



DON'T TAX YOURSELF

A Publication of Bowditch & Dewey's Estate, Financial & Tax Planning Group

Equifax Breach: What Can the Hackers Do with Your Information and How Can You Protect Yourself?

BY MATTHEW A. MORRIS • SEPTEMBER 22, 2017

The Equifax breach is not the biggest in terms of the number of people affected (the 2016 Yahoo breach compromised data associated with over 500 million user accounts compared to the 143 million people affected by the Equifax breach), but it is the worst in terms of the scope of personal identifying information that was hacked. The Equifax breach compromised full names, social security numbers, birth dates, addresses, and, in some cases, driver's license numbers. The Yahoo breach may have included names, email addresses, and passwords, but it did not include social security numbers or any other personal identifying information.

What can the hackers responsible for the Equifax breach do with the personal identifying information that they acquired? Sell the information to identity thieves, most likely in exchange for Bitcoin or other cryptocurrency via the dark web. What can identity thieves do with this information?

- Open and quickly max out new credit card accounts;
- File fraudulent U.S. and state income tax returns with new addresses (most likely P.O. boxes opened under a false name) claiming refunds of overpaid tax; and/or
- Use the information as part of a more comprehensive identify theft scheme (e.g. prepare fraudulent identification documents such as driver's licenses or even passports; fraudulently open new bank accounts in victims' names and arrange for wire transfers from victims' legitimately-opened bank accounts).

How can victims protect themselves? The first step might be to enroll in Equifax's credit monitoring service ("Trusted ID Premier") that Equifax is apparently offering as a free service to affected consumers. But affected customers will understandably be skeptical of the ability of this credit monitoring service when the company offering this service couldn't keep their information safe in the first place.

The better question may be what type of federal oversight is necessary to ensure that such a widespread data breach

never happens again without significant civil or even criminal penalties against the companies whose data was compromised. Massachusetts Attorney General Maura Healey [plans to sue Equifax](#) over a data breach that has threatened the personal information of nearly 3 million of the state's residents.