CYBERSECURITY NOTICE

You are responsible for taking reasonable measures to keep all of your on-line account and personal information secure. The Fund is providing you with some tips to help protect the overall security of your personal and other sensitive information. The Fund Office also has various privacy, security, and anti-fraud measures in place to safeguard your confidential information and the Fund's assets.

1. ROUTINELY CHECK YOUR RETIREMENT ACCOUNT TO REDUCE THE RISK OF FRAUDULENT ACCOUNT ACCESS.

- Carefully review and follow security requirements and recommendations in notices and alerts you receive from the Fund.

2. USE STRONG AND UNIQUE PASSWORDS.

- Don't use dictionary words.
- Use letters (both upper and lower case), numbers, and special characters.
- Don't use letters and numbers in sequence (no "abc", "567", etc.).
- Consider using 14 or more characters.
- Don't write passwords down.
- Consider using a secure password manager to help create and track passwords.
- Consider updating passwords periodically.
- Update passwords immediately if you've experienced a security breach.
- Don't share, reuse, or repeat passwords.

3. ACTIVATE ENHANCED SECURITY FEATURES

- Consider using multi-factor authentication, automatic account lock, and other enhanced security features where available.

4. KEEP PERSONAL CONTACT INFORMATION CURRENT.

- Update your contact information on file with the Fund Office when it changes.
- Provide the Fund Office multiple options to communicate with you.

5. BE WARY OF FREE WI-FI.

- Free Wi-Fi networks, such as the public Wi-Fi available at airports, hotels, or coffee shops, pose greater security risks that may give cyber criminals access to your devices and personal information.
- Always use secure, private network connections (e.g., a home, cellphone, or virtual private networks) when sending or receiving sensitive data.

6. BEWARE OF PHISHING ATTACKS AND SCAMS.

- Phishing and other social engineering attacks aim to trick you into sharing your passwords, account numbers, and other sensitive information, to enable cyber criminals to gain access to your accounts. A phishing message may look like it comes from a trusted organization to lure you into clicking on a dangerous link or sharing 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 urgency, or are aggressive and scary.
- Strange or mismatched sender addresses.
- Anything else that makes you feel uneasy.

7. 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.
- Turn on your firewall.
- Keep your software (apps, web browsers, operating systems) up to date with the latest patches and upgrades.

8. SECURE AND PROPERLY DISPOSE OF SENSITIVE MATERIALS.

- Securely store your sensitive information. Shred or otherwise securely dispose of all documents containing any sensitive or personal information.

9. 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
- The Federal Trade Commission encourages consumers to report identity theft and obtain a personal recovery plan at https://www.identitytheft.gov/#/
- Immediately report any suspicious or unusual activity to the Fund Office.

If you have questions about these tips or the security of your account or Fund information, please contact the Fund Office at (217) 793-7200.