Cooley

FTC Issues Business Guide for Responding to Data Breaches

November 1, 2016

The Federal Trade Commission ("FTC") has released a 16-page guide on steps that businesses should take once a data breach has occurred. The FTC's guidance addresses three primary areas: securing operations, fixing vulnerabilities, and notifying appropriate parties.

Securing operations

Companies should move quickly to secure their systems to prevent additional breaches. The FTC makes the following recommendations:

- Assemble a team of experts that, depending on the size and nature of the company, may include hiring an independent forensic team to determine the source and scope of the breach, and hiring outside legal counsel with privacy and data security expertise.
- Secure physical areas related to the breach, including changing access codes.
- Stop additional data losses by taking all affected equipment offline immediately and update credentials.
- Remove any personal information that may have been posted on your website, and contact search engines that may have stored or cached the information.
- Interview those who discovered the breach, document the investigation, and preserve forensic evidence.

Fixing vulnerabilities

The FTC outlines a number of steps to help prevent further data loss, including:

- Consider whether service providers with access to your network need to have their access privileges changed and confirm whether they have remedied any vulnerabilities.
- Check whether any network segmentation that was established to isolate breaches is intact.
- Work with forensic experts to get an assessment that is as complete as possible and act on remedial recommendations as soon as possible.
- Create a communications plan that reaches all affected audiences, including employees, customers, investors, business partners, and other stakeholders.

Notifying appropriate parties

Most states have laws requiring companies to notify individuals who were affected by security breaches involving certain types of personal information. Work with counsel to understand your obligations. Among other guidance, the FTC explains that there are several types of entities that may also need to be notified, including law enforcement authorities, federal agencies such as the FTC or the U.S. Department of Health and Human Services in the case of health data, or the FCC in the case of breaches involving covered communications companies. The FTC's guidance also addresses how and when to notify individuals, and includes a model letter for notifying individuals whose names and Social Security numbers have been stolen.

The FTC guide contains additional detail that would be useful for companies to review as they plan in advance for how they will respond to a data breach. The FTC notes that its new guide addresses the steps companies should take once a breach has occurred, but that companies also should implement measures to reduce the risk of breaches in the first instance.

Our privacy & data protection practice group tracks these and other regulatory issues involving the FTC and cybersecurity, and we have a dedicated team of attorneys and third party technical experts to address any incident response needs. We can provide you with additional information or insights, tailored to your or your organization's needs.

Key Contacts

Matthew D. Brown **San Francisco**	**brownmd@cooley.com** **+1 415 693 2188**
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090