receiving boxes of items, all addressed to him in his name. Over the next month, he handled roughly 40 boxes, containing items such as cordless drills, jewelry, phones and laptop computers. He shipped them to a variety of different addresses, all within the United States. He uploaded photos and other items into the company web portal as instructed.

Daniel reached out to the company when, after a month, he had not been paid. He never received a call back and was never paid for his work.

The study describes how "operators" set up web sites and recruit people, described as "mules" or "drops," to work for them. Once this framework is in place, "stuffers" pay for access to this system.

Mules are recruited by job ads, sometimes on sites such as Craigslist, promising as much as $2,500 per month. As part of the application process, the operators obtain copies of passports, driver's licenses, and other information from these victims.

Stuffers typically buy stolen credit and debit cards on the dark web and use these to buy goods from online sites, frequently purchasing high value goods such as laptops, phones, and luxury goods. They ask to have these addressed in the name of the card holder, but shipped to the mule's address. They contact the mules and have them open the boxes, take photos of the contents and the packing list, and provide those to the operators. (This may help lessen the risk that the mules will steal goods). Stuffers then provide mules with pdfs of shipping labels they are to use in shipping the goods to another address, which may even be initially in the U.S. The bank accounts used to pay for shipping labels are often opened by scammers using the information from their scam victims Scammers are continually recruiting new mules, and rarely use them for more than 30 days. The mules not only perform this work for free, they may be targets for law enforcement agencies tracing the stolen goods. Mule victims are at times victims of identity theft.

Often scams adapt and try new tactics. The **USPS warns** that in addition to Moscow, reshipping scams may have victims send goods to addresses in Nigeria, Estonia, Lithuania, Romania, and Germany.

Email sent from scam employer to candidate (typos left in)

Dear Daniel XXXX,

Accounting Department is requesting your payment information to add you to the payroll.
Distribution Associate is paid **$2200 fixed** and additional bonus **$40**for successful package sent on time (paid monthly). **Average monthly income after Federal and State taxes is $3600**. Tax will be taken out automatically and at the end of the year, employee will receive W-2 Form in order to files tax return.

Payments are issued once a month on your pay day. All packages MUST BE SENT before the paycheck is issued every month. Any delayed tasks might cause payroll being on hold. The first payment is issued **after 30 or 31 days** from the date the first package has been shipped out. It might take additional 24-48 hours for the banks to process your payment ONLY for the first time for security purposes. We want to make sure that your payment information is accurate, thus we check it twice for you.

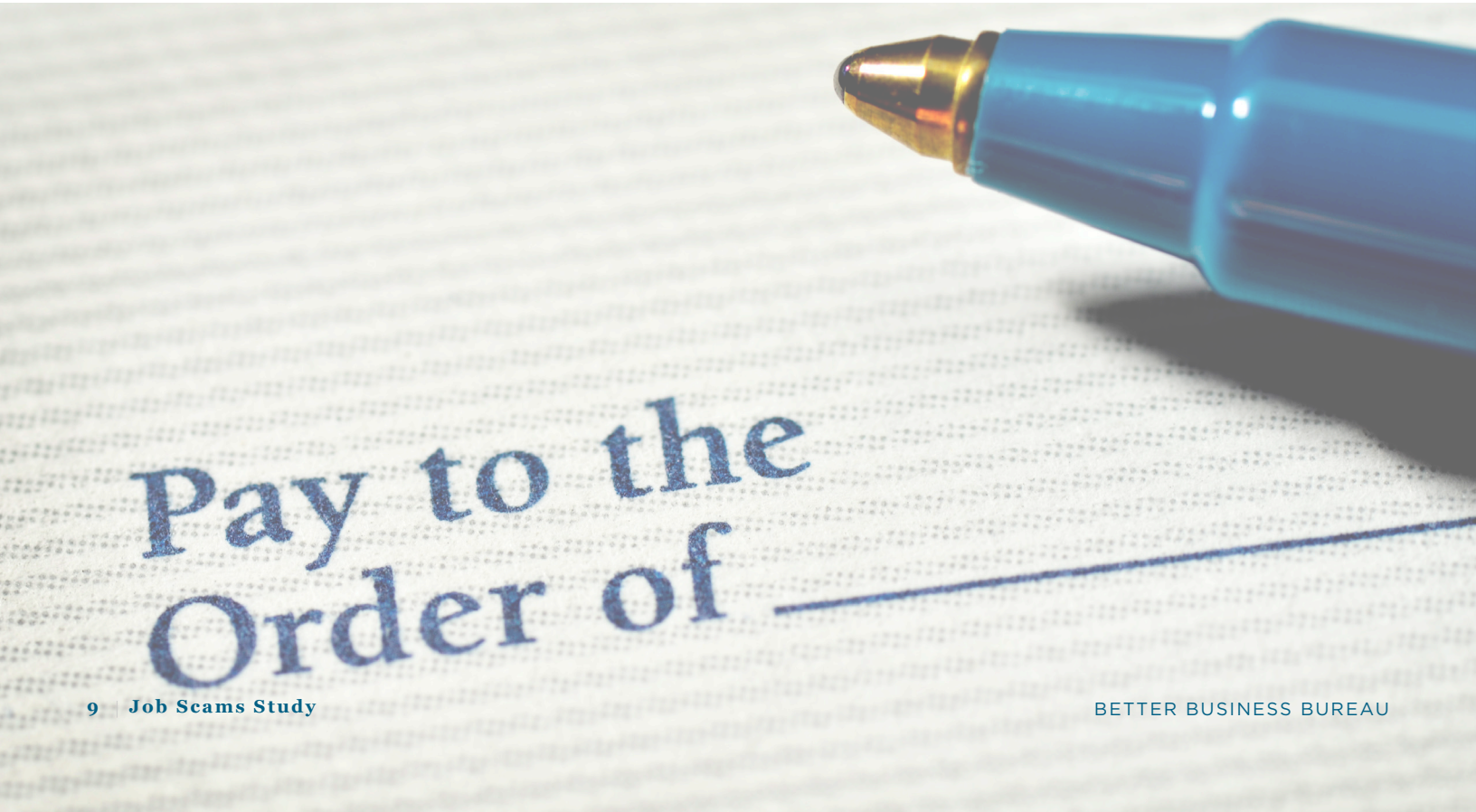
1. **If you would like to be paid by direct deposit to your personal bank account, pls provide the following information.**

Bank Name:
Bank Address:
Account Holders Name:
Account Number:
Routing Number:
Account type (Checking/Saving):
Note: The account you would like to use to get your salary needs to be registered on your name.

2. **If you would like to be paid by PayPal, please provide the email address linked to your PayPal account. Note: 3.4% commission fee is deducted by PayPal.**
3. **If you would like to be paid by check, please provide your mailing address.**

Other job scams that hire victims to aid fraud activities

International scam gangs not only rely on "hiring" victims in the U.S. and Canada to reship goods, they also want help in receiving and laundering money from other fraud victims, mailing fake checks or other scam materials to victims, or otherwise providing assistance in furthering the scams and making it difficult to learn who is truly behind them. Many victims do not realize that they are helping a fraud gang, and may well end their involvement when the pay promised does not arrive. Unfortunately, some become active paid co-conspirators who can be and are prosecuted for their activities.



JOB SCAMS INVOLVING FAKE CHECKS

While 36% of those responding to a BBB survey said that they had encoutered fake checks scams, the actual number is likely higher. Fake checks are a groing fraud problem with a variety of different job scams employing them.

HOW BIG OF A PROBLEM ARE FAKE CHECKS?

Bogus check fraud was the **subject of a 2018 BBB study.** Most fake checks are business checks, often stolen by scammers from mail and then altered by Photoshop or similar programs. They usually look professional, and victims believe they are real. Scammers may change the phone number of the business on the check so that it is answered by another scammer if someone calls to see if it is legitimate.

The FTC also gave fake checks a hard look in a **report issued in February 2020**, which found that 51% of those reporting a fake check were victims of a job scam. The FTC also similarly reported a big increase in complaints involving fake checks, finding that they increased 65% between 2015 and 2019.

Since then, the number of reports of fake checks has increased substantially, even though the overall use of checks in general use has gone down. The banking system updates fake check fraud data every two years. As the **previous BBB study on fake checks** noted, in 2016 fake checks cost the banks $789 million that they could not recoup from customers, up 25% from two years before. The **newest data**, released in January 2020 but providing results for 2018, shows that over two years these losses went up to $1.3 billion, a 40% increase.

Banks are obviously trying hard to detect and prevent fake checks from entering their systems. They report that they were effectively able to stop 91% of these checks, preventing $13.5 billion in annual potential losses. Despite these efforts, it is clear that fake check fraud continues to be a growing problem.

Two things everyone needs to know about checks

1. Having funds credited to a bank account does not mean the 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 when the check works its way back to the bank that supposedly issued the check and it is discovered to be counterfeit, the bank has the right to recover the money from the account holder.

2. Cashier's checks and postal money orders can be forged. A cashier's check is 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, 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 the next day. The same holds true for postal money orders. But they can be counterfeit.

Common fraud that employ fake checks

The majority of complaints about fake checks involve some sort of employment. But for fraudsters, the possibilities are almost endless, so the frauds covered below are far from exclusive. Again, the central message is the same – just having the money credited to a checking account does not mean the check is good, and you should never have to pay in advance to get a job.

Laptops or other equipment needed to do the job

BBB complaints reveal a wide variety of scams that contact victims, do at least a cursory interview, and then offer them a job working from home. What all of these have in common, however, is that victims supposedly need to buy a new phone, laptop computer, or other equipment in order to perform the job. But the scammers tell people not to worry about this cost, because they will provide a check in advance to cover the expenses. Victims deposit the check, and when the bank has credited the money to their account they believe that the check is valid. Victims then send money to pay for the items needed for the "job," (which they never receive). When the bank discovers that the check is no good it takes money from the victim's bank account to cover the loss.

There are several basic fake job scams that use these tactics.

Lisa lives in Oakland and was out of a job due to the pandemic. After posting her resume on Indeed.com, she received an offer for a chauffeur job, driving a Dr. Barron in San Francisco to Los Angeles for $1,000 per week. In interviews, email and text messages, Dr. Barron said she would mail Lisa money to cover initial expenses, such as getting a suit and renting a car. Lisa received a $6,000 cashier's check, which gave her confidence that it was valid, and deposited it into her bank account. She bought a suit at Men's Wearhouse. To pay for the car rental, she had to deposit $5,000 into a specified account at a Bank of America branch in Alameda. She never received paperwork for the car rental.

Lisa also received text messages asking her to buy four $100 gift cards at Walgreens for items the doctor needed. She scratched off the numbers and texted photos of the numbers to Dr. Barron. But Lisa soon learned that her bank account was overdrawn because the cashier's check was fake. Lisa had to take out a loan to cover the check and is still making payments to the bank. She has not been able to reach Dr. Barron.

Secret shopper 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 issue warnings about this fraud on almost a daily basis. Those operating this fraud contact victims offering jobs as mystery shoppers and later sending them fake business checks. Victims are directed to deposit the check into their own checking account, then to mystery shop a retail location, often Walmart. Every U.S. Walmart has a MoneyGram counter (Walmart in Canada has Western Union). **The FTC found** that nearly half of fake check job scams involved mystery shopping fraud.

Consumers are told to wire transfer part of the money from the check they had received, write up a report on their experience at the store, and keep the rest. For example, the fake check is for the sum of $2500, and victims are directed to send $2100 and keep the "remainder" as their pay. But the checks are fake, and victims are simply sending their own money to the crooks. Walmart reports that it never hires mystery shoppers and does not do business with anyone who does. In fact, the company actively attempts to combat this type of fraud. Walmart trains its employees about common frauds, such as fake check frauds, and even gives them an award if they spot and stop a fraud transaction.

More recent variations of this fraud provide fake checks and ask people to visit Walmart, drug stores, or other retailers and ask their "shoppers" to buy gift cards, take a photo of the numbers on the back of the card, send that back to the fraudsters, and complete their report. After being supplied with the gift card number the fraudsters can sell those on underground marketplaces and get the money.

There is a real mystery shopping industry – but none of them ever send checks in advance to such shoppers. Businesses do at times hire people to visit a retail location to evaluate it and often have them make a small purchase and report back. This allows a business to gauge the levels of customer service, cleanliness, and other aspects of a location. Most of those engaged in this business are part time workers who are normally paid after their efforts are completed.

This industry is organized as MSPA Americas. The MSPA is regularly contacted by victims of these frauds. Executive Director Rich Bradley says that the MSPA hears from victims every day, and may even hear from five to ten people per day. In addition, the frauds often impersonate the MSPA or its members. **BBB has warned the public about mystery shopping fraud. The FTC has warned of this as well.**

Car wrap frauds

BBB receives many complaints from victims who are approached by email or on social media to "shrink wrap" their cars with advertisements for Red Bull, Monster Energy Drinks, Budweiser, or other companies and receive a monthly payment, often in the range of $200 per month, for doing so. Fraudsters tell victims that companies are happy to pay for this type of advertising. **BBB**, **AARP** and **FTC have issued warnings** about this type of fraud.

For younger victims the promised money could go a long way to helping with car payments. Victims receive a counterfeit check, which they are told to deposit, and then to send money through Western Union, MoneyGram, or gift cards -- 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.

Energy drink company Red Bull has worked with law enforcement, including the FBI, on this problem. The company's **website has 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 some businesses that really do pay people to place ads on their cars. Greg Starr, one of the owners of **carvertise.com** in Delaware, pays people, often Uber or Lyft drivers, to wrap their cars for hospitals, colleges or businesses like Buffalo Wild Wings. They typically pay drivers $300 to $1,000 per campaign for two to twelve months.

Starr says that they never send people checks, instead sending drivers to the locations where they can have their cars wrapped with an ad. Carvertise pays the company that wraps the cars. He also says that the frauds have begun impersonating his business and that they hear from victims once or twice a week. He says that this has been a growing problem, and that many of the victims they hear from are vulnerable and have low incomes.

Nanny or caregiver scams

Fraudsters often advertise "jobs" for nannies, baby sitters, caregivers for the elderly or disabled, housekeepers or tutors on Craigslist, at Care.com or at other job platforms. 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 a **consumer warning** and a short video explaining caregiver frauds and how to avoid them.

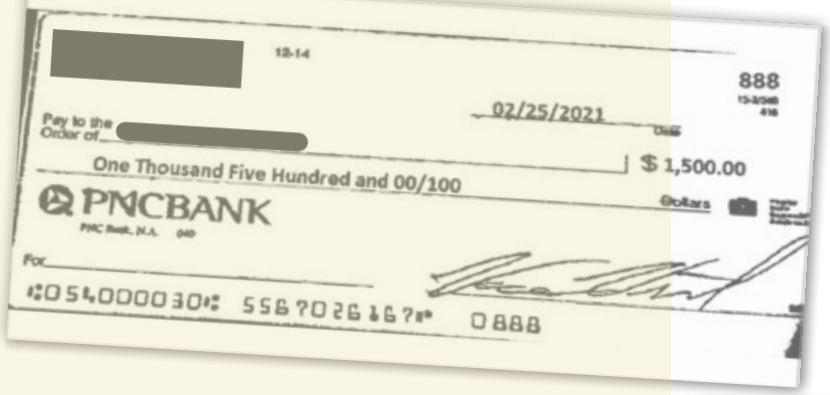
Care.com is the largest online forum for caregivers or potential employees, operating in 20 countries. They frequently hear about these frauds trying to operate on their system, almost all of which involve fake checks. This company made efforts to prevent fraud through its services, and complaints received have dropped by "high double digits."

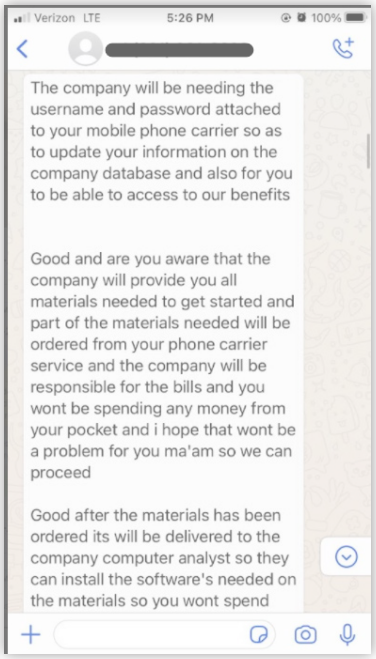
Both caregivers and members have to create a profile to take part. The company examines the "digital fingerprint" of those joining their service. For example, they try to see if the IP address of the computer matches the location claimed in the profile. Care.com provides **extensive resources in its Safety Center** so that members learn how to identify, avoid, and report instances of fraud.

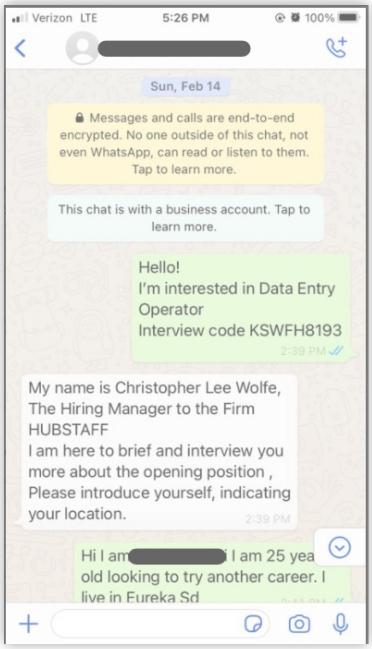
Small business scams

Many victims of fake checks scams are small businesses. Often these include a small business supposedly being hired to do work. House painters, for example, often encounter fake check fraud. BBB Scam Tracker also received many complaints from people who believed that they had been hired to do photography work.

A recent BBB survey of frauds affecting small businesses, the Scams and Small Business Research Report, found that fake checks were one of the top five scams identified as putting small businesses at risk.

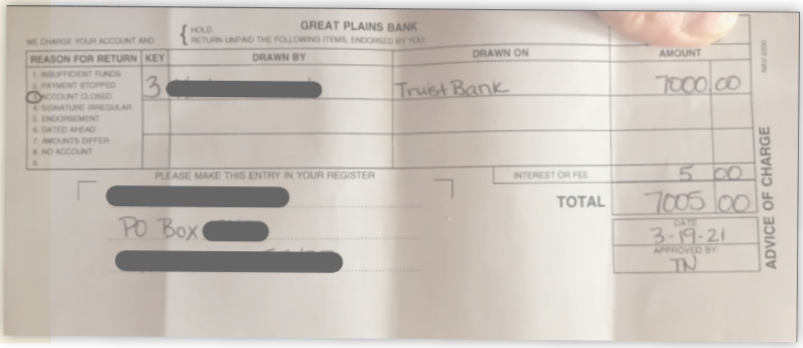






Tasha, who lives in South Dakota, wanted to earn some extra money. She saw an ad on Facebook for a data entry job paying $20 per hour, handling payroll and other items for a company claiming to be Hubstaff. She applied, interviewed through some questions on Whatsapp and was told she was hired. The interviewer wanted to know what kind of phone she had so that she could get the equipment needed to do the job. They asked her for a $500 downpayment for the phone, which they said would be reimbursed. She didn't have that much money, so they asked her to buy two eBay gift cards for $250. Tasha bought two gift cards in that amount, scratched off the numbers on the back, and texted those numbers to Hubstaff. She was then told that they would send her a check to deposit to cover the additional costs needed before she could start work.

Tasha got a pdf of a business check for $1500, and tried to deposit it using her banking app. It was rejected. The "employer" then sent her a check for $7,000 in the mail and told to deposit it at an ATM or with a bank app. Since it was a large check, she went to a teller at her bank and asked if the check was good. The bank told her it looked legitimate, but that they could put a hold on it for ten days. A few days later, the bank told her that the check was counterfeit.



Other types of fake check scams

The frauds discussed here are not exclusive. In any transaction where a check arrives, consumers need to remember that the fact the money is credited to the bank account does not mean the check is good.

Who is behind job scams?

An in-depth study of **reshipping scams** found that most of the goods purchased with stolen credit cards were shipped to Russia. The evidence suggests that many of these scams are operated from Eastern Europe.

Many **fake check scams originate in Nigeria,** and are a hallmark of organized criminal gangs operated from there. **Another recent look at this area** similarly found that Nigerian scam gangs are involved in Business Email Compromise, fake checks and other scams at the same time.

ACTIONS TAKEN AGAINST JOB SCAMMERS

The FTC has been actively combating some types of job scams, but those employing fake checks or reshipping have generally not been in its domain, since it does not have criminal enforcement authority. The FTC has taken action against a fake job placement company that claimed to have high paying jobs available for private equity and venture capital firms and that charged up to $2500 for "recruiting fees." In addition, the FTC has taken action against a variety of work from home business opportunity companies. It charged that some multilevel marketing companies touting work from home businesses were actually pyramid schemes and made false earnings claims.

- **Singapore police recently busted a Malaysia based job scam that operated internationally.**
- **Law enforcement has been very active recently in addressing the activities of money mules and others that have, knowingly or unknowingly, assisted international scam operations. In December 2020, for example, the DOJ announced the results of a worldwide effort to deal with money mules, resulting in action taken against 2300 people.**
- **DOJ also brought criminal cases against reshipping scams in at least Oakland, California and in Idaho.**

BBB EFFORTS *to* COMBAT JOB SCAMS

BBB actively attempts to help fight job scams in several ways. Those seeking a job can research employers at BBB.org to learn whether they are a real company and, if so, learn about its reputation. **BBB recently warned consumers about a West Virginia company that was hiring staff as part of a reshipping scheme.**

In addition, **BBB has conducted research on job scams**, done consumer education on this topic, and posted profiles about business entities running job scams.

BBB has released tips and warnings about **holiday job scams**, **summer job scams**, **job scams that target college students**, and the extent of **job scams in particular locales such as Maryland** and **New York City.**

TIPS TO AVOID JOB SCAMS

- Research the job offer. Call or go directly to the actual company's website for contact information to verify the job posting.
- Check on businesses offering jobs at BBB.org.
- Do an internet search with the name of the employer and the word "scam" to see if there are reports involving job scams.
- Examine the email address of those offering jobs to see if it matches the protocols used by an actual company. Be alert to gmail business email addresses.
- Consider creating a separate email address when posting a resume on job boards or applying for jobs. This can help detect "offers" from scam employers you did not contact.
- Consider setting up a second bank account simply to handle pay for jobs where you have never met the employer in person.
- If you're paying for the promise of a job, it's most likely a scam.
- Be very wary of mystery shopping or secret shopper positions.
- Work-from-home jobs that involve receiving and reshipping packages are likely scams.
- Beware of jobs that involve receiving and forwarding money.
- Don't fall for a fake check scam. BBB is not aware of any legitimate job offers that send checks to applicants and ask them to send money to a third party.
- Be cautious in providing personal information such as your full address, birthdate and financial information in your resume or to unverified recruiters and online applications.
- Be wary of vague job descriptions.
- Even if you do the work, it still may be a scam.
- Do not respond to calls, text messages or emails from unknown numbers or suspicious addresses.
- Do not click any links in a text message from a number you do not recognize. If a friend sends you a text with a suspicious link that seems out of character, call them to make sure they weren't hacked.

Where to complain?

It is important that victims of job scams report them to:

Better Business Bureau - BBB.org or BBB.org/scamtracker.
Federal Trade Commission (FTC) - reportfraud.ftc.gov or call 877-FTC-Help.
Internet Crime Complaint Center (IC3) - ic3.gov/complaint.
Canadian Anti-Fraud Centre - antifraudcentre-centreantifraude.ca or 1-888-495-8501.

Recommendations

- BBB suggests that job boards posting resumes for job seekers make extra efforts to screen out job scams
- Banks should enhance efforts to warn their customers about fake check scams.
- Employers should post all jobs online so people can check to see if offers are really being made by the employer.
- More efforts can be made to warn the public that job scams are common and on ways to avoid them.


BBB