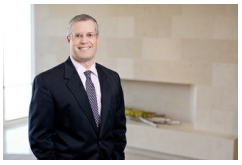
Key Contacts

Steve Bunnell
Washington, DC
D: +1-202-383-5399



Randall W. Edwards
San Francisco
D: +1-415-984-8716

Related Practices

Data Security & Privacy

PDF

Best Practices: Managing Impacts of the Theft of Personal Information

September 19, 2017

Over the past several years, numerous major data breaches have resulted in the theft of personally identifiable information (PII) affecting millions of people. By some estimates, most adults in the United States have been affected by at least one of these breaches.[1] For example, Equifax Inc. announced a cybersecurity breach on September 7, 2017, that potentially impacted over 140 million US consumers. In its public statement, Equifax explained that customer data including names, social security numbers, birth dates, addresses, driver's license numbers, and credit card numbers were accessed by an unknown intruder. There are several steps that can help minimize, although not eliminate, the risk from stolen PII. This document summarizes several proactive steps and other options that regulators and security experts have encouraged individuals to consider when deciding how best to protect themselves.

5 Options to Manage Personal Risk

1. Sign up for credit monitoring
Description: Credit monitoring services send an alert, usually via email or a mobile application, when anyone accesses your credit file for any purpose. Major credit bureaus and third-party companies offer this service for a recurring fee.

Considerations

- **Increased Awareness**: Monitoring allows an individual to have more awareness of when their credit may be at risk.
- **More Control**: An individual will be able to access their own credit file

and constantly monitor any potential transactions.

- **Limited Effectiveness**: Although an individual can monitor their credit more easily, such monitoring may provide a false sense of security as this option does not actively prevent identity theft. For example, any notification may occur after your credit has been used for an unauthorized purpose.
- **Active Engagement Necessary**: Monitoring requires involvement from an individual to take action if they are notified of a suspicious transaction. This may be a nuisance for certain individuals.
- **Cost**: Credit monitoring services are sold by the three credit bureaus (Experian, TransUnion, and Equifax) or third-party companies for a recurring monthly fee, ranging from $10/month to $30/month. Additionally, several companies provide free credit monitoring services in exchange for permission to send the customer targeted advertisements. Some companies impacted by a data breach will offer their customers free monitoring services.[2]

2. Place a credit fraud alert on your credit file

Description: A credit fraud alert requires potential creditors to verify your identity, generally by telephone, before opening a new account, issuing a credit card, or taking other actions requiring a credit check. You can open an “initial credit alert” by notifying any of the three major credit bureaus. The notified bureau must ensure that the alert is applied by the other two bureaus. An “initial credit alert” is valid for 90 days and can be renewed every 90 days through an additional request to any of the three credit bureaus. You can alternatively apply for an “extended fraud alert,” which remains in place for seven years but requires proof of identity theft. An extended fraud alert requires submission of an Identity Theft Report to the FTC at www.IdentityTheft.gov.

Considerations

- **Limits Risk of Identity Theft**: Fraud alerts make it harder for cyber criminals to use your information for unauthorized purposes.
- **Retain Control Over Your Credit**: Allows you to use your own credit file to open new accounts, apply for loans, and other purposes with minimal hassle.
- **Minimal Burden**: Easier administratively as you only have to go to one bureau, and it is extended to the other two automatically, but must be manually renewed every 90 days to remain in place, unless an extended fraud alert is in place.
- **Only Applies to Unauthorized Attempts To Open New Accounts**: Does not protect against unauthorized use of current accounts.

3. Freeze your credit

Description: A security freeze prevents creditors from accessing your credit file and provides protection against unauthorized use of your identity. You must request a credit freeze from each of the three major credit bureaus individually; a request to one bureau will not be automatically implemented by the other bureaus.

Considerations

- **Proactive Defense**: Prevents new creditors from accessing your credit file and opening accounts in your name.
- **Only Prevents Unauthorized Attempts to Open New Accounts**: Does not prevent unauthorized use of active accounts, such as credit cards.
- **Limits Use of Your Own Credit**: Generally prevents you from accessing your own credit file or applying for new credit, including a loan or credit card, as long as the freeze is in place. Certain credit bureaus may provide a unique personal identity number (PIN) allowing you to lift the credit freeze for specific transactions.
- **Higher Burden**: A credit freeze must be requested from each of the three bureaus individually.

4. Proactively identify whether your data is being sold
Description: Cyber criminals often sell stolen personally identifiable information on the “dark web,” a constantly changing array of websites only accessible by a specialized Internet browser. Several companies offer a service to scan these illicit sites and provide an alert if your information is being sold on the “dark web.” Upon receiving an alert, a customer must then take additional action such as requesting a credit freeze from each of the three major credit bureaus.

Considerations

- **Increased Awareness**: Allows you to actively understand and manage your risk of identity theft and unauthorized account access.
- **Retain Control Over Your Credit**: Does not impact your ability to access your own credit.
- **Does Not Itself Protect Against Identity Theft**: Requires additional action, such as a credit freeze, to prevent unauthorized use of your credit after receiving an alert.
- **May Not Provide Certainty**: “Dark web” sites are constantly changing, so scanning services cannot provide absolute assurance whether your data is being sold.

5. Consider filing your taxes as early as possible
Description: Cyber criminals have also used information stolen from data breaches to file fraudulent tax returns in which the Federal or state refund is sent to the criminal rather than the legitimate taxpayer. This risk can be mitigated by filing taxes early and therefore reducing the time window in which criminals can file a fraudulent return.

Considerations

- **Prevents Tax Fraud**: Eliminates one particular risk resulting from a major data breach.
- **Potentially High Burden**: Filing early may be inconvenient or infeasible for some taxpayers.

Additional Resources:

The Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and several state attorneys general provide information about preventing identify theft and have established websites with updates about the Equifax data breach. These resources can be accessed at:

- FTC
- CFPB
- New York Attorney General
- California Attorney General

As noted above, individuals must contact any of the three major credit bureaus to initiate a fraud alert and each of the three major credit bureaus individually to execute a credit freeze. The credit bureaus can be contacted at:

- Experian
  - www.experian.com/fraudalert
  - 1-888-397-3742
- TransUnion
  - www.TransUnion.com/fraud
  - 1-800-680-7289
- Equifax
  - www.equifax.com/CreditReportAssistance
  - 1-888-766-0008

---

[1] In January 2017, the Pew Research Center concluded that nearly two-thirds of all Americans have been immediately impacted by a data breach. Pew Research Center, Americans and Cybersecurity, (2017) www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

[2] The Federal Trade Commission recommends that individuals potentially affected by the Equifax data breach access a website established by the company to verify whether their information was compromised. Upon verifying that a given individual was impacted by the breach, Equifax is offering one year of free credit monitoring. Equifax originally made this offer contingent on acceptance of a binding arbitration clause; however, the company has subsequently removed this requirement and “will not apply any arbitration clause or class action waiver against consumers for claims related to” the data breach. This Equifax website can be accessed at: www.equifaxsecurity2017.com/enroll/.

This memorandum is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, may not be relied upon as legal advice, and does not purport to represent the views of our clients or the Firm. Steve Bunnell, an O'Melveny partner licensed to practice law in the District of Columbia, Ron Cheng, an O'Melveny partner licensed to practice law in California, Danielle Gray, an O'Melveny partnerl licensed

to practice law in New York, Randall Edwards, an O'Melveny partner licensed to practice law in California, and Kiran Raj, an O'Melveny partner licensed to practice law in the District of Columbia and Georgia, contributed to the content of this newsletter. The views expressed in this newsletter are the views of the authors except as otherwise noted.

Portions of this communication may contain attorney advertising. Prior results do not guarantee a similar outcome. Please direct all inquiries regarding New York's Rules of Professional Conduct to O'Melveny & Myers LLP, Times Square Tower, 7 Times Square, New York, NY, 10036, Phone:+1 212 326 2000. © 2017 O'Melveny & Myers LLP. All Rights Reserved.

Attorney Advertising © 2019 O'Melveny & Myers LLP. All Rights Reserved.