7 Ways to Avoid Online Fraud
by: Keith Hughes, Vice Chairman and CEO

Internet fraud continues to be a growing problem in the U.S. According to the FBI's Internet Crime Complaint Center, the agency received approximately 270,000 complaints from consumers who were exposed to online fraud in 2014 — up from nearly 263,000 in 2013.

Fraudsters use many tools, resources and tactics to access your personal information. If you navigate the web, as most of us do every day, it's extremely important that you safeguard your personal information by developing stronger passwords and ensuring that your online security software is up to date.

The First recommends the following tips to keep you safe online:

- **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. Never 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 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.

    This article edited from information provided by the American Bankers Association.