KEEP YOURSELF SAFE FROM DATA HACKS

DATA SECURITY, while always an important concern, has been highlighted recently in light of the Equifax data hack. On September 7, 2017, Equifax, one of the three major credit reporting bureaus, reported that the data of 143 million Americans was exposed in a cyber hack occurring as early as mid-May 2017. The data breach included Social Security numbers, home addresses, birthdates, credit card numbers and driver's license numbers. Here are some options to protect yourself and loved ones in the aftermath of the recent breach and in general:

ASSUME YOU WERE AFFECTED BY THE EQUIFAX HACK

With half of the U.S. population affected, it's safest to assume that your data was breached and respond accordingly. Equifax has set up a website that consumers can visit to determine whether their information was compromised as a result of the hack. Generally, don't ever assume that your data is safe - take whatever steps you can to protect your information.

ENROLL IN AN IDENTITY PROTECTION PROGRAM

Many third party companies offer identity theft protection services for a fee. In response to the recent hack, Equifax is offering its own program, TrustedID Premier, free for one year to anyone who wants to enroll (regardless of whether you were affected by the breach). However, some consumer groups have counseled regarding finding another credit bureau for identity theft protection over concerns of the level of security provided by TrustedID Premier, and a potential mandatory arbitration clause.

MONITOR YOUR CREDIT REPORTS

Each consumer is entitled to one free credit report per year. Check your credit report for new accounts you didn't open, debts you don't recognize, late payments and any other suspicious or unfamiliar activity. Pay particular attention to the time between May, 2017 and the present, since the hack could have affected individuals months ago. Continue to monitor your credit into the future as anyone affected will remain vulnerable to identity theft.

REPORT ANY SUSPICIOUS TRANSACTIONS

If you identify any suspicious or unfamiliar activity on your credit reports or in your bank or credit card accounts, immediately contact the company's fraud department, and the credit reporting agency from which you obtained the credit report. While you are not liable for fraudulent charges, you do need to report such activity within a certain time frame.

FREEZE YOUR CREDIT/PLACE A FRAUD ALERT

Freezing your credit will prevent anyone from opening new credit in your name. "Anyone" includes you, so when you freeze your credit you will receive a PIN number that you will later need to provide to unfreeze your credit whenever you need to open a new credit account. You can freeze your credit by contacting each of the credit bureaus: Equifax, Experian and TransUnion. If you have experienced any fraudulent activity, you can also place a fraud alert, which requires credit providers to verify your identity before opening an account. To place a fraud alert, contact one of the three credit bureaus, which will prompt the information to be shared with the other two bureaus. The fraud alert will be valid for 90 days, which can be renewed at that time.

PLAN TO FILE YOUR TAXES EARLY

Tax fraud is a common goal of identity thieves, who use stolen Social Security numbers to file fraudulent returns and receive refunds. When the legitimate taxpayer files taxes, the IRS informs the taxpayer that his or her return has already been filed. Plan to file your taxes early, both in 2018 and in future years, especially if you anticipate a refund, to avoid this outcome.

If you need assistance with any of the foregoing, contact a Couzens Lansky estate planning attorney.