



Congressman Gene Green 29th District of Texas

DC Office
2470 Rayburn HOB
Washington, DC 20515
(202) 225-1688 tel
(202) 225-9903 fax

District Offices
256 N. Sam Houston Pkwy, E.
Suite 29
Houston, TX 77060
(281) 999-5879 tel
(281) 999-5716 fax

11811 I-10 East
Suite 430
Houston, TX 77029
(713) 330-0761 tel
(713) 330-0807 fax

www.house.gov/green

What to do after the Equifax Data Breach

Sensitive data for 145.5 million Americans, including Social Security numbers and birthdates, have been obtained by hackers in the recent breach at Equifax. This leaves almost all adult Americans vulnerable to identity theft and other forms of fraud. Thieves may be able to use this information, coupled with information that can be found in online searches such as your mother's maiden name, high school mascot, address, etc. to answer knowledge-based authentication questions on your online accounts and change your password, granting them access to online accounts.

While Equifax has set up a website on which you can check whether your information was stolen, its reliability is unclear. The safest choice is to assume that you were impacted and take steps to protect yourself. It's important to note that, due to the volume of information stolen, there is a good chance you will not experience fraud or identity theft. However, resolving identity theft and fraud can be expensive and take a long time, so you may wish to act now to save yourself the headache later.

For some kinds of fraud, little can be done in advance to prevent it; rather, you should try to monitor your accounts and benefits (including Medicare, Medicaid, and Social Security) carefully to ensure that you catch it as soon as possible. This includes tax refund fraud and Social Security fraud.

For other kinds of fraud (such as a criminal accessing your personal brokerage or bank accounts, or taking out a mortgage, loan, or credit card in your name), you can take the below steps to decrease the likelihood of becoming a victim.

- 1) **Seniors should be on the alert for Social Security benefits fraud.** For those who are delaying drawing on their Social Security benefits, criminals could access your information and change the linked bank account or the address, and withdraw benefits in your name for years without your knowledge. If you are already receiving Social Security benefits, make sure that your payments arrive to you on schedule, and if you notice any missed payments, report it immediately.

The most important step that all seniors can take is to create a "My Social Security account" online on the Social Security Administration's website, if you have never done so. This will allow you an online portal to closely monitor your benefits activity so that you notice more quickly if there is something wrong. You should also keep all documentation that you receive from Social Security so that if you do end up having to prove your identity, you'll have documents to help support your claims.

- 2) **Get a free copy of your credit report, and verify that all the information on it is correct.** This can be done at annualcreditreport.com; you are legally entitled to one copy each once a year from the three largest credit bureaus (Equifax, Experian, and TransUnion). You should stagger your requests so that you can receive a free copy of it every four months. Look for names, addresses, phone numbers, and accounts that you do not recognize.
- 3) Consider **signing up for a free credit monitoring service.** While this won't help prevent identity theft or fraud, it may help you to notice and fix the problem more quickly. You should do this before freezing your credit (the next step), as you will not be able to sign up for monitoring if your credit is frozen. Equifax is offering all consumers free credit monitoring for a year, with a signup deadline of Jan. 31, 2018. Credit monitoring is a better bet than

fraud alerts, which are often ignored by companies issuing a store credit card or other credit product, and they need to be reset every 90 days.

- 4) Consider **freezing your credit** at all four of the major credit bureaus (TransUnion, Equifax, Experian, and Innovis, a smaller credit bureau). While **this is the most important step you can take to prevent a criminal opening up a new line of credit in your name**, it is not practical for everyone. A credit freeze blocks potential lenders from seeing your credit score, and thus prevents them from approving a loan or other line of credit. However, a freeze on your credit needs to be unfrozen in order to apply for a mortgage, credit card, retail credit card, or any other loan. Even some entities that do not issue credit require credit checks, such as cell phone companies (when switching plans or buying a new phone) and potential landlords. Freezing your credit, in other words, prevents you from instant approval if you're shopping and want to take advantage of a deal by signing up for that store's credit card, or if you want to rent a new apartment or change cellular plans, etc.

To unfreeze credit, you'll need to have the PIN given to you by each credit bureau at the time you froze it. **You should make sure you keep your PIN in a safe place if you decide to implement a freeze.** Credit can generally be unfrozen in 24 hours, but if you often take out new credit cards or if you expect to move or change phone plans soon, you may prefer to "lock" your credit. Locking your credit is less secure, and not guaranteed by law, but is easier to undo.

- 5) **Change your passwords and your security questions** to make them as secure as possible, and if your online financial accounts allow it, turn on multifactor authentication. You should try to avoid incorporating information that can easily be found online or through your social media accounts, such as the names of family members, date of birth, etc.
- 6) **Watch out for fraudulent e-mails**, particularly those that seem to be from financial institutions in connection with the breach. Would-be thieves know that in the wake of the breach, people will be more likely to open e-mails from banks or credit bureaus, and will take advantage to send fraudulent phishing e-mails. Do not download an attachment, press on a link, or call the phone number provided in a suspicious e-mail. Rather, look up the number directly and call the bank or credit card company that the e-mail purports to be from to verify the reason for the e-mail.
- 7) **Watch out for fraudulent phone calls.** Criminals sometimes do automatic dialing and calling, possibly even offering "protection" from identity theft and fraud. Do not trust caller ID, which can be manipulated, and do not give out sensitive personal information (such as your Social Security number or date of birth) over the phone when you receive calls to verify accounts.

It's important to note that Americans will have to maintain vigilance for fraud for years to come. Criminals that may have your data now may be more likely to act later, after victims have presumably let down their guard. For example, knowing that many are signing up for credit monitoring services, criminals may seize upon the expiration date of Equifax's free year of credit monitoring to send phony e-mails ostensibly from Equifax selling an extension of the service.