WNB FINANCIAL
MORE THAN A BANK

Tips to improve your identity safety:

- Social networking sites are quickly becoming a potential hazard in information breach and theft of contacts; do not reveal any sensitive personal information on your site. Be sure to adjust your privacy settings to ensure unauthorized individuals cannot access your information.
- Exercise extreme caution and avoid accessing Web sites displaying personal or account information using unsecured Wi-Fi connection such as coffee shops, libraries, airports, and any other wireless access points. Do not access any financial information when using an unsecured Wi-Fi connection to avoid others seeing and potentially obtaining this information.
- By choosing to not receive any kind of e-mail or mobile alert you are putting yourself and identity at extreme risk. Almost half of consumers detect fraud first. Self-detection also results in lower consumer costs and faster resolution and enabling yourself to know of any unauthorized account changes or charges will drastically reduce the amount of fraudulent charges accrued in addition to reducing the time spent resolving the issue.
- In Javelin's 2009 Identity Fraud Survey Report, of the 35% of victims who knew how their information was obtained, 18% reported having their information obtained while making a purchase or transaction in person. With that being said, it is important to be cognizant of your surroundings and make sure you shield your PINs and credit card numbers at all times.
- In cases where the fraud victim identified the fraudster as someone they knew (e.g., friend, family member, coworker, neighbors, etc.), these fraudsters were able to use the stolen information for significantly longer periods of time and cost the victim more to resolve when compared to victims who did not know the perpetrator. Thus it is imperative to keep highly sensitive financial information away from where others could potentially access it, including family members, friends, neighbors and domestic employees.
- Refrain from leaving unnecessary sensitive information where others could potentially access it such as in your wallet, purse, car or at the workplace.

- Beware of unsolicited phone calls from financial institutions. They may be fraudsters attempting to obtain your account information by posing as your bank. When receiving phone calls from your financial institution, ignore any requests asking you to provide your account number or any other

  identifying information. Instead place a call to the financial institution on your own to resolve the account issue.

Avoid Becoming an Identity Theft Victim

Even though 85 percent of Americans worry about the threat of identity theft, fewer than 50 percent believe they are protecting their identity effectively, according to a consumer survey*. By taking the following basic and effective precautions, you can significantly decrease your chances of becoming a victim of identity theft:

Pay attention

- **Know what information about you is floating out in cyberspace**
  Check by entering your name in a search engine and see what comes up
- **Be aware that the Web sites you frequent may be duplicated by identity thieves to look authentic**
  Check for “https” in the URL and look in the bottom corner before you enter in any sensitive information
- **Review your bank statements and bills monthly**
  Call if a bill or statement doesn’t arrive on time, or if you notice any suspicious charges
- **Stop using paper bills and banking statements**
  Online account management is the most effective way to eliminate theft of paper-based information
- **Comb through your credit report**
  Look for any inconsistencies or suspicious activities

Trust your instincts

- **Question companies that ask for your Social Security number**
  Avoid giving it out unless absolutely necessary. If you do give it out, ask why they need it and how they will secure it. Also ask that it be blacked out on any paper forms
- **Don’t open emails from addresses you don’t recognize or click on links in emails**
  Open a new browser and type in the URL of the link

- **Avoid giving out your address or phone number on social Web sites**
  These sites can be great fun for pedophiles and identity thieves
- **Cover your card or checkbook if someone stands too close to you in the checkout line**
  Thieves could be taking a picture of your credit card or personal check
- **Watch the store clerk or server who takes too long to run your card**
  Service personnel are often a 'front' for identity scams and can quickly skim or memorize your account number
- **Don’t allow any company or individual to perform a background check on you**
  Make sure you have met and trust the person who will be running a background check and that there is a valid reason for them to do so. Identity thieves may be posing as a legitimate entity

Don’t broadcast your personal information

- **Speak quietly when giving out your Social Security, address or phone numbers in public**
  Better yet, write them down, then rip them up and throw them out
- **Before and after you swipe your card, turn it over in your hand so the numbers aren’t exposed**
  Sign with “See ID” rather than your name in the signature block on the card
- **Cross out your account number on restaurant or other receipts**
  It’s against the law for your entire account number to be there
- **Clear your cell phone of data before you trade it in or donate it**
  Data erasers are readily available online
- **Use credit and identity monitoring like ID Guard**
  This will alert you of certain changes to your credit file and help protect you from identity theft

Tips provided by Deluxe Corporation.