Crossing the Digital Divide (v80)

"Time for a Change"
By Joseph Feigon
For the Observer

You've heard Equifax was hacked, three times before they went public with the information? One of three big companies entrusted by the big banks to catalog, manipulate, and assign risk factors to how well you earn and manage money. Equifax is one of three credit management companies with access to your social security number, bank accounts, health accounts, and mortgage accounts. Equifax was hacked, and may still be vulnerable. There are no secrets on the Internet, and the gross negligence of Equifax reinforces that fact – there is no consequence when consumer privacy is compromised.

What do you do? Change your passwords…and prepare.

Identity theft impacts millions of consumers every year, and consumers over 50 can be particularly vulnerable. But there are a few key ways to protect yourself from becoming an identity theft victim and taking action if your identity is stolen.
There are really two types of identity theft: *account takeover* and *identity takeover*.

Two Types of Identity Theft

Account takeover is the most common and refers to the fraudulent use of an existing, open account. For example, a thief could hack your online banking login and then transfer funds out of your savings account into his own. Or a crook could steal your credit card number and then use your account information to make online purchases.

Identity takeover is the trickier form of fraud. It happens when a scammer opens new accounts in your name and without your knowledge. For example, someone could steal your Social Security Number and then apply for a credit card. Or someone could use your Social Security number at a doctor's office and never pay, leaving you on the hook when the bill arrives.

Although the data breach headlines are frightening, most identity theft victims suffer no financial loss. That's because there are strong legal protections that minimize liability. However, even you don't lose money after your identity has been stolen, the time and stress of dealing with the crime can be significant, especially for identity takeover. You might need to place a fraud alert with credit bureaus, order credit reports from all three credit reporting agencies and create an identity theft report. The Federal Trade Commission (FTC) has a 68-page guide explaining all the steps required.

Just creating the identity theft report requires submitting a complaint to the FTC and filing a police report. You'd then need to dispute errors with credit reporting agencies and contact the fraud departments of every business where an account was opened. The whole process could take months to resolve.

Steps to Prevent Identity Theft

Unfortunately, it's impossible to prevent identity theft completely because so much of your data is outside of your control. If you have a bank account, you're dependent on the bank's security protection. If you use a credit card in a restaurant, you're hoping the waiter doesn't skim it once he's out of your eyesight.

That said, here's what you *can* do to reduce the risk of identity theft from happening:

Avoid sharing your Social Security number, especially at hospitals and doctor's offices. Personal finance expert Clark Howard has very simple advice: "Do not give a doctor's office, hospital, lab or any medical facility your Social Security number on any form. Leave it blank."

Only use your home computer for online banking and make sure you have anti-virus protection for it. Even more importantly, avoid opening attachments from suspicious emails or clicking on links in emails that direct you to websites asking for personal information. Those links might lead you to download software that will enable the fraudster to spy on your computer and obtain your online banking passwords or other personal information stored on your computer.

Be very suspicious of phone calls supposedly from the Internal Revenue Service (IRS) or Microsoft. That's especially true when the caller starts demanding personal information or payment information. These are complete frauds. The IRS does *not* cold call customers and Microsoft does not call users to help update their computers. Just hang up.

Consider placing a credit freeze on your credit report with all three credit bureaus (Equifax, Experian and TransUnion). That's particularly worth considering if you don't plan to apply for any credit cards, mortgages or credit lines in the near future. A credit freeze restricts access to your credit report. That makes it more difficult for identity thieves to open new accounts in your name.

Be very careful when using your mobile phone. If you get a text message from a suspicious phone number, don't click on the link. And avoid downloading suspicious apps, especially if you find yourself redirected to the app store automatically.

Avoid using your mobile phone for banking when you're on public Wi-Fi networks. In general, you are much safer if you use cellular networks or your personal, password-protected Wi-Fi network.

Avoid sharing your Social Security number, login information or other financial details with family members and friends. Fraud often comes from people we know and (thought) we trusted. Keep your information to yourself to reduce the risk of being put into a compromising situation.

How to Detect Identity Theft

As a general rule, the quicker you spot identity theft, the easier it is to fix. If you learn you're a victim after one credit card or loan is opened in your name, that's relatively easy to fix. But if someone opens five or six accounts in your name, the resolution process will become much more difficult.

With credit monitoring, however, you'd know as soon as the first collection item is registered in your name. Fortunately, it is relatively easy to set up a strategy to monitor your credit report. At a minimum, you should check a report for free once a year at AnnualCreditReport.com.

Monitor the transactions on your accounts regularly (at least monthly) and report any suspicious transactions immediately. You might want to sign up for email or text message alerts so you receive notifications when suspicious transactions take place.

How to Resolve Identity Theft

Once you discover you've become an identity theft victim, take action immediately. If your ATM card is lost or stolen, you'll have a maximum loss of $50 if you report it within two business days after learning about the incident. Wait longer, but less than 60 days and you could be on the hook for $500. If you don't report the theft within 60 days, your losses won't be capped.

If your credit card is stolen or skimmed, just call your bank or card issuer and report it. Typically, you'll get a new card and all fraudulent charges will be forgiven.
If your identity is stolen and the thief starts opening new accounts in your name, visit IdentityTheft.gov, a free one-stop resource from the federal government. It will explain all the steps necessary to reach a resolution.
If you have an elderly parent who would be overwhelmed by the need to contact creditors, collection agencies, credit bureaus and local police departments, a good resolution service could be useful, if not a necessity. Many credit monitoring services include resolution services as part of the package.

Control those things you can, and keep the surprises to a minimum!