WSGR ALERT

MAY 2010

NEW WASHINGTON STATE DATA SECURITY LAW EFFECTIVE JULY 1, 2010; COMPANIES SHOULD ASSESS COMPLIANCE WITH SEVERAL NEW STATE DATA SECURITY LAWS

A new Washington state law, effective on July 1, 2010,[1] will give financial institutions a cause of action against certain entities involved in payment card transactions that fail to take reasonable care to guard against unauthorized access to payment card information, where that failure is found to be the proximate cause of a data security breach.

The Washington statute is the third state law to incorporate all or a portion of the Payment Card Industry Data Security Standard (PCI DSS), the industry data security standard for the protection of credit card numbers and other payment card information.[2] Minnesota's 2007 Plastic Card Security Act adopted portions of the PCI DSS, and Nevada statutory amendments effective on January 1, 2010, required companies doing business in Nevada that accept credit card payments to comply with the PCI DSS in its entirety.

These state laws are part of a trend toward greater specificity, and more substantial burdens for businesses, in state data security laws.

The following WSGR Alert summarizes the key provisions of Washington's new statute and provides brief overviews of related laws and regulations in Massachusetts, Nevada, and Minnesota.

Washington Law

Washington's new law applies to businesses, processors, and vendors, all of which are defined in the bill. A "business" is defined as an entity "that processes more than six million credit card and debit card transactions annually, and who provides, offers, or sells goods or services" to Washington residents. A "processor" is defined as an entity "that directly processes or transmits account information for or on behalf of another person as part of a payment processing service." A "vendor" is defined as an entity "that manufactures and sells software or equipment that is designed to process, transmit, or store account information or that maintains account information it does not own."

The law provides for processors and businesses whose failure to "take reasonable care to guard against unauthorized access" to account information in their possession or control, where that failure is found to be the proximate cause of a breach in which account information is compromised, to be liable to a financial institution for "reimbursement of reasonable actual costs related to the reissuance of credit and debit cards" incurred by the financial institution in efforts to mitigate current or future damages to its cardholders. It also provides for a vendor to be liable to a financial institution for the same damages, to the extent that the damages were proximately caused by the vendor's negligence, unless the claim is limited by another law or by contract.

"Account information" is defined as: (i) the full, unencrypted magnetic stripe of a credit card or debit card; (ii) the full, unencrypted account information contained on an identification device; or (iii) the unencrypted primary account number on a credit card or debit card or identification device, together with an unencrypted cardholder name, expiration date, or service code. An "identification device" is defined as "an item that uses radio frequency identification technology or facial recognition technology."

A "breach," for purposes of the law, has the same meaning as defined under Washington's security breach notification law: that is, the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. "Personal information" is defined in Washington's breach notification statute as an individual's name together with any of the following elements, when both the name and element are not encrypted: (i) Social Security number, (ii) driver's license number or Washington identification card number, or (iii) account number, credit card number, or debit card number, together with any required security

[1] Wash. H.B. 1149 (2010), *available at* http://apps.leg.wa.gov/documents/billdocs/2009-10/Pdf/Bills/Session%20Law%202010/1149-S2.SL.pdf.

[2] The PCI DSS is a standard consisting of six principles and twelve accompanying requirements. *See* https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

Continued on page 2...

New Washington State Data Security Law . . .

Continued from page 1...

code, access code, or password permitting access to an individual's financial account.

Washington's law exempts entities from liability if the account information was encrypted at the time of the breach or if the business was "certified compliant with the payment card industry data security standards" in effect at the time of the breach. The bill specifies that a business will be considered "compliant" if its PCI DSS compliance was validated by an annual security assessment that took place no more than one year prior to the breach.

Minnesota Plastic Card Security Act

Washington's statute comes on the heels of two prior efforts to codify all or part of the PCI DSS. The pioneering effort, Minnesota's 2007 Plastic Card Security Act,[3] prohibits the retention of card security code data, PIN verification codes, or the full contents of magnetic stripe data for more than 48 hours after authorization of a transaction.

The Minnesota statute provides that in the event of a security breach, any person or entity that has violated the law and that processes 20,000 or more transactions per year must reimburse a financial institution affected by the breach for the costs of reasonable actions undertaken to protect the information of its cardholders.

The Minnesota law specifies that these actions may include, but are not limited to, the following:

- cancelling existing debit or credit cards and replacing such cards;
- closing any financial accounts affected by the breach, as well as undertaking actions to stop payments or block transactions with respect to the financial accounts;
- opening or reopening any financial accounts affected by the security breach;
- issuing refunds or credits to cardholders to cover the costs of unauthorized transactions related to the breach; and
- notifying cardholders affected by the breach.

Nevada Statutory Amendments

Amendments to Nevada's laws pertaining to the security of personal information,[4] effective on January 1, 2010, require all "data collectors" who are "doing business in" Nevada and who accept credit cards or other payment cards for the sale of goods or services to comply with the current version of the PCI DSS.[5] As of the date of this alert, the amended Nevada statute is the only state law that makes compliance with the PCI DSS a specific legal obligation.

Nevada's amended statute further requires companies doing business in Nevada to encrypt personal information when it is transferred electronically "outside of the secure system" of the company, or when a data storage device, such as a computer, cellular telephone, computer drive or tape, etc., containing personal information is transferred beyond the company's "logical or physical controls."[6]

The Nevada statutory amendments repealed a statute in effect since 2008 that had required encryption of personal information transferred outside of a company, but had defined "encryption" in a broad manner. Nevada's amended statute now defines permitted encryption methods with greater specificity.

Nevada's amended statutes provide a safe harbor for data collectors, providing that a data collector "shall not be liable for damages for a breach of the security of the system data" if the data collector is in compliance with the requirements of Nevada's data security statute and the breach is not caused by the gross negligence or willful misconduct of the data collector, its officers, employees, or agents.

Massachusetts Data Security Rules

On March 1, 2010, data security regulations adopted by the Massachusetts Office of Consumer Affairs and Business Regulation[7] went into effect. Unlike the Washington, Minnesota, and Nevada statutes, the Massachusetts regulations are not limited to payment transactions, but apply to any entity that owns, licenses, stores, or maintains personal information about Massachusetts residents.[8]

---

[3] Minn. Stat. § 325E.64.

[4] Nev. Rev. Stat. Ch. 603A.

[5] *See* Nev. SB 227 (2009).

[6] The Nevada statute defines "personal information" to include a person's first name or first initial and last name with (i) Social Security number, (ii) driver's license or identification card number, or (iii) financial account number (with security code, access code, or password).

"Encryption" is defined by the Nevada statute as the protection of data in electronic or optical form, in storage or transit, using (a) encryption technology adopted by an established standards-setting body, such as the National Institute of Standards and Technology (NIST), and (b) "[a]ppropriate management and safeguards of cryptographic keys" promulgated by an established standards-setting body, such as the NIST.

[7] 201 Mass. Code Regs. 17, as authorized under Mass. Gen. Laws Ann. Ch. 93H.

[8] "Personal information" is defined to include a combination of a resident's first and last name and Social Security number, driver's license or state ID number, or financial account number or payment card number that would permit access to the individual's financial account.

Continued on page 3...

New Washington State Data Security Law . . .

Continued from page 2...

The Massachusetts regulations require all companies that own or license personal information about Massachusetts residents to develop, implement, and maintain a written, comprehensive information security program that contains administrative, technical, and physical safeguards that are appropriate to: (a) the size, scope, and type of its business; (b) the amount of resources available to it; (c) the amount of stored data that it maintains; and (d) the need for security and confidentiality of both consumer and employee personal information. The regulations also specify a number of particular safeguards that the required information security program must include.

Additionally, the regulations specify that all entities that own or license personal information about a Massachusetts resident and electronically store or transmit such information must include in its written security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, "to the extent technically feasible," contains eight required elements.

Notably, the required technical elements require encryption of "all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly," as well as "all personal information stored on laptops or other portable devices." The definition of encryption, however, is relatively flexible and permissive. "Encrypted," under the Massachusetts regulations, means "the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key."[9]

Impact of the New State Laws and Regulations

These new state data security statutes may appear to impose significant new burdens upon businesses. In most respects, however, they simply provide specific directives to businesses to comply with more general obligations to which they may already be bound, and provide additional financial incentives for businesses to comply with those obligations.

First, regarding the laws adopting all or part of the PCI DSS, any business that accepts credit cards is likely already bound by contract to comply with the PCI DSS. Compliance with the PCI DSS, and with card-brand-specific security standards prior to the PCI DSS being created, has been required for several years, and credit card companies have reserved the right to levy hefty fines upon merchants that suffer a breach of credit card data and were not in compliance with the PCI DSS or its predecessors at the time of the breach. More recently, payment card brands have provided financial incentives to companies to become certified against the PCI DSS. From a practical standpoint, companies that fail to comply with the PCI DSS also may find it difficult to obtain a merchant account.

The Minnesota Plastic Card Security Act simply made mandatory one aspect of PCI DSS compliance—not storing security codes, full payment card magnetic stripe information, or PIN codes—and gave financial institutions an explicit means to recover the costs of dealing with a breach resulting from a failure to comply with that obligation.

The new Washington statute simply allocates liability in the event of a data security breach suffered by large merchants and credit card processors, but provides an exemption for those that have undergone annual security assessments to maintain PCI DSS compliance. This exemption provides an additional incentive for companies to comply with the PCI DSS.

The Nevada statute requires PCI DSS compliance, but does not identify a party responsible for enforcing the law, and does not provide a private right of action. The statute's broad safe harbor for entities that are in compliance with the requirements of the statute, however, also should provide a significant incentive for companies to comply with the PCI DSS and with the statute's additional encryption requirements.

Second, as for the Massachusetts regulations, many other states long have had general data security laws that obligate companies to use reasonable measures to protect the security and confidentiality of personal information pertaining to those states' residents,[10] and require that companies take reasonable steps to dispose of records containing personal information.[11] Also, many states have had laws imposing various protections upon the use, display, and disclosure of Social Security numbers, including requirements that Social Security numbers be encrypted or transmitted over a secure connection when transmitted online.[12]

The Massachusetts regulatory effort is, however, the first requirement under state law to require a written information security plan and to elucidate the required elements of the plan. It is most notable for its explicit

---

[9] Finally, the regulations require covered entities to take steps to select and retain service providers that are capable of appropriately safeguarding personal information in accordance with the Massachusetts regulations and any applicable federal regulations. Covered entities must require all service providers to safeguard personal information by contract in accordance with the Massachusetts regulations and applicable federal requirements. The regulations do, however, exempt existing service provider contracts (i.e., entered into prior to March 1, 2010) from complying with this requirement until March 1, 2012.

[10] *See, e.g.*, Cal. Civ. Code § 1798.81.5(b); Ore. Rev. Stat. § 646A.622; Tex. Bus. & Com. Code Ann. § 48.102(a).

[11] *See, e.g.*, Cal. Civ. Code § 1798.81 (providing that "[a] business shall take all reasonable steps to dispose, or arrange for the disposal, of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means."

[12] *See, e.g.*, Cal. Civ. Code § 1798.85; N.Y. Gen. Bus. Law § 399-dd.

Continued on page 4...

New Washington State Data Security Law . . .

Continued from page 3...

obligations regarding encryption and for addressing data security obligations in contracts with third-party service providers. Previous versions of the Massachusetts regulations had contained obligations that were much more onerous for covered companies, but the regulations as adopted still will present significant compliance burdens for companies with employees or customers located within Massachusetts, as well as service providers that provide relevant services to such companies.

Conclusion

Generally, these new state laws and regulations emphasize the importance of data security and evidence a clear trend toward expanded obligations to protect payment card information and other types of personal information. Companies should assess the scope and nature of their operations, particularly in view of the Massachusetts regulations, and consider whether they need to make internal changes in order to comply.

The attorneys of Wilson Sonsini Goodrich & Rosati routinely counsel clients on compliance with state and federal data security laws and regulations, as well as other privacy and data security issues. If you have questions in these areas, please contact Lydia Parnes at (202) 973-8801, Sara Harrington at (650) 320-4915, or Matt Staples at (206) 883-2583.

WSGR

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on May 19, 2010. To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.

650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com