Please use the following tips to help protect your self from phishing scams:

- Treat with caution unsolicited emails that claim to come from a trusted company. Be particularly cautious about emails that reference fictitious business interactions, supposed fraudulent transactions, or communications/requests for information that you do not recall.

- Become naturally suspicious of any email that includes links to websites or attachments, even if sent by family or friends, as their computers may be infected with malware. By visiting the websites or opening the attachments, malware may be injected into your computer.

- Ask yourself, "Why is the company writing to me about this?" If you have any doubts, call the company or go to its website by performing a Google search to locate the organization's true Web address.

- Do not click or open any attachments, as they could contain viruses or spyware that record where you go online and capture any passwords or card numbers you type online.

- Look for "https" in URLs displayed in your browser's address bar (the "s" stands for secure). If you do not see it, the data you send is passed over public networks in an unencrypted manner, which leaves it exposed to eavesdropping by attackers who may access the data in transit. You should not enter any personal or financial data.

- If you see "@" in the middle of the URL, there is a good chance it is a phishing site. Legitimate companies use the domain name in their Web addresses (such as www.company .com) and do not have "@" in their URL addresses.

- Maintain up-to-date firewalls and security patches.

- If your information is compromised, place a fraud alert on your credit report by contacting the fraud department of any one of the three major credit bureaus.

- Visit the Federal Trade Commission's ID Theft page at <www.consumer .gov/idtheft> for more information on how to protect yourself from identity theft.