Morrison & Foerster Client Alert.

August 8, 2011

The Massachusetts AG Reaches Agreement With Bank Over Alleged Violations of the State's Data Security Regulations

By Nathan D. Taylor

On July 28, 2011, the Massachusetts Attorney General ("AG") entered into an agreement with a Massachusetts bank regarding alleged violations of the state's data security regulation. Specifically, the Massachusetts AG entered into an Assurance of Discontinuance with the bank (in lieu of an enforcement action), in which the bank agreed to comply with the state's data security regulations, as well as to pay a civil penalty of $7,500.

According to the Massachusetts AG's press release, a bank employee left an unencrypted backup tape, containing, among other things, Social Security numbers and account numbers of Massachusetts residents, on a desk at the end of the work day, rather than storing the tape in a vault.[1] Reportedly, surveillance footage showed that the backup tape then was inadvertently thrown away by the bank's cleaning crew. The AG's press release, however, indicates that ultimately the tape was likely to have been "incinerated" by the bank's waste disposal company.

In its Assurance of Discontinuance, the Massachusetts AG alleged that this incident involved two violations of the state's data security regulations. First, the AG alleged that the bank violated the regulations by "maintaining personal information on unencrypted backup data tapes." Second, the AG alleged that the bank violated the regulations by "failing to follow its own Written Information Security Program . . . resulting in the improper handling and subsequent loss of a backup data tape." The AG raised this second allegation even though neither the AG nor the bank had any information indicating that any personal information had been acquired or used by an unauthorized person.

Beijing
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364

Hong Kong
Gordon A. Milner 852 2585 0808
Nigel C.H. Stamp 852 2585 0888

London
Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Russell G. Weiss (213) 892-5640

New York
Madhavi T. Batliboi (212) 336-5181
John F. Delaney (212) 468-8040
Sherman W. Kahn (212) 468-8023
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia
Daniel P. Westman (703) 760-7795

Palo Alto
Anna Ferrari (650) 813-5681
Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco
Roland E. Brandel (415) 268-7093
Jim McCabe (415) 268-7011
James R. McGuire (415) 268-7013
William L. Stern (415) 268-7637

Tokyo
Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

Washington, D.C.
Nicholas A. Datlowe (202) 887-1590
Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Kimberly Strawbridge Robinson (202) 887-1508
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

[1] The Massachusetts AG's press release is available at http://www.mass.gov/?pageID=cagopressrelease&L=1&L0=Home&sid=Cago&b=pressrelease&f=2011_07_29_belmont_savings&csid=Cago.

© 2011 Morrison & Foerster LLP | mofo.com | Attorney Advertising

The Massachusetts AG's action in this matter raises at least five important implications for businesses.

- First, it is important to keep in mind that a business can be found to have violated the Massachusetts data security regulations, even if the business does not suffer a security incident that requires notice to consumers under the state's security breach notification law. As indicated above, the Assurance of Discontinuance highlights that neither the AG nor the bank had information indicating that "any consumer's personal information has been acquired or used by an unauthorized person or used for an unauthorized purpose." This quoted language reflects the Massachusetts security breach law's consumer notice trigger. *See* Mass. Gen. Laws § 93H-3(b). As a result, the Massachusetts AG apparently believes, based on the known facts, that the incident was not an actual "security breach" and did not require notice to consumers. It is important for businesses to understand that the Massachusetts AG intends to enforce the data security regulations even in situations such as this where there was no actual security breach and even though the incident was of an accidental and isolated nature.

- Second, while the Assurance of Discontinuance and the Massachusetts AG's press release provide quite limited facts or background, the AG's second allegation seems to be framed in such a way that a violation of the data security regulations was presupposed simply because the bank suffered an information security incident. As noted above, the second allegation stated that the bank violated the regulations by "failing to follow its own Written Information Security Program . . . resulting in the improper handling and subsequent loss of a backup data tape." While a bank employee clearly failed to follow appropriate procedure to secure a backup tape, it is not clear how this single failure (*i.e.*, not a systemic issue) resulted in the bank not "follow[ing]" its information security program. In this regard, the data security regulations require that a person "develop, implement, and maintain a comprehensive information security program that . . . contains administrative, technical, and physical safeguards." 201 C.M.R. § 17.03(1). This requirement is procedural in nature, and it is not clear from the facts how the bank violated this requirement simply because a single employee made an error.

- Third, this action follows, four months to the day, an earlier information security enforcement action by the Massachusetts AG in which the AG referenced the state's data security regulations (*see* "The Massachusetts AG Has Not Forgotten About the State's Data Security Regulations – and Neither Should You"). In that action, the conduct at issue preceded the effective date of the data security regulations, but seemed to highlight the apparent inclination of the AG to enforce the regulations. This current action confirms that the Massachusetts AG intends to vigorously enforce the regulations.

- Fourth, this action confirms (again) that the Massachusetts AG believes that backup tapes are subject to the data security regulations' encryption requirement. In this regard, the regulations require that a person that electronically stores or transmits personal information must include in its information security program, "to the extent technically feasible," the "[e]ncryption of all personal information stored on laptops or other portable devices." 201 C.M.R. § 17.04(5). The Massachusetts AG had previously indicated in Frequently Asked Questions that backup tapes must be encrypted "on a prospective basis" where technically feasible.[2] In this regard, the AG apparently interprets the term "portable device" to include backup tapes, even though backup tapes are not commonly considered to be "portable" or "devices." With respect to backup tapes, one critical issue is whether or not it is actually technically feasible to encrypt such tapes. Nonetheless, the Assurance of Discontinuance was silent regarding whether the backup tape involved in the incident could have actually been encrypted.

- Finally, the Assurance of Discontinuance highlights a critical information security "procedure" that is commonly overlooked. Specifically, as part of the Assurance, the bank agreed to comply with its information security program, including by "effectively training the members of its workforce on the policies and procedures with respect to maintaining the security of personal information." While the data security regulations actually require that an information security program include "ongoing employee (including temporary and contract employee) training," 201 C.M.R. § 17.03(2)(b)(1), the AG did not allege that the bank violated the regulations' training requirement. But, the

[2] The Frequently Asked Questions are available at http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf.

© 2011 Morrison & Foerster LLP | mofo.com | Attorney Advertising

drafting of the bank's assurance seems to indicate that one aspect of its information security program that it may have failed to follow was employee training.

PRACTICAL IMPLICATIONS FOR BUSINESSES

There are some fairly significant lessons to be drawn from this Assurance of Discontinuance:

- The Massachusetts AG clearly takes seriously the information security obligations imposed by the data security regulations and appears intent on actively enforcing such regulations.
- A violation of the regulations can occur even if there has been no unauthorized access to, or acquisition of, personal information.
- The failure to encrypt backup tapes, where technically feasible, is a violation of the regulations.
- Training of employees is crucial to any compliant information security program.

As we have previously indicated, businesses that have not taken steps to address compliance with the Massachusetts data security regulations should quickly begin to take such steps. For those businesses that have previously addressed their compliance with the regulations, they may wish to consider revisiting their compliance programs to ensure they comply with the detailed regulations. Nonetheless, while the Massachusetts data security regulations may be the most detailed state information security requirements, they are certainly not the only state requirement relating to the security of personal information, and they will not be the last.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for seven straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations.

© 2011 Morrison & Foerster LLP | mofo.com | Attorney Advertising