October 2017, Issue 90
mi.gov/ce

*Keeping Michigan consumers safe and informed.*

Attorney General Bill Schuette's

# CONSUMER **EDUCATION**

## YOU CAN'T AFFORD DATA BREACH FATIGUE

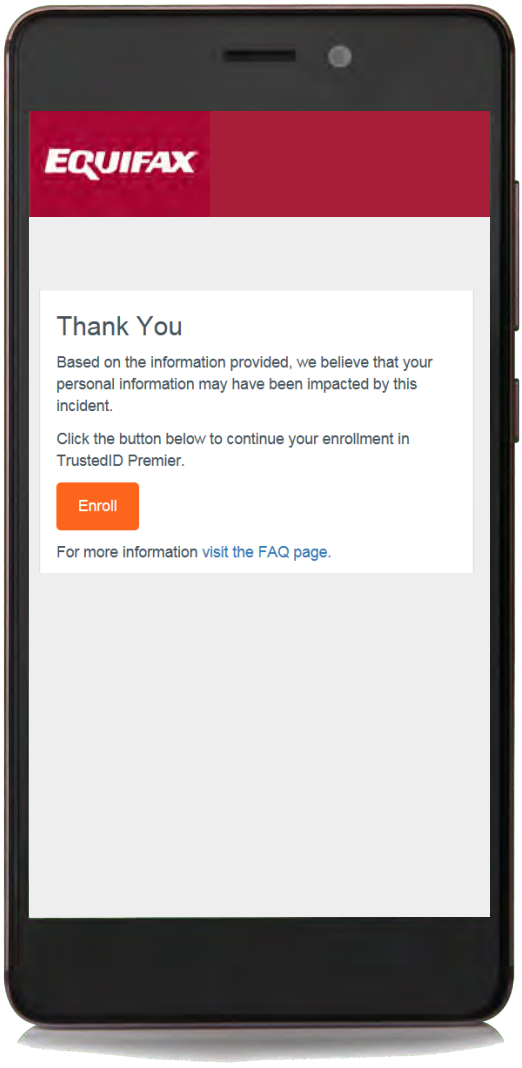
The number of data breaches and reported incidents of identity theft continues to set records nearly every year. According to the Identity Theft Resource Center's (ITRC) Mid-Year Review, more than 1,000 data breaches have been recorded as of September 13, 2017, resulting in the exposure of more than 163 million records. **That's almost four breaches and 636,000 records a day.**

And just as education efforts have raised awareness of scams, frauds, cyberattacks, and data breaches, another challenge has emerged: data breach fatigue. Data breach fatigue causes people to stop listening to breach information and advice. The result: consumers are less likely to take any action to protect their information—especially when they do not immediately experience any negative financial ramifications.

But you cannot afford to take a timeout now—especially since last month's news of the epic Equifax breach that impacted more than 143 million Americans, including more than 4.3 million Michigan citizens.

When breaches occur from hacking or unauthorized access, the stolen personal information is more likely to be used to commit identity theft. Thus, if your information was impacted, you need to take the threat seriously and take steps to prevent becoming an identity theft victim.

Still not convinced? **On average, there is one identity theft victim in the U.S. every two seconds.** And for Michigan consumers, the Federal Trade Commission reports that six of the top 15 cities for identity theft reports in 2016 were in Michigan—including the number one city: Ann Arbor.



## How worried should you be?

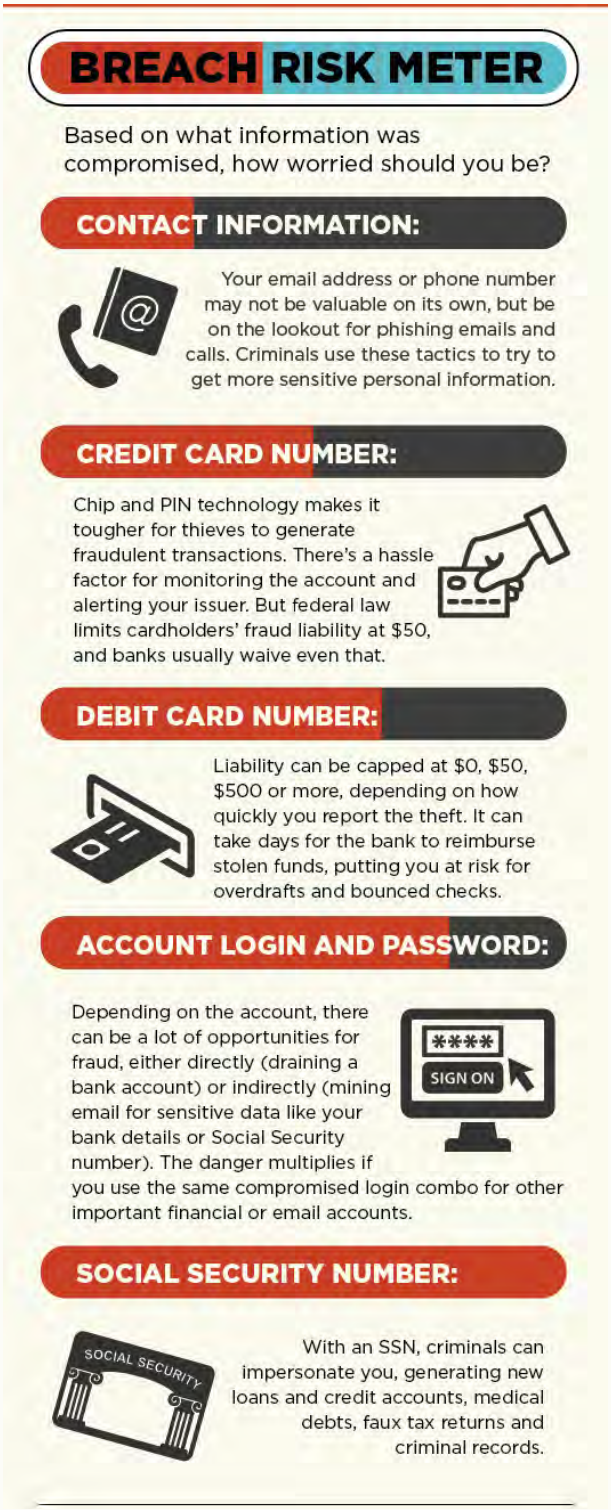
Quartz Media recently interviewed the Identity Theft Resource Center's president and chief executive, Eva Casey Velasquez, about the Equifax breach who cautioned, "'[t]he reality is this is one of the few situations where sitting back and taking a wait-and-see approach is really detrimental . . . and the steps that you can take [pull and read your credit report, put a fraud alert on your credit file; and seriously consider freezing your credit reports] are good steps regardless of whether . . . you have been affected.'"

Experts suggest that the most likely thing that will happen to your information after the data breach is that it will be misused in some manner and you will have to resolve that.

Best case scenario, you will suffer only minor distress and inconvenience and you will resolve it within weeks to a couple months.

Worst case, you ignore the breach, take no action, and you end up the victim of multiple identity-theft incidents that will take you years to clean up.

Even worse: the negative impact hits you at the same time you are trying to secure financing to buy a home, get a car loan, or student loans for college.




Risk breach meter from CNBC.com Reporting

## Nightmare Scenario

You become the victim of medical identity theft. This occurs when someone uses your personal information–your name, social security number, or health insurance ID–to get medical care, submit claims, or buy drugs or expensive medical equipment. Imagine if someone pretending to be you, uses your health insurance to get services. This can result in you getting improper care because the thief's medical information becomes mixed with yours.

If that is not bad enough, it can take more than a year to clear up medical identity theft, and the average cost to consumers: $22,346 per victim. Because of state and federal privacy rules and the way insurance works (operate today, bill and verify claim later), it is hard to track down.

Preventative measures include: safeguarding your social security number and medical insurance card; treat medical bills, prescription drug labels, and insurance statements like you would all sensitive personal information and shred them. Most important, read your Explanation of Benefits (EOB) statement from your medical insurance company and call if any claim or service looks unfamiliar.

For more information on the Equifax data breach and ways to protect your information, review the Attorney General's Consumer Alerts on the Equifax Data Breach and Credit Freeze; Fraud Alert; & Credit Monitoring.


Consumer Protection Division
P.O. Box 30213
Lansing, MI 48909
Phone: 517-373-1140
Toll-free: 877-765-8388
Fax: 517-241-3771
Online complaint form


**CONNECT WITH US:**


Department of Attorney General
P.O. Box 30213
Lansing, MI 48909
877-765-8388
Email (agcp@mi.gov)


**Bill Schuette**
**Attorney General**