Identity Theft and Fraud Prevention Tips

The security of your personal information and your accounts are our highest priority. As such, we have implemented a variety of methods to protect your online accounts. You can take proactive steps to protect yourself from identity theft and fraud. We advise our clients to utilize the following safe practices.

Protect your identity

- Carry only necessary information with you. Leave your Social Security card and unused credits cards at home in a safe and secure location.
- Do not give your Social Security number to anyone unless absolutely necessary.
- Shred documents containing personal or financial information before discarding.
- Most legitimate companies will not call you and request personal information or account information. If this happens either hang up, or find out the purpose of the call. Then contact the company directly from a legitimate source such as your account statement or a phone number on the company's web site.
- Never provide payment information on a call that you did not initiate.
- Know your billing and statement cycles. Contact the company's customer service department if you stop receiving your regular bill or statement.
- Replace paper invoices, statements and checks with electronic versions. Use Online Banking and e-statements to prevent theft of account information in the mail. Sign up for Bill Payment services so you don't have to reveal your account number to third parties.
- Review your credit report at least once a year to ensure there are no unauthorized accounts. You can get a free credit report once a year from each of the three major credit bureaus at www. annualcreditreport .com.

Protect your accounts

- Always keep your cards and checks in a safe and secure place.
- Report lost or stolen cards and checks immediately.
- Review account statements carefully. Regular account review helps to quickly detect and stop fraudulent activity. Contact us immediately if you detect any discrepancies. Online Banking allows you to check your accounts at any time, 24x7x365. (See *Safe Online Banking Practices*, below.)
- If you notice suspicious account activity, report it immediately.
- Limit the amount of personal information on checks. Don't write your driver's license number or Social Security number on your checks.
- Store new and cancelled checks in a safe and secure location.
- Carry your checkbook with you only when necessary.
- Use tamper-resistant checks with security features such as chemically sensitive paper to deter alterations.
- Don't send your account numbers through email, as it is typically not secure.

Safe Debit and Credit Card Practices

- When selecting a card PIN, don't use a number or word that appears in your wallet, such as name, birth date, or phone number.
- Memorize your PIN. Don't write it down anywhere, especially on your card. Do not disclose your PIN to anyone.
- Cancel and destroy unused cards. If you receive a replacement card, destroy your old card.
- Shop with merchants you know and trust.
- Make sure online purchases are secured with encryption to protect your account information. Look for secure transaction symbols such as a lock symbol in the lower right-hand corner of your web browser, or "https://…" in the address bar of the website. The "s" indicates "secured" and means the web page uses encryption.
- Always log off from any website after a purchase transaction and close the browser to prevent unauthorized access to your account information.

Safe Online Banking Practices

- Don't give your passwords or security question answers to anyone and store them in a secure location.
- Change your passwords frequently and avoid using passwords that others may be able to guess (e.g., Social Security Number, date of birth, your child's name). Use complex passwords combining letters, numbers and special characters.
- Interaudi Bank's online banking system resides on a secure web site. When accessing your account online, be sure to check the address bar for **https://online.interaudibank.com/**. If the address bar appears differently, do not log in, and report it to us immediately.
- Don't allow your browser or computer software to store passwords for online banking, your email account or other sensitive web sites. Many identity thieves use your email account as a gateway to your personal information and your financial institutions. Set your Internet options to clear your browser's history each time you log off.
- Avoid accessing your accounts from high-risk computers that permit anonymous access to anyone (e.g., public hotspots, copy centers, libraries, or unsecured wireless networks).When traveling, use a computer at your hotel instead of an Internet café.
- Be sure to log out of your online banking session and close your browser when you are done accessing your account or if you need to leave your computer unattended.
- Install anti-virus, anti-spyware, and other Internet security software on your PC. Be sure to use software from reputable vendors. It is often the free "prevention" software that is actually intended to cause malicious activity on your computer. Don't download software online from an unknown vendor. Going to a software store is a safe practice if you are unsure of what you need.
- Use secure websites for transactions and shopping. Shop with merchants you trust. Make sure internet purchases are secured with encryption to protect your account. Look for secure transaction signs like a lock symbol in the lower right-hand corner of your browser or "https" in the address bar.
- Prevent unauthorized people from using your personal computer at home and at work.

- If you notice suspicious account activity, report it immediately.

Safe Email Practices

- Interaudi Bank will never send an email requesting personal or account information. If you receive an email like this, please report it to us immediately.
- Be wary of suspicious emails. 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.
- If you respond to a phish email with personal or account information, report it immediately.

Safe Mobile Device Practices

- Be sure to protect the information on your mobile device by using the keypad or phone lock function when it is not in use.
- Never share your personal or financial information in a text message, cell phone or email.
- If you lose your mobile device or change your mobile phone number, please notify us as soon as possible.
- Avoid storing your banking password or other sensitive information on your smartphone or in an app where it could be discovered if your phone is stolen.
- When you finish banking online, always log off and clear your browser history. This reduces the risk of others accessing your information from your device.
- Keep your mobile operating system up to date to ensure the highest level of protection. Be sure to go to the company's website to confirm the update is legitimate.
- Be cautious when using Wi-Fi hotspots. Check your security settings as fraudsters can spoof the name of reputable hotspots.
- Download banking applications from reputable sources only to ensure the safety of your account information.
- For your security, sign off when you finish using a banking app rather than just closing it.
- QR codes (quick response codes) are two-dimensional barcodes that can be scanned with a mobile device to provide easy access to online information. Treat QR codes with the same suspicion as you would a link in an email.