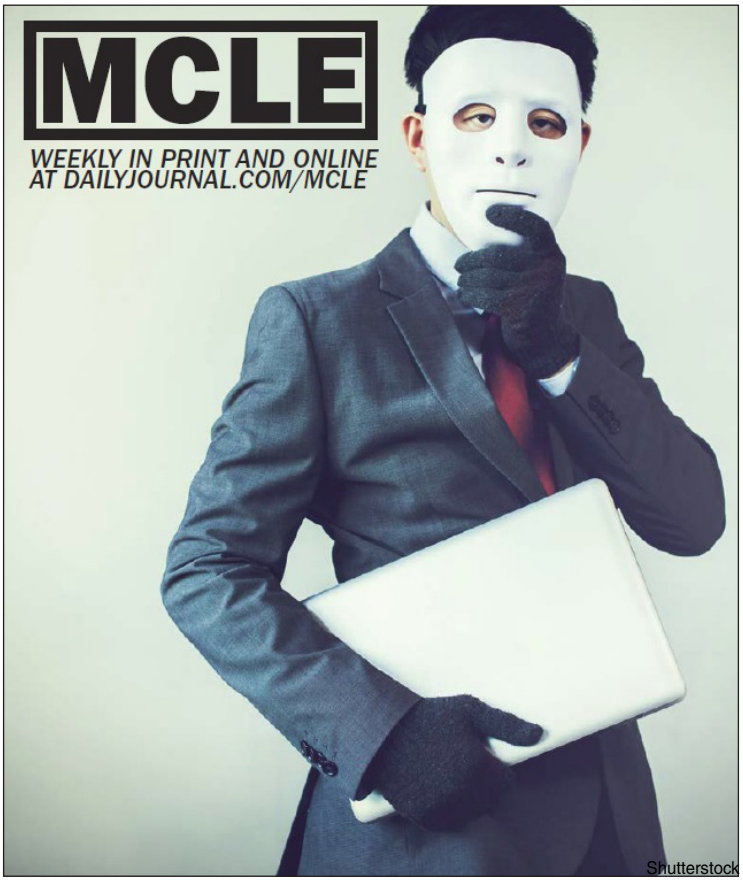
LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
FRIDAY, NOVEMBER 9, 2018

Ethical duties and data breaches

By Alison Buchanan



On Oct. 17, the American Bar Association's Standing Committee on Ethics and Professional Responsibility issued Formal Opinion No. 483, which provides guidance on lawyers' ethical obligations following an electronic data breach or cyberattack. The opinion was born from the fact that data breaches and cyber threats involving or targeting law firms "are a major professional responsibility and liability threat facing the legal profession."

For purposes of the opinion, a data breach is "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." Data breaches and cyber threats can occur in a variety of ways, including hacking, phishing, ransomware, electronic scams, internal breaches, and even the old-fashioned physical theft of an electronic device. According to one source cited by the Standing Committee, firms fall into two categories: those who have suffered a breach and those who will in the future. Much like being struck by lightning, and although it would be very unlucky indeed, a breach or cyberattack can certainly strike the same firm or lawyer more than once.

Guidance for Lawyers Following a Data Breach or Cyberattack

Formal Opinion No. 483 builds on ABA Formal Opinion 477R (2017), which addressed lawyers' ethical obligations when communicating confidential client information using the internet. Formal Opinion No. 483 takes the analysis further, focusing on lawyers' duties after discovering a data breach or cyberattack.

Organized into three main parts, the opinion explores a lawyer's ethical obligations in the context of the duties of competence and supervision, confidentiality, and communication. Those obligations are dependent on "the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations." Specifically excluded from the opinion is any opinion or analysis relative to a lawyer's duties arising from privacy laws and other statutory schemes (i.e., state notification law, HIPAA, or the Gramm-Leach-Bliley Act).

Duties of Competence and Supervision

A. Duties of competence and supervision include detecting breaches and attacks. ABA Model Rule 1.1 requires lawyers to provide competent representation. "Competence" includes the legal knowledge, skill, thoroughness, and preparation "reasonably necessary for the representation." In the context of using technology and, specifically, preventing data breaches and cyberattacks, Comment [8] to Rule 1.1 was modified in 2012. Under new comment [8], to maintain competence, lawyers will need to keep abreast of the benefits and risks associated with relevant technology. Lawyers are obligated "to use technology competently to safeguard confidential information against unauthorized access or loss." Of course, with this, as with other areas, lawyers may retain qualified non-lawyer assistants to facilitate a lawyer's competency. As such, a lawyer's duty to monitor and detect breaches or attacks also implicates by Rules 5.1 and 5.3, which impose on lawyers duties to supervise subordinate lawyers and non-lawyer staff.

A lawyer's duty of competence and supervision includes the duty to monitor and detect breaches and attacks. To satisfy one's duty to detect such breaches or attacks, a lawyer must make reasonable efforts to monitor his or her technology resources to detect a breach. A lawyer must take reasonable steps to ensure that the firm and its lawyers and non-lawyer staff "employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relate to data and the use of data." As with prevention, a lawyer's failure to detect a breach or attack does not necessarily constitute an ethical violation.

B. Once a lawyer learns of a breach, she must take steps to stop the breach and restore systems. If a lawyer detects a data breach or cyberattack, the lawyer may not sit on her hands. Rather, her duty of competence requires her to act.

While the opinion declines to mandate specific steps (given that each incident — and appropriate response to same — will be fact-specific), the opinion suggests that lawyers should develop and have in place an incident response plan to allow them to deal with a data breach immediately. The opinion provides some examples of common incident response plan features, such as the identification of team members and backups, the means for communicating with the team members, steps to be taken at each phase of the process (and identification of which team member is responsible for each step), and the identification of a lead team member.

As a practical matter, any incident response plan should be accessible by means other than electronic means (i.e., the data response plan should be printed and kept in hard copy format somewhere the lawyer can access it in the event of a data breach).

Once a lawyer discovers a breach, she must take "prompt action" to

stop the breach and then make "all reasonable efforts" to restore systems so that the lawyer can resume serving client needs. The lawyer may employ an expert or professional to assist in this phase. Depending on what the investigation reveals, the lawyer may need to implement new systems, so as to avoid a recurrence of the breach or attack. The opinion contemplates that, in certain specific circumstances, it may be appropriate to refrain from further use of technology.

C. Following a breach, lawyers have a duty to find out what happened. Just as a lawyer must act once she is aware of a breach, a lawyer cannot simply address the breach and then act as though it never happened. A lawyer's duty to communicate requires the lawyer to determine why the breach or attack occurred, so that, when the lawyer advises the client of the breach, the lawyer can communicate to the client as much information as possible about what happened. Indeed, the client will want answers and the lawyer will need to be equipped to provide them.

Duty of Confidentiality

The duty of confidentiality includes the duty use reasonable efforts to "prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." See ABA Model Rule 1.6(c). Factors to consider in determining what constitutes "reasonable efforts" include: the sensitivity of the information, the likelihood of disclosure without additional safeguards, the costs associated with employing such safeguards, the difficulty in implementing safeguards, and the extent to which such safeguards would inhibit the lawyer's representation.

Additionally, the opinion reminds that the standard for the duty of confidentiality is not one of strict liability. Rather, a lawyer who has employed reasonable efforts will not be deemed to be in violation of Rule 1.6, even if a data breach occurs.

Finally, a lawyer's implied authorization to reveal client information to the extent necessary to implement the representation likely allows the lawyer to reveal information to law enforcement necessary to stop the breach and recover the compromised information.

Duty to Communicate

Model Rule 1.4 requires lawyers to keep clients reasonably informed about the status of the matter and provide sufficient information to clients to allow them to make informed decisions about the representation. As such, Formal Opinion No. 483 instructs that when a lawyer is aware of a data breach or cyberattack involving client information, a lawyer must communicate that information to current clients.

Conversely, with respect to notification to former clients, the Standing Committee concludes that there is no similar ethical duty. (Again, Formal Opinion No. 483 specifically focuses on ethical duties of lawyers; lawyers may have other notice obligations pursuant to privacy laws and other statutory schemes).

In instances where a lawyer is obligated to notify a client of a data breach or cyberattack, "[t] he disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything." Of course, different scenarios will necessitate different approaches to notification. Regardless, the opinion unequivocally provides that "[l] awyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact."

Takeaways

Formal Opinion No. 483 provides several important takeaways for lawyers relative to detecting, responding to, and informing clients of a date breach or cyberattack.

First, lawyers using technology (or lawyers in managerial or supervisory roles overseeing other lawyers or non-lawyers using technology) should take reasonable steps to prevent such breaches or attacks, including establishing internal procedures and policies. Second, lawyers utilizing technology should monitor the security of electronically stored client property and information, so that a breach can be detected. Third, lawyers who discover a breach should promptly take steps to stop the breach and recover the compromised information. Fourth, lawyers must notify current clients if the clients' data has been the subject of a breach or attack.

While some consider data breaches and cyberattacks to be an inevitability, the corresponding client damage and fallout does not have to be. In the event of an attack, having systems in place and understanding one's obligations to one's affected client(s) will go a long way toward preventing significant and long-term damage.

Alison Buchanan *is a shareholder with Hoge Fenton in San Jose, where her practice focuses on business litigation and professional liability. Alison is a certified specialist in legal malpractice law and recently completed a three-year term serving as a member of the State Bar's Standing Committee on Professional Responsibility and Conduct.*

BUCHANAN