UGEFCU
UTICA GAS & ELECTRIC FEDERAL CREDIT UNION
Celebrating 81 Years…1937 - 2018

215 Old Campion Road
New Hartford, NY 13413
(315) 733-1596
www.ugefcu.com

For more identity theft prevention tips, call or stop in to UGEFCU today. And if you ever become a victim of identity theft, remember that we're here to help.
(315) 733-1596
Toll-free 800-990-7499
www.ugefcu.com

NCUA

Census Related Fraud

by usa.gov

The U.S. Census Bureau collects data about the people and economy of the United States. It collects personal and demographic information from people and businesses. Some scam artists may pretend to be working for the Census Bureau. They'll try to collect your personal information to use for fraud or to steal your identity. These scam artists may send you letters that seem to come from the U.S. Census Bureau. Others may come to your home to collect information about you.

Report Census Related Fraud

If you suspect fraud, report it to the Census Bureau's regional office for your state.

Forward scam emails to the Census Bureau at ois.fraud.reporting@census.gov.

How to Protect Yourself. Follow these tips to ensure that your personal information stays safe:

Do:

- Verify that the study is legitimate. Check the survey name on the Census Bureau's list of surveys .
- If someone comes to your home and claims to be a census worker, verify that they work for the Census Bureau.
- Look up the employee's name in the Census staff directory.
- Ask to see their badge. A Census Bureau badge has a picture of the field agent, a Department of Commerce watermark, and an expiration date.
- Follow these tips to help you spot census scams, so you don't become a victim.

Don't:

- Don't share your full Social Security number, bank or credit card account numbers, or your mother's maiden name. The Census Bureau won't ask for this type of information.
- Don't trust emails claiming to be from the Census Bureau. This agency sends letters to invite individuals to take part in its surveys. If you get an email from the Census Bureau, it's probably a scam.
- Don't trust caller ID. Call the Census Bureau's National Processing Center to verify a telephone survey.

Ticket Scams

by usa.gov

Ticket selling scams happen when a scammer uses tickets as bait to steal your money. The scammer usually sells fake tickets or you pay for a ticket, but never receive it. They are common when tickets for popular concerts, plays, and sporting events sell out. Scammers, including individuals and fake resale companies, take advantage of the situation by:

- Charging prices much higher than the face value of a ticket
- Creating counterfeit tickets with forged barcodes and logos of real ticket companies
- Selling duplicates of a legitimate ticket and emailing it to several buyers.
- Pretending to sell tickets online to steal your credit card information

Report ticket scams

There are several options to report a ticket scam.

- Contact your state consumer protection office.
- Contact the Federal Trade Commission (FTC) using the Online Complaint Assistant.
- File a local police report, especially if you met the scammer in person or have a picture of them to give the police.
- File a complaint about a ticket company using the Better Business Bureau's Scam Tracker.
- If you paid by credit card, report the problem to the card company. You may be able to dispute the charge.

How to protect yourself

Learn what you can do to avoid becoming a victim:

Do:

- Buy tickets at the venue box office.
- Buy tickets from authorized brokers and third party sellers, with verified contact information.
- Verify that the seller has a real physical addresses and phone numbers. Scammers often post fake addresses, PO Box, or no address on their websites.
- Check the actual web address of the resale ticket seller. Some scammers create phony websites that closely resemble authentic ticket company websites.
- Search for negative reviews about the seller. Use the seller's name, email address, and phone number, along with the words "fraud," "scams," and "fake tickets" for your online search.
- Look at the tickets before you buy and verify the date and the time printed on them.
- Make sure the section and seat numbers on the tickets actually exist at the venue.
- Have the seller meet you in person in a public place for the ticket exchange.
- Ask the seller for proof that they bought the tickets, if you are buying from an individual.
- Use a credit card to pay third party sellers. Your credit card offers protections, if you need to dispute a charge.
- Check for complaints against a ticket seller with your state's consumer protection agency.

Don't:

- Don't wire transfer money to pay for tickets.
- Don't trust sellers who want you to pay with a prepaid money card.
- Don't pay before seeing the tickets
- Don't meet an individual ticket seller alone or in a low-traffic area.
- Don't automatically trust online search results for ticket sellers. Search results can include paid ads, sellers that charge high fees, and scams.

Social Security Imposter Scam

by Fraud.org

One of the most sensitive pieces of personal information is a consumer's Social Security number (SSN), used by companies, the government, and other institutions to identify individuals--and highly sought-after by identity thieves.

In our era of data breaches, electronic transactions, and privacy concerns, scammers are aware of how concerned consumers are about guarding their SSNs, and that is why we are seeing an increase in the "Social Security imposter scam."

The Federal Trade Commission received more than 76,000 reports about the Social Security imposter scam in the past 12 months alone. With average losses of $1,500, this new scam is quickly becoming one of fraudsters' favorite tricks.

The scam usually begins with a consumer receiving a call from someone claiming to be with the Social Security Administration. The caller informs the victim that their SSN has been suspended because it was stolen or has been involved in a crime.

In a variation on this scam, the caller may also reach out to tell a victim that they qualify for an increase in benefits. All they need to do is provide the scammer with some information. Typically, these callers will ask their victims several questions to get personal information that they can then use to steal their identity or drain their bank accounts.

Because of the numerous data breaches, these scammers may have access to accurate personal information—such as an individual's real SSN—that they can use to build trust and appear legitimate. Regardless, before concluding the scam, fraudsters will almost always request payment to "unfreeze" the SSN or to process the increase in benefits. The scammer may request that they be paid via an unusual payment method such as by gift card, or some form of cryptocurrency like Bitcoin.

One complaint we received from a consumer in Florida is typical of the scam:
"I received a call from the Social Security office explaining my Social Security number had been stolen and someone is committing money laundering [with the number]." The thieves had "abandoned a car with drugs in it, [that was] purchased in my name [and] found in Texas."

In order to resolve the issue, the consumer was "told to secure assets by purchasing gift cards," and provide the gift card numbers to the Social Security office. The consumer was told that he would receive a refund equal to the amount he paid to unfreeze their account by the Federal Reserve in a few weeks.

Unfortunately, the consumer never received a refund, and he lost nearly $20,000 to this scam.

While the scam can be devastating, there are several steps you can take to prevent yourself, and your loved ones, from falling victim to this scam:

(continued next column)

• Don't trust caller ID. Scammers are very good at spoofing your caller ID to make it appear they are calling from a government agency. If you receive an unexpected call from Social Security, don't answer it. **Instead, call Social Security's customer service number at 1-800-772-1213 to see if they were actually trying to contact you.**

• Remember, Social Security will never suspend your Social Security number. If someone contacts you saying your number has been suspended, they are trying to steal from you.

• Social Security will never call and demand that you wire them money or pay them with gift cards or cryptocurrencies like Bitcoin. Any supposed Social Security officer that makes this request is a fraudster.

• Don't give out your personal information on request. If you are asked to confirm your Social Security number or bank account number by a phone call or email you did not initiate, it is a scam.

• Don't trust a caller just because they know some of your personal information. Sadly, due to numerous data breaches, we have received reports that fraudsters are providing victims with their SSN to build trust. Just because an individual knows your Social Security number or some other piece of personal information, they are not necessarily legitimate.

• Spread the word. The Social Security imposter scam is relatively new, and many Americans may be unaware of it. To prevent additional victims from falling for this scam, we need your help. Please mention this scam, or forward this alert, to friends and loved ones. Together, we can stop this scam from growing, and protect Americans from identity theft, and prevent victims from losing their savings to fraudsters.

The Social Security imposter scam can be difficult to detect and is growing in popularity. If you come across this scam, or if you fall victim to it, report it! You can file a complaint at Fraud.org via our secure online complaint form. We'll share your complaint with our network of more than 90 law enforcement and consumer protection agency partners who can and do put fraudsters behind bars.

Become a Smarter Consumer

Avoid Fraud:

- Know who you're dealing with
- Pay the safest way
- Guard your personal information
- Stay safe online
- Be cautious about unsolicited emails
- Resist pressure
- Don't believe promises of easy money
- Fully understand the offer
- Get off credit marketing lists
- Check your credit reports regularly
- Be cautious about offers for credit monitoring services

Protect Your Digital Data

by Fraud.org

In today's connected world, protecting your online data is one of the most important things you can do to prevent fraud.

You can do this by:

• Never reuse passwords across different websites. Reusing passwords allows hackers access to several accounts if one of them is compromised by a data breach. A password manager program can help you here, since it relieves you of having to remember multiple passwords for different sites.

• Opting-in to multi-factor authentication whenever possible. TwoFactorAuth.org is a good resource for finding out which services offer multi-factor authentication to their users.

• Using strong passwords. Strong passwords are longer and utilize both uppercase and lowercase letters, as well as numbers, and do not contain common phrases.

• Checking out Fraud.org's Latest Breaches HQ for the most up-to-date information on recent data breaches. Educate yourself on the more prevalent scams.

Check out some of the worst scams featured in our past Fraud Alerts. Getting familiar with those scams and learning how to identify the red flags of fraud is a good way to avoid falling for it.

Listen to your gut. Scammers tend to play on our sense of hope and optimism. If you get an offer that seems too good to be true, it probably is.

Never pay for a prize in a lottery or sweepstakes. If you are asked to pay for your prize, it is a scam.

Take a breath. If you receive an urgent request, take a moment before acting. Scammers often rely on creating a false sense of urgency to get their victims to act without thinking clearly. If someone is pressuring you to act immediately, take a moment to think about what they are asking you to do.

If something seems off, do some research. Do a web search to see if other people have been approached with a similar situation and if it was a scam. Likewise, if you think someone is acting suspicious but is affiliated with an organization, contact that organization directly to see if the individual in question actually works there.

Unfortunately, even if we do everything we can to protect ourselves, fraudsters can still trick us. If you have fallen victim to a scam, you should file a complaint at Fraud.org via our secure online complaint form. We share complaints with our network of nearly 200 law enforcement and consumer protection agency partners who put fraudsters behind bars.

FRAUD!ORG
a project of the National Consumers League

Report scams to the National Fraud Information Center/ Internet Fraud Watch at fraud.org.
Sign up for email scam alerts and read more scam articles.

Long-distance Free Cruise Scam

by Fraud.org

In this scam, a victim receives a piece of mail notifying them that they won a free cruise. All they need to do is call a number in the envelope to claim it. Unbeknownst to the consumer, the number, which appears to be American, is really from a foreign country, and calls to claim the prize can cost as much as $5.00 per minute. The scammers on the other end of the line will try to extract as much personal information as they can from their victim--like their Social Security number and bank account info--so that they can steal their victim's identity or sell their information to other scammers. In the end, there is no cruise. Instead, the victim is left with an astronomically high phone bill and an increased risk of becoming a victim of identity theft.

The hidden sales pitch scam

In this scam, the fraudster uses the offer of a free cruise to lure their victim into a lengthy, high-pressure sales pitch for a timeshare. Under the ruse of coming in to pick out their accommodations, the "lucky winner" will be subjected to an hours-long timeshare presentation. In some cases, these pitches may even take place on the cruise ship, where attendees are held captive and have no other choice but to be subjected to lengthy pitches for an overpriced timeshare.

Many consumers who are able to endure these high-pressure sales tactics and actually receive their free trip are then subjected to more high-pressure sales tactics to upgrade their trip. These passengers often report dismal cruise conditions and ships that lack common amenities like air conditioning.

The not-so-free "free" cruise offer

In this iteration of the free cruise scam, a consumer is informed that they have won a cruise, and they just need to provide their credit card number for "incidentals" like port fees and taxes. These "incidental" costs, however, quickly add up to more than what they would have paid had they purchased a trip through a respected travel agent or directly from a cruise line. To make matters worse, the cruise they purchased may be on a very old and outdated ship that is woefully in need of a renovation.

While it is certainly possible to win a free cruise, it is important to keep these tips in mind to navigate around any potential scams:

1. <u>You cannot win a prize from a contest that you did not enter.</u> If you don't remember entering any contest where a cruise was a prize, you are probably talking to a scammer.
2. <u>Do your homework.</u> If you are offered a free cruise from a contest you entered, ask for the name of the travel agency and then check their online reviews and Better Business Bureau rating. Some state Consumer Protection departments may also have business-lookup services that share data about complaints. As a big destination for cruising, Florida's lookup service is especially useful. If a cruise operator or travel agent has received a lot of complaints, if they aren't registered in the state they say they are, or if consumer reviews describe hidden sales pitches or complain about additional fees, it is probably a scam.
3. <u>If you purchase any upgrades, pay with a credit card.</u> By paying with a credit card, you have more options to dispute the charge if it turns out to be a scam. Avoid a business that asks for payment through a wire transfer or cash, which leave you no way of getting your money back if it turns out to be a scam.
4. <u>Never pay for a prize.</u> If you really won a cruise, it should be free and include all taxes and fees. You may be offered to book a night at a hotel the night before your trip or to upgrade your room, but the base prize (and fees) should be free.
5. <u>Be wary of high-pressure tactics.</u> If the prize giver is pressuring you to make a decision or to act quickly, there's probably a catch. Carefully study the documents they provide and ask them to clearly explain any vague fees, your accommodation class, the ship's name, and cruise line, etc. If they refuse to provide you with the details you request, it is probably a scam.