Consumer Tips from the VBA

Banks are national leaders in preserving the security of customer data. The industry dedicates hundreds of millions of dollars annually to data security, and adheres to strict regulatory and network requirements. The banking industry's first priority is to protect consumers.

Protecting your debit card:

- Always protect your debit card and keep it in a safe place, just like you would cash, credit cards or checks.
- Do not leave your debit card lying around the house or on your desk at work. No one should have access to the card but you. Immediately notify your bank if it is lost or stolen.
- Keep your Personal Identification Number (PIN) a secret. Never write it down anywhere, especially on your debit card.
- Never give any information about your debit card or PIN over the telephone. For example, if you receive a call, supposedly from your bank or possibly the police, wanting to verify your PIN, do not give that information. Notify the police immediately.

In the event of a data breach:

- Report any suspected fraud to your bank immediately.
- Use online banking to protect yourself. Monitor your financial accounts regularly for fraudulent transactions. Sign up for text or email alerts from your bank for certain types of transactions, such as online purchases or transactions of more than $500.
- Beware of phishing scams. Never give out personal financial information in an email or over the phone unless you have initiated the contact.
- Monitor your credit report. Order a free copy of your credit report every four months from one of the three credit reporting agencies at annualcreditreport.com.

If you suspect your identity has been stolen:

- Call your bank and credit card issuers immediately so they can start working on closing your accounts and clearing your name.
- File a police report and call the fraud unit of three credit-reporting companies. The fraud unit numbers are:

  TransUnion (800) 680-7289
  Experian (888) 397-3742
  Equifax (800) 525-6285
- Consider placing a victim statement in your credit report.
- Make sure to maintain a log of all the contacts you make with authorities regarding the matter. Write down names, titles, and phone numbers in case you need to re-contact them or refer to them in future correspondence.
- For more advice, contact the FTC's ID Theft Consumer Response Center at 1-877-ID THEFT (1-877-438-4338) or www.ftc.gov/idtheft.

Consumer Tips from the VBA

Protecting your mobile device:
Your mobile device provides convenient access to your email, bank and social media accounts. Unfortunately, it can potentially provide the same convenient access for criminals.

- Use the passcode lock on your smartphone and other devices. This will make it more difficult for thieves to access your information if your device is lost or stolen.
- Log out completely when you finish a mobile banking session.
- Protect your phone from viruses and malicious software, or malware, just like you do for your computer by installing mobile security software.
- Use caution when downloading apps. Apps can contain malicious software, worms, and viruses. Beware of apps that ask for unnecessary "permissions."
- Download the updates for your phone and mobile apps.
- Avoid storing sensitive information like passwords or a social security number on your mobile device.
- Tell your financial institution immediately if you change your phone number or lose your mobile device
- Be aware of shoulder surfers. The most basic form of information theft is observation. Be aware of your surroundings especially when you're punching in sensitive information.
- Wipe your mobile device before you donate, sell or trade it using specialized software or using the manufacturer's recommended technique. Some software allows you to wipe your device remotely if it is lost or stolen.
- Report any suspected fraud to your bank immediately.

Protecting yourself online:
Though the internet has many advantages, it can also make users vulnerable to fraud, identity theft and other scams. According to a Norton Cybercrime Report, 556 million adults worldwide were victims of cybercrime in 2012.

- Keep your computers and mobile devices up to date. Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Turn on automatic updates so you receive the newest fixes as they become available.
- Set strong passwords. A strong password is at least eight characters in length and includes a mix of upper and lowercase letters, numbers, and special characters.
- Watch out for phishing scams. Phishing scams use fraudulent emails and websites to trick users into disclosing private account or login information. Do not click on links or open any attachments or pop-up screens from sources you are not familiar with. Forward phishing emails to the Federal Trade Commission (FTC) at spam@uce.gov – and to the company, bank, or organization impersonated in the email.
- Keep personal information personal. Hackers can use social media profiles to figure out your passwords and answer those security questions in the password reset tools. Lock down your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc. Be wary of requests to connect from people you do not know.
- Secure your internet connection. Always protect your home wireless network with a password. When connecting to public Wi-Fi networks, be cautious about what information you are sending over it.
- Shop safely. Before shopping online, make sure the website uses secure technology. When you are at the checkout screen, verify that the web address begins with https. Also, check to see if a tiny locked padlock symbol appears on the page.
- Read the site's privacy policies. Though long and complex, privacy policies tell you how the site protects the personal information it collects. If you don't see or understand a site's privacy policy, consider doing business elsewhere.
- Be wary of pop-ups or ads offering free security scans. Many messages are designed to scare you into believing your device is infected so you will purchase their service. These scams may actually end up causing you money and possibly cause you to download malware.