UFCW ALBERTSONS VAPF
UFCW
America's Food and Retail Union

UFCW International Union-Albertsons Variable Annuity Pension Fund

P.O. Box 4568 • Oak Brook, Illinois 60522-4568
Toll Free (833) 651-2370 • Fax (312) 329-7923
www.ufcwvapfalbertsons.org

The Fund is providing you with a copy of some security tips to help you protect the security of your retirement benefits with the Fund, as well as the overall online security of your personal information.

If you have an account under the Fund participant portal, you should:

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

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.).
   - Use 14 or more characters.
   - Don’t write passwords down.
   - Consider using a secure password manager to help create and track passwords.
   - Change passwords every 120 days, or if there’s a security breach.
   - Don’t share, reuse, or repeat passwords.

3. **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.

4. **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.

5. **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.

6. 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.

7. 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

If you have questions about these tips or the security of your Fund information, please contact the Fund Office at (833) 651-2370.