 **Credit Card**

**Holder Security Guidelines**

* Never leave your credit card unattended or in an unlocked location. This includes at work or in your vehicle. Credit cards left out in the open are prime targets, all it takes is a quick picture of your card for someone to have all your information. Don’t let any unauthorized persons view your card. You should not write down your credit card information, this includes in unsecure electronic documents and files.
* If you must give your credit card information out over the phone, make sure to verify the identity of the person you are giving it to. Make sure to only verbally relay the card information in a secure location where you cannot be over heard, you should never give out a credit card number verbally, in a public area where others can hear and copy the information.
* Never give out credit card information over email. Email can be very unsecure and numbers can be easily stolen. Be warry of anyone asking for account information via email even if it appears to be from a reputable source.
* Never enter your credit card information on a public or shared computer. Make sure you are only using your own or a secure work computer not a public kiosk.
* Do not enter any information on unsecure websites. Most modern internet browsers will show you a lock and green text or other indications that the site is secure. Secure sites will always start with “HTTPS” the S at the end stands for secure. If the website pops up with any errors or security warnings be mindful and don’t enter your information.
* Keep passwords and PINs secret. Do not write them down or give them to others. This includes things like email and non-credit card related accounts as they may be used to try to gain access to your credit card information.
* Make sure you are buying from reputable sources, especially online. Anyone can setup a website that accepts credit cards, make sure you know who you are giving your credit card information to.
* Watch using your card on public devices, skimmers can be attached to gas pumps and other card readers, if the reader you are using looks funny, or too bulky, or seems to be loose and wiggles, it may be an indication that a scam device has been added over top of the normal device.
* Report any strange activity, especially if you think your card has been compromised. It is much easier to fix right away instead of waiting until there is a larger problem.