MORRISON | FOERSTER

Morrison & Foerster Client Alert.

April 6, 2011

The Massachusetts AG Has Not Forgotten About the State's Data Security Regulations – and Neither Should You

By Miriam H. Wugmeister and Nathan D. Taylor

Just because we have not heard much about the Massachusetts data security regulations in the past year does not mean that the regulations should be forgotten. On Monday, March 28, 2011, the Massachusetts Attorney General ("AG") entered into a settlement with the owner and operator of several Boston bars and restaurants with respect to a security breach and related data security failings.[1] Importantly, the Massachusetts data security regulations played a prominent role in the settlement.

According to the Massachusetts AG's complaint, the restaurant chain experienced a data breach in April 2009 in which malware on its computer systems allowed hackers to access customer payment card information. Moreover, the AG's complaint alleged, among other things, that the restaurant chain did not follow a number of basic computer security precautions, including, for example, failing to change the default usernames and passwords on its computer system and permitting employees to share common usernames and passwords. Although the lack of these controls occurred before the effective date of the Massachusetts data security regulations, this conduct would appear to have stood in stark contrast to the controls required by the regulations (let alone basic industry best practices).

The settlement requires the restaurant chain, among other things, to pay $110,000 in civil penalties, as well as to comply with the Massachusetts data security regulations. In making this announcement, the Massachusetts AG acknowledged that the breach at issue occurred prior to the date that compliance with the Massachusetts data security regulations was required (March 1, 2010), but "the data security standards set forth in the regulations were used in the settlement."

While many U.S. state laws require that businesses adopt reasonable measures to protect personal information and/or dispose of personal information in an appropriate manner, the Massachusetts data security regulations impose far more

Beijing

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

Brussels

Karin Retzer 32 2 340 7364
Joanne Lopatowska 32 2 340 7365

Hong Kong

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

Los Angeles

Mark T. Gillett (213) 892-5289
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Russell G. Weiss (213) 892-5640

London

Ann Bevitt 44 20 7920 4041
Anthony Nagle 44 20 7920 4029
Chris Coulter 44 20 7920 4012

New York

Joan P. Warrington (212) 506-7307
John F. Delaney (212) 468-8040
Madhavi T. Batliboi (212) 336-5181
Suhna Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam Wugmeister (212) 506-7213
Sherman W. Kahn (212) 468-8023

Northern Virginia

Daniel P. Westman (703) 760-7795
Timothy G. Verrall (703) 760-7306

Palo Alto

Bryan Wilson (650) 813-5603
Christine E. Lyon (650) 813-5770

San Francisco

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

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.

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

detailed and comprehensive data security requirements than most, if not all, other states.

PRACTICAL IMPLICATIONS

In light of this settlement, businesses should revisit their compliance programs to ensure that they comply with the specificity of the Massachusetts data security regulations. For example, the regulations impose a number of significant administrative responsibilities on covered businesses.[2] In this regard, a covered business must:

- develop, implement, maintain, and monitor a comprehensive, written information security program that contains administrative, technical, and physical safeguards to ensure the security and confidentiality of records containing personal information;
- conduct a risk assessment to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of electronic, paper, and other records containing personal information and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks;
- designate one or more employees to maintain the information security program;
- regularly monitor to ensure that the information security program is operating in a manner reasonably calculated to prevent unauthorized access to, or unauthorized use of, personal information;
- take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with the regulations and any applicable federal regulations, including requiring service providers by contract to implement and maintain such security measures (there is a limited safe harbor for the contract requirement until March 1, 2012); and
- educate and train employees regarding personal information security.

Beyond its general, risk-based information security program requirement and related administrative requirements, the Massachusetts data security regulations also require that a business implement a number of detailed and specific technical security controls. Among other things, the regulations require that an organization:

- implement reasonable restrictions on physical access to records containing personal information and store such records in locked facilities, storage areas, or containers;
- implement secure user authentication protocols and access control measures for computer systems;
- encrypt all transmitted records and files containing personal information that will travel across public networks and that will be transmitted wirelessly;
- encrypt all personal information stored on laptops and other portable devices; and
- maintain firewall protections, operating system security patches, and malware and virus protection.

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 taken steps to address their compliance with the regulations, consider revisiting the compliance program to ensure it complies with the detailed regulations. Nonetheless, while the Massachusetts law may be the most detailed, it is certainly not the only state regulation relating to the security of personal information, and it 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.

[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_03_28_briar_group_settlement&csid=Cago.

[2] The Massachusetts data security regulations apply to any person who receives, maintains, processes, or otherwise has access to "personal information" relating to a resident of Massachusetts in connection with the provision of goods or services, or in connection with employment. For purposes of the regulations, the term "personal information" is defined as an individual's first name or initial and last name, in combination with any one of the following data elements: (1) Social Security number; (2) driver's license number or state-issued identification card number; or (3) financial account, credit card, or debit card number, with or without any required security code or password that would permit access to the account.