December 15, 2016

# New Cybersecurity Regulations: Impact on Representing Financial Institutions

Barry R. Temkin

New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 256—NO. 115
THURSDAY, DECEMBER 15, 2016

Outside Counsel

Expert Analysis

# New Cybersecurity Regulations: Impact On Representing Financial Institutions

By **Barry R. Temkin**

Lawyers who represent insurance companies, banks, insurance agents and other financial institutions in New York should be aware of new Department of Financial Services (DFS) cybersecurity regulations that become effective Jan. 1, 2017. The new DFS cybersecurity regulations require covered entities, including insurance companies, mortgage brokers, insurance agents and banks, to appoint a chief information security officer (CISO) and to develop a comprehensive cybersecurity program in order to prevent hacking and other data breaches.[1] In addition, the new DFS regulations will require the filing of an annual cybersecurity report, which must explain the state of the company's compliance with the new regulations, identify any soft spots or potential areas for improvement, and be signed and certified by the company's board chair or CEO.[2] The new regulations are codified at 23 NYCRR §500.0 and can be found at the DFS website, http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

BARRY R. TEMKIN *is a partner at Mound Cotton Wollan & Greengrass.*

This article will explain the new DFS regulations as proposed at the time of writing, and discuss their implications for law firms that represent financial institutions doing business in New York. Since the cybersecurity regulations are subject to a 45-day commentary period, there is a possibility that they could be subject to further revisions by the time of implementation.

> Encryption is a key part of the new regulations, which require each covered entity to "encrypt all nonpublic information held or transmitted by the covered entity both in transit and at rest."

The news abounds with almost daily reports of hacking and other cybersecurity breaches. Professional liability insurers estimate that many of the largest U.S. law firms have experienced hacking or other forms of data breaches recently. External hacking is not the only threat faced by law firms. Numerous data breaches may be attributable to mere negligence, such as a law firm employee's leaving a laptop, cell phone or other electronic device in a taxi, coffee shop or other public place. Moreover, information stored in the cloud, or transmitted via an unsecured server, may be vulnerable or unsecured. In 2016, there were several press reports of law firms being hacked, including Cravath, Swaine & Moore and Weil Gotshal & Manges.[3]

A data breach of Panamanian financial law firm Mossack Fonseca made international headlines, embarrassing the firm's roster of affluent and politically powerful clients with the unauthorized release of the so-called "Panama Papers."[4] With clients coming to expect their law firms and other vendors to safeguard and encrypt confidential information, the organized bar is not far behind.

## New Regulations

The new DFS cybersecurity regulations apply to "any person operating under or required to operate under a

license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law."[5] Among other covered entities, DFS exercises jurisdiction over banks, insurance companies, charitable foundations, holding companies, mortgage brokers, mortgage loan originators, insurance agents and premium finance agencies. A limited exception to the regulations is carved out for otherwise covered entities with fewer than 1,000 customers, less than $5 million in gross annual revenue and less than $10 million in year-end total assets. The rules provide for a 180-day transitional period to comply with their requirements.

Encryption is a key part of the new regulations, which require each covered entity to "encrypt all nonpublic information held or transmitted by the covered entity both in transit and at rest."[6] Nonpublic information that could not be feasibly encrypted must be secured with additional or alternative controls. The DFS regulations require encryption of "nonpublic information," which includes personal identification information (PII), competitively sensitive information and any information that would be considered nonpublic under the Gramm-Leach Bliley Act of 1999.

The encryption requirement is set forth in Section 500.15, which provides as follows:

(a) As part of its cybersecurity program, each Covered Entity shall encrypt all Nonpublic Information held or transmitted by the Covered Entity both in transit and at rest.

(b) To the extent encryption of Nonpublic Information in transit is currently infeasible, Covered Entities may instead secure such Nonpublic Information using appropriate alternative compensating controls reviewed and approved by the Covered Entity's CISO. Such compensating controls shall not be used in lieu of meeting the requirements of subsection 500.15(a) after one year from the date this regulation becomes effective.[7]

Recent ethics opinions, most notably in California, have suggested that lawyers have ethical duties to familiarize themselves with and ensure literacy with their clients' electronic storage systems, particularly in the context of litigation involving electronically stored information.

Thus, encryption of sensitive data is now required for nonpublic information. However, the encryption requirement is delayed until one year from the effective date of the regulation.

The DFS encryption requirement is part of a growing national trend, pioneered by Massachusetts with its data protection law. See, Mass. Gen. L. Ch. 93H, 201 C.M.R. 17 (requiring the encryption of personal information stored on portable devices and personal information transmitted across public networks or wirelessly).

Under the proposed regulations, each firm must appoint a chief information security officer, who reports to the board of directors and is required to prepare an annual report, setting forth the nature of the registrant's cybersecurity program, any risks or challenges identified by the CISO and proposed steps to remediate any identified problems. In addition, the regulated entity must prepare a written incident response plan designed to respond to and recover from a potential data breach. The registrant must notify the superintendent of DFS within 72 hours in the event of a known material data breach.

The new regulations also propose "limitations on data retention," mandating the destruction of nonpublic information that is no longer necessary. This requirement could place these regulations in potential conflict with a body of case law about electronically stored information, spoliation and maintenance of electronically stored data as required by financial industry regulations and court rules.

### Implications for Law Firms

Lawyers who represent regulated financial service companies in New York, including banks, insurance agents and insurance companies, should familiarize themselves with these regulations. Significantly, the new DFS regulations would look not only to the registrants, but also upon

third-party vendors with which they do business. According to Section 500.11 of the new DFS regulations:

(a) Third Party Information Security Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, third parties doing business with the Covered Entity. Such policies and procedures shall address, at a minimum, the following areas:

(1) the identification and risk assessment of third parties with access to such Information Systems or such Nonpublic Information;

(2) minimum cybersecurity practices required to be met by such third parties in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such third parties; and

(4) periodic assessment, at least annually, of such third parties and the continued adequacy of their cybersecurity practices.

Thus, financial companies doing business with vendors such as law firms will be required to affirm that these vendors maintain minimum cybersecurity practices, including, ultimately, encryption of electronic data. Accordingly, law firms that represent covered entities, including insurance companies and banks, should ensure that their information technology systems—including email—are appropriately encrypted as well. Needless to say, no lawyer would want to be responsible for a client's violation of a DFS regulation.

Recent ethics opinions, most notably in California, have suggested that lawyers have ethical duties to familiarize themselves with and ensure literacy with their clients' electronic storage systems, particularly in the context of litigation involving electronically stored information. See, California Standing Committee on Professional Responsibility and Conduct Formal Op. 2015-193 (attorney lacking the required e-discovery competence must either acquire the requisite skill and technical expertise in e-discovery, associate with technical consultants or competent counsel, or decline the representation).

Other recent opinions have agreed that lawyers should act diligently to maintain the confidentiality of electronically stored client data. And some jurisdictions have begun imposing requirements that lawyers undergo mandatory continuing legal education in technology and electronic data skills. See, Florida Rules of Professional Conduct, Rule 6-10.3(b) (imposing three credit hours of mandatory CLE training in approved technology programs).

## Conclusion

Lawyers representing financial institutions should be sure to engage appropriate encryption technology. The trend among ethics committees and regulators suggests that lawyers have an ongoing obligation to become cognizant of new developments in technology and to take reasonable steps to prevent data breaches.

While lawyers, as a rule, tend to be less tech-savy than their clients, lawyers who fail to keep up with the times could conceivably find themselves left in the dust, as regulated clients move on to engage law firms that are willing to undertake the investment necessary to keep up with cybersecurity technology.

1. See New York DFS Proposed Regulations, http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf

2. See 23 NYCRR Section 500.09, http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

3. Nicole Hong and Robin Sidel, "Hackers Breach Law Firms, Including Cravath and Weil Gotshall," The Wall Street Journal, March 29, 2016, http://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

4. Frances Ivens, "Panama Papers Put Spotlight on Law Firm Data Security," The American Lawyer, April 4, 2016, http://www.americanlawyer.com/id=1202753986288/Panama-Papers-Put-Spotlight-on-Law-Firm-Data-Security?slreturn=20161109122347.

5. See 23 NYCRR Section 500.01 (c).

6. 23 NYCRR Section 500.15, http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

7. 23 NYCRR Section 500.15, http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.