Fraud

We keep you updated
on the latest fraud schemes.

AMERANT

Fraud Advisor

Fraud can impact anyone at any time. Proactive prevention is the most cost-effective way to deal with the potential losses and inconveniences that can result from fraud. Amerant is committed to taking the necessary steps to prevent fraudulent activity before it happens, helping you gain increased knowledge about fraud, and helping you learn some of the proactive measures you can take to avoid or mitigate fraud.

ONLINE AND E-MAIL FRAUD

Phishing

Phishing is the act that occurs when an entity falsely claiming to be an established, legitimate enterprise sends you an e-mail in an attempt to "fish" for personal information. The e-mail may direct you to visit a website and/or include an attachment or form as a way to update personal information, such as passwords and credit card, social security and bank account numbers. The website, however, is false and set up only to steal your information. These e-mails usually have a sense of urgency.

Amerant will never request personal identifiable information or PIN numbers in an e-mail:

- Be suspicious of any e-mail with urgent requests for personal financial information.
- Don't use links embedded in suspicious e-mails.
- Avoid filling out forms in e-mail messages that ask for personal financial information.

Tips to minimize the chances of becoming victim to Phishing:

- Never open e-mails from unknown senders.
- Never provide sensitive information through e-mail or outside of a secure website.
- Never follow unsolicited web links or open attachments in e-mail messages.
- Never forward unsolicited e-mails or initiate chain letters.
- Avoid "too good to be true" deals.

- Verify charity authenticity when making a donation via a website through the https:// and lock icons.
- Be aware of Phishing SMS texts ("smishing") on your cell phone.
- Use firewalls, anti-spyware and anti-virus software and keep them up-to-date.
- Avoid public Wi-fi networks when performing financial business.

Malware/Spyware

Malware (short for "malicious software"), includes viruses and spyware to steal personal information, send spam, and commit fraud. Criminals create appealing websites and downloads to attract you to links that will download malware – especially on computers that don't use adequate security software.

Tips to minimize the chances of malware/spyware:

- Talk about safe computing with your kids – Avoid free games or posting personal information.
- If you suspect malware on your computer, stop banking, shopping, and other online activities that involve user names, passwords, or other sensitive information.
- Update your operating system and Web browser software.
- Use anti-virus and anti-spyware software, as well as a firewall, and update them regularly.
- Download free software from websites you know and trust.
- Don't click on any links within pop-ups.

E-Mail Spoofing

E-Mail Spoofing is referred to fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. This involves a request from a fraudster that appears from a government agency, an official business, online payment, or bank.

Some tips to keep in mind:

- Avoid e-mails with distorted or oddly sized logos, poor grammar, odd links, sense of urgency and/or personal information request.

CARD FRAUD

ATM Card, Debit Card and Credit Card Fraud

ATM/Debit Card fraud has the potential to drain your checking account and tap into any back-up credit line you may have established. Vigilance and quick action is the best way to limit losses. The charges are simply deducted directly from your checking or savings account, and you may not be aware of the fraudulent activity until you review your bank statement.

How to Avoid ATM Card, Debit Card and Credit Card Fraud

- Only give out your Card number when you initiate the contact and believe the business to be reputable.
- Never give your Card information out when you receive a phone call from someone asking you to verify your information. (For example, don't provide your Card number if a caller tells you there has been a "computer problem" and they need you to verify information).
- Keep an eye on your Card every time you use it and make sure you get it back as quickly as possible. Try not to let your Card out of your sight whenever possible to avoid "skimming".
- Never provide your Card information on a website that is not a secure site. A secure site's URL begins with https:// and/or has a locked padlock symbol on the site.
- Sign the back of your Cards as soon as you receive them.

- Be aware of faulty ATMs or other individuals that may be nearby when entering your PIN.
- Never write your PIN number on a Card or where Card is kept.

CHECK FRAUD

What is Check Fraud?

Check fraud is one of the biggest challenges facing individuals, businesses and financial institutions. Advanced computer technology enables criminals, either independently or in organized gangs, to alter the appearance of your existing checks, create fake checks or forge your signature on a legitimate check. Desktop computer publishing programs and photocopying are often used to create or duplicate an actual financial document; chemical alteration can remove some or all of the information on the check; and stealing check(s) and forging your signature to withdraw funds from your account or make a fraudulent payment are common types of check fraud.

There are several ways that criminals commit check fraud:

- Forgery
- Counterfeiting
- Alteration
- Check Kiting

How To Avoid Check Fraud:

Tips for Individuals

- Keep your checkbook in a safe place, and carefully consider who can access it, even possible extended family members (some check fraud is committed against one family member by another.
- Review your monthly statements frequently and be on the alert for any suspicious or forged checks.
- Never print or write unnecessary personal information on your check, such as Cedula, Social Security Number, credit card number or telephone number.
- Shred old checks, bank statements and any other bank account information after you have verified that all statements are correct and you have balanced your checkbook. Do not pre-sign checks thinking you will have them handy "in case of an emergency" or for any other reason.

Tips for Businesses

Forgery of a business account typically takes place when someone issues a check without proper authorization. Criminals will also steal a check, endorse it and present it for payment at a retail location or at a bank teller window, commonly using bogus personal identification.

- Have internal controls in place to ensure that no single individual has the authority to access every aspect of your company's check-writing or printing system
- Payroll checks are the most frequently altered checks so inspect every payroll check you sign to make sure the check is complete and the check numbers are in sequence

SAMPLE FRAUD SCHEMES

Pretexting Calling

Pretexting is the practice of gaining someone's trust by pretending to be someone else. The objective of these calls, is to get your personal information, such as social security number, passport, date of birth, or bank account number, under false pretenses. This may be someone posing as a Financial Institution, a bill Collection agency or a Government agency.

Another way that criminals improperly obtain personal information of bank customers is by contacting the bank, posing as a customer or someone authorized to have the customer's information, and through the use of trickery and deceit, convincing an employee of the bank to release customer identifying information.

Nigerian Email Fraud

Nigerian Email Fraud proposes to offer large sums of money to individuals in the U.S. who help criminals, impersonating as government officials, move millions of dollars out of Nigeria or another foreign country. The impersonators promise to transfer funds into a victim's U.S. bank account after receiving a fee. The fees are usually passed off as taxes, or processing fees in violation of the section 419 of the Nigerian criminal code. The fraud is sometimes referred to as the "419 Fraud." Because the fee is paid in advanced of receiving the promised large fee payoff, this type of fraud is referred to at an Advance-Fee Fraud. In addition to email, Advanced Fee Frauds commonly reach victims through chat rooms, phone and fax, as well as dating/matchmaking and gaming websites.

Lottery and Award Frauds

Lottery or Award Frauds lure victims to pay significant fees in advance of receiving winnings from a nonexistent lottery. Because the fee is paid in advance of receiving the promised significant cash prize money, this type of fraud is referred to as an Advance-Fee Fraud.

Counterfeit Cashier's Check Frauds

Schemes involving fraudulent cashier's checks usually begin with a receipt of the check in the mail. Commonly, the criminals position the check as prize money awarded to the victim. The victim is instructed to deposit the check and return a portion to the impersonating contest organizers to pay for fees, usually by wire transfer to a foreign country. Because banks release funds from cashier's checks before funds are actually cleared, the victim assumes the funds have cleared and arranges for the wire transfer.

Work at Home/Mystery Shopper Schemes

Victims of Work at Home/Mystery Shopper Schemes are hired by scandalous companies to shop retailers and take note of the shopping experience, merchandise or other dimensions associated with the retailer. In return, the criminal sends the victim a cashier's check to pay for the shopping services. Typically, the check is for an amount significantly higher than the fee owed. The victim is instructed to deposit the check and return the overage amount, usually by wire transfer. Or, the victim is instructed to return the amount of the check to cover initial fees with a promise that a larger check will be forthcoming. Because banks release funds from cashier's checks before funds are actually cleared, the victim assumes the funds have cleared and arranges for the wire transfer. A variation of this scheme is for the criminal to ask for the shopper's bank information in order to send a direct deposit for the services rendered.