# *Client Alert*: Equifax Data Breach: Another Reminder to be Proactive in Protecting Your Business

**Related Attorneys**

John L. Landolfi

Natalia Steele

**Related Services**

Data Strategy, Privacy and Security

**CLIENT ALERT** | 9.12.2017

Some may say that it was only a matter of time. On September 7, 2017 Equifax, one of the country's three main credit reporting agencies, reported that it has been hacked. It appears that the breach took place from mid-May through July, during which the hackers accessed names, Social Security numbers, personal ID numbers, birth dates, addresses, and, in some cases, driver's license numbers and credit card numbers. This breach affects at least 143 million U.S. consumers.

Although not every breach results in misuse of all records potentially exposed, the Equifax breach is yet another reminder that no matter how sophisticated a business may be, taking steps to minimize data breach risks is key to ensuring a business' ability to avoid and survive an attack.

## Steps for businesses to take to avoid the Equifax fate

The weeks and months ahead should provide some clarification on how the thieves wormed their way into Equifax's systems. Lack of or lax adherence to company policies concerning password security and treatment of suspicious emails are among the top two causes of data breaches.

Thus, for a business aiming to avoid becoming the next Equifax, the following considerations are of critical importance:

1. **Create and securely store strong passwords**
   Data breaches often are a result of weak or lost passwords – a vulnerability that opportunistic hackers are happy to exploit. A solution is to use complex passwords and do not allow sharing of passwords. Consider whether using software that provides strong password generation and storage services, such as LastPass, KeePass, Dashlane would be appropriate for your business. Of course, even these services are not immune to hacking.
2. **Foster end user security awareness/vigilance about phishing emails**
   End user security awareness training creates tangible benefits but

only when it is done frequently and when it actually changes the culture of the company to be more security minded. Training employees helps eliminate mistakes that could lead to a breach, as well as helps them notice odd behavior by malicious insiders or fraudsters. Employees must be trained to be vigilant about unsolicited emails that request them to enter passwords, provide personal information, or click on various links or download attachments.

3. **Monitor insider behavior/establish employee exit strategies**
   Data loss prevention technologies where you can set rules and, based on those rules, block content that you do not want to leave the network and to replay insider online behavior is invaluable in day-to-day data breach prevention. When employees depart your company, managing their exit should include changing passwords, ensuring that computers and personal devices no longer have sensitive information available on them, and developing contracts that include legal repercussion for sharing or utilizing sensitive data after termination of employment.
4. **Create clear procedures for use of personal electronic devices, remote network access, and on- and off-site data storage**
   The same standards for data security must be applied to all of your personnel, regardless of location. Provide mobile workers with straightforward policies and procedures, ensure that security and authentication software is installed on mobile devices are kept up-to-date, and provide adequate training and technical support for mobile workers.
5. **Routinely evaluate and update of software and network security/deploy intrusion detection and download monitoring**
   Applying patches takes time and resources, thus allocations and expectations should be addressed upfront, keeping in mind the organization's risk assessment. Intrusion detection and prevention should be used for all systems that are accessible via the internet, such as web servers, email systems, servers that house customer or employee data. Also block or limit insider access to potentially malicious or compromised web sites that can exploit your machines when visited.
6. **Minimize, purge data**
   Reduce the number of employees that have access to at-risk information. Do not collect or store information that is not relevant to your business. Only grant data access on an as-needed basis, and revoke access as soon as information is no longer necessary.
7. **Actively manage outside vendors**
   Define your security requirements upfront with vendors—third-party service providers may be required to maintain appropriate security measures in compliance with certain state and federal regulations. Ensure that your organization maintains control of data at all times, especially with offshore data storage or services.
8. **Regularly update risk assessments and conduct audits of company policies, and compliance**
   Routine audits of processes, policies, and compliance is necessary to allow for new risks to be addressed, policies to be modified, and dangerous behaviors corrected before issues crop up.
9. **Establish and practice disaster management plans**
   Establish disaster management plans and breach protocols that would guide the organization's actions should a breach occur. Being prepared allows the entire team to have a full understanding of their jobs in order to prevent the breach from growing or causing an unnecessary customer backlash. Preparations for managing a data breach must include putting breach protocol to the test with a mock breach/tabletop exercise to evaluate how well your team is prepared for a potential breach and

troubleshoot problems with your protocol before potential becomes a reality.

For questions on cybersecurity programs, breach response, tabletop exercises, breach preparedness or planning, please contact John Landolfi, Natalia Steele or your Vorys attorney.