The Commercial & Savings Bank

www.csb1.com
800.654.9015

S C A M S

Have you ever....

....been threatened in some way for a demand of money?

....been told there is money waiting for you but you need to send money to cover various expenses?

.....been pushed to act "before time runs out"?

.....been asked to buy a gift card and send the card number to someone else?

.....been told your social security account has been deactivated and can only be resolved with payment?

....been asked to initiate this transaction through a social media platform?

.... "met" someone online who is asking you for money?

.....been told not to say anything to your bank or family members?

.....been told there is a warrant for your arrest and can only be resolved with payment?

Do Not Let Yourself Become a Victim of Fraud!

Selling Scams

If you attempt to sell something online, you could encounter this type of scam. A buyer wants to send you a check for a higher amount than your asking price. You are instructed to deposit the check and then wire the extra amount back to the buyer.

With this scam, the check is deemed fraudulent (after you've deposited and wired the extra funds). If this occurs, you are responsible for the full amount of the check, including the amount you sent to the buyer.

Here's what you can do:

- Do not accept overpayments and do not send any funds back to a buyer.
- Don't accept checks or money orders. It is safer to accept cash or official checks.
- Be wary of buyers claiming to be overseas.
- Meet buyers in person in a safe, public place. Many police departments have a "safe lot" available for a meeting place.

Buying Scams

Online shopping is very popular and convenient. However, you need to practice safe shopping habits. Scammers may pose as a genuine seller, post fake ads (often with very low prices), or ask you to send payment before you see the item.

Here's what you can do:

- When buying an item online, only shop on trustworthy and reputable sites.
- Be wary of listed prices that appear too good to be true. If you have any doubts, don't go through with the purchase.
- The safest option is to pay the seller after you have inspected the item in person. Meet sellers in person in a safe, public place. Many police departments have a "safe lot" available for a meeting place.

Mystery Shopper Scams

Retailers will sometimes hire companies to help evaluate how their stores are doing. These companies hire people to go into a certain store, buy a specific product, and report back to them about their experience. The mystery shopper is then reimbursed for the cost of the product purchased in addition to being able to keep the product purchased, and sometimes paid an extra stipend.

This sounds like a great way to make some extra cash, right? Unfortunately, scammers think it's a great way for them to make some extra cash from you as well. In the attempt to try to trick perspective mystery shoppers, scammers will post opportunities but with stipulations.

Most commonly, scammers will post a fake opportunity and when you reach out with interest, they will send you a check, tell you to cash it, then to wire it back to them in the attempts to evaluate the money transfer service, such as Western Union or MoneyGram. The check will be found fraudulent weeks after you've sent the money back to the scammer, and you will be responsible for reimbursing the bank their money.

Scammers will also use tactics such as posting fake opportunities in the newspaper's "help wanted" section or sending them through email, requiring you to purchase a costly certification from them before being eligible for any assignment, or sell the jobs by guaranteeing that working as a mystery shopper for them will eventually lead to a higher-paying job with a well-known company later on.

Scammers will also tell you that you must pay them a fee for access to a full listing of available mystery shopping opportunities.

In any situation, the scammer is going to take your money and leave you without any mystery shopper job.

Here's what you can do:

- Never pay or wire money as a requirement to be a mystery shopper. The Mystery Shopping Providers Association (MSPA) website (mysteryshop. org), offers a free database of mystery shopper

opportunities available, as well as a free certificate that can earned but isn't necessary to access the database or apply for any of the assignments.

- Do your research before applying for or accepting a mystery shopper assignment. Gather as much information about mystery shopper programs and companies as you can before applying. Looking for reviews on the internet can be helpful, but do not be tricked by scammers posting fake positive comments or reviews for a company that is fraudulent.

Digital Currency and Bitcoin Scam

You are contacted by an individual that informs you there is a warrant out for your arrest, your social security number has been compromised, or some other threat or concern is brought to your attention by this individual. This person may even tell you they are with the IRS, law enforcement, or another organization.

Next, this individual tells you the only way to remedy this issue is through immediate payment, but not normal payment by cash, check, or wire, but using digital currency purchased at a digital currency or Bitcoin ATM or on the internet. After purchasing the digital currency or Bitcoin, the individual then instructs you to send them these funds electronically.

Always be careful anytime you are contacted by a person claiming you owe them money and never trust an individual that says payment can only be made through digital currency or Bitcoin. Digital currencies and Bitcoin are currencies with little government regulation and are often used by scammers. Whenever an individual requires you to purchase digital currency or Bitcoin in cash at a Bitcoin ATM or through the internet for payment, know this request is most likely not legitimate, but a scam.

Here's what you can do:

- Always resist the pressure to act quickly to any threat requiring immediate payment.
- Always remember legitimate agencies and organizations will never require digital currency or Bitcoin payment. Do no purchase or send the digital currency or Bitcoin to scammers.
- If contacted by phone, scammers may frequently call. You may need to consider blocking the scammer's phone number from your phone or change your phone number.

Pet Scams

You decide you want to adopt a pet for you or your family. You start looking online and find the perfect one, but the next thing you know, you've lost your money and still don't have the pet you wanted. With the rising popularity of selling things online, it has become common to look for pets this way too, but it comes with its risks.

Many scammers will create ads, social media posts, or even entire websites in the attempt to sell fake pets, most commonly puppies. Typically these ads, posts, and websites will look legitimate because they are copied exactly from an actual and legitimate business or person trying to sell their puppies.

You find a pet you want to adopt, contact the seller, and they insist that if you wire them money or send a prepaid debit card through the mail, they will ship the puppy to you. You send the money, but the pet never arrives.

Or the scammer is selling the animal for a very cheap price but requires a deposit from you to hold it until it is old enough to be adopted. But after the money is sent, the post for the pet disappears and the seller becomes unreachable. Either way, you never end up with the new pet because it was never real to begin with. The scammer was using pictures of an animal they found online and made the information up to trick you into buying the pet from them.

Here's what you can do:

- Do an online search of the exact ad, information posted on the website, and pictures of the animal. Since scammers will often copy the information verbatim and use fake photos, an online search will often turn up the original seller or possibly multiple other fraudulent ads with the exact same information.
- Always insist on visiting the animal and the breeder before purchasing, or only picking up and

paying for the pet in person to avoid being scammed out of your money and never being shipped the pet.

- If you're not paying for the pet in person, it's safer to use a credit card or a check instead of a wire transfer or a prepaid debit card so that your funds can be tracked and you have a chance of fighting the possibly fraudulent charge with your credit card company if the sale goes wrong.

- If the person and your intended future pet live too far away to visit and you still want to go through with the sale and have the seller ship the pet, always ask for the name and contact information of the shipping company and obtain all of the details of the pets shipment to verify the validity of the seller and their plans.

Family Emergency Scams

You get a call: "Grandma, I need money for bail." Or money for a medical bill. Or some other kind of trouble. The caller says it's urgent – and tells you to keep it a secret. But is the caller who you think it is?

Scammers are good at pretending to be someone they're not. They can be convincing: sometimes using information they've obtained from social networking sites or hacking into your loved one's email account, to make it seem more real. They'll pressure you to send money before you have time to think.

Here's what you can do:

- If you ever receive a phone call from a grandchild or other relative in danger or in trouble, and the immediate request is for cash – stop. Resist the pressure to act quickly.

- Hang up the phone and look up you grandchild's phone number yourself, or call another family member and then try to contact the person directly.

- Don't send money unless you have confirmed the legitimacy of the family member and the situation.

Online Dating Schemes

You meet someone special on a dating website. Soon the conversations move to email or phone calls. They profess their love, and soon thereafter request money, typically for some type of urgent scenario.

A scammer will create an account on a dating site or any form of social media with made up information and fake pictures, usually tailored to mirror your interests to create similarities between yourself and the fake profile. They may claim to be living, working, or traveling overseas. Therefore, they cannot meet in person. Some scammers go as far as making fake travel plans or even wedding plans, before always cancelling due to some extreme reason.

They will frequently ask for money for various reasons, such as to travel to meet them, for medical expenses for themselves or their fictitious family, or to help tide them over after a significant and financial setback that is usually caused by a traumatic event to help create a sense of urgency.

Here's what you can do:

- Never send money, credit card numbers, account information, or wire transfers to someone you met online, especially if you have never met in person.

- Only use dating sites that are well-known and reputable.

- Do a reverse image search using the profile picture of the person requesting money. You can try Google's reverse image lookup.

Charity Scams

Someone contacts you asking for a donation for a group that maybe you have heard of before. It seems legitimate and you want to help. How do you know if it is a legitimate group or not?

Here's what you can do:

- Never feel pressured to donate. Scammers may make it seem like you need to make a decision and pay immediately. This is simply not the case. Take your time and tell callers to send you more information by mail.

- Always do your research. Is it a real group? What percentage of your donation goes to the charity?

Is your donation tax deductible? How do they want you to pay? Rule out anyone who asks you to send cash or wire money, chances are that's a scam. You should also be careful with giving your payment information over the phone.

"You've Won" Scams

You get a call, card, or email telling you that you've won! The offer may be a trip, a prize, a lottery, or a sweepstakes. The sender is excited and can't wait to give you your earnings.

But here's what happens next: they tell you there's a fee, some taxes, or customs duties to pay. Then they ask for your credit card number or bank account information, or they ask you to wire money in order to claim your prize.

Either way, you lose money instead of winning it. You don't ever receive the big prize. Instead, you get more requests for money, and more promises that you've won big.

Here's what you can do:

- Keep your money – and your information – to yourself. Never share your financial information with someone who contacts you and claims to need it, and never wire money to anyone who asks you to without a legitimate business reason to do so.
- Think through the winning process. Did you enter the contest in the first place?
- Do your research. Try typing the company or product name into your favorite search engine with terms likes "review", "complaint", or "scam".

Ponzi/Pyramid Schemes

Ponzi and Pyramid schemes are types of investment fraud, promising high financial returns not available through traditional investments. Instead of investing funds, the scammer pays "dividends" to investors using the funds of other investors.

Many of these schemes will operate as legitimate selling-based companies, but eventually the scheme will fall apart, leaving many people without their money.

Here's what you can do:

- Watch for investments promising very little or no risk with a high return, investments and sellers that are not registered or licensed with the proper regulators, and investments that are secretive or have overly complicated strategies.
- Be sure your income is based on sales to the public, not on what you buy yourself or based on the number of people you recruit.
- Consult an unbiased third party – like an unconnected broker or licensed financial advisor – before investing.

Investment Fraud

Scammers will try to trick you into investing your money with them for one reason or another. They make it seem like the offer is too good to pass up by guaranteeing high returns or promising low- to no-risk.

Here's what you can do:

- If the opportunity to invest your money seems too good to be true, it probably is.
- Ask questions, and do your own research before investing any money. Be suspicious of any unsolicited investment offers.
- Don't invest in anything you are not absolutely sure about. Research the company to ensure it is legitimate.
- Always inquire about all the terms and conditions.
- Consult an unbiased third party – like an unconnected broker or licensed financial advisor – before investing.

IRS Imposter Scams

You get a call from the IRS, a federal agent, or even your local utilities office. The caller states you owe back taxes, or that there is a warrant out for your arrest, or that you have late or unpaid bills.

The caller threatens to sue you, arrest or deport you, revoke your license, or shut off your utilities if you don't pay right away. They tell you to put money

on a prepaid debit card and provide them with the card numbers.

The caller may know part of your Social Security number, and your caller ID might show a Washington, DC area code; but is the call valid?

These are not legitimate calls. The real IRS won't ask you to pay with prepaid debit cards or wire transfers. They also won't ask for a credit card or other personal information over the phone.

When a legitimate request comes from the IRS or your utilities office, it arrives first by mail, not by phone. These agencies will not ask you for credit card or other personal information over the phone. The police will also never use the phone to clear up warrants.

Here's what you can do:

- Stop. Don't wire money or pay with a prepaid debit card.
- Ask the caller if you can call them back. Hang up the phone and call back using a publically listed phone number for the agency. Do not simply call back the number used to reach you.

Tech Support Scams

You get a pop-up or other urgent message from someone saying your computer is infected. It might seem like the message comes from a well-known company like Microsoft, Apple, or maybe your internet service provider. It tells you there are viruses or other malware on your computer.

It says you have to call a number or risk losing your personal data. But is this threat real? Judging by reports to the Federal Trade Commission, no. These are scammers who want to sell you useless services, steal your credit card number, or get access to your computer to install malware, which could then let them see everything on your computer.

Here's what you can do:

- Stop. Don't call a phone number and do not click any links.
- Don't send money, give your credit card number, or give control of your computer to anyone who contacts you.
- Update or scan your computer using your security software.

Identity Theft

What is it?
Identity theft occurs when someone steals your personal information, such as name, address, Social Security number, credit card, bank account numbers, or even medical insurance account numbers.

This information can be used to make purchases, open new credit cards in your name, charge medical bills to your insurance, open utility accounts, and more.

Here's what you can do:

- Check your monthly statements and credit card bills for any unusual charges. Keep track of what bills you are expecting and contact the biller if a monthly statement is not received.
- Regularly check your credit report for unexplained changes.
- Keep a close eye on your wallet, credit cards, passwords, and any other personal information that could give someone else access to your money.
- Be careful how and where you use your credit cards, both in person and online. Only shop from stores and on websites that are trustworthy and reputable.

There are many types of scams and fraudulent scenarios beyond those included here. Education is the best method for prevention, and applying a healthy amount of skepticism when faced with financial decisions is helpful in protecting yourself. You can also count on CSB and your local banker as a resource when you are in doubt.

We may not always have the answers, but we are committed to keeping your financial and personal information safe and will do our due diligence to help you.

How to Report Identity Theft

If you believe your identity has been stolen, there are a few ways you can report it:

Report your identity theft to the Federal Trade Commission (FTC), either online at IdentityTheft.gov or by phone by calling 1.877.438.4338 or TTY 1.866.653.4261. If you report online with the FTC, you will be provided with an identity theft report and recovery plan. If you create an account, you will be able to manage your recovery plan and will have access to prefilled form letters to send to creditors.

You may also report identity theft to your local police. This may be necessary if you know who the thief is, if the thief used your identity in an interaction with the police, or if a police report is required by any of your creditors affected by the theft.

Specific types of identity theft can be reported to other federal agencies as well.

Medical identity theft can be reported to Medicare's fraud office or your health insurance company's fraud department.

Tax identity theft should be reported to the Internal Revenue Service (IRS), as well as your state's Department of Taxation or Revenue.

After reporting your identity theft to the federal government agencies, it should also be reported to various other organizations as well: One of the three major credit reporting agencies, Equifax, Experian, or TransUnion, should be contacted so a freeze or alert can be added to your accounts so no one can try to open any new accounts or cards with your name. Also ensure that the credit reporting agency will communicate this with the other two credit reporting agencies.

Report the theft to any of the financial institutions that you have accounts with.

If the thief has used your information to open an account or apply for a job anywhere, alert those companies about the identity theft.

If your identity was stolen after a stay in a nursing home or long-term care facility, report it to the National Long-Term Care Ombudsman Resource Center.

Trustworthy and Reliable Site Criteria

A trustworthy and reliable website will be one that has a website certificate and uses encryption to protect information submitted on the website.

To know if a site has a website certificate, check for a closed padlock icon, either up by the URL or at the bottom of the window in the status bar. This indicates that the website is secure.

Also check that the URL includes "https:" and not just "http:" as this means they encrypt any information submitted on their website to protect the customer's information.

Make sure it is a reputable site and not a fake, malicious site designed to look like the legitimate website. Scammers will create these deceiving websites that are not secure to trick customers into giving their personal information. The scammers can then use this information to take your money or your identity.

Attackers will try to send phishing emails, where they ask consumers to submit personal information through email, or link them to a malicious website. A reputable business will never ask for personal information through email, and they rarely send unsolicited links via email. If something is suspicious, open a new browser window and type in the website address directly instead of replying to an email or clicking any links in the email.

Credit cards are safer to use when purchasing online. If fraud takes place on your debit card, you may have to wait for the refund process to complete prior to regaining access to your funds. With a credit card, you are not out any of your own money during the reversal process. Credit cards are not tied to any of your deposit accounts.

It is also useful to check a website's privacy policy before providing any personal information on the site. The privacy policy will outline how the website intends to use and store the information it is asking for.

Checking your Credit Report

Check your credit report regularly to help prevent identity theft. The Fair Credit Reporting Act (FCRA) allows everyone to check their credit report once every 12 months for free from each of the three national credit reporting agencies: Equifax, Experian, and TransUnion.

Be careful of imposter sites promising free credit reports. There is only one website, annualcreditreport.com that has the authority to fill orders for free credit reports, under law. When other sites offer any sort of free credit scores or reports, be wary of the stipulations that may be hidden.

The three nationwide credit reporting companies or annualcreditreport.com will never ask you to submit any personal information through email or on the phone. If you are ever asked to provide personal information, be suspicious of a possible scam. The only information you need to provide to receive your annual free credit report is your name, address, Social Security number, and date of birth.

While you are eligible to receive a free credit report from each nationwide credit reporting companies, you do not have to order them all at one time. It is suggested that you stagger your credit report orders from each company so that you can keep a better eye on your credit report for suspicious activity.

It is suggested that you take advantage of your three free credit reports annually. Requesting your credit report will not harm your credit score since it is not an inquiry about new credit. Therefore, checking your credit report regularly can only help protect you from possible identity theft.

EQUIFAX: https://www.equifax.com/
888.298.0045

EXPRIAN: httsp://www.experian.com/
888.397.3742

TRANSUNION: https://www.transunion.com/
800.909.8872

Sources

https://www.consumer.ftc.gov
https://www.bbb.org/en/us
https://www.fbi.gov
https://www.usa.gov
https://www.consumerfinance.gov
https://www.ipata.org