RECENT STATE DATA PRIVACY LAWS AND COURT DECISIONS IMPOSE EXTENSIVE OBLIGATIONS ON COMPANIES THAT COLLECT AND PROCESS PERSONAL INFORMATION

During the latter part of 2008, state legislatures, agencies, and courts have been increasingly active in imposing more stringent requirements on companies that do business in their states regarding the companies' disclosure, safeguarding, and disposal of the nonpublic personal information they collect. In particular:

- Massachusetts' Regulation Regarding Safeguarding of Personal Information mandates that companies develop and implement by January 1, 2009 a comprehensive, written personal information security program that includes a host of specific and potentially costly obligations;
- Nevada's Encryption Law, effective October 1, 2008, is the first state law that mandates encryption for the electronic transmission of customer personal information (faxes exempted);
- Connecticut's Law on Social Security numbers ("SSN" or "SSNs") requires that, effective October 1, 2008, companies create and display a new privacy protection policy concerning the collection and disclosure of SSNs; and
- In *American Bankers Assoc. v. Lockyer*, the Ninth Circuit held that California privacy law "SB1" is not preempted by federal privacy law and imposes more stringent affiliate-sharing rules on companies for all nonpublic personal information except for consumer report information.

Companies doing business in these states must carefully review these new requirements and develop and implement compliance procedures to protect adequately the nonpublic personal information they collect, store, and distribute.

Massachusetts' Regulations Requiring Comprehensive Security Programs and Enhanced Data Security

On September 19, 2008, the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") issued a set of sweeping new regulations ("Regulations"), which become effective on January 1, 2009, in an effort to better safeguard consumers' personal information.[1]

The Regulations require all "persons" (which includes corporations and certain other legal entities[2])

[1] Massachusetts Rule 201 CMR 17.00: M.G.L. c. 93H.

[2] The definition of "person" includes 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. *Id.* at § 17.02.

that own, license, store, or maintain "personal information"[3] about Massachusetts residents to develop, implement, maintain, and monitor a comprehensive, written information security program applicable to any records containing such personal information. This program must: (i) be reasonably consistent with industry standards; (ii) contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records; and (iii) be consistent with the safeguards required for information of similar character as set forth in any state or federal regulations by which the person who owns, licenses, stores, or maintains such information may be regulated.[4]

Specifically, every comprehensive information security program must include the following elements:

- Designating one or more employees to maintain the information security program;
- 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;
- 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;
- Imposing disciplinary measures for violations of the information security program rules;
- 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;
- Taking reasonable steps, including through contracts, to ensure that third-party service providers with access to personal information have the capacity to protect such personal information, and that service providers also have written, comprehensive information security programs that are in compliance with the provisions of the Regulations;

---

[3] "Personal information" is defined as 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) SSN; (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. *Id.*

[4] *Id*. at § 17.03.

- 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;
- Imposing reasonable restrictions on physical access to records containing personal information;
- 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;
- 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; and
- 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.

In addition to the foregoing obligations, the Regulations require, among other things, the establishment and maintenance of a security system covering computers, including any wireless systems, which:

- Employs secure user authentication protocols covering the use of user IDs and passwords; restricts access to personal information on a need-to-know basis; and conducts periodic system monitoring for signs of unauthorized use or access;
- Encrypts to the extent technically feasible all transmitted records and files containing personal information that will travel across public networks, and encrypts all data that is to be transmitted wirelessly or stored on laptops or other portable devices;
- Ensures 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; and
- Ensures education and training of employees on the proper use of the computer security system and the importance of personal information security.

Dan Crane, Undersecretary of OCABR, has stated that the Regulations are "necessary because of the growing concern among consumers about the large number of breaches of data containing their personal information."[5] Crane further explained that these guidelines "promise to give consumers

[5] Todd Wallack, "Tougher consumer data rule adopted: Businesses must improve safeguards," *The Boston Globe*, 23 Sept. 2008, http://www.boston.com/business/articles/2008/09/23/tougher_consumer_data_rule_adopted/.

greater peace of mind that every effort is being made to minimize their exposure to identity theft and fraud."[6] There is no requirement that a person or company maintain a place of business or conduct operations in Massachusetts for the Regulations to apply.

The above list is not exhaustive with respect to which procedures companies may implement to comply with the Regulations. Each company's compliance plan is expected to be evaluated differently by Massachusetts, based upon: (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.

Due to the highly comprehensive nature of the Regulations, it is likely that many companies may not currently have policies and procedures in place to cover each of the aforementioned requirements. Therefore, it is important for companies subject to the Regulations to have their policies and procedures reviewed to ensure compliance by the January 1, 2009 effective date.

Nevada's Encryption Law to Protect Personal Information

Nevada has enacted a new data security law ("Law"), effective October 1, 2008, that mandates encryption for the transmission of customer personal information.[7]

Specifically, the Law states that a "business in this State shall not transfer any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission."[8]

As the text of this Law is brief and Nevada has not yet issued any guidance on the Law, some important open questions remain. For instance, what does it mean to be a "business in this State"?

---

[6] Office of Consumer Affairs and Business Regulation, "Patrick Administration Issues Comprehensive Identity Theft Prevention Regulations & Executive Order: New data security breach report shows ongoing risks for consumers, need for businesses to improve security standards," Massachusetts Rule 201 CMR 17.00: M.G.L. c. 93H, http://www.mass.gov/?pageID=ocapressrelease&L=1&L0=Home&sid=Eoca&b=pressrelease&f=080922_IDTheft_regsandexecorder&csid=Eoca (Sept. 22, 2008).

[7] "Personal information" means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:

1. SSN.
2. Driver's license number or identification card number.
3. Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to the person's financial account.

The term does not include the last four digits of a SSN or publicly available information that is lawfully made available to the general public. *Nev. Rev. Stat.* § 597.970 (2007).

[8] "Encryption" means the use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding, or a computer contaminant, to:

1. Prevent, impede, delay, or disrupt access to any data, information, image, program, signal, or sound;
2. Cause or make any data, information, image, program, signal, or sound unintelligible or unusable; or
3. Prevent, impede, delay, or disrupt the normal operation or use of any component, device, equipment, system, or network. *Id.*

Perhaps one can look to a previous decision of the Nevada Supreme Court, which interpreted whether a company was "doing business" in Nevada by employing a two-pronged fact-sensitive test, which takes into consideration: (i) the nature of the company's business in the state; and (ii) the quantity of business conducted by the company in the state.[9] Other terms and phrases contained in the Law that are open to interpretation are the definition of "customer" and the meaning of "secure system of the business."

Until further guidance is issued by the state, the practical effect of the Law is to require that companies with more than minimal business contacts in Nevada should encrypt the personal information that such companies transmit electronically outside their secure systems.

Connecticut's Safeguarding and Disposal Rule for Personal Information

Effective October 1, 2008, a new Connecticut privacy law ("Privacy Law") requires companies to: (i) create and display a "privacy protection policy" concerning the collection and use of SSNs; and (ii) safeguard and properly dispose of "personal information."[10]

Specifically, the Privacy Law mandates that companies create a privacy protection policy if they collect SSNs in the course of business. This new policy shall: (i) protect the confidentiality of SSNs; (ii) prohibit unlawful disclosure of SSNs; and (iii) limit access to SSNs. The Privacy Law requires the privacy protection policy to be published or "publicly displayed," which includes, but is not limited to, posting the policy on an Internet web page. However, the Privacy Law does not further explain the phrase "publicly displayed," and does not define the term "published."[11]

The new requirements of the Privacy Law are in addition to Connecticut's existing law contained in the Connecticut General Statutes § 42-470 that restricts the use and display of SSNs. Among other restrictions, § 42-470 forbids the intentional public display or public posting of an individual's SSN and restricts a company from requiring an individual to use or transmit his/her SSN over the Internet.[12]

The Privacy Law also requires any person in possession of the personal information of another person to: (i) safeguard the data, computer files, and documents containing the personal information from misuse by third parties; and (ii) "destroy, erase or make unreadable such data, computer files and documents prior to disposal."[13] It is important to note that these requirements differ from the current Securities and Exchange Commission and Federal Trade Commission

---

[9] *Executive Mgmt. Ltd. v. Ticor Title Ins. Co.*, 38 P.3d 872 (Nev. 2002).

[10] *An Act Concerning the Confidentiality of Social Security Numbers*, H.B. 5658, Pub. Act. No. 08-167, 2008 Gen. Assem., Feb. Sess. (Conn. 2008). "Personal information" is defined under the Privacy Law as information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a SSN, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number, or a health insurance identification number.

[11] *Id*.

[12] Conn. Gen. Stat. § 42-470 (2003).

[13] *An Act Concerning the Confidentiality of Social Security Numbers*, H.B. 5658, Pub. Act. No. 08-167, 2008 Gen. Assem., Feb. Sess. (Conn. 2008).

Disposal Rules, which apply to a more limited scope of information, namely consumer report information.[14] Another difference is that the Privacy Law specifically enumerates the methods of disposal that it requires (as described above), unlike the aforementioned federal rules, which merely offer guidelines as to proper disposal.[15]

An *intentional* violation of the Privacy Law could be very costly, with a civil penalty of $500 per violation and a maximum penalty of $500,000 for any "single event" (undefined in statute). Accordingly, any entity or individual that does business in Connecticut should consider implementing the policies described in the Privacy Law, and devising procedures to ensure their proper execution.

Ninth Circuit's Partial Reinstatement of California's SB1 Affiliate-Sharing Restrictions

On September 4, 2008, the Court of Appeals for the Ninth Circuit partially reinstated the affiliate-sharing restrictions pertaining to nonpublic personal information contained in California's privacy law known as "SB1."[16]

One of SB1's provisions contains a notice and opt-out requirement for a financial institution[17]

---

[14] Regulation S-P, *17 C.F.R. § 248.30(b)*, Consumer report information means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer report information also means a compilation of such records. Consumer report information does not include information that does not identify individuals, such as aggregate information or blind data; FTC Privacy Rule, *16 C.F.R. § 682*, "Consumer Report" includes information obtained from a consumer reporting company that is used – or expected to be used – in establishing a consumer's eligibility for credit, employment, or insurance, among other purposes. Credit reports and credit scores are consumer reports. So are reports businesses or individuals receive with information relating to employment background, check writing history, insurance claims, residential or tenant history, or medical history.

[15] *See* Regulation S-P, *17 C.F.R. § 248.30(b);* FTC Privacy Rule, *16 C.F.R.§ 682.*

[16] *Am. Bankers Ass'n v. Lockyer*, No. 05-17163, 2008 WL 4070308 (9th Cir. Sept. 4, 2008). *California Financial Information Privacy Act, California Financial Code* § 4050 *et seq.*

[17] "Financial institution" means any institution the business of which is engaging in financial activities as described in § 1843(k) of Title 12 of the United States Code and doing business in California. An institution that is not significantly engaged in financial activities is not a financial institution. The term "financial institution" does not include: (i) any institution that is primarily engaged in providing hardware, software, or interactive services, provided that it does not act as a debt collector, as defined in 15 U.S.C. § 1692a, or participate in activities for which the institution is required to acquire a charter, license, or registration from a state or federal governmental banking, insurance, or securities agency; (ii) the Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. § 2001 et seq.), provided that the entity does not sell or transfer nonpublic personal information to an affiliate or a nonaffiliated third party; (iii) institutions chartered by Congress specifically to engage in a proposed or actual securitization, secondary market sale, including sales of servicing rights, or similar transactions related to a transaction of the consumer, as long as those institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party; (iv) any provider of professional services, or any wholly owned affiliate thereof, that is prohibited by rules of professional ethics and applicable law from voluntarily disclosing confidential client information without the consent of the client; or (v) any person licensed as a dealer under Article 1 (commencing with § 11700) of Chapter 4 of Division 5 of the Vehicle Code that enters into contracts for the installment sale or lease of motor vehicles pursuant to the requirements of Chapter 2B (commencing with Section 2981) or 2D (commencing with § 2985.7) of Title 14 of Part 4 of Division 3 of the Civil Code and assigns substantially all of those contracts to financial institutions within 30 days. *California Financial Information Privacy Act, California Financial Code* § 4052(c).

seeking to share "nonpublic personal information"[18] with an affiliate.[19] In 2004, the American Bankers Association, the Financial Services Roundtable, and the Consumer Bankers Association challenged the validity of the affiliate-sharing restrictions in SB1 in federal court, claiming that the Fair Credit Reporting Act ("FCRA")[20] preempted the SB1 restrictions.[21] Their allegations were based on the fact that the FCRA contains its own affiliate-sharing requirements, and that § 625(b)(2) of the FCRA preempts states from regulating the exchange of information among affiliates. However, a key distinction between the affiliate-sharing restrictions in SB1 and those contained in the FCRA (which becomes critical in the 2008 Ninth Circuit decision) is that the FCRA's affiliate-sharing restrictions apply *solely* to consumer report[22] information, whereas SB1's affiliate-sharing restrictions apply more broadly to nonpublic personal information.

In 2005, the district court in *ABA v. Lockyer* held that the FCRA preempted the affiliate-sharing provisions of SB1 in their entirety.[23] On September 4, 2008, the Ninth Circuit reversed, holding that the FCRA preempts the affiliate-sharing provisions of SB1 *only* to the extent that the SB1 provisions regulate the sharing of consumer report information with affiliates.[24] Therefore, the court determined that SB1's provisions regulating the sharing of *other* nonpublic personal information with affiliates are *not* preempted. The court reasoned that it must interpret the statute to allow this partial affiliate-sharing restriction provision, given that the Legislature's intent "clearly would be furthered by application of the revised version rather than by the alternative of invalidation."[25]

---

[18] "Nonpublic personal information" means personally identifiable financial information: (i) provided by a consumer to a financial institution, (ii) resulting from any transaction with the consumer or any service performed for the consumer, or (iii) otherwise obtained by the financial institution. Nonpublic personal information does not include publicly available information that the financial institution has a reasonable basis to believe is lawfully made available to the general public from: (1) federal, state, or local government records; (2) widely distributed media; or (3) disclosures to the general public that are required to be made by federal, state, or local law. Nonpublic personal information shall include any list, description, or other grouping of consumers, and publicly available information pertaining to them, that is derived using any nonpublic personal information other than publicly available information, but shall not include any list, description, or other grouping of consumers, and publicly available information pertaining to them that is derived without using any nonpublic personal information. *Id*. at 4052(a).

[19] It should be noted that it has been a practice for a number of years, both at the federal and state level (including California), to require a notice and opt-out clause for sharing between *non*-affiliates.

[20] 15 U.S.C. § 1681 *et seq.*

[21] *Am. Bankers Ass'n v. Lockyer*, 2004 WL 149030 (2004).

[22] As defined by FCRA, a consumer report is "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for: A) credit or insurance to be used primarily for personal, family, or household purposes; B) employment purposes; or C) any other purpose authorized under § 1681b of the FCRA." 15 U.S.C. § 1681a(d)(1).

[23] *Am. Bankers Ass'n. v. Lockyer*, No. Civ. S 04-07798 MCE KJM (E.D. Cal., Oct. 5, 2005).

[24] *Am. Bankers Association v. Lockyer*, No. 05-17163, 2008 WL 4070308 (9th Cir. Sept. 4, 2008).

[25] *Id.*

The practical effect of this decision is that a financial institution doing business in California and collecting nonpublic personal information beyond consumer report information should review its privacy notices and procedures to ensure that it is in compliance with the affiliate-sharing restrictions of SB1.[26]

* * * * * * * * * * * * * * *

If you have any questions regarding this memorandum, please contact, Francis M. Buono (202-303-1104, fbuono@willkie.com), Marc J. Lederer (212-728-8624, mlederer@willkie.com), McLean B. Sieverding (202-303-1163, msieverding@willkie.com), Melissa A. Troiano (202-303-1183, mtroiano@willkie.com), or the attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099 and has an office located at 1875 K Street, NW, Washington, DC 20006-1238. Our New York telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our Washington, DC telephone number is (202) 303-1000 and our facsimile number is (202) 303-2000. Our website is located at www.willkie.com.

October 10, 2008

[26] However, it should be noted that SB1, much like Regulation S-P and the FTC Privacy Rule, also contains exceptions to its opt-out clause requirements. One of the opt-out exceptions that is commonly relied upon for sharing with affiliates can be utilized when the nonpublic personal information is "necessary to effect, administer, or enforce a transaction requested or authorized by the consumer, or in connection with servicing or processing a financial product or service requested or authorized by the consumer, or in connection with maintaining or servicing the consumer's account with the financial institution." *California Financial Information Privacy Act, California Financial Code* § 4056(b)(1).