Department of Business Regulation
Insurance Division
1511 Pontiac Avenue, Bldg. 69-2
Cranston, Rhode Island 02920

Consumer Alert 2017-5

Credit Freezes and the Burn They Have on Hackers

More than 143 million Americans' personal information was exposed when Equifax announced earlier this year it was the victim of a data breach. Hackers accessed names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. Guarding against identity theft is important because bankers and insurers reward good credit. Bankers and insurers use your credit information when granting loans and pricing and underwriting insurance products. A favorable credit score often results in lower interest and insurance rates.

If you have a credit report, chances are you were impacted by the Equifax breach. Equifax took immediate steps to help affected consumers, including freezing customers' credit. Before you take this step, the Rhode Island Insurance Division and the National Association of Insurance Commissioners (NAIC) offer these tips for your consideration.

What happens when you freeze your credit?

A credit freeze or security alert, restricts access to your credit report, thwarting would-be hackers from gaining access to your personal information. Without a credit report, most creditors won't approve or open a new account.

A credit freeze does not:

- Impact your credit score.
- Prevent you from getting a free annual credit report.
- Stop you from opening a new account, applying for a job, renting an apartment or buying insurance. Note: you can temporarily lift the credit freeze for a specified time to conduct this business. You may have to pay for the temporary lift, so check with one of the credit reporting agencies. There is no charge for consumers impacted by the Equifax data breach of 2017.

A hacker cannot lift your credit freeze and open a new line of credit. A personal identification number (PIN) is required to lift it.

Some states allow insurers to access your credit information to underwrite or rate. In other cases, a policyholder may want to consider temporarily lifting a credit freeze. If a freeze renders a consumer's credit report inaccessible, the insurer may rate the consumer as if they have neutral credit information or exclude the use of credit information as a factor. This means that a consumer who is up for renewal and has excellent credit may experience an increase in their rate. If you receive an adverse action notice based on the freeze, you should contact your agent or insurer.

Credit freeze versus fraud alert

According to the Federal Trade Commission, a credit freeze locks down your credit. A fraud alert allows creditors to obtain a copy of your report, as long as they take steps to verify your identity. Fraud alerts can stop someone from opening a new account in your name, but may not prevent them from misusing existing accounts.

There are three types of alerts:

- Initial Fraud Alert – protects your identity for 90 days from unverified access.
- Extended Fraud Alert – protects your credit identity for seven years, if you are a victim of identity theft.
- Active Duty Military Alert – protects deployed military for one year.

How to know if your information has been breached

You should check your credit report and look for any errors, new and unauthorized open accounts or any unauthorized charges on your credit cards. For the Equifax data breach, the company set up equifaxsecurity2017.com to help consumers find out if their information was compromised. You should check your credit report on an annual basis, but if you think your identity has been compromised, do so immediately.

What to do if your information is breached?

1. **Contact one of the three reporting credit agencies** – Equifax, TransUnion and Experian can investigate fraudulent activity on your credit report and remove it.

   Equifax Fraud Department
   1-800-525-6285

   Experian Fraud Department
   1-888-397-3742

   TransUnion Fraud Department
   1-800-680-7289

2. **Notify your lenders, banks, and insurance companies** - Alert them of the situation. Close your accounts, change any passwords and PINs associated with these accounts.

3. **File a police report** - Notify authorities of a potential identity theft. It provides documented proof that a crime occurred.

Periodically check your credit reports, especially during the first year after a breach to confirm there has been no additional fraudulent activity. Working with credit card companies to reverse fraudulent charges to your credit card will cut down on this type of fraud.

About the RI Insurance Division

The mission of the Rhode Island Insurance Division is to assist, educate and protect Rhode Islanders through the implementation and enforcement of state laws mandating regulation and licensing of the regulated industries while recognizing the need to foster a sound business environment in the state. We are also committed to treating everyone who comes before us fairly, efficiently and with respect. Please visit our website to obtain additional consumer information and alerts issued by the Rhode Island Insurance Division, or you may contact us at 401-462-9520 or email dbr.insurance@dbr.ri.gov for assistance.

A**bout the NAIC**

The National Association of Insurance Commissioners (NAIC) is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC staff supports these efforts and represents the collective views of state regulators domestically and internationally. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S. For unbiased consumer information and resources, visit insureUonline.org

Elizabeth Kelleher Dwyer
Superintendent of Insurance
December 27, 2017