Frankfurt Kurnit Klein + Selz PC

Focus on the Data

Unique Insights and Practical Guidance on Privacy and Data Security Issues Worldwide

Latest on the FTC Data Security Front

By Tanya Forsheit & Daniel Goldberg on December 29, 2016

On October 25, 2016, the Federal Trade Commission (FTC) issued a guide — **Data Breach Response: A Guide for Business** — on steps companies should take in responding to a data breach. This latest regulatory guidance at the federal level is only the most recent in a long list of resources with which companies that deal in data (yes, that means every company) are expected to acquaint themselves for purposes of their incident response preparedness efforts. Those resources include, but are not limited to, the 47 state breach notification laws (constantly subject to amendment) and related State Attorney General guidance, the Health Insurance Portability and Accountability Act (HIPAA), and FTC consent decrees entered into with organizations that have been the victims of a data security breach and with respect to which the FTC has brought an enforcement action under its Section 5 authority.

A few weeks later, on November 10, 2016, the Eleventh Circuit Court of Appeals issued an order in the long-running and much-watched LabMD data security breach matter staying the FTC's order in that case and, in so doing, questioning the reasonableness of the FTC's interpretation of the unfairness standard under Section 5 pursuant to which it takes enforcement action for allegedly deficient data security practices.

Below we lay out some key takeaways from the FTC's new data breach guide and explain what really happened at the Eleventh Circuit (not exactly what the media reported). The following must be prefaced with a significant disclaimer — the recent Presidential election is likely to have an impact on the FTC's current approach to data security enforcement and it is far too early to gaze into our crystal balls on that front.

With that, a few takeaways:

The Historical Pattern is One of Continued and Increasingly Aggressive FTC Enforcement of Data Security Practices

The data breach guide is the latest signal from the FTC that it means business about data security. To date, the FTC has brought over 60 enforcement actions against companies under Section 5 of the FTC Act for what it alleges are unfair or deceptive data security acts or practices. The data breach guide also follows two recent guides from the FTC on **how to protect personal information** and **how to keep data secure**, as well as **statements** by FTC Chairwoman Edith Ramirez strongly suggesting that failure by companies to address system vulnerabilities could lead to FTC enforcement. For the most part, in the past, the FTC has pointed to consent decrees reached with alleged violators in order to educate companies about expected practices related to data security. The data breach guide, along with the FTC's other recent guides and statements, gives the FTC additional footing to argue that companies are or should be on notice as to the FTC's expectations. That being said, some **organizations** and **senators** continue to challenge the FTC's enforcement authority, and the Donald Trump Administration may mean a dialing back of the FTC's aggressive pursuit of organizations, large and small, that it views as having deficient security practices. Nonetheless, companies should assume for now that the FTC, as well as State Attorneys General, will continue to bring enforcement actions. As such, organizations should endeavor to incorporate the FTC's guidance and **State Attorney General guidance** as to what constitutes "reasonable security" into their own internal data security practices and policies.

If A Breach is Suspected or Occurs, Secure, Fix and, Possibly, Notify

The data breach guide outlines expected response measures in three parts — securing operations, fixing vulnerabilities, and notifying appropriate parties.

Setting aside the data breach guide, even just as a matter of best practice, securing operations in the wake of a breach should be priority number one. Upon discovering a suspected or actual breach, companies should secure both physical areas and potentially affected networks. For example, companies should, depending on the circumstances, consider changing lock and access codes, taking affected equipment offline, resetting user credentials and passwords, and interviewing anyone (internal and external) who might have relevant information. The FTC recommends that companies assemble a team of experts to assist with this process, which may include forensic investigators, legal counsel, and other specialists. All this being said, it is critical that organizations not jump the gun and delete log files or other critical evidence that might help determine the existence, breadth and scope of a breach, or even help establish that no breach actually occurred. As such, the FTC correctly stresses that companies must not destroy any forensic evidence during this process — for instance, taking affected equipment offline before a forensic investigator arrives could constitute a destruction.

Fixing vulnerabilities focuses on preventing additional data loss, i.e., containing the incident. Companies should work with forensic investigators to evaluate their encryption methods, network segmentation plans, backup and preserved data, and access restrictions. Where data breaches involve service providers, companies must ensure that those service providers take necessary steps to help ensure another similar incident does not occur. The FTC highlights that companies should implement any recommended remedial measures as soon as possible, and verify that their service providers have actually fixed internal vulnerabilities. In addition (while not clear as to why it falls under the topic of “fixing vulnerabilities”), the FTC also specifies that companies should have a comprehensive plan to address questions related to the breach, and provide clearly written questions and answers on their websites.

The third measure, notifying appropriate parties, requires companies to review applicable data breach laws and determine whether those laws require notification of the applicable state (and possibly federal under HIPAA) regulators, individuals whose information has been compromised, business partners or vendors affected by the breach, law enforcement, credit card companies and/or banks if the breach involves credit card or bank numbers, and credit bureaus. The FTC recommends that companies

consult with law enforcement prior to notifying affected individuals, designate a point person with the company regarding the breach, and offer at least one year of free credit monitoring or other support if the breach involves financial information or Social Security numbers. This echoes the long-time recommendations of many State Attorneys General.

Notice Content Should Reflect State Law Requirements (Plus a Little Bit More)

The data breach guide sets out what must be disclosed to affected individuals in situations where notice is required. Unless the applicable state law provides otherwise, companies should describe how the breach happened, what information was taken, how the thieves used the information (if thieves are involved), what actions have been taken by the company to remedy the situation, what actions have been taken by the company to protect the affected individuals, and how to reach the relevant contact at the company. The FTC provides a model letter for notification on **page 10**— that letter might look familiar as it essentially mirrors the model letter under **California law**. However, the FTC model letter includes several minor additions, including describing how the company will contact consumers in the future, providing information about the law enforcement agency working on the case (if the law enforcement agency agrees), and enclosing/linking to the FTC's **Identity Theft: A Recovery Plan** and identity theft **website**.

The Eleventh Circuit Cast Doubt on the FTC's Interpretation of its Unfairness Authority Under Section 5 in Data Security Matters, But Did Not Revise the Unfairness Standard

The Eleventh Circuit's November 10, 2016 order in the LabMD case did not, contrary to some headlines, "narrow" the FTC's unfairness standard in data security cases. The decision was a procedural one. The Court found, in the context of determining whether a stay was appropriate, that LabMD made a substantial case on the merits and presented a serious legal question by making a showing that the FTC's interpretation of Section 5 "may" not be reasonable because "it is not clear that" a reasonable interpretation of Section 5 includes intangible harms or that the FTC reasonably interpreted "likely to cause" since it found that phrase to mean "significant risk" instead of "probable". The Eleventh Circuit's ruling is not on the merits. That being said, it is significant that at least one appellate court has questioned the FTC's confidence in asserting its Section 5 unfairness authority in cases where harm is merely speculative.

We have certainly not seen the last of this saga — either in the LabMD case itself or more broadly with respect to the FTC's unfairness authority and future plans for data security enforcement. We will keep you posted during the Trump years and beyond.

Focus on the Data

Klein+Selz