ONLINE SECURITY TIPS

You can reduce the risks of fraud and the loss of personal data and assets from your health, welfare, or retirement account by following these basic rules:

• REGISTER, SET UP AND ROUTINELY MONITOR YOUR ONLINE ACCOUNT

- Maintaining online access to your retirement account allows you to protect and manage your investment.
- Regularly checking your health/retirement account reduces the risk of fraudulent account access.
- Failing to register for an online account may enable cybercriminals to assume your online identify.

• USE STRONG AND UNIQUE PASSWORDS/PASSPHRASES

- Don't use common passwords.
- Don't use letters and numbers in sequence (no "abc", "567", etc.).
- Don't write passwords down.
- Consider using a secure password manager to help create and track passwords.
- Use 14 or more characters.
- Change passwords annually, or if there's a security breach.
  - » National Institute of Standards and Technology guidance suggests favoring longer passwords/passphrases instead of requiring regular and frequent password resets
- Don't share, reuse, or repeat passwords.

• USE MULTI-FACTOR AUTHENTICATION

- Multi-Factor Authentication (also called two-factor authentication) requires a second credential to verify your identity (for example, entering a code sent in real-time by text message or email).

• KEEP PERSONAL CONTACT INFORMATION CURRENT

- Update your contact information when it changes, so you can be reached if there's a problem.
- Select multiple communication options.

• CLOSE OR DELETE UNUSED ACCOUNTS

- The smaller your on-line presence, the more secure your information. Close unused accounts to minimize your vulnerability.
- Sign up for account activity notifications.

• BE WARY OF FREE WI-FI

- Free Wi-Fi networks, such as the public Wi-Fi available at airports, hotels, or coffee shops pose security risks that may give criminals access to your personal information.
- A better option is to use your cellphone or home network.

• BEWARE OF PHISHING ATTACKS

- Phishing attacks aim to trick you into sharing your passwords, account numbers, and sensitive information, and gain access to your accounts. A phishing message may look like it comes from a trusted organization, to lure you to click on a dangerous link or pass along confidential information.
- Common warning signs of phishing attacks include:
  - » A text message or email that you didn't expect or that comes from a person or service you don't know or use.
  - » Spelling errors or poor grammar.
  - » Mismatched links (a seemingly legitimate link sends you to an unexpected address). Often, but not always, you can spot this by hovering your mouse over the link without clicking on it, so that your browser displays the actual destination.
  - » Shortened or odd links or addresses.
  - » An email request for your account number or personal information (legitimate providers should never send you emails or texts asking for your password, account number, personal information, or answers to security questions).
  - » Offers or messages that seem too good to be true, express great urgency, or are aggressive and scary.
  - » Strange or mismatched sender addresses.
  - » Anything else that makes you feel uneasy.

• USE ANTIVIRUS SOFTWARE AND KEEP APPS AND SOFTWARE CURRENT

- Make sure that you have trustworthy antivirus software installed and updated to protect your computers and mobile devices from viruses and malware. Keep all your software up to date with the latest patches and upgrades. Many vendors offer automatic updates.

• KNOW HOW TO REPORT IDENTITY THEFT AND CYBERSECURITY INCIDENTS

- The FBI and the Department of Homeland Security have set up valuable sites for reporting cybersecurity incidents:
  - » https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view
  - » https://www.cisa.gov/reporting-cyber-incidents