BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

PRESS RELEASE

Attorney General Frosh Sends Letter Directing Equifax to Revise Confusing Messaging to Consumers and Remove All Potential for Profit

BALTIMORE, MD (September 13, 2017) – Maryland Attorney General Brian E. Frosh today issued a letter to Equifax CEO Richard F. Smith, addressing Equifax's behavior in the wake of its data breach, affecting approximately 143 million Americans, and approximately 3 million Marylanders.

Attorney General Frosh writes: "I am extremely concerned that a company that is in the business of collecting and maintaining private information, and providing credit monitoring and identity theft protection for consumers, exposed the social security numbers and other personal information of 143 million Americans. I want to know exactly how that happened, but more immediately, I am concerned about the confusion that you have caused for consumers."

The letter continues to address how Equifax publicized the breach, and the confusing messaging it provided to consumers who want to take steps to protect their information. In particular, Attorney General Frosh notes: "Many consumers who initially visited your website were steered toward your paid products rather than your free offer. Those that did find their way to your free offer were hesitant or unwilling to sign up for your offer because of unacceptable terms, some of which you have since deleted. Others never saw the terms of use, because they are effectively hidden. Those who began enrollment in your offer received a message that starts with 'Thank You' in large bold font. This message appears very similar to the types of messages consumers are accustomed to seeing after making online purchases. Many consumers are likely to ignore this message. Many will assume that they have signed up and will not read the message to realize that they have been assigned a future date to come back and actually start the registration. As a result, many will not return on their designated date to actually sign up for the offer. I believe that certain aspects of your messaging to consumers in the wake of this breach have the capacity to mislead consumers and may violate the Maryland Consumer Protection Act."

Attorney General Frosh urges Equifax to take the following steps to help stem confusion for consumers:

1. Suspend the sale of all credit monitoring and services.
2. Suspend the practice of charging Maryland consumers for credit freezes.
3. Provide information for non-English speakers.

4. Reconsider asking consumers for the last 6 digits of the Social Security Number and last name. Consumers are already wary of providing additional information.
5. Clearly state the free credit monitoring enrollment process and steps consumers must take, especially if they must follow up on another date.
6. Ensure consumers see the terms of use before agreeing to them, rather than providing them as a hard to find link.
7. Do not automatically re-enroll consumers in any of Equifax's products.
8. Do not advertise any products to any consumer who signed up for the free credit monitoring.

BACKGROUND

On September 7, 2017, Equifax publicized that the company experienced a data breach. According to the company, the breach lasted from mid-May through July of 2017. The data breach exposed full names, Social Security Numbers, birth dates, addresses, and driver's license numbers. For another 209,000 consumers, it also included credit card information.

The Equifax data breach puts consumers at risk for new account fraud, since it exposes personal information necessary to open new accounts at any point in the future. This information can be used to take out loans, open new credit accounts and other illegal and potentially damaging actions.

Attorney General Frosh encourages consumers to take the following steps:

- Check your credit reports from all three of the major credit reporting agencies: Equifax, Experian, and TransUnion. Reports can be obtained for FREE by visiting www.annualcreditreport.com or by calling 1-877-322-8228. Unrecognizable accounts or activity could indicate identity theft.
- Carefully monitor your financial accounts and statements for unauthorized activity. Many financial institutions offer additional layers of protection. It is okay to call your bank to ask if there are any additional steps you can take to protect your account.
- Consider signing up for the free credit monitoring service from Equifax. This service is designed to notify you of any changes to your credit reports. Equifax has created a dedicated website to assist consumers: https://www.equifaxsecurity2017.com/
- Consider placing a credit freeze at all three credit reporting agencies. A credit freeze is **extremely** effective at preventing identity thieves from opening new accounts in your name without your consent. A credit freeze won't prevent a thief from making charges to your existing accounts, such as debit and credit cards. Parents or guardians of minor children may also place a credit freeze on behalf of their child. For more information on how to obtain a credit freeze, please visit http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/freezing.aspx
- Visit www.identitytheft.gov/databreach to learn more.

The Office of the Attorney General recommends that consumers review their account statements, online accounts, and credit files regularly for suspicious activity. If consumers feel they have been harmed and want to file a complaint, please call our Identity Theft Unit at1-888-743-0023, or visit our website at www.marylandattorneygeneral.gov.

A copy of the letter sent to Equifax CEO Richard Smith can be found here.