CYBERSECURITY AND DATA PRIVACY

SO…EVERYONE'S BEEN COMPROMISED? WHAT TO DO IN THE WAKE OF THE EQUIFAX BREACH.

by Justin L. Root and Sara H. Jodka

By now, you've probably heard that over 143 million records containing highly sensitive personal information have been compromised in the Equifax data breach. With numbers exceeding 40% of the population of the United States at risk, chances are good that you or someone you know—or more precisely, *many* people you know—will be affected. But until you know for certain, you are probably wondering what to do until you find out.

To be sure, there has been a lot of confusion. Many feel there was an unreasonable delay in reporting the breach. And now that it has been reported, some have suggested that people who sign up with the Equifax website to determine if they were in the breach might be bound to an arbitration clause and thereby waive their right to file suit if necessary later (although Equifax has since said that is not the case). Others have reported that the "personal identification number" (PIN) provided by Equifax for those who do register with the site is nothing more than a date and time stamp, which could be subject to a brute-force attack, which is not necessarily reassuring when dealing with personal information. Still others have reported that the site itself is subject to vulnerabilities such as cross-site scripting (XSS), which could give hackers another mechanism to steal personal information. And some have even questioned the validity of the responses provided by Equifax when people query to see if they might have been impacted.

In all the chaos, it's hard to know how to best proceed. Fortunately, you have options other than using Equifax's website.

1. Place a Credit Freeze

Know that if you are a victim of the breach, you *will* be notified by Equifax eventually. In the meantime, consider placing a credit freeze on your accounts with the three major credit reporting bureaus. All three major credit reporting bureaus allow consumers to freeze their credit reports for a small fee, and you will need to place a freeze with each credit bureau. If you are the victim of identity fraud, or if your state's law mandates, a credit freeze can be implemented without charge. In some states, you may incur a small fee. Lists of fees for residents of various states can be found at the TransUnion, Experian, and Equifax websites. Placing a freeze on your credit reports will restrict access to your information and make it more difficult for identity thieves to open accounts in your name. This will not affect your credit score but there may be a second fee associated with lifting a credit freeze, so it is important to research your options before proceeding. Also, know that you will likely face a delay period before a freeze can be lifted, so spur-of-the-moment credit opportunities might suffer.

Here is information for freezing your credit with each credit bureau:

Equifax Credit Freeze

- You may do a credit freeze online or by certified mail (return receipt requested) to:
  Equifax Security Freeze
  P.O. Box 105788
  Atlanta, GA. 30348

- To unfreeze, you must do a temporary thaw by regular mail, online or by calling 1-800-685-1111 (for New York residents call 1-800-349-9960).

Experian Credit Freeze

- You may do a credit freeze online, by calling 1-888-EXPERIAN (1-888-397-3742) or by certified mail (return receipt requested) to:
  Experian
  P.O. Box 9554
  Allen, TX. 75013

- To unfreeze, you must do a temporary thaw online or by calling 1-888-397-3742.

Transunion Credit Freeze

- You may do a credit freeze online, by phone (1-888-909-8872) or by certified mail (return receipt requested) to:
  TransUnion LLC
  P.O. Box 2000
  Chester, PA 19016

- To unfreeze, you must do a temporary thaw online or by calling 1-888-909-8872.

After you complete a freeze, make sure you have a pen and paper handy because you will be given a PIN code to keep in a safe place.

2. Obtain a Free Copy of Your Credit Report

Consider setting up a schedule to obtain a copy of your free annual credit report from each of the reporting bureaus on a staggered basis. By obtaining and reviewing a report from one of the credit reporting bureaus every three or four months, you can better position yourself to respond to unusual or fraudulent activity more frequently. Admittedly, there is a chance that one of the reporting bureaus might miss an account that is reported by the other two but the benefit offsets the risk.

3. Notify Law Enforcement and Obtain a Police Report

If you find you are the victim of identity fraud (that is, actual fraudulent activity—not just being a member of the class of affected persons),

notify your local law enforcement agency to file a police report. Having a police report will help you to challenge fraudulent activity, will provide you with verification of the fraud to provide to credit companies' fraud investigators, and will be beneficial if future fraud occurs. To that end, be aware that additional fraud may arise closer to the federal tax filing deadline and having a police report already on file can help you resolve identity fraud problems with the Internal Revenue Service if false tax returns are filed under your identity.

4. Obtain an IRS IP PIN

Given the nature of the information involved in the breach, an additional option for individuals residing in Florida, Georgia, and Washington D.C. is to obtain an IRS IP PIN, which is a 6-digit number assigned to eligible taxpayers to help prevent the misuse of Social Security numbers in federal tax filings. An IP PIN helps the IRS verify a taxpayer's identity and accept their electronic or paper tax return. When a taxpayer has an IP PIN, it prevents someone else from filing a tax return with the taxpayer's SSN.

If a return is e-filed with a taxpayer's SSN and an incorrect or missing IP PIN, the IRS's system will reject it until the taxpayer submits it with the correct IP PIN or the taxpayer files on paper. If the same conditions occur on a paper filed return, the IRS will delay its processing and any refund the taxpayer may be due for the taxpayer's protection while the IRS determines if it is truly the taxpayer's.

Information regarding eligibility for an IRS IP PIN and instructions is available here and to access the IRS's FAQs on the issue, please go here.

CONCLUSION

Clearly, the Equifax breach raises many issues about which many individuals need to be concerned—and the pathway forward is uncertain at the moment. But by being proactive, being cautious, and taking appropriate remedial measures available to everyone, you can better position yourself to avoid fraud, protect your rights, and mitigate future fraud that might arise.

If you have questions or concerns about protecting your or your clients' personally identifiable information; questions about identity theft or fraud; or need guidance regarding data privacy and cybersecurity in general, the Dickinson Wright Data Privacy and Cybersecurity attorneys invite you to contact us for additional information.

This client alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of Cybersecurity and Data Privacy law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Justin L. Root is Of Counsel in Dickinson Wright's Columbus office. He can be reached at 614.591.5465 or jroot@dickinsonwright.com.

Sara H. Jodka is Of Counsel in Dickinson Wright's Columbus office. She can be reached at 614.744.2943 or sjodka@dickinsonwright.com.