



## Equifax Cybersecurity Incident Memo September 11, 2017

On September 7, 2017, Equifax announced what it describes as a "cybersecurity incident" involving consumer information affecting up to 143 million customers. According to an Equifax statement the incident of unauthorized access occurred from mid-May through July 2017. Information accessed primarily included names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers. More information on the breach can be found at <https://www.equifaxsecurity2017.com>.

**It is important to note that this is an Equifax incident and is not related in any way to Schwab data or systems.**

Below is some useful information about the security of your Schwab account(s):

- Remember that Schwab provides you with the "Schwab Security Guarantee"  
[https://www.schwab.com/public/schwab/nn/legal\\_compliance/schwabsafe](https://www.schwab.com/public/schwab/nn/legal_compliance/schwabsafe)
- Schwab offers Voice ID Authentication or verbal passwords as a means of authentication when you call in to Schwab
- Use strong online security practices such as using a unique id/password combination on SchwabAlliance.com
- Schwab offers the additional security of Two Factor Authentication through the use of security tokens offered by Schwab
- Review account activity and Schwab Advisor Center alerts to ensure there is no suspicious activity occurring in your clients' accounts such as unexpected money movements, changes to contact information and adding web access.
- If you would like additional information, please contact your Service Team. Clients wishing to establish Voice ID, verbal passwords, or request tokens may do so by calling Schwab Alliance at 800-515-2157.

In the future, if you ever suspect fraud or identity theft, the faster you act the better. Here is what you should do right away if you suspect fraud.

- 1) Call the Schwab Identity Theft Team at 877-862-6352. If you're abroad, call +1-602-355-7300
- 2) Schwab will evaluate the circumstances and may suggest one or all of the following:
  - a. Verbal password on your accounts
  - b. Use of a security token and key fob for online access
  - c. The cloning of your accounts to new account numbers
- 3) If Schwab determines unauthorized activity, contact the following:
  - a. Equifax-Call 800-525-6285 or visit [www.equifax.com](http://www.equifax.com) or write P.O. Box 740250, Atlanta, GA 30374
  - b. Experian-Call 888-397-3742, or visit [www.experian.com](http://www.experian.com) or write P.O. Box 9556, Allen, TX 75013
  - c. TransUnion-Call 800-680-7289, or visit [www.transunion.com](http://www.transunion.com) or write P.O. Box 6790, Fullerton, CA 92634
- 4) After contacting the credit bureaus, notify your bank(s) and credit card company(ies)
- 5) After contacting the bank and credit card companies, notify the appropriate government agency.
  - a. Visit the FTC's Identity Theft Site [www.ftc.gov/bcp/edu/microsites/idtheft](http://www.ftc.gov/bcp/edu/microsites/idtheft) to learn more
  - b. Forward suspicious emails to [nophishing@cbbb.bbb.org](mailto:nophishing@cbbb.bbb.org)
- 6) Consider an identity monitoring service. These firms monitor your personal information such as bank account information or Social Security, driver's license, passport, or medical ID number and alert you when your information shows up in many kinds of public databases such as: change of address requests, court or arrest records, orders for new utility, cable, or wireless services, check cashing requests, social media websites that identity thieves use to trade stolen information, etc.

As always, please contact us if we can be of further assistance.