THE
NATIONAL LAW REVIEW

The ABA Says Lawyers Have Obligations Before and After a Data Breach

Tuesday, November 6, 2018

In the age of the data breach, lawyers and law firms have a lot in common with comic book superheroes: they are locked in a relentless battle against a cunning, ever-changing threat. This past week, Foley & Lardner experienced a "cyber event," adding its name to the list of cyber attack victims which, according to Bloomberg Law, includes DLA Piper, Cravath, Swaine & Moore, Weil, Gotshal & Manges, over one third of small and medium-sized firms, and just under one quarter of large firms. Because of this growing and serious threat to the legal profession, the ABA published Formal Opinion 483 to direct attorneys and law firms on how they should handle data breaches before, during, and after an event. In short, lawyers are not expected to be as bulletproof as Superman, but they must take proactive steps to protect sensitive client data and they must disclose material data breaches.

The entire ABA opinion can be accessed here and a summary of the opinion is below.

Article By
Trusts and Estates Practice Group Murtha Cullina
Murtha Cullina
Privacy and Cybersecurity Perspectives
Communications, Media & Internet
Law Office Management
All Federal

The ABA states that data breaches pose a "major professional responsibility and liability threat" to the entire legal profession. It defines a data breach as "a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode."

When there is data breach, attorneys must first comply with state and federal legislation. Next, attorneys must disclose a breach to a current client if (a) that client's material, confidential information is or reasonably may have been compromised (*e.g.*, unauthorized access, use, theft, or destruction), or (b) the breach has materially disrupted the attorney's ability to serve the client (*e.g.*, ransomware limiting access to client information for any material amount of time). In essence, lawyers must notify clients when incidents like ransomware materially impair operations—even when there is no evidence of exfilatrated or compromised data. Here, strong defense mechanisms include up-to-date, accessible, and easily restorable back-ups to fend off disruption of legal services.

What are a lawyer's ethical duties concerning a data breach?

- Make reasonable efforts to understand the risks and benefits of technology relevant to the practice of law;
- Monitor for data breaches;
- Hold electronic property with the same fiduciary care required of physical property;
- Implement reasonable precautions to limit vulnerabilities;
- Act reasonably and promptly to stop a breach and mitigate damage;
- After a breach, investigate its cause and evaluate notice obligations; and
- In the case of a data breach that rises to the level of a notice-triggering event, provide current, affected

clients with notice of such data breach.

What can lawyers do to prepare for and respond to a data breach?

- Preemptively develop an incident response plan;
- Analyze compliance on an ongoing basis;
- Keep abreast of regulatory and statutory notice requirements;
- Reach an agreement with clients before conclusion of services, or when client-attorney relationship terminates, about how to handle the client's electronic information still in attorney's possession;
- Absent agreement otherwise, maintain physical and electronic document retention schedules in compliance with applicable rules; and
- Inform clients affected by a breach about the lawyer's plan to respond to the incident.

Are there any instances when a lawyer or firm does not have to disclose a data breach?

Notably, Formal Opinion 483 states that lawyers are not required to give notice of a breach to a former client unless black letter law requires otherwise. Similarly, a breach that limits access to information for an immaterial amount of time, or consists of non-confidential or publicly available information, does not rise to the level of a data breach requiring disclosure to a client.

As a best practice, lawyers and firms should be well-versed in local and federal data breach and privacy laws, as those laws may require action where the Rules of Professional Responsibility do not.

Dayle Duran authored this post.

Source URL: https://www.natlawreview.com/article/aba-says-lawyers-have-obligations-and-after-data-breach