MEMO

Date
TO: All Employees
FROM: Human Resources
RE: **[PLAN NAME]**

Keep your plan assets safe!

You work hard for your money. You wisely choose to defer a portion of your salary for your interests in your retirement years. **[IF EMPLOYER CONTRIBUTIONS ARE MADE INCLUDE:** We support your savings effort by making a [matching/profit sharing/matching and profit sharing**]** contribution on your behalf into the plan. The plan is designed to help you grow your savings to an appropriate amount of money to support you once you reach your retirement years.

But as you are aware, the plan is only as effective as you make it. If you defer too little, or make unwise investment decisions there is a chance that you will not reach your goals. Similarly, if you drain your plan balance over the years, you understand you will find a shortfall in retirement. What many participants do not think about is being responsible for the security of their savings as well.

Cyber fraud has been a growing concern globally for years. Individuals are typically very careful to keep their security measures (passwords, authentication codes, etc.) private with regards to their banking and electronic mail accounts. However in the past few years there have been breaches of major companies containing personal information of individuals. And unfortunately much of the personal information has become accessible by bad actors on the dark web.

Participants need to be vigilant with their retirement savings accounts as well. In the past 12 months there have been a slew of cases of attempted fraud, some successful, enacted on retirement savings plan participants. And these attempts have occurred across a multitude of recordkeepers. The good news is that virtually all recordkeepers have security as a prominent priority and spend. They are constantly updating their security technology and protocols. But their security can only go so far if the participant is not being equally vigilant.

The following are a few prudent tips for participants in ensuring the security of their retirement savings accounts:

- Use multiple levels of security and authentication – if your plan's recordkeeper comes out with a new level/type of authentication, engage it immediately.
- If you frequent a website, or have an account with a company, whose website and information has been compromised, change all your

passwords. For example, Yahoo recently had a large breach – a breach containing passwords – if you ever had a Yahoo account you should change your password.

- Make sure your password is strong – utilize letters, capitalization, numbers, and symbols. Don't use recognizable words. Don't use the same password for multiple purposes. Have the password be at least 14 characters in length. Consider changing your password on a frequent basis.
- Never send your authentication to anyone requesting it. It should be limited to use on sites on which you navigated to independently of any outside request.
- Check your account on a semi-regular basis for any irregularities.
- Immediately contact your plan administrator and/or the recordkeeper if you receive any update that sparks your concern – do not wait, the money could leave the U.S. quickly.

As your employer we are always looking out for your wellbeing. We trust that the plan is in good hands with **[RECORDKEEPER]**. We have reviewed their cyber security protocals and technology. But we felt a need to provide a gentle reminder that your involvement is crucial in maintaining the security of your account too.

We want your savings experience to be as simple and easy as possible. We want you to someday enjoy your retirement years. If you have any questions please contact **[CONTACT INFORMATION]**.