October 2017

Dear Participant,

I understand that you are concerned about the breach announced by Equifax. I appreciate the opportunity to provide you with some perspective on how we protect client information and accounts at Fidelity, as well as a few steps you may want to consider taking.

While we cannot comment on a matter that occurred at another firm, we can tell you that we take security very seriously and closely monitor our online environment. Fidelity has a range of safeguards and multiple layers of security in place to protect customer accounts and information, our sites, and our systems. For security reasons, some of these protections are visible, while some are not.

We believe that applying multiple layers of protection is a "best in class" approach. That's why we offer customers several means of using two-factor authentication to enhance the protection of their accounts, and, as part of our regular security measures, we monitor to protect against fraudulent account activity and require additional authentication steps for certain online transactions, such as setting up new instructions for transferring funds electronically from a Fidelity account to another account, such as a bank.

We invite you to learn more about some of the ways we protect you, as well as what you can do to protect yourself online by visiting www.fidelity.com/security.

We recommend that clients who believe that they may be affected by the Equifax breach take the steps that Equifax recommends (www.Equifaxsecurity2017.com). The Federal Trade Commission has also published some guidance on the topic: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

Please be alert for updates from Equifax and if you have further questions regarding their data breach, please contact Equifax directly.

You may want to consider taking these additional steps as well:

- Set up two-factor authentication on your Fidelity accounts, if you have not already done so. Please make sure we have your current cellphone number (for SMS messages, used in two- factor authentication.)
- Update your Fidelity security questions and answers.
- Regularly monitor your Fidelity accounts and promptly report any concerns to us.
- Check with your wireless and Internet service providers for steps they may recommend for protecting your mobile phone and Internet accounts.

We also offer the Fidelity Customer Protection Guarantee. Under the terms of the Guarantee, cash and securities in your retirement and non-retirement accounts with Fidelity Brokerage Services LLC, as well as individual workplace retirement accounts under a 401(k), profit sharing, 403(b), or 457 plan for which Fidelity is the record keeper, are covered. We will reimburse Fidelity accounts for losses due to unauthorized activity if we conclude that unauthorized activity occurred through no fault of your own and subject to the Guarantee's terms and conditions. For specific terms and conditions of the Guarantee, please see https://www.fidelity.com/security/customer-protection-guarantee.

If you need assistance and/or have questions regarding these additional steps, you can call 1-800-FIDELITY anytime and we will be happy to help.

I hope you find this perspective and information helpful.

Sincerely,
Fidelity Investments

Fidelity Investments Institutional Services Company, Inc., 500 Salem St., Smithfield, RI 02917

817244.1.0