Date: **12/29/17**

Subject: **Internet Security**

Dear Customer:

Listed below are guidelines for proper internet security that can help protect you from fraud.

Online Banking - Our online banking system provides you with the date and time of your last session ("last login") located in the upper right-hand corner when you sign in. This allows you to check the most recent online session. If you notice a date and time when you believe you did not sign-on, someone else may have been accessing your information.

User ID and Password - Please follow these rules to protect yourself:

1. Never disclose your user ID or password to anyone.
2. Memorize your user ID and password; do not write them down.
3. Use a mix of letters (capital and lower case), numbers, and symbols.
4. Change your password frequently.
5. Do not use birth dates, names, or other easily guessed letters or numbers.

Do not be fooled by fraud: WE WILL NEVER SEND YOU AN EMAIL OR TEXT MESSAGE ASKING FOR YOUR USER ID OR PASSWORD.

Log Out - When you have completed using our online site, "Sign Out" using the Sign Out link in the upper right-hand corner of the website. We suggest you do this before you shut your computer off and before you surf to any other websites.

Email - Do not use your personal email account to send us sensitive information (such as social security numbers, account numbers, etc.). Send us messages through our secured website using our messaging system by clicking on "Messages" located on the top right-hand corner of the website.

Public Computers, Internet Access - Do not use public computers or public Internet access such as "Internet Cafes" or "Free Wi-Fi" to conduct online banking.

Phishing, Spoofs, Hoaxes and Other Deceptive Emails - Be careful when responding to email messages that appear to be from us, a regulator or an auditor. Thieves or hackers send email messages which direct you to click on a link which then redirects you to a fraudulent website, or pop-up window where you may be asked to "confirm", "verify", "update", or otherwise provide sensitive information (such as your account number, sign-on ID, password, or social security number). Sometimes these email messages will falsely say that your account will be shut down if

you do not act quickly. Do not be intimidated by these threats. These links, websites and pop-up windows may look like ours, but they are not. Clicking a link in one of these emails can expose your computer to viruses and spyware, even if you do not supply the sensitive information thieves want. We will never send you an email that asks you to verify an account number, sign-on ID, password, or social security number. If you receive such a request, it is fraudulent. If you have any doubts about whether an email from us is authentic, do not reply to it, do not open any attachment, and do not use the link in the email. Instead, contact us through our website by clicking on "Messages" located on the top right-hand corner of the website, or calling us at 1.800.807.1666.

Spam - Do not open attachments in email messages if you do not know the sender. Attachments can contain viruses and spyware. Delete unwanted email.

Links to Other Websites - If you click a link to another website, that website may collect, use, and disclose information about you in ways that are different from what we do. You should review that website's policies. We are not responsible for what the operators of other websites do with your information. We will give you a pop-up notice to let you know you are going to an unaffiliated third party's website.

Security for Your Own Computer - Protect your own computer by doing these things:

1. Keep your operating system and browser up-to-date.
2. Install anti-virus suite, including firewall and malware protection, and keep it up-to-date.
3. Scan your computer for spyware on a regular basis.
4. Do not download programs or files from unknown sources.
5. Install a pop-up blocker from a trustworthy source.

If you have any questions, please call Customer Service at 1.800.807.1666.

Thank you for your continued business.

Sincerely,

Daniel J. Machon, Jr.
President and CEO