January 22, 2020 is the Deadline to Claim Equifax Data Breach Reimbursement

NATIONAL CENTER ON LAW & ELDER RIGHTS

PRACTICE TIP • December 2019

Odette Williamson, National Consumer Law Center

The Consumer Financial Protection Bureau (CFPB), the Federal Trade Commission (FTC), and state Attorneys General announced a settlement with Equifax regarding its 2017 data breach that exposed the personal information of 147 million people. The data breach exposed consumers' names, social security numbers, birth dates, addresses, and in some instances, driver's license numbers. **The final settlement includes a restitution fund of $425 million to help people affected by the data breach.**

Consumers affected by the data breach can receive up to 10 years of free credit monitoring; cash payment (capped at $20,000 per person) for expenses incurred as a result of the breach; assistance recovering from identity theft; and six free credit reports from Equifax. The credit reports are in addition to the one free credit report Equifax is required to provide consumers by law.

Learn more details and apply for reimbursement before the deadline of **January 22, 2020**.

Exposure of personal information through the Equifax data breach, or another data breach, puts consumers at risk for identity theft. An identity thief, for example, may use a consumer's name, address, social security number, and date of birth to open a credit account. Though the consumer is not responsible for charges to this account, resolving the issue can be time consuming. Recovering from identity theft involves closing fraudulent accounts, correcting credit reports and responding to other issues caused by the identity theft. To lessen the risk of identity theft or to respond to the theft, consumers can take several actions.

- A credit freeze or security freeze is the most effective measure a consumer can take to prevent identity theft. The freeze prevents creditors from accessing consumers' credit files or credit scores without authorization. This is especially critical if a scammer has the information necessary to apply for credit in the consumer's name. Consumers affected by the Equifax breach should freeze their credit files if they are concerned about identity theft. The consumer must place a credit freeze with each of the three credit reporting agencies. The credit freeze, however, does not prevent the thief from making charges to existing accounts.
- Consumers can request a fraud alert from one of the credit reporting companies. A fraud alert is a statement added to a consumer's credit report asking creditors to contact the consumer before issuing credit. Experian, Equifax, or TransUnion can place an alert on the record of an identity theft victim, and alert the other credit reporting companies to do the same. The initial fraud alert lasts 90 days and can be renewed. Extended fraud alerts work for seven years and require consumers to first file an identity theft report.
- Consumers can order copies of their credit report from the three companies and review them to make sure no additional fraudulent accounts have been opened or unauthorized charges made to existing accounts. The credit reporting companies are:
  - » EXPERIAN: 1-888-EXPERIAN (1-888-397-3742), TTY (1-800-972-0322)
  - » EQUIFAX: 1-800-685-1111
  - » TransUnion: 1-800-888-4213

- Victims of identity theft can contact companies where accounts have been opened fraudulently and ask that the accounts be closed or frozen. Identity thieves may open accounts with credit card companies, and to obtain cell phone, utility, or other services. Closure of fraudulent accounts should be confirmed in writing. Passwords and PINs for existing accounts should be changed.
- Consumers can also file a report with the FTC. The site allows consumers to create a personalized recovery plan that outlines steps to recover from identity theft. A report can also be filed with the local police or the police in the community where the identity theft took place. Consumers should consider other actions, such as contacting the Social Security Administration or IRS if a social security number was misused.

Please contact ConsultNCLER@acl.hhs.gov for free case consultation assistance. Sign up for our email list and access more resources at NCLER.acl.gov.