Season's Greetings Everyone!!!

Being that we are at the heart of holiday shopping and many of us are using online shopping websites, here are a few tips to keep you safe.

Three common ways that attackers can take advantage of online shoppers:

- **Creating fraudulent sites and email messages** – Unlike traditional shopping, where you know that a store is actually the store it claims to be, attackers can create malicious websites or email messages that appear to be legitimate.
- **Intercepting insecure transactions** – If a vendor does not use encryption, an attacker may be able to intercept your personal and credit information as it is transmitted.
- **Targeting vulnerable computers** – If you do not take steps to protect your computer from viruses or other malicious code, an attacker may be able to gain access to your computer and all of the information on it.

How can you protect yourself?

- **Do business with reputable vendors**
  Before providing any personal or financial information, make sure that you are interacting with a reputable, established vendor. Some attackers may try to trick you by creating malicious websites that appear to be legitimate, so you should verify the legitimacy before supplying any information
- **Make sure your information is being encrypted**
  Many sites use secure sockets layer to encrypt information. Indications that your information will be encrypted include a Uniform Resource Locator (URL) that begins with "https:" instead of "http:" and a padlock icon. If the padlock is closed, the information is encrypted. The location of the icon varies by browser; for example, it may be to the right of the address bar or at the bottom of the window. Some attackers try to trick users by adding a fake padlock icon, so make sure that the icon is in the appropriate location for your browser.
- **Be wary of emails requesting information**
  Attackers may attempt to gather information by sending emails requesting that you confirm purchase or account information. Legitimate businesses will not solicit this type of information through email. Do not provide sensitive information through email. If you receive an unsolicited email from a business, instead of clicking on the provided link, directly log on to the authentic website by typing the address yourself.
- **Use a Credit Card vs a Debit Card**
  There are laws to limit your liability for fraudulent credit card charges, but you may not have the same level of protection for your debit cards. Additionally, debit cards

draw money directly from bank accounts, unauthorized charges could leave you with insufficient funds to pay other bills. You can minimize potential damage by using a single, low-limit credit card to make all of your online purchases. Also, use a credit card when using a payment gateway such as PayPal, Google Wallet, or Apple Pay.

- **Check your shopping app settings**
  Look for apps that tell you what they do with your data and how they keep it secure. Keep in mind that there is no legal limit on your liability with money stored in a shopping app (or on a gift card). Unless otherwise stated under the terms of service, you are responsible for all charges made through your shopping app.
- **Check your statements**
  Keep a record of your purchases and copies of confirmation pages and compare them to your bank statements. If there is a discrepancy, report it immediately.

- **Check privacy policies**

  Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.

Have a Safe & Wonderful Holiday Season