

WHERE DID YOUR STOLEN EQUIFAX INFORMATION GO?

Let's review. On September 7, 2017, Equifax, one of the three major credit monitoring services in the United States, reported they detected a major breach to their data on July 29, 2017. Their review showed hackers inside the Equifax system from May 2017 to July 29, 2017. At last report, Equifax acknowledged the files of 145 million people accessed and compromised. What was compromised? According to Equifax, "Most of the information accessed included names, social security numbers, birthdates, addresses, and in some instances, driver's license numbers." It's hard to over-state the magnitude of this affair. I discussed this in a previous column at length, but I want to reinforce that we should all be very, very concerned.

But what happened to all the hijacked personal data? That kind of personal information is a fantastic bonanza for identity thieves, but how do they convert 145 million stolen files into money? Do they stand on corners in seedy parts of major cities, whispering to passers-by, offering to sell a stolen file? Do they offer it up for sale on Craigslist?

Well, maybe. But far more likely, the next stop for stolen data like this is the dark web. What's that? The dark web is the term describing those sites on that part of the internet known as the darknet. The darknet is not indexed or searched by the familiar search engines. You won't use Google to look for something on the dark web. You can only access the dark web websites using special networks like TOR (The Onion Router) or I2P (Invisible Internet Project). What makes this "dark"? The software configurations used in these networks make it anonymous. The traditional, or "clearnet", assigns every computer, smartphone, or other internet-accessible device a return address, called an IP (Internet Protocol) address. Nothing like that happens on the darknets.

So, no surprise here, the dark web is a very popular place for criminals who want to sell illegal commodities or services. The dark web is not illegal, it's not illegal to use it, and not every site there is involved with crooks, but a lot of crooks hang out there. This is a black market where you can find stolen credit cards, bank accounts, health records, phony documents, stolen wallets, birth certificates, child pornography, illegal drugs, plus computer hacking tools, even passwords and usernames.

The dark web hosts sites selling stolen credit cards – the going rate is \$15 to \$50 each, price depending on how new the card is, or if it's a "platinum" card. Some sites allow thieves to place custom orders for specific card types, issuing banks, or even zip codes of the victims.

The dark web is where our stolen Equifax files will appear. We don't know when they will hit this market. The kind of information stolen is not very "perishable". If your credit card is compromised, you alert the card company when you discover it, and the card is cancelled. End

of story. That card is useless. But you can't call anyone to change your name, your address history, or easily change your social security number. That information will be the same in 2023 as it is now, so these thieves aren't facing a time crunch to market this stuff.

So knowing the capacity of the dark web to create ongoing mischief for those of us who lost our Equifax data, what's a body to do? I am noticing a definite shift in the recommendations of the consumer protection agencies in their advice. For years, they recommended placed a fraud alert on credit accounts for victims of identity theft, with advice, almost as an afterthought, to consider credit freezes. Since the announcement of the Equifax breach, this is just reversed. The recommendation is to strongly consider a credit freeze, and if you are unwilling to do that, to place a fraud alert on your account. I'd go with the credit freeze.

CONTACT SENIORS VS. CRIME

Let me know about scams, fraud, or other crookedness you run across. Most of what I learn, I learn from you. Contact me at Seniors vs. Crime, Clinton County Sheriff's Office, 563-242-9211 extension 4433, or email me at randymeier@gapa911.us