92559-IDTHEFT-1021

Identity THEFT

Keeping You Informed!

MERCK SHARP & DOHME
FEDERAL CREDIT UNION
(215) 996-3700
msdfcu.org

Identity Theft NEWSLETTER

Vol. 23, No. 1 | Don't become the next victim... | Fall 2021

Reporting Fraud Just Got Easier

When you tell the FTC about frauds, scams, and other kinds of bad business practices, you're helping the FTC and law enforcement partners spot and stop scams. To make it easier, the FTC just launched **ReportFraud.ftc.gov**—a new version of the FTC's consumer reporting website.

By following a few short steps on **ReportFraud.ftc.gov**, your report is instantly available to more than 3,000 federal, state, and local law enforcers across the country. After you tell them what happened, you'll get advice from **ReportFraud.ftc.gov** on what you can do next to recover and protect yourself against fraud. ■

Avoiding Post-Disaster Scams and Fraud

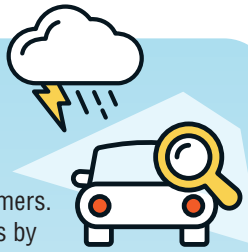
Coping with the aftermath of a natural disaster in never easy. As disaster victims find themselves in vulnerable financial situations, they can be targets of scammers pretending to be government employees, creditors, mortgage servicers, insurance adjusters, and contractors. Be alert to and aware of potential scams and fraud after a disaster strikes.

Adhere to the following basic practices to avoid scams:

1. **Do not be pressured into taking immediate action.**
   If someone is telling you that you need to act now, they are likely trying to prevent you from verifying whether the business is legitimate. Take your time.
2. **Be wary of anyone going door to door.**
   Scammers may pose as contractors, charity workers, or even government officials. Remember that if someone is trying to sell you something or asking for a donation, you can say no and then do the necessary research.
3. **Work with charities and services you know and trust.**
   Do research before donating to new organizations or using new services.
4. **Pay with a credit card whenever possible.**
   Paying with a credit card gives you the ability to reverse any fraudulent charges, adding an extra layer of protection.
5. **Ask for references, licenses, and certifications.**
   Make sure that anyone you hire is qualified and has all applicable licenses or certifications required by their field.
6. **Obtain offers in writing.**
   Ask for written estimates and contracts before you do business.
7. **Initiate communication.**
   Never make payments or give out personal information to someone on a phone call you did not initiate. ■

According to data from the Federal Trade Commission, by the end of 2020, consumers reported losing more than **$3.3 billion to fraud,** up from $1.8 billion in 2019. Nearly **$1.2 billion of losses reported last year were due to imposter scams,** while online shopping accounted for about $246 million in reported losses from consumers.

Don't Be Fooled Into Buying A "FLOOD CAR"



Damaged cars can be resold to unsuspecting consumers. When vehicles damaged by floods are deemed a loss by insurers, owners are paid off and the cars are moved to a salvage yard to be sold for parts. However, roughly half of these "flood cars" are instead purchased, cleaned up, and resold to dealers and individual buyers.

Flood water can do an amazing amount of damage to a vehicle, ruining nearly every system. Even if a vehicle is cleaned up, there can still be lingering issues. Rust, mold and mildew can attack critical parts, compromising the vehicle's safety and endangering occupants.

Tips to avoid buying a flood car:

- **Enter the vehicle identification number (VIN) at VINCheck, nicb.org/vincheck** (a free service from the National Insurance Crime Bureau, which could reveal a vehicle's flood damage).
- **Have a trusted auto repair person inspect the car prior to purchasing.**
- **Look for signs of water damage,** such as musty smells or fragrances that suggest the seller is trying to coverup smells, and carpeting that looks too new, is discolored, or has water stains.
- **Look for mud, silt, or rust.** Check engine crevices and exposed screw heads, the glove compartment, door panels, and under seats and the spare tire well for water lines or signs of mud, silt, or rust.
- **Look out for water condensation, fogging, or water lines** inside headlights, taillights, and dashboard gauges.
- **Repeatedly test electrical equipment,** such as wipers, turn signals, the heater and air conditioner, and power windows and locks. Also check engine wires; if they do not bend easily, they may soon crack due to water damage. ■

How to Recognize and Avoid Imposter Scams

Imposter scams often begin with a call, text message, or email. The scams may vary, but work the same way—a scammer pretends to be someone you trust and attempts to convince you to send them money or share personal information.

Scammers may ask you to transfer money from your bank, wire money using a company like Western Union or MoneyGram, put money on a gift card, or send cryptocurrency, because they know these types of payments can be hard to reverse. Scammers call, email, or text and claim to be:

- **A family member** (or someone acting for them), saying your relative is sick, has been arrested, or is in serious trouble and needs money right away.
- **From the Social Security Administration,** claiming that COVID-19-related office closures mean your benefits have been suspended.
- **From your bank,** claiming they need to verify personal information before they can send you a new debit or credit card.
- **A court official,** indicating that you failed to appear for jury duty and need to pay a fine or you will be arrested.
- **The police,** saying you'll be arrested, fined or deported if you don't pay taxes or some other debt right away.
- **From the IRS,** saying you owe back taxes, there's a problem with your return or they need to verify information.

Follow these tips to help protect your money and personal information:

- **Be suspicious of any call from a government agency asking for money or information.** Government agencies don't use threats and they don't call you with promises of or demands for money.
- **Don't trust caller ID**—it can be faked.
- **Never** pay with a gift card, wire transfer, or cryptocurrency to anyone who tells you to.
- **Check with the real agency, person, or company.** Don't use the phone number they give you. Look it up yourself.

Report any fraud, tell your bank or credit union and be sure to share these tips with friends and family.

– FTC and the American Bankers Association Foundation

Scams that Start on Social Media Platforms Skyrocket

As of April 2021, 3.96 billion people identified as users of social media, representing half of the 7.7 billion of the world's population, including more than 70% of the population of the United States. Globally, the average person spends more than 2 hours per day on social media. It is not surprising that criminals have focused their attention on these internet platforms as a way to gather personal information, gain trust, and socially engineer their way to fraud that results in billions of dollars of losses annually.

Important tips to always follow:

- **Don't take the "bait."** Never click on pop-up messages, posts that contain content that seems shocking, scandalous, or too good to be true, or links or attachments in unsolicited emails and text messages.
- **Create a strong password.** This means that it is a minimum of seven characters and contains a mixture of upper and lower case letters, symbols, and numbers. You should never provide your password to someone you do not know.
- **Don't provide your information (personal or financial) online unless you know the website you are using is legitimate, secure, and encrypted.** It is also important to make sure that you are dealing with the right entity and using its real website and not a look-alike site created by a scam artist. Also, look for "https://" (the "s" stands for secure) before a web address.
- **Delete unsolicited emails and text messages that request personal or account information.** Companies you do business with already have this information and do not need to verify or confirm it. If there is a security breach, most companies contact their customers in writing to alert them of the breach.
- **Contact companies only through trusted channels.** If you are concerned about an email or other message you received, call the company immediately at its publically-listed phone number. Never trust the phone number or email address given in the message.
- **Verify the person you are dealing with is who they claim to be, and not an imposter.** Contact a friend or family member who could confirm the person's story, or try contacting the real person at a phone number you know is correct.
- **Don't be rushed into sending money immediately or secretly.** Don't send money by wire transfer, overnight delivery, or reloadable cards unless you are absolutely certain that you are sending money to a real friend or family member. ■

Federal law allows you to get a **FREE COPY** of your credit report, at your request, every 12 months from each credit reporting company—Equifax, Experian, and TransUnion.

AnnualCreditReport.com
877.322.8228

Scammers Advertise Jobs the Same Way Legitimate Employers Do

Scammers promise you a job, but what they want is your money and personal information.

Here are just some examples of job scams:

- ✓ **Work-from-home job scams**
- ✓ **Mystery shopper scams**
- ✓ **Nanny, caregiver, and virtual personal assistant job scams**
- ✓ **Job placement service scams**
- ✓ **Government and postal jobs scams**

Before you accept a job offer, take these steps to protect yourself from job scams:

Do an online search. Look up the name of the company or the person who's hiring you, plus the words "scam," "review," or "complaint." You might find out they've scammed other people.

Never respond to ads guaranteeing you'll get a job. Even if your qualifications are ideal, it's never a sure thing that you'll get the job.

Never pay to get a job. Scammers may say they have a job waiting if you just pay a fee for certification, training, equipment, or supplies. But, after you pay, you find out the job is fake—and you won't get your money back.

Don't bank on a "cleared" check. No legitimate company will ever send you a check and then tell you to send on part of that money, or gift cards. It's a scam—that check is a fake and you'll lose your money.

Don't believe ads for "previously undisclosed" federal government jobs. Information about federal jobs is publicly available at **usajobs.gov**

Find legitimate job listings. Try visiting sites like your state's **CareerOneStop.org** ■