

Peter G. Shaheen**
Nicholas S. Guerrero**
Sean P. O'Leary**
Carol A. O'Leary†
Michelle L. Doucette*

SHAHEEN GUERRERA & O'LEARY, LLC

Jefferson Office Park
820A Turnpike Street
North Andover, Massachusetts 01845
Telephone: (978) 689-0800 Toll Free: (866) 665-5834
Facsimile: (978) 794-0890
E-mail: pshaheen@sgolawoffice.com

* Admitted in MA
** Admitted in MA and NH
† Admitted in MA, NH,
ME and CT

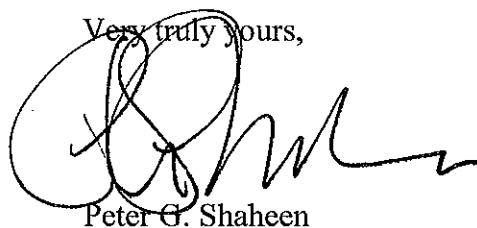
January 14, 2009

Important Notice to Client:

Effective January 1, 2009, a new Massachusetts data privacy regulation mandating steps a company must take if it captures/stores consumer credit card information went into effect. Many "commercial businesses" purchasing products and/or services pay using a consumer credit card which falls under this regulation. The regulation (which can be found online at Mass.gov) and an October WSJ article about this new regulation are attached for your review. Everyone is encouraged to speak to your CPA/Attorney and IT department to insure that your company is compliant.

Thank you for your attention to this matter. Kindly contact me should you have any questions or concerns.

Very truly yours,



Peter G. Shaheen

PGS/jcj
Enclosures

[Home >](#)

201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth

Section:

[17.01: Purpose and Scope](#)

[17.02: Definitions](#)

[17.03: Duty to Protect and Standards for Protecting Personal Information](#)

[17.04: Computer System Security Requirements](#)

17.01 Purpose and Scope

(a) Purpose

This regulation implements the provisions of M.G.L. c. 93H relative to the standards to be met by persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts. This regulation establishes minimum standards to be met in connection with the safeguarding of personal information contained in both paper and electronic records. Further purposes are to (i) ensure the security and confidentiality of such information in a manner consistent with industry standards, (ii) protect against anticipated threats or hazards to the security or integrity of such information, and (iii) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud against such residents.

(b) Scope

The provisions of this regulation apply to all persons that own, license, store or maintain personal information about a resident of the Commonwealth.

17.02: Definitions

The following words as used herein shall, unless the context requires otherwise, have the following meanings:

"Breach of security", the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. A good faith but unauthorized acquisition of personal information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the personal information is used in an unauthorized manner or subject to further unauthorized disclosure.

"Electronic," relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

"Encrypted," the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the office of consumer affairs and business regulation.

"Person," a natural person, corporation, association, partnership or other legal entity, other than an agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any of its branches, or any political subdivision thereof.

"Personal information," a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

"Record" or "Records," any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

17.03: Duty to Protect and Standards for Protecting Personal Information

Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information. Such comprehensive information security program shall be reasonably consistent with industry standards, and shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records. Moreover, the

safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns, licenses, stores or maintains such information may be regulated.

Whether the comprehensive information security program is in compliance with these regulations for the protection of personal information, whether pursuant to section 17.03 or 17.04 hereof, shall be evaluated taking into account (i) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information. Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

- (a) Designating one or more employees to maintain the comprehensive information security program;
- (b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: (i) ongoing employee (including temporary and contract employee) training; (ii) employee compliance with policies and procedures; and (iii) means for detecting and preventing security system failures.
- (c) Developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.
- (d) Imposing disciplinary measures for violations of the comprehensive information security program rules.
- (e) Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.
- (f) Taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including (i) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (ii) contractually requiring service providers to maintain such safeguards. Prior to permitting third-party service providers access to personal information, the person permitting such access shall obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations.
- (g) Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limiting the time such information is retained to that reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.
- (h) Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information.
- (i) Reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers.
- (j) Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.
- (k) Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- (l) Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, shall have the following elements:

- (1) Secure user authentication protocols including:
 - (i) control of user IDs and other identifiers;
 - (ii) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
 - (iii) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
 - (iv) restricting access to active users and active user accounts only; and
 - (v) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;
- (2) Secure access control measures that:
 - (i) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
 - (ii) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;
- (3) To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data to be transmitted wirelessly.
- (4) Reasonable monitoring of systems, for unauthorized use of or access to personal information;
- (5) Encryption of all personal information stored on laptops or other portable devices;
- (6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.
- (7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
- (8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

17.05: Effective Date

These regulations shall take effect on January 1, 2009.

REGULATORY AUTHORITY:
201 CMR 17.00: M.G.L. c. 93H

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

See a sample reprint in PDF format.

Order a reprint of this article now

THE WALL STREET JOURNAL

WSJ.com

TECHNOLOGY | OCTOBER 16, 2008

New Data Privacy Laws Set For Firms

By BEN WORTHEN

Alicia Granstedt, a Las Vegas-based hair stylist who works for private clients and on movie sets, never worried about conducting most of her business through email.

Ms. Granstedt regularly receives emails from customers containing payment details, such as credit-card numbers and bank-account transfers. Since she travels frequently, she often stores the emails on her iPhone.

But a Nevada law that took effect this month requires all businesses there to encrypt personally-identifiable customer data, including names and credit-card numbers, that are transmitted electronically.

After hearing about the new law, Ms. Granstedt started using email-encryption software, which requires her clients to enter a password to read her messages and send responses. It is a hassle, "but I can't afford to be responsible for someone having their identity stolen," she said.

Nevada is the first of several states adopting new laws that will force businesses -- from hair stylists to hospitals -- to revamp the way they protect customer data. Starting in January, Massachusetts will require businesses that collect information about that state's residents to encrypt sensitive data stored on laptop computers and other portable devices. Michigan and Washington state are considering similar regulations.

While just a few states have adopted such measures so far, the new patchwork of regulations is something many businesses will have to navigate, since the laws apply to out-of-state companies with operations or customers in those states.

That's one reason the Massachusetts law has the attention of Andrew Speirs, information security officer for National Life Group, an insurance company based in Montpelier, Vt. "We do business in all 50 states so we're definitely reviewing it," he said. Mr. Speirs said that National Life has a program in place to protect data, but that the Massachusetts law "is a little more particular" than other state laws. He is checking his company's program for any holes.

While it isn't clear if state authorities intend to crack down on mom-and-pop businesses -- the attorney general in Massachusetts is still developing an

enforcement policy, a spokeswoman said -- the laws establish a liability that could be used in civil suits against businesses following a data breach, privacy lawyers said.

In Nevada, companies that suffer a security breach but comply with the new law would cap their damages at \$1,000 per customer for each occurrence. Those that don't comply would be subject to unlimited civil penalties under the proposed enforcement plan, said James Earl, executive director of the state's task force for technological crimes.

Some businesses have already started buying security technology in anticipation of the new laws. Papa Gino's Inc., a Dedham, Mass.-based pizza and sandwich chain, began purchasing laptops with encrypted hard drives from Dell Inc. for its workers last year. Dell sells these computers for about \$100 more than those with unencrypted drives. So far, the company has bought about 80 of the computers.

Papa Gino's is also purchasing encryption software -- which costs about \$50 per computer -- to protect files containing sensitive information on the 170 or so laptops that don't have encrypted drives, said Chris Cahalin, manager of network operations for the company, which has 370 locations.

The new regulations mean "anybody in IT has to become a security guy," he said.

Getting compliant with the new laws will require most businesses to open their wallets. According to Forrester Research, about 31% of large corporations and 22% of small- and medium-size firms currently have at least some laptops with encrypted hard drives, a way of protecting information on a computer if it is lost or stolen.

The Massachusetts government estimates that a business with 10 employees will need to spend \$3,000 up front, plus an additional \$500 a month in order to comply. Security executives at larger firms said they expect to spend a similar amount per employee.

Partners HealthCare System Inc., a Boston-based hospital operator, will have to spend more than \$100,000 to comply with the new regulations, said Karen Grant, the company's chief privacy officer. Partners is looking into encryption for laptops and technology that can trace lost or stolen devices.

The company may need to reprioritize its current projects in order to get the new technology in place by January, said Ms. Grant. "It's a burden," she added, "but it's something you have to do."

The new state data-security laws are stricter than past regulations, which only required businesses to notify people whose personal information they lost. The new laws establish a standard that can be used by plaintiffs in civil suits to argue that a business that lost data was negligent, said Miriam Wugmeister, an

attorney with Morrison & Foerster LLP.

The so-called breach-notification laws, which were enacted in more than 40 states, ended up doing little to tamp down security breaches.

So far this year, more than 500 organizations have publicly disclosed a breach, up from the 446 disclosed in all of 2007, according to the Identity Theft Resource Center, a San Diego nonprofit group. In a September study, researchers at Carnegie Mellon University found that notification laws only reduce identity theft by around 2%.

"Breach-notification laws deal with what happens after the horse leaves the barn," said Daniel Crane, undersecretary of the Massachusetts Office of Consumer Affairs and Business Regulation. The new regulation in his state "is intended to prevent the horse from getting out of the barn in the first place."

Write to Ben Worthen at ben.worthen@wsj.com

Copyright 2008 Dow Jones & Company, Inc. All Rights Reserved
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com