Attorneys Must Consider Ethical Obligations Associated with a Data Breach

Insights
10.31.18

Most attorneys are well aware of statutory obligations that require private and governmental entities to notify individuals of data breaches that involve the loss or disclosure of personally identifiable information. An area that may be less clear, however, is what ethical obligations attorneys have to guard against data breaches involving client information and what steps attorneys must take when a data breach occurs.

On October 17, 2018, the American Bar Association Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 483. The Opinion addresses attorneys' obligations after an electronic data breach or cyberattack, including the applicability of the Model Rules of Professional Conduct when a data breach is detected or suspected. The Opinion also provides input regarding best practices in preventing and responding to data breaches, and emphasizes the importance for attorneys to plan ahead.

For purposes of Formal Opinion 483, a data breach is defined as "a data event where material client 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." Given this definition, not every cyber event will trigger an attorney's ethical obligations. Attorneys should focus on events that may or do result in an actual compromise of material client confidential information.

Attorney obligations discussed in the Opinion can be broken down into four components: (1) an obligation to monitor for data breaches; (2) prompt action to address a data breach; (3) evaluation of what occurred; and (4) providing notice, if necessary.

Obligation to Monitor
Model Rules 5.1 and 5.3 require reasonable efforts to establish policies and procedures designed to provide reasonable assurances that all lawyers and staff comply with the Model Rules. In Formal Opinion 483, the Committee concluded that, in order to comply with these Rules, "lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data."

This conclusion indicates that, even before a breach occurs, an attorney has a responsibility to monitor for data breaches. This obligation to monitor does not mean, however, that an ethical

violation occurs each time a data breach is not immediately detected. Instead, the potential for an ethical violation is present when an attorney fails to undertake reasonable efforts to avoid data breaches or where the lack of reasonable efforts is the cause of a breach.

Prompt Action

Model Rule 1.1 requires attorneys to develop sufficient competence in technology to meet their obligations after a breach. To comply with Model Rule 1.1, an attorney must act reasonably and promptly when a breach of protected client information is suspected or detected. Although Formal Opinion 483 does not identify specific actions that attorneys must take to stop a breach or mitigate damage from a breach, the Committee suggests that having an incident response plan, with specific plans and procedures for responding to a data breach, is a best practice. The Opinion also explains that after taking prompt action to stop a breach, a lawyer "must make all reasonable efforts to restore computer operations to be able to service the needs of the lawyer's clients."

Evaluation

Model Rule 1.6 requires attorneys to make reasonable efforts to prevent inadvertent or unauthorized disclosure of, or access to, client information. Compliance with this Rule requires attorneys to evaluate what occurred during a data a breach and how to prevent a reoccurrence. During the process of restoring computer operations to be able to continue client work, attorneys should evaluate exactly what occurred and what needs to be done to prevent the same issue in the future. This process may require input from technical experts.

Notice

Model Rule 1.4 states that attorneys must keep their clients reasonably informed and that an attorney shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation. To comply with Rule 1.4, an attorney must communicate with current clients in the event of a data breach. Pursuant to Formal Opinion 483, "[w]hen a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach." The Opinion did not, however, impose a similar notice requirement relating to former clients.

When a notification is provided, it must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything. The Committee did not identify specific information that must be included in a notification, recognizing that the communication will depend on the type of breach and the nature of the data compromised by the breach. The Committee did direct, however, that "lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients' information."

As expressed by Formal Opinion 483, attorneys must consider their ethical obligations to prevent and address data breaches, as well as statutory breach notification laws. Ethical violations can lead to malpractice lawsuits, disciplinary actions and potentially court sanctions. In the event of a data breach, ethical obligations to should be at the forefront of a competent attorney's consideration.

Related People

Heather Zalar Steele
Partner
610.230.2134
Email