Welcome to the Union Bank Security Center.

Our Security Center will show you the fraudulent tactics criminals use and how you can protect your business online.

You will learn about the different types of fraud, the current trends and techniques criminals are using, and ways your business can help avoid becoming a victim of fraud.

Learn more about our set of security tools, designed to provide an additional layer of protection to your online transactions.

Contents

Fraud Center

Authorities and industry experts agree that you are your own best protection against fraud. Union Bank is pleased to provide you with information from industry leaders and links to additional great resources.

Identity Theft

Learn about identity theft and ways to recognize it.

- What is Identity Theft
- Types of Identity Theft
- Identity Theft Tips

Online Fraud

Learn about some of the most common internet and email scams, and how to identify them.

- Types of Online Fraud
- Internet Scams
- Online, Email and Scam Tips

Elder and Dependent Adult Financial Fraud

Learn how to stay safer by taking preventive measures to help protect you from Elder Financial Fraud.

- Educating Yourself on Elder and Dependent Adult Financial Fraud
- If you suspect Elder and Dependent Adult Financial Fraud
- Elder and Dependent Adult Financial Fraud Contacts

Bank Account, Credit Card, and Debit Card Security

Learn how to safeguard your account, credit card and debit card against fraud.

- Protect Your Bank Account
- Use ATMs Safely
- Credit Card and Debit Card Security Tips

Identity Theft

What is Identity Theft?

Identity theft occurs when someone illegally obtains your personal information – such as your Social Security number, bank account number or other identification – and uses it to open new accounts or initiate transactions in your name. Examples of fraudulent activities conducted by criminals include: opening new credit cards, opening new bank accounts, forging or counterfeiting checks, and applying for new loans and even mortgages in your name. Such activity can cause financial loss and damage to your credit, which can lead to a lengthy resolution process.

Criminals can obtain personal information via online and offline methods. Stealing wallets and purses, intercepting or rerouting your email, and rummaging through your garbage are some of the common tactics that thieves may use to obtain personal information.

Recognize Identity Theft and Fraud

Identity thieves can strike even if you have been very careful with your personal information. The following may be signs of identity theft:

- If you find new accounts on your credit report that are not yours
- If you did not receive an expected bill or statement by mail
- If you receive credit cards or billing statements on accounts you didn't apply for
- If you are denied credit or are offered less than favorable credit terms for no reason
- If you get calls from creditors or debt collectors regarding merchandise or services that you did not buy

Fraud is an act that occurs when someone uses your account to make unauthorized transactions, usually when the account number or card has been stolen. The following may be signs of fraud:

- If you did not receive an expected bill or statement by mail
- If unexpected charges occurred on your account
- If there are charges on your account from unrecognized vendors
- If posted checks appear on your account significantly out of sequence

Types of Identity Theft

Mailbox Theft

Only use secured mailboxes to deposit your mail, such as those provided by the post office. If your home mailbox is unsecured, consider changing it to a locked box with a mail slot to ensure your incoming mail is secure. Collect your mail promptly, and if you do not receive an expected piece of mail, such as a billing statement, make a call to the company to ask when they sent it out and make sure no unauthorized change of address has been made. For your eligible accounts, consider switching to online banking eStatements, such as Union Bank's Online Banking (see ID Theft Prevention – The Computer to learn about security your online activity and Online Banking Security Measures for information on how we work to protect your online activity).

If you have any reason to believe your bank information was stolen, report the incident immediately by calling us at 888-328-6466.

Onlookers

Before you begin to use your debit card, take a look around you. Do you have enough personal space, or is someone crowding you, such as in a busy supermarket line? Is there someone hovering around your area for no apparent reason?

If you feel uncomfortable completing the transaction, don't. Additionally, be sure to secure your wallet in a safe space, such as an inner zipped pocket, especially when securing your card back into place in public.

Insider Threat

Make it a point to know how any organization requesting your personal information secures it.

Safekeeping of customer information is a high priority at Union Bank. We will continue to maintain the high standards necessary to help ensure that your information is kept private and secure.

Internet

Avoiding email phishing attempts. Understand that a criminal may use the name of a trusted source to gain your information, so you cannot rely on name alone to make a judgement. Know the policies of the various institutions you interact with so that if you are faced with this type of scheme, you are prepared to protect yourself.

Take a look at what kind of information on you is available on the internet. View your internet networking sites and profiles to ensure you are not inadvertently giving out information that can be used to steal your identity.

Computer

Make sure that your computer has a firewall installed. Firewalls are designed to block unsolicited attempts to access your system. If you do have a firewall, make sure that it is turned on. If you do not have a firewall installed, you can purchase one.

Make sure that you have antivirus software installed and update it regularly. Run the antivirus software on a regular basis to identify and remove viruses from your computer.

Do not open any attachments or go to any links from a source that you are not familiar with. Delete any unsolicited emails with attachments and links immediately. You can report suspicious communications to us at custservice@hometownbanc.com.

Skimmers

Skimmers are devices used to read the magnet strip from your credit or debit card. They can be used on any ATM type of device, such as at the local gas station or a restaurant. The devices are often well-concealed. Criminals who use skimmers typically use the information they gather from you within 24 hours. It is always important that you regularly check your account balances and reconcile them with any purchases you have made. Be wary of any ATM device that appears to have been altered or appears suspicious. Always cancel a transaction if you feel uncomfortable in any way.

Theft by Phone

Organizations and financial institutions typically do not have a reason to unexpectedly call to ask for you to verify your personal information.

If you feel that it may be a legitimate call from a company known to you, tell them that you will call back through the listed number for the organization and ask for their name so that you can get to them. If it is an organization you do not know of, satisfy yourself of the legitimacy of the organization before giving any information about yourself. When in doubt, do not provide any information.

Identify Theft Security Tips

Follow these tips to help protect yourself from identity theft:

- Carefully review websites, online advertisements, and emails before taking any action or submitting any personal information online.
- Memorize your password and pins. Do not write them down, save them on your computer or reveal them to anyone.
- Create a complex password that:
    - Is 10-17 characters in length. The longer the password, the better.
    - Includes letters and numbers.
    - Has at least four different characters (no repeats).
    - Has at least one special character.

    - Is a sequence of random letters and numbers.
    - Is not obvious or easily obtainable information.
- Change your Union Bank password every 365 days. You can easily change your password by visiting the Profile page within Online Banking.
- Never email your account number, Social Security number or other sensitive information to anyone.
- Never leave your computer unattended while logged in. Complete your banking tasks and end your web sessions by always logging out.
- When visiting social networks, remember that sharing information like your birth date, phone number, email address, location and photos can put your identity at risk.
- Carry only necessary information with you. Leave your Social Security card and unused credit cards at home in a safe and secure location.
- Make photocopies (front and back) of vital information you carry regularly and store them in a secure place, such as a safety deposit box. Then, if your purse or wallet is lost or stolen, you have the relevant contact information readily available.
- Do not provide your Social Security number unless absolutely necessary.
- Replace paper invoices, statements and checks with electronic versions, if offered by your employer, bank, utility provider or merchant.
- Know your billing and statement cycles. Contact the company's customer service department if you stop receiving your regular bill or statements.
- Shred documents containing personal or financial information before discarding. Many fraud and identity theft incidents happen as a result of mail and garbage theft.
- If you are uncomfortable with a phone call that was not initiated by you, hang up or ask for the purpose of the call. Then contact the company using legitimate sources such as contact phone numbers found on the company's website, your bank statements, and those listed on your ATM, debit or credit cards.
- Maintain a close watch of your bank accounts, credit card accounts, loan accounts and review your credit report at least twice annually. Check for unauthorized charges and new accounts in your name. Report any loss or theft immediately.
- Make sure we have your current contact information so we can reach you if fraudulent activity is suspected on your account(s).
- For consumers, annually, obtain a free credit report from each of the credit reporting companies and review it carefully. (See the Federal Trade Commission's website Free Credit Reports | Consumer Advice (ftc.gov)). Contact the applicable credit reporting companies immediately if you find any unknown or suspicious activity on your credit reports.
- Consider subscribing to a credit monitoring service and monitor your credit reports regularly.

Additional Resources

- To take advantage of your free credit report, visit www.annualcreditreport.com
- You can also contact the three major bureaus to obtain a copy of your credit report directly:
    - Equifax: 1-800-685-1111 or www.equifax.com
    - Experian: 1-888-397-3742 or www.experian.com
    - Transunion: 1-800-916-8800 or www.transunion.com
    - View Don't be an Online Victim from the Federal Deposit Insurance Corporation (FDIC)

Online Fraud

Types of Online Fraud

Spoof Websites/Phishing

Through the use of fraudulent emails, internet thieves attempt to "phish" for your confidential information. They attempt to steal this information from you by means of "pop-ups" or emails with internet links to deceive you into disclosing sensitive information (such as bank account numbers and Social Security numbers).

Often the email appears to be from a trusted source (such as your bank) and directs you to a "spoof" website that requests you to divulge sensitive information or even ask you to call a phone number and provide account information. But the website is a fake.

What you should look for:

- Asking for personal information should raise a flag since Union Bank will never send you unsolicited emails with embedded links or pop-up windows that ask for confidential information, such as your Social Security number, account numbers, ATM or Debit Card PIN.
- Urgent appeals claim that your account may be closed if you fail to confirm, verify or authenticate your personal information. Union Bank will never ask you to verify information in this way.
- Messages about system and security updates claim that the bank needs to confirm important information due to upgrades and state that you must update your information online. Union Bank will not ask you to verify information in this way.
- Offers that sound too good to be true often are. You may be asked to fill out a short customer service survey in exchange for money being credited to your account, and you are then asked to provide your account number for proper routing of the supposed credit. Union Bank will never send an email asking for your account information.
- Typos and other errors are often the mark of fraudulent emails or websites. Be on the lookout for typos or grammatical errors, awkward writing and poor visual design.

Malware

Malware, short for "malicious software" includes viruses, spyware and Trojans that are designed to infiltrate or damage a computer system.

Malware is often used to steal personal information and commit fraud. There are several easy ways to minimize the risk of malware:

- Avoid downloads from file sharing and social networking sites, which can be distribution points for malware.
- Do not open email attachments or install free software from unknown sources shouldn't be opened or installed.
- Do not click on pop-up advertisements asking for personal or financial information, simply close them.
- Regularly update your security and system software and protect your computer from malware threats.

Vishing

Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by Voice over IP (VoIP), to gain access to private personal and financial information from the public for the purpose of financial reward.

Typically, when the victim answers the call, an automated recording, often generated with a text to speech synthesizer, is played to alert the consumer that their credit card has had fraudulent activity or that their bank account has had unusual activity. The message instructs the consumer to call the phone number provided immediately. The same phone number is often shown in the spoofed caller ID and given the same name as the financial company they are pretending to represent.

When the victim calls the number, it is answered by automated instructions to enter their credit card number or bank account number on the key pad. Once the consumer enters their credit card number or bank account number, the visher has the information necessary to make fraudulent use of the card or to access the account.

Money Mules

Money mules are unsuspecting victims who become middlemen for criminals trying to launder stolen funds or merchandise. This type of online scam preys on victims who are unaware that the money or merchandise they are transferring is stolen. In these scams, the stolen money or merchandise is transferred from the victim's country to the scam operator's country. Money mules are commonly recruited with job advertisements for "payment processing agents," "money transfer agents," "local processors," and other similar titles. Criminals recruit money mules, send them stolen money and then ask the money mules to wire or transfer the money unwittingly to the criminals. Using the money mule masks the criminal's identity.

The money mule may keep a commission for performing the transfer or wire. Victims of these scams may not only have their bank accounts closed, but are often held financially responsible for returning the stolen funds.

Common signs of a money mule scam:

- Overseas companies requesting money transfer agents in the US.
- Opening new bank accounts to receive money from someone you don't know.
- Accepting large sums of money into your bank account for a new job.
- Transferring or wiring funds out of your bank account to people you do not know.

Internet Scams

The internet has provided consumers with more transaction and business offerings that ever before. An individual can bid on a luxury item and a business owner can advertise to a global market at a click of the button. As a consumer you must be aware that internet scams are as varied and abundant as the legitimate offerings on the internet.

We've listed some of the most common internet scams and some ways to identify them. For more detailed information on internet scams, please see the Federal Trade Commission website.

Auction Fraud

Internet auction fraud involves the misrepresentation or non-delivery of an advertised product through an internet auction site. Internet auction fraud is among the top consumer complaints reported to the Federal Trade Commission.

Know the auction site you are doing business with. Find out what protections the site offers you, such as guarantees for services not delivered.

You should never have to provide your Social Security or driver's license number online.

Do not provide the account number you are using for the purchase, until you have done your research and are ready to make your purchase.

It is likely that you will have to use an online payment method to complete your purchase as a buyer. This may be a service like PayPal or an escrow service. Check out the company handling the payment by reading through their website and calling their customer service to ask specific questions about their security policy and terms of service. You need to make sure that you are protected should the seller renege on their side of the bargain.

Be cautious of sellers who give the appearance of being within the United States but reveal themselves to be out of the country when you are preparing to make your payment for the goods.

Wiring funds directly to the seller leaves you with no options should you find yourself a victim of internet auction fraud. Even wires through well-known banks or an escrow service will not protect you.

Email Fraud/SPAM

There are very few of us who have never received unsolicited offers through email, better known as SPAM. For many fraudsters, the objective of spamming is to gather personal information that can be used to steal your money and/or your identity. Criminals may also send you attachments and links that will lead you to spoof sites or cause you to inadvertently download harmful software to your computer. Never send your personal information to an unknown source via email. Criminals may try to entice information out of you by stating that an offer is only good if you buy now or give them your information immediately. No legitimate business would deny you the time to check out their claims.

If you do not know the source of an email, delete it. Even if a co-worker or friend you trust sends you a link or attachment such as in an email chain, it may be infected.

Keep your computer firewall, anti-virus, and anti-spyware software up to date.

Nigerian Letter/419 Scam

This scam typically begins with an unsolicited communication from individuals representing themselves as Nigerian or foreign government officials. This "official" offer will give you a percentage of a large amount of money in exchange for your assistance in placing money in overseas bank accounts. You may be asked to send your account numbers, blank letterhead stationery, or other kinds of identifying information via a provided fax number.

Follow the old saying, "if it sounds too good to be true, then it probably is".

Avoid any offers to get rich quick through the complex transfer of funds, particularly if it involves sending money overseas. It is highly unlikely that the scheme will deliver to you what is promised, and even if it does, it is very likely illegal. Do not put your money, identity, and reputation at stake.

Lottery or Sweepstakes Scam

Lottery and sweepstakes scams are on the rise. Scam operators, often based in Canada, are using email, telephone, fax and direct mail to trick U.S. consumers into believing they have won large sums of cash through foreign lotteries.

The details of the lottery scams vary with regard to the name of the lottery itself, the country of origin, the sponsoring organization, the amount of the prize and other particulars. Scammers will add a patina of legitimacy to their claims by mentioning real financial institutions, government agencies or well-known companies.

The scam begins with a notice that you are the winner of a lottery or sweepstakes that you did not enter. You may be asked to provide banking details, a large amount of personal information, and copies of your driver's license and passport to prove your identity and to facilitate the

transfer of your winnings. If you comply with these requests, the scammers will have enough information to steal your identity. In order to receive the winnings, you must first pay a small percentage for fake taxes or other fees. The scammer typically instructs the victim to wire advance fees through Western Union. Once the money is transferred, the scammer moves on or in some cases comes back to request additional funds but the "lottery winnings" never appear.

Legitimate lotteries or sweepstakes will not require payment to receive the winnings. Do not respond to emails/letters/faxes that claim you have won money. Never give out your confidential personal or bank account information to anyone claiming to hold your "winnings". Participation in foreign lotteries is against the law.

Overpayment Scam (Counterfeit Check)

Someone responds to your posting or ad, and offers to use a cashier's check, personal check or corporate check to pay for the item you're selling. At the last minute, the so-called buyer (or the buyer's "agent") comes up with a reason for writing the check for more than the purchase price, and asks you to wire back the difference after you deposit the check. You deposit the check and wire the funds back to the "buyer". Later, the check bounces, leaving you liable for the entire amount.

Overpayment scams are primarily perpetuated through internet-based transactions (i.e. eBay or Craiglist) but can also be phone-based transactions. Scams frequently consist of a counterfeit cashier's check or another monetary instrument for payment of an item. The counterfeit item looks legitimate and often contains watermarks and other security features. The check amount is usually greater than the purchase price of the item. The seller or business deposits the checks into their account believing that the counterfeit item legitimate.

Know who you're dealing with. In any transaction, independently confirm the buyer's name, street address, and telephone number. Don't accept a check for more than the selling price, no matter how tempting. If the buyer insists that you wire back funds, end the transaction immediately.

Collection Scam

Criminals have devised counterfeit check schemes targeting attorneys. Scammers will use the names of legitimate companies to gain credibility and use email addresses created to show a possible connection to the legitimate company. Scammers will email, fax, or call the law firm requesting legal services in connection with a settlement.

If the attorney responds, the scam begins and the attorney will eventually receive a fraudulent settlement check that usually appears to be a cashier's check or business check. The attorney is asked to deposit the settlement check, keep a retainer fee and wire the remainder of the settlement to the client's (scammer's) overseas account. The original settlement check is later returned as unpaid/fraudulent and the attorney is left responsible for the funds wired out of the attorney's bank account overseas.

Be suspicious of a solicitation that offers a relatively large fee for minimal work and is outside your usual practice. Carefully scrutinize unsolicited email/phone calls from individuals or entities requesting services with whom you have no prior dealings, particularly if the solicitation originates from a foreign country. Educate your staff to be on the lookout for these types of schemes. If you accept payment by check, ask for a check drawn on a local bank, or a bank with a local branch. That way, you can make a personal visit to make sure the check is valid. If that's not possible, call the bank where the check was issued and verify that the check is valid. Get the issuing bank's phone number from directory assistance or an internet site that you know and not from the check or the person who gave you the check. Monitor your bank accounts and

ensure that settlement checks you deposit, clear through the banking system and you have received good funds before you issue or pay monies to clients.

Online Job Scam

Another common internet scam involves soliciting individuals for what appears to be a lucrative position that will allow them to work as an independent agent or from their home.

Job scammers use reputable online job boards to offer work-at-home jobs or accounting positions. These job scams may require employees to receive money into their existing bank account (or open new accounts) and then transfer the money to another account, often overseas. As payment, the job seeker is instructed to keep a small percentage of the transfer.

Be cautious of employer offering employment without an interview (either in person or by phone). Thoroughly research any employer requesting that you transfer funds of receive packages for shipment, especially if they are located overseas. Most of these employment offers are check-cashing or shipping scams. Do not provide your Social Security number or any other sensitive information unless you are confident that the employer is legitimate.

Protect yourself:

- Help keep your operating system and browser up to date and help create a safe browsing environment.
- Review your credit report at least twice a year. Check for unauthorized changes and new accounts in your name. Remember, consumers can obtain free copies of their credit reports once each year from the credit reporting companies. See the Federal Trade Commission's website for more information.
- Use virus protection software

Online, Email, and Scam Security Tips

Online Security Tips

- Memorize your user name and password. Your online user name and password authenticate you when you begin an Online Banking session. You should memorize your Password and never write it down anywhere, save to your computer, or reveal it to anyone.
- Create a complex password that:
    - Is 10-17 characters in length. The longer the password, the better.
    - Includes letters and numbers.
    - Has at least four different characters (no repeats).
    - Has at least one special character.
    - Is a sequence of random letters and numbers.
    - Is not obvious or easily obtainable information.
- Change your password regularly. You can easily change your password by visiting the Profile page of Online Banking.
- Remember to logout of online banking and close all browsing sessions for security. Don't rely on our session time-out feature.
- Verify the security certificate of any website you're going to input sensitive information into.
- Union Bank uses Secured Socket Layer Technology (SSL "lock"). Click on the lock in the status bar of your browser to confirm the site's authenticity. When conducting online transactions involving sensitive information such as passwords, PINs or account numbers, look for the SSL lock first.

- Check for the lock icon in the status bar of your browser. This means that the website uses encryption to protect your information. Make sure the lock icon is closed, indicating that the encryption is on. Double-click it to display the security certificate. The security certificate information should match the name of the site you intended to be on.
- Do not share any confidential information through suspicious emails, websites, social media networks, text messages or phone calls.
- Protect your personal and account information, including your Online Banking user name, password, and answers to security questions. Do not write this information down or share it with anyone.
- If you receive a suspicious email, do not click on any links or reply to it. Simply delete it.
- Avoid using a public or shared computer for personal and financial transactions. Only conduct Online Banking and financial transactions using a trusted computer.
- If your computer is infected with a virus, run anti-virus software to remove the infection and change passwords on all your financial and personal accounts. Including your email using a secure device.
- Make sure the computer(s) you use have current software security patches and anti-virus software. Anti-virus software requires frequent updates to guard against new viruses.
- Install a personal firewall to help prevent unauthorized access to your home computer.
- Wireless access should be secured with strong password encryption. Be cautious when using public hotspots and consider your Wi-Fi auto-connect settings.

Email Security Tips

Scam Prevention Tips

- Be wary of unsolicited email containing urgent appeals for security or personal information.
- Spelling errors can help fraudulent emails get through your spam filters.
- Never open attachments, click on links, or respond to emails from suspicious or unknown senders.
- If you receive a suspicious email that you think is a phish, do not respond or provide any information. Simply delete it.
- To report a suspicious email that uses Union Bank's name, forward it to custservice@hometownbanc.com.
- You may send us account or sensitive information via custservice@hometownbanc.com as this is a secure and encrypted email address. If you are using online banking, please send a secure message through the Mail tab located at the top of your screen.
- Use common sense. If it sounds too good to be true, it probably is.
- Never give personal information to a stranger who contacts you, whether by phone, email or other means.
- You are responsible and liable for items you cash or deposit into your account.
- Be wary of offers of mortgage modification, foreclosure rescue, or short sale scams involving money-back guarantees, title transfers, up-front fees, or high pressure sales tactics.
- No matter how urgent someone claims a deal or job offer is, you should research and confirm its legitimacy.

Elder and Dependent Adult Financial Fraud

Educating Yourself on Elder and Dependent Adult Financial Fraud

Elder financial fraud is projected to grow as baby boomers age. At Union Bank, we believe that one of the keys to enjoying a healthy and long life is financial security. We can help you understand how to stay safer by taking preventive measures to secure your finances, detecting the signs that someone is targeting you for fraud, and resolving an incidence of fraud should you find yourself a victim.

New Acquaintances

Consider the circumstances under which you build a new friendship. How did this person enter your life, and what are they getting out of the friendship? Where is the person from, what does he or she do for a living, and who are his or her close friends or family?

A common ploy of fraudsters is to befriend you and increasingly gain your trust over time. You may eventually ask this new friend to come with you make a purchase at the grocery store, or to help you to order new bank checks. By gaining access to your trust and financial accounts, the fraudster may deplete your finances without your knowledge. Or, the fraudster may make you reliant on him or her and threaten to not assist you anymore or even harm you in order to get your money.

Discourage fraudsters by having a strong financial plan in place and planning out how you are going to get the physical assistance you may need on a day-to-day basis well ahead of time. A friendship based on your dependence is one you should avoid.

Friends and Family

Unfortunately, many elder and dependent adult financial fraud cases involve family members.

A family member may be given the authority to make legal decisions for you and abuse that right. Do not put any one person in absolute control over your finances, and you will avoid being put in position of absolute dependence. Anticipate your needs over time and plan ahead.

If you need help with handling your financial affairs, consult with an attorney about setting up a trust or other actions you can take to protect your assets. Also see an attorney about executing a Power of Attorney naming a person you know well and trust. This person may be an attorney, a family member, or a friend. Once executed, give Union Bank a copy of the Power of Attorney. Be sure to notify us of any changes to the Power of Attorney.

Sign your own checks and do not write out blank checks for anyone.

Treat every request for your signature very seriously. Read the fine print and ask questions. If you are unsure, consult with an attorney.

When seeking assistance with your finances, ask for help from more than one source in order to be sure that you get an objective view. Should you have any questions, have your local bank representative help you to reconcile any discrepancies you have found.

When you are signing over money or property to anyone in exchange for your care, have an agreement written out and reviewed by your attorney.

Have your financial instructions written out and reviewed by your attorney. Notify the people you trust that you have already written out your instructions and retain them in a safe location. Your attorney should be able to give you more detailed advice on how to proceed.

Contractors, Merchants, Landlords and Others

It is not uncommon for senior citizens to be tricked into paying higher prices for goods or even paying for services he/she never signed up for. A contractor may raise the price of work after starting. A landlord may increase your rent without following the proper legal procedures. Even when you said no to unsolicited offers to purchase magazines or enter sweepstakes by phone, in person, or by email, the goods appear along with a bill.

Educate yourself on the various fraud scams out there. Read through the ID Theft and Internet Scam sections in this document. Before signing up for any service, get the agreement in writing and read it thoroughly. If you are approached with unsolicited services, it is probably best to say no.

Before hiring a contractor, check the validity of their contractor's license. Never fully pay for work in advance of its completion.

If any of your service providers, such as your care providers or landlords, increase their charges, get an explanation in writing. By formally documenting their excuses you may discourage them from defrauding you at the risk of their losing their business license or facing other legal repercussions. No criminal wants to get caught.

Place your name and telephone (number)s including cell phone number(s) on the Do Not Call Registry. Do not accept services from solicitors. You do not have the time to effectively establish the validity of their offer on the spot.

If You Suspect Elder and Dependent Adult Financial Fraud

Elder victims of fraud often feel embarrassed and betrayed, particularly if it is a situation involving a family member or business transaction gone awry. Many victims will not report fraud due to shame or fear. Fraud, regardless of whether it is a trusted family member or a complete stranger, is a crime and you have a right to defend yourself and you are protected by the law. Here are some tips to help.

- If you feel that you are in imminent physical danger, contact your local police department and/or the adult protective services.
- If you find unauthorized financial activity, or believe that your authorization for specific financial activity has been abused, contact your financial institution immediately. Ideally, visit your local branch in person and ask to speak to a supervisor. If it is a credit company, call their customer service line and have them forward your call to their fraud department and/or a supervisor.
- Union Bank has specific policies and procedures for handling potential financial elder and dependent adult abuse. You will find our bank representatives to be understanding and sensitive to your situation. Do not hesitate to contact us at custservice@hometownbanc.com if you have any concerns.
- Try to gather as much information together as you can so that the proper authorities can quickly investigate your case. Some information you might want to gather includes:
    - All of your legal documents specifying who has authorization to access your accounts and to what extent.
    - A list of your regular expenses and sources of income prepared so that an institution representative can quickly look for suspicious activity.
    - Reconciliations of your statements of all financial accounts to make sure the fraud has not affected them.

Elder and Dependent Adult Financial Fraud Contacts

Union Bank, Inc

888-328-6466
Report suspicious emails: custservice@hometownbanc.com

Adult Protective Services

Each county has an APS agency offering services to any elder or dependent adult regardless of income. This website contains additional information along with contact number for the APS agency near you. https://dhhr.wv.gov/bcf/Services/Pages/Adult-Protective-Services.aspx.

Federal Trade Commission (FTC)

The FTC has educational information specific to seniors as well as a fraud reporting system. It also manages the Do Not Call Registry.

600 Pennsylvania Avenue, NW
Washington, DC 20580
202-326-2222
https://reportfraud.ftc.gov/#/

Personal Bank Account, Credit Card and Debit Card Security Tips

Protect Your Bank Account

- Monitor your account online at least once a week or more frequently and review your account details and transaction history for suspicious activity.
- Sign up for online statements and shut off paper statements.
    - Simply login to your online banking account and click the Profile tab to signup for eStatements.
    - Review your account statements carefully and report any unauthorized charges immediately.
- Set up account alerts – Sign up to receive email alert messages via Online Banking.
    - Simply login to your online banking account and click the Alerts tab to setup your alert preferences.
- Do not write or print your Social Security number or your driver's license number on checks.
- Store new and cancelled checks in a secure location accessible only to trusted persons.
- Shred old checks, receipts, account statements, and documents that contain sensitive information.
- Do not carry your checkbook with you unless it is necessary.

Use ATMs Safely

- Be aware of people and your surroundings. If you observe suspicious persons or circumstances, do not use the ATM at that time, come back later or use an ATM elsewhere.
- After completing a withdrawal, secure your card and cash immediately before exiting the ATM area. Count your cash later in the safety of your locked car or at home.
- Shield the ATM keypad with your hand or body while entering your PIN.
- Report all crimes immediately to the ATM operator or local law enforcement.

Credit Card and Debit Card Security Tips

- Never lend your ATM/Debit/Credit Card to anyone.
- Never let anyone watch you enter your PIN at an ATM or Point of Sale terminal.

- Memorize your passwords and PIN numbers and change them regularly.
- Avoid using obvious or easily obtainable information as your passwords or PIN numbers, and never write them down anywhere or reveal them to anyone.
- Don't trust a site just because it claims to be secure. Before using the site, check out the security/encryption software it uses. Obtain a physical address rather than a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Check out the Better Business Bureau from the seller's area.
- Be cautious when dealing with individuals/companies from outside your immediate area or locale.
- Do not send your card number through email or SMS text as it is typically not secure.
- Do not give out your card number over the phone unless you initiated the call.
- Review your statements to verify that they properly reflect the amounts you have authorized. Also, watch for multiple charges.
- Keep a list of your card account numbers and telephone numbers to call if your cards are lost or stolen Make sure the information is stored in a secure place.
- If you receive a replacement card, activate it properly and destroy your old card.
- Safe-keep or securely dispose of your transaction receipts.