# *Client Alert*: FTC Releases Breach Notification Guide for Businesses

**Related Professionals**

Christopher L. Ingram

**Related Services**

Data Strategy, Privacy and Security

Litigation and Appeals

**CLIENT ALERT** | 10.28.2016

On Wednesday, the Federal Trade Commission (FTC) released its new *Data Breach Response: A Guide for Businesses*. On the go or don't have time to review the guide? The FTC also released this helpful video. The guide focuses on steps to take once a breach has occurred.

The guide provides high level practical advice on what to do when your organization suspects that a data breach has occurred, such as securing physical areas, identifying the forensic investigation team, and consulting with legal counsel. The guide also emphasizes the importance of containing the incident to prevent additional data loss and removing improperly posted information from websites. Once contained, the guide recommends moving to identifying and remedying vulnerabilities exploited during the breach, and notifying stakeholders such as law enforcement, business partners and affected individuals.

Although there is no federal data breach notification law (so long as protected health information (PHI) is not involved), the FTC includes a model notification letter in the guide and recommends that a business consult with its law enforcement contact, designate a point person within the organization for releasing information, and consider offering at least a year of free credit monitoring services.

Outside of the PHI context, notification to affected individuals of data breaches involving their personal information is governed by 47 state laws, and the laws of D.C., Puerto Rico and the Virgin Islands. The model letter adopts the headings recommended under California's amended breach notification law that went into effect earlier this year. The model letter also recommends including copies of the FTC's *Identity Theft: A Recovery Plan*, a 40 page publication, and an "optional attachment" from identitytheft.gov. Inclusion of these documents, while not required under any state or federal law, could significantly increase the cost to businesses providing mailed notifications. Because there is no law requiring this information be included, it will be interesting to see whether the FTC will use the model letter in its guide as a new standard for regulating companies' data breach response efforts under its general unfair and deceptive authority. Moreover, the letter, while a

good starting point, may not be fully compliant with all legal requirements under the patchwork of state and US territory notice of breach laws.

Nevertheless, the guide is free and provides helpful information for organizations facing a breach that have not yet implemented a customized incident response plan, or for organizations at the initial stages of preparing and implementing an incident response plan. For assistance when facing a breach or planning for a breach, please contact Heather Enlow-Novitsky, Chris Ingram or your Vorys attorney.