What to do if your identity was stolen in mass identity breach

March 14 2019, by Kristen Jordan Shamus

Credit: CC0 Public Domain

News recently that a malware attack at Detroit-based Wolverine Solutions Group, which handles mailing and other services for hundreds of health care companies, potentially exposed the personal information

of hundreds of thousands of medical care patients, has many Michiganders concerned about whether their identities are at risk.

To find out what you need to know about the data breach, the Free Press interviewed Paige Hanson, chief of identity education at Norton LifeLock, an expert in cyber security, along with Wolverine Solutions Group President Darryl English, and people at various hospitals, insurance companies and health care plans.

More: Security breach grows: Hundreds of thousands of health care customers affected

More: Credit freeze: A misunderstood freebie that you actually want

Q: How will I know if my personal information is at risk?

A: Wolverine Solutions Group is in the process of mailing letters to all those who have been affected. Each letter is individualized and spells out the level of information that may have been exposed in the malware attack, English said.

The attack encrypted many of the company's records as part of an extortion scheme. Wolverine Solutions Group hired an outside team of forensic experts, who were able to determine which clients were affected and what data might have been compromised.

" ... Given the nature of the affected files, some of which contained individual patient information (names, addresses, dates of birth, Social Security numbers, insurance contract information and numbers, phone numbers, and medical information, including some highly sensitive medical information), out of an abundance of caution, we mailed letters to all impacted individuals recommending that they take immediate steps to protect themselves from any potential misuse of their information,"

Wolverine Solutions Group posted in a statement on its website.

Q: Which companies are involved?

A: A Beaumont Health spokesman acknowledged the personal data of 56,000 of its patients might have been compromised as part of the breach.

Covenant HealthCare said Friday that the data of 45,284 patients was potentially exposed.

At Health Alliance Plan, 120,344 customers' data may have been compromised; Blue Cross Blue Shield of Michigan reported 150,000; McLaren Health Care, 300,000; Three Rivers Health in southwestern Michigan, 8,200; North Ottawa Community Health System in Grand Haven, 15,000; and at least two hospitals in northwestern Pennsylvania: Warren General Hospital and the University of Pittsburgh Medical Center Kane.

Sparrow Health System refused to acknowledge whether any of its patients were included in the breach and directed anyone with questions to call Wolverine Solutions Group at 855-263-1282. But two Sparrow patients have contacted the Free Press to say they were among the patients whose data was exposed in the Wolverine malware attack.

Spectrum Health and Ascension did not respond to the Free Press' request for information about whether any of their patients were involved in the security breach.

Henry Ford Health System, the University of Michigan Health System, the Detroit Medical Center and its affiliated hospitals, and the St. Joseph Mercy Health System all reported that their patients were not impacted by the malware attack.

Wolverine Solutions Group would not disclose a full list of affected clients. English said that the true depth and scale of the security breach has yet to be fully revealed as the investigation is ongoing. The impact of the problem won't be completely known until April, he said.

Q: I got a letter saying my personal information may have been compromised. What should I do now?

A: "People should be extremely concerned when they hear of these large breaches that include name, address, Social Security number that can then be misused to create new lines of identity or fraudulently pose like they are them," Hanson said.

"The first thing they should do is establish what information has been breached because your plan of remediation or the steps you will take to recovery are going to be different depending on what pieces of personally identifying information have been compromised."

It's best to contact the three major credit reporting companies—Experian (P.O. Box 9532, Allen, TX 75013, 888-397-3742, www.experian.com), Equifax (P.O. Box 740241, Atlanta, Georgia 30374-0241, 800-685-1111, www.equifax.com), and TransUnion (P.O. Box 1000, Chester, PA 19022, 800-888-4213 www.transunion.com) - and put a credit freeze and a fraud alert on your account.

If, Hanson said, you discover online account information was compromised, immediately change your password and set up two-factor authentication, which requires two steps of identity verification to log into your account, Hanson said.

"If I knew my credit card was part of a breach, I would contact that credit card company and ask for a new card with a new number," she said.

It's also a good idea to sign up with a credit monitoring service, Hanson said.

Wolverine Solutions Group is offering free credit monitoring through AllClear ID for one year or two years, depending on the company involved, for those who were affected by the breach. To learn more about AllClear ID or to enroll, go to: allclearid.com or call 855-861-4034.

Q: Should I check my credit report?

A: Yes.

"You need to make sure you're checking your credit, and staying vigilant, keeping that guard up because fraudsters can do multiple things with your personal information," Hanson said. "One, they can sit on it, which is what happened with the Equifax breach back in September of 2017.

"Or maybe they do start to sell it. They can do account takeovers and do targeted attacks. They might text you something to try to get you to respond. They might do a phishing email to try to look like a legitimate organization. We have to keep our guard up."

Q: How do I get a free credit report?

A: Hanson recommends going to annualcreditreport.com to get a copy of your free credit report.

"It is federally mandated that every consumer get access to their credit report at no charge and that they will not sell your information to a third party," she said. "So those two things are very important. This company is not selling your information."

Q: What should I look for on my credit report to suggest there might be a problem?

A: First, make sure that you initiated all the lines of credit listed on your report, Hanson said.

Then, double check that all the mailing addresses, and names/aliases are places where you've lived at and names that you've gone by.

"Lastly, you want to look at the inquiries," Hanson said. "At the very bottom of the credit report, it will list soft inquiries and hard inquiries. Soft inquires don't actually have any impact on your credit. They are often from pre-approved credit card companies.

"Hard inquiries, on the other hand, happen when we go to open up a new line of credit. We always sign a release form that gives the lender the authority to review your credit. Hard inquiries can have a negative impact on your credit if you have too many in a row.

"Oftentimes, identity theft victims will find there's a number of hard inquiries they did not authorize and it's because someone is trying to open up new lines of credit. They might not have been successful, but when you look at your credit report, you don't recognize the vendors."

Q: What should I do if I see something suspicious on my credit report?

A: In the event any of these things happen, contact Equifax, Experian and TransUnion and dispute those line items on your credit report, Hanson said.

Q: Should I contact the police?

A: Yes.

"The biggest thing about identity theft is making sure that we report that we actually are a victim," Hanson said. "Even though you may have gotten it re-mediated right away for a particular account that has been opened, something might happen down the line that you need a little bit more proof that you're a victim of identity theft.

"By reporting it to law enforcement, it's one more step to adding to the credibility of your claim, and hopefully, whatever lender is working with them and disputing that claim, then they will be able to reverse it more easily."

In addition to reporting the fraud to police, Hanson also recommends going through the Federal Trade Commission.

"They have an identity theft affidavit form," she said, "which is a really user-friendly way to report your identity theft, and it also ... will come up with recovery plan with step-by-step instructions on what to do to re-mediate your particular form of identity theft or fraud."

To see the FTC identity theft affidavit form online, go to: identitytheft.gov/

Q: My child's information was compromised in a data breach. Do I have to worry about my child's identity?

A: Yes.

"If you have a 7-year-old, you're not likely to be checking the credit of that child or using credit until they get their first job or buy their first car or go to college or something like that," Hanson said. "That is very appealing to an identity thief.

"What we recommend for parents or guardians to do is to go to

annualcreditreport.com and check the child's credit as well."

You should then place a fraud alert on the child's credit, which lasts one year, Hanson said. But she also suggested taking one more step: Freeze your child's credit.

"That would stop credit-based identity theft," Hanson said. "The freeze will last until you lift it. In the event that he wants to open up a line of credit when it is time, then you would contact the credit bureaus and lift the freeze.

"Unfortunately, that does only stop credit-based identity theft. Sadly, there's nothing stopping someone from getting a driver's license, a job, from misusing medical information using your child's identity."

Q: For how long do I need to monitor this stuff?

A: Once your personal information has been compromised, you ought to be vigilant for the rest of your life.

"It truly is lifelong monitoring or at least keeping it in top of mind versus putting your guard down," Hanson said.

Q: The company says the data that was compromised was encrypted. Does that mean I don't have to worry as much?

A: No, said Hanson.

"Depending on the level of encryption, there are ways to un-encrypt it, she said. "We still need to be aware that the information and the personally identifying information could be out there. It really just depends on the skill set of whoever stole the information."

Q: Wolverine Solutions Group is offering free credit monitoring through AllClear ID. Should I sign up for that?

A: Hanson recommends signing up for the free credit monitoring being offered by Wolverine Solutions Group.

"But just note that fraudsters know that if you have been offered one year free of something, the chances and likelihood of you enrolling in and paying for a service go down tremendously," she said. "So they will wait that one year, and then misuse the information."

Q: How can I protect from identity theft in the future?

A: Try to be more personally aware about the kind of information you may be giving out going forward. Limit personal information you allow to be collected by apps, personal computers, internet networks, phones and devices, Hanson said.

Don't volunteer your Social Security number and other key information. If someone asks for it, challenge them about why they need it.

And, said Hanson, don't ignore the problem.

"Ignoring it could end up costing you a lot of time and effort and headaches down the road," she said. "Identity thieves might not necessarily be doing anything with your information now, but down the road, they might.

"If you would have just put a fraud alert, a credit freeze or enrolled in a service like LifeLock you could have been notified way before the collection agency was calling or sending you letters and now your credit is in the 500s. It would definitely save you headaches down the road by taking a couple of small steps now."

Q: I still have questions. How do I find out more about what happened at Wolverine Solutions Group?

A: The company has posted to its website answers to some frequently asked questions. To learn more, go to: wolverinemail.com