LAW.COM
New York Law Journal

New Developments in Law Firms' Obligations To Protect Against Data Breaches

In addition to a 2018 ABA ethics opinion which outlines when law firms are ethically obligated to notify clients of data breaches jeopardizing the security of their confidential information, the California Bar Association has handed down additional guidance on the subject, which is helpful to all law firms.

By **Jennifer Goldsmith, David Standish and Barry R. Temkin** | January 15, 2021 at 11:00 AM

In 2018, the American Bar Association Standing Committee on Ethics issued its **Formal Opinion 18-483**, which outlines a framework for when law firms are ethically obligated to notify clients of data breaches jeopardizing the security of their confidential information. In its ethics opinion, the ABA noted that law firms should employ reasonable efforts to monitor the security of their information, and advised lawyers to “act reasonably and promptly to stop the breach and mitigate damage from the breach.” Law firms should, as a matter of professional responsibility, have data breach plans in place in order to remediate cyber intrusions.

In addition, the committee wrote that, “an obligation exists for a lawyer to communicate with current clients about a data breach.” However, not all cyber episodes require client notification. While a cyber intrusion which does not gain access to client confidential information needn’t be disclosed, “disclosure

will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach."

The California State Bar Association, in September 2020, has handed down **additional guidance** on the subject, which is helpful to all law firms, especially those who represent California clients. California State Bar Formal Opinion No. 2020-203 answers the question, "What are a lawyer's ethical obligations with respect to unauthorized access by third persons to electronically stored confidential information in the lawyer's possession?" In its opinion, the California State Bar writes that law firms should take reasonable steps to secure their electronic data storage systems to minimize the risk of unauthorized access to client confidential information, and should provide for remote lockdown and scrubbing in the event a portable device is lost or compromised. In the event of a breach, "lawyers have an obligation to conduct a reasonable inquiry to determine the extent and consequences of the breach and to notify any client whose interests have a reasonable possibility of being negatively impacted by the breach."

In Opinion No. 2020-203, the California State Bar posits several key principles of professional competence. In the first instance, lawyers' duty of professional competence includes knowledge about cybersecurity technology, and managing partners in law firms should familiarize themselves with the tools and procedures for protecting client confidential information. In addition, the association advises that law firms and corporate legal departments should have internal policies and procedures to protect against inadvertent disclosure of client confidential information, and should require staff training to protect against phishing attacks and other cyber intrusions.

The California Bar also recommends that law firms should be able to lock down or scrub lost devices remotely, to prevent unauthorized access of client

confidential information in the event that a portable device is lost or stolen. Finally, the state bar advises against using unprotected public networks, recommending instead that lawyers resort to virtual private networks (VPN) or encrypted networks.

Four Hypotheticals

In its opinion, the California State Bar helpfully outlines four hypothetical factual scenarios. Lawyer A's laptop was stolen, but he did not use it to store confidential information. Rather, the pilfered laptop was only used for remote access to the lawyer's desktop, and the firm had software that allowed it to be wiped clean remotely. Promptly after the theft, Lawyer A notified his firm's information technology department, which remotely cleansed the device of confidential information. This was held by the state bar to be a prudent and reasonable procedure which did not require client notification, as no confidential information was accessed or penetrated.

Lawyer B left a smart phone in a bag in a restaurant, which was retrieved undisturbed and in the same pocket of the bag the next morning after the lawyer realized that the phone was missing. The phone had a four digit password and no biometric code, and the restaurant assured the lawyer that the phone had been placed in a secured cabinet overnight. In this circumstance, while it would have been preferable to have a biometric code on the smart phone and a more complex password, there was no evidence that the phone had been disturbed or that client confidential information had been accessed. Accordingly, Lawyer B has no obligation to notify firm clients.

Statutory Basis

In addition to the 2018 ABA ethics opinion, the California Bar Association opinion was based on the **California Business and Professions Code**

§6068(e), which requires lawyers “to maintain inviolate the confidence, and at any peril to himself or herself to preserve the secrets, of his or client.” In addition, that statute requires lawyers to keep clients reasonably informed of “significant developments in matters” for which the attorneys are providing legal services.

Lawyers who represent clients in California should also take note of **California Civil Code §1798.82**, which imposes confidentiality and notification obligations upon any “person or business that conducts business in California.” That provision requires any business which does business in California and owns or licenses confidential client data to “disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California” when encrypted personal information is believed to be “acquired by an unauthorized person.”

The statute further provides that notification must be promptly made when encrypted personal information is acquired by an unauthorized person whom the business owner “has a reasonable belief that the encryption key or security credential could render that personal information readable or usable.” Cal. Civil Code 1798.82(a). Thus, where encrypted data is accessed by an unauthorized user, client notification must be made in circumstances in which there is a reasonable possibility of a breach of encryption. The statute implies that data which is subject to impenetrable encryption (if such a thing exists) would not trigger the notification obligations of the statute.

The California Civil Code requires disclosure “in the most expedient time possible and without unreasonable delay,” consistent with any ongoing law enforcement investigation. Of course, lawyers representing clients in multiple states should familiarize themselves with the requirements of each state in which they do business. For example, law firms might be subject to consumer

privacy laws enacted in other states, such as Maryland, Hawaii, New York and Massachusetts. See, e.g., Maryland Online Consumer Protection Act, SB 613, Massachusetts Data Privacy Law, (S-120), Hawaii Consumer Privacy Protection Act, SB 418, North Dakota HB 1485. Lawyers are well-advised to consult the laws of the jurisdictions in which they practice, and in which their clients do business.

Lawyers Working Remotely

In another recent development, the New York County Lawyers Association (NYCLA) Professional Ethics Committee has issued its ethics opinion 754-2020, which recommends steps that lawyers may take when working remotely to ensure the confidentiality of client confidential information. NYCLA's "**Ethical Obligations When Lawyers Work Remotely**," is specifically designed to address issues that arose or accelerated when law firms began working remotely in March 2020 due to the COVID-19 pandemic. Formal Opinion 754-2020 recommends that lawyers take the following measures to ensure the confidentiality of client information when working remotely:

(1) Avoiding use of unsecured Wi-Fi systems when accessing or transmitting confidential client information.

(2) Using virtual private networks that encrypt information and shield online activity from third-parties.

(3) Using multifactor authentication to access firm information and networks.

(4) Ensuring that computer systems are up to date, with appropriate firewalls and anti-malware software.

(5) Backing-up data stored remotely.

(6) Requiring strong passwords to protect data access in devices.

(7) Creating a written work-from-home protocol that specifies procedures to safeguard confidential information.

(8) Training employees on security protocols, data privacy and confidentiality policies.

The NYCLA committee concludes that lawyers may ethically work remotely, but should take the foregoing precautions in order to safeguard client confidential information.

Conclusion

Lawyers working remotely should exercise reasonable diligence to secure the confidentiality of confidential client information, and should ensure that their portable electronic devices either do not contain client information, or can be remotely deactivated and scrubbed. Law firms subject to cyber intrusions should consider the four hypothetical situations outlined by the California State Bar in determining when to notify clients, and should resolve reasonable doubts in favor of prompt client notification. Lawyers should consult the laws of the jurisdictions in which they practice, and in which their clients do business, as different states may vary in their interpretation of lawyers' professional responsibilities with respect to data breaches.

Jennifer Goldsmith, *an attorney, is vice president, professional liability claims, at Ironshore Insurance.* **David Standish**, *an attorney, is an assistant vice president and cyber/tech claims manager at at Ironshore Insurance.* **Barry Temkin** *is a partner at Mound Cotton Wollan & Greengrass in New York, an adjunct professor at Fordham University School of Law and immediate past chair of the New York County Lawyers' Association*

Committee on Professional Ethics. The views expressed in this article are the authors' alone and do not reflect the views of Ironshore Insurance, Fordham University or NYCLA.

Dig Deeper

- Bar Associations
- Cybersecurity
- Law Firms - Large
- Legal Ethics and Attorney Discipline

Law Firms Mentioned

- **Mound Cotton Wollan & Greengrass**

Trending Stories

1. **Seeing 'Political Grandstanding' in Election Lawsuit, Judge Orders Attorney to Face Grievance Committee**

   NATIONAL LAW JOURNAL

2. **US Attorney Launched Criminal Investigation into Cuomo's Handling of COVID-19, Nursing Homes After Aide's Call Leaked**

   NEW YORK LAW JOURNAL

3. **Early Reports: The 2021 Am Law 200 Financials**

   THE AMERICAN LAWYER

4. **SDNY Judge Calls for DOJ Probe of Prosecutorial Misconduct in Iran Sanctions Case**

   NEW YORK LAW JOURNAL

5. **Climbing Profits and Expanding Nonequity Tier Stand Out as More Firms Post Results**

   THE AMERICAN LAWYER

Global Briefing

A weekly, curated selection of our international content from around the globe, across the business of law, in-house, regulatory, technology and more, with expert insights from our senior editors.

Learn More

Recommended Stories

PI