UIC John Marshall Journal of Information Technology & Privacy Law

Volume 31 | Issue 4 Article 4

Spring 2015

Selected State Laws Governing the Safeguarding and Disposing of Personal Information, 31 J. Marshall J. Info. Tech. & Privacy L. 487 (2015)

Bruce Radke

Michael Waters

SELECTED STATE LAWS GOVERNING THE SAFEGUARDING AND DISPOSING OF PERSONAL INFORMATION

BRUCE RADKE, ESQ. & MICHAEL J. WATERS*

Numerous states have adopted laws mandating the protection and disposal of personal information. Under those laws, businesses are required to implement and maintain reasonable security procedures and practices appropriate to the nature of the information in order to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

Although the definition of "personal information" varies from state to state, "personal information" is generally defined as an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (1) Social Security number; (2) driver's license number or other state-issued identification card number; or (3) account number, credit or debit card number, or another account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

The scope of these state laws may be broad, imposing a duty not only on a business that is physically located in one of those states but also extends to any business located outside of the state that obtains personal information from residents of those states. Certain states' laws not only require that the business undertake sufficient measures to protect personal information in its possession, but, to the extent that personal information is provided to third parties, those laws require that the business contractually require the third parties to implement and maintain reasonable security measures to safeguard the personal in-

* Bruce Radke, Esq. & Michael J. Waters are co-chairs of Vedder Price P.C.'s Data Privacy and Information Management practice group.

formation that has been disclosed to third parties.

The nature and extent of these requirements vary greatly from state to state. Certain states, such as Indiana and Texas, generally require that covered businesses implement and maintain "reasonable procedures" to protect against the unauthorized access to or disclosure of personal information of their states' residents.[1] In contrast, Massachusetts and Oregon have adopted statutory or regulatory requirements that provide for detailed safeguards to ensure the security and confidentiality of records (both hardcopy and electronic) containing personal information of their residents.[2]

Massachusetts law mandates that every business covered by the Massachusetts Data Security Regulations develop, implement and maintain a comprehensive written information security program ("WISP") applicable to records (both paper and electronic) containing personal information of a Massachusetts resident.[3] The WISP must contain minimum:

> [A]dministrative, technical, and physical safeguards that are appropriate to:
>
> (a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;
>
> (b) the amount of resources available to such person;
>
> (c) the amount of stored data; and
>
> (d) the need for security and confidentiality of both consumer and employee information.[4]

Likewise, Oregon's Consumer Identity Theft Protection Act requires that businesses covered by the Act implement an information security program that includes certain minimum administrative, technical, and physical safeguards. These, include conducting a risk assessment to identify the reasonably foreseeable internal and external risks to the personal information of Oregon residents maintained by the business, employee training on the business's information security program practices and procedures, and testing and monitoring of key controls, systems, and procedures.[5]

Further, Oregon and Nevada impose an affirmative obligation on a business to dispose of records (both physical and electronic) containing personal information after such records are "no longer needed for busi-

---

1. TEX. BUS. & COM. CODE ANN. § 521.052(a) (2015); IND. CODE § 24-4.9-3-3.5 (2015).
2. 201 MASS. CODE REGS. 17.02 (2015); OR. REV. STAT. § 646A.602(11) (2015).
3. 201 MASS. CODE REGS. 17.03(1) (2015).
4. *Id*.
5. OR. REV. STAT. § 646A.622 (2015).

ness purposes" or when "the business decides that it will no longer maintain the records."[6] Those states' laws also impose certain requirements regarding the method for disposing of such records by burning, pulverizing, shredding, or modifying a physical record and destroying or erasing electronic media so that the information cannot be read or reconstructed.[7]

In addition to these security procedures and measures necessary to proactively protect personal information from unauthorized access, destruction, use, modification or disclosure, federal and state laws require organizations to notify affected individuals (and in some instance regulators, the media, and credit agencies) in the event of a data breach.[8]

I. MASSACHUSETTS

A. SCOPE OF THE REGULATIONS

The Massachusetts Data Security Regulations, 201 Mass. Code. Regs. 17.00-05 (the "Massachusetts Regulations"), establishes certain minimum requirements to safeguard personal information obtained from Massachusetts residents.[9] The Massachusetts Regulations are broad in their scope, covering any "person that owns or licenses personal information about a resident of [Massachusetts]" (a "Covered Entity").[10] "Persons" are defined to include corporations and other legal entities.[11] Thus, the Massachusetts Regulations potentially apply to a Covered Entity regardless of whether the business is physically located

---

6. OR. REV. STAT. § 646A.622(2)(d)(C)(iv) (2015); NEV. REV. STAT. § 603A.200(1) (2015).

7. *Id*.

8. *See, e.g.*, 45 C.F.R. § 164.400-14 (2014) (Subpart D) (notification of breach of unsecured protected health information); 815 ILL. COMP. STAT. 530/1-40 (2015) (requiring notification in the event of an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information); IND. CODE § 24-4.9-1-1 to -5-1 (2015) (mandating notification where there has been an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information); TEX. BUS. & COM. ANN. § 521.053 (2015) (requiring notification of an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information).

9. 201 MASS. CODE REGS. 17.00(1) (2015); *see also* MASS GEN. LAWS, ch. 93H, § 2(a) (2015) (directing the Commonwealth's Department of Consumer Affairs and Business Regulation to adopt regulations covering any business "that owns or licenses personal information about a resident of" Massachusetts to "insure the security and confidentiality of customer information in a manner fully consistent with industry standards; protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.").

10. 201 MASS. CODE REGS. 17.00(2) (2015).

11. *Id*. at 17.02.

or has operations in Massachusetts.

"Personal information" is defined as a Massachusetts "resident's first name and last name or first initial and last name in combination with… (a) Social Security number, (b) driver's license number or state-issued identification card number, and/or (c) financial account number, or credit or debit card number" (regardless of whether such account number or debit or credit card number is accompanied by any required security code, access code, PIN, or password that would permit access to the account).[12] Personal information does "not include any information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public."[13]

B. REQUIREMENTS OF THE MASSACHUSETTS REGULATIONS

1. Written Information Security Program

The Massachusetts Regulations mandate that every Covered Entity develop, implement, and maintain a comprehensive WISP, applicable to records (both paper and electronic) containing personal information of a Massachusetts resident. The WISP must contain administrative, technical, and physical safeguards (the "Safeguards") to ensure the security and confidentiality of records containing personal information. The Safeguards are to be appropriate to (a) the size, scope, and type of business of the Covered Entity; (b) the amount of resources available to the Covered Entity; (c) the amount of stored data; and (d) the need for security and confidentiality of both consumer and employee information. Additionally, the Safeguards must be consistent with any similar requirements governing the protection of personal information set forth in any other state or federal regulations applicable to the Covered Entity.[14]

The Massachusetts Regulation, 201 CMR 17.03(2), requires that every WISP must include, at a minimum, the following:

> (a) Designating one or more employees to maintain the WISP;
>
> (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

12. *Id*.
13. *Id*.
14. *Id*. at 17.03(1).

(iii) means for detecting and preventing security system failures;

(c) Developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of the Covered Entity's business premises;

(d) Imposing disciplinary measures for violations of the WISP rules;

(e) Preventing terminated employees from accessing records containing personal information;

(f) Overseeing service providers by (i) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with the Massachusetts Regulations and any applicable federal regulations[15] and (ii) requiring such third-party service providers by contract to implement and maintain such appropriate security measures for personal information;

(g) Imposing reasonable restrictions upon physical access to records containing personal information, and storage of such records and data in locked facilities, storage areas or containers;

(h) Conducting regular monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information, and upgrading Safeguards as necessary to limit risks;

(i) 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

(j) 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.[16]

2. Computer System Security Requirements

Under Section 17.04 of the Massachusetts Regulations, 201 MASS. CODE REGS. 17.04, the WISP of a covered entity that electronically stores or transmits Massachusetts residents' personal information must also include security measures covering its computers, including any wireless system. These computer systems security requirements must,

15. Note that, to comply with the Massachusetts Regulations regarding the selection and retention of third-party service providers, a Covered Entity may need to engage in some level of due diligence to determine the data security measures such service providers have in place, and should also obtain assurances from such providers that they maintain adequate cyber insurance in the event of a data security breach.

16. 201 MASS. CODE REGS. 17.03(2) (2015).

at a minimum, and to the extent technically feasible,[17] include the following elements:

> (1) Secure user identification protocols, including (a) control of user IDs and other identifiers, (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices, (c) 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, (d) restricting access to active users and active user accounts only, and (e) 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 (a) restrict access to records and files containing personal information to those who need such information to perform their job duties, and (b) 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) 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;
>
> (4) Reasonable monitoring of systems for the unauthorized use of or access to personal information;
>
> (5) Encryption of all personal information stored on laptops or other portable devices;
>
> (6) Reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, for files containing personal information on a system that is connected to the Internet;
>
> (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, set to receive the most current security updates on a regular basis; and

---

17. While the phrase "technically feasible" is not defined in the Regulations, a definition is provided in the frequently asked questions issued by the Massachusetts Office of Consumer Affairs and Business Regulation in connection with the Regulations ("FAQ"). The FAQ provide that "technically feasible" means "that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used." OFFICE OF CONSUMER AFFAIRS, COMMW. OF MASS., FREQUENTLY ASKED QUESTIONS REGARDING 201 CMR 17.00 at 2, *available at* http://www.mass.gov/ocabr/docs/idtheft/201cmr17faqs.pdf (last visited Apr. 28, 2015).

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.[18]

C. ENFORCEMENT

Pursuant to MASS. GEN. LAWS, ch. 93H, § 6 (2015), the Massachusetts Attorney General may bring an action against a Covered Entity to remedy violations of the Massachusetts Regulations.

II. OREGON

A. SCOPE OF THE CONSUMER IDENTITY THEFT PROTECTION ACT

The Oregon Consumer Identity Theft Protection Act, OR. REV. STAT § 646A.622, covers any person (which is defined under the statute to include any private or public corporation) that owns, maintains or otherwise possesses data that includes a "consumers personal information."[19] The statute defines a "consumer" as an individual who is a resident of Oregon.[20]

"Personal information" is defined by the Oregon law as a "consumer's first name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not rendered unusable through encryption, redaction or other methods, or when the data elements are encrypted and the encryption key has also been acquired:

(A) Social Security number;

(B) Driver license number or state identification card number issued by the Oregon Department of Transportation;

(C) Passport number or other U.S.-issued identification number; or

(D) Financial account number, credit or debit card number in combination with any required security code, access code or password that would permit access to a consumer's financial account.[21]

Alternatively, "personal information" may also mean any of the individual data elements or any combination of the data elements described above when not combined with the consumer's first name or initial and last name "when the data elements are not rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft

18. 201 MASS. CODE REGS. 17.04 (2015).
19. OR. REV. STAT. § 646A.622(1) (2015).
20. *Id*. at § 646A.602(2).
21. *Id*. at § 646A.602(11).

against the consumer whose information was compromised."[22]

1. Requirements to Develop Safeguards for Personal Information

A business covered by the Oregon Consumer Identity Theft Protection Act "must develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of the data."[23] To comply with this standard, such a business must implement an information security program that includes certain minimum administrative, technical and physical safeguards.[24]

With regard to the administrative safeguards required to be included in the information security program, the business must:

> (1) Designate one or more employees to coordinate the security program;
>
> (2) Identify reasonably foreseeable internal and external risks;
>
> (3) Assess the sufficiency of safeguards in place to control the identified risks;
>
> (4) Train and manage employees in the security program practices and procedures;
>
> (5) Select service providers capable of maintaining appropriate safeguards and require those safeguards by contract; and
>
> (6) Adjust the security program in light of business changes or new circumstances.[25]

With regard to the technical safeguards that must be included in the information security program, the business must:

> (1) Assess risks to its network and software applications;
>
> (2) Assess risks in its processing, transmission and storage of personal information;
>
> (3) Detect, prevent and respond to attacks or failures of systems containing personal information; and
>
> (4) Regularly test and monitor the effectiveness of key controls, systems and procedures.[26]

With regard to the physical safeguards that must be included in the information security program, the business must:

> (i) Assess risks of the storage and disposal of records containing per-

---

22. *Id*.
23. *Id*. § 646A.622(1).
24. *Id*. § 646A.622(2)(d).
25. OR. REV. STAT. § 646A.622(2)(d)(A)(i)-(vi).
26. *Id*. at § 646A.622(2)(d)(B)(i)-(iv).

> sonal information;
>
> (ii) Detect, prevent and respond to intrusion; and
>
> (iii) Protect against unauthorized access to or use of personal information during or after the collection, transportation and destruction or disposal of such information.[27]

In addition to the physical safeguards set forth above, the Oregon Consumer Identity Theft Protection Act requires that a business dispose of personal information "after it is no longer needed for business purposes or as required by local, state[,] or federal law by burning, pulverizing, shredding, or modifying a physical record and by destroying or erasing electronic media so that the information cannot be read or reconstructed."[28]

B. ENFORCEMENT AND PENALTIES

Pursuant to ORS § 646A.624, the Oregon Attorney General can investigate potential violations of the Consumer Identity Theft Protection Act, and can impose a penalty of not more than $1,000 for every violation of the Act, up to a maximum of $500,000 per occurrence.

III. ILLINOIS

Unlike Massachusetts, Oregon and the other states discussed below, Illinois has not currently enacted legislation or adopted regulations that expressly mandate that a business operating in Illinois or that obtains personal information from Illinois residents undertake affirmative steps to generally safeguard such information. However, similar to forty-five other states, Illinois requires that, in an event of unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information of an Illinois resident, notification of such a breach must be sent to the affected Illinois residents.[29] The Illinois Personal Information Protection Act defines "personal information" as:

> An individual Illinois resident's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

---

27. *Id*. at § 646A.622(2)(d)(C)(i)-(iii).

28. *Id*. at § 646A.622(2)(d)(C)(iv). The Oregon Consumer Identity Theft Protection Act also includes certain restrictions and limitations on the use and disclosures of Social Security numbers. *See Id*. at § 646A.620.

29. 815 ILL. COMP. STAT. 530/10 (2015).

> (1) Social Security number;
>
> (2) driver's license number or other state-issued identification card number; and
>
> (3) account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.[30]

Additionally, the Illinois Personal Information Protection Act requires companies to "dispose of the materials containing personal information in a manner that renders the personal information unreadable, unusable, and undecipherable."[31] The Act empowers the Illinois Attorney General to levy civil fines of up to $50,000 for each instance of improper disposal of materials containing personal information. Further, a violation of the Act constitutes an "unlawful practice" under the Illinois Consumer Fraud and Deceptive Business Practices Act.[32] Thus, a violation of the destruction provision of the Act is subject to all of the remedies provided under the Consumer Fraud and Deceptive Business Practices Act, including the ability of persons who are injured by a violation to bring a private cause of action.

IV. CALIFORNIA

A. SCOPE OF THE CALIFORNIA DATA PROTECTION STATUTE

The California Data Protection Act, CAL. CIV. CODE § 1798.80-84 (2015), broadly apply to any business that "owns or licenses" personal information of California residents. The statute defines "owns or license" to include "personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates."[33]

The California statute defines "personal information" broadly as an individual California resident's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

> (A) Social Security number;
>
> (B) driver's license number or California identification card number;
>
> (C) account number, credit or debit card number, in combination with

---

30 *Id*. at 530/5.

31. *Id*. at 530/40(b).

32. *Id*. at 530/20.

33. CAL. CIV. CODE § 1798.81.5(a) (2015).

> any required security code, access code, or password that would permit access to an individual's financial account; and
>
> (D) medical information (which is further defined as "any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional").[34]

B. DUTY TO IMPLEMENT SECURITY PROCEDURES AND PRACTICES TO SAFEGUARD PERSONAL INFORMATION

Under the California Data Protection Act, a business owning or licensing personal information of a California resident must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[35] Additionally, to the extent that a business discloses personal information about a California resident pursuant to a nonaffiliated third party, such a business is obligated under CAL. CIV. CODE § 1798.81.5(c) (2015) to contractually require any third party to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Further, when disposing records (either physical or electronic) containing personal information of California residents, such disposal must be done by either (a) shredding, (b) erasing, or (c) otherwise modifying the personal information in those records "to make it unreadable or undecipherable through any means."[36]

C. ENFORCEMENT

The California statute provides a private right of action in favor of a California resident that has been injury by a violation of the statute to recover actual damages caused by the violation.[37]

---

34. *Id*. at § 1798.81.50(d)(1).

35. *Id*. at § 1798.81.5(b).

36. *Id*. at § 1798.81. Note that to the extent that certain personal information of California consumers is shared or otherwise disclosed with an unaffiliated third-party for use by the third party for direct marketing, certain disclosures must be made to those California customers pursuant to CAL. CIV. CODE § 1798.83 (2015). Additionally, California imposes certain restrictions and limitations on the use and disclosure on California residents' Social Security numbers. *See* CAL. CIV. CODE § 1798.85-89 (2015).

37. *Id*. at § 1798.84.

V. TEXAS

A. SCOPE OF THE TEXAS IDENTITY THEFT ENFORCEMENT AND PROTECTION ACT

The scope of the Texas Identity Theft Enforcement and Protection Act covers any a business that does business in Texas or any business outside of the state that collects or maintains "sensitive personal information" of Texas residents in its regular course of business.[38]

Similar to the definition of personal information under California law, the Texas statute broadly defines "sensitive personal information" to mean either:

> (1) "Personal identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's:
>
> > (A) name, social security number, date of birth, or government-issued identification number;
> >
> > (B) mother's maiden name;
> >
> > (C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
> >
> > (D) unique electronic identification number, address, or routing code; and
> >
> > (E) telecommunication access device as defined by Section 32.51, Penal Code.
>
> (2) "Sensitive personal information" means, subject to Subsection (b), an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
>
> > (A) social security number;
> >
> > (B) driver's license number or government-issued identification number; or
> >
> > (C) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.[39]

B. BUSINESS'S DUTY TO PROTECT SENSITIVE PERSONAL INFORMATION

The Texas Identity Theft Enforcement and Protection Act requires that a covered business must "implement and maintain reasonable pro-

---

38. TEX. BUS. & COM. CODE ANN. § 521.052 (2015).
39. *Id*. at § 521.002(a)(2).

cedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business."[40] Additionally, covered businesses are required to destroy or arrange for the destruction of records containing sensitive personal information of Texas residents by "(1) shredding, (2) erasing, or (3) otherwise modifying the sensitive personal information contained in the records in a manner to make the [personal] information unreadable or indecipherable through any means."[41]

C. ENFORCEMENT AND CIVIL PENALTIES

Under the Texas law, a business that violates the statute may be liable for a civil penalty of at least $2,000 but not more than $50,000 for each violation. The Texas Attorney General may bring an action to recover the civil penalty.[42]

VI. INDIANA

A. SCOPE OF THE CONSUMER IDENTITY THEFT PROTECTION ACT

Indiana law, under IC 24-4.9-3-3.5, also imposes an affirmative obligation on a "data base owner" to protect personal information of Indiana residents collected or maintained by the data base owner. A "data base owner" is defined under the Indiana statute as a person or business that "person that owns or licenses computerized data that includes personal information" of an Indiana resident for commercial purposes.[43]

> "Personal information" is defined under the Indiana law as either:
>
> (1) a Social Security number that is not encrypted or redacted, or
>
> (2) an individual's first and last names, or first initial and last name, and one or more of the following data elements that are not encrypted or redacted:
>
> (A) a driver's license number;
>
> (B) a state identification card number;
>
> (C) a credit card number; and
>
> (D) a financial account number or debit card number in combination with a security code, password, or access code that would

40. *Id*. at § 521.052(a).
41. *Id*. at § 521.052(b).
42. *Id*. at § 521.151(a).
43. IND. CODE § 24-4.9-2-3 (2015).

permit access to the person's account.[44]

B. DUTY TO SAFEGUARD PERSONAL INFORMATION

The Indiana law mandates that a data base owner "shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner."[45] Additionally, a data base owner is prohibited under the Indiana statute from "disposing of records or documents containing unencrypted and un-redacted personal information of Indiana residents without shredding, incinerating, mutilating, erasing or otherwise rendering the personal information illegible or unusable."[46]

C. ENFORCEMENT AND PENALTIES

Pursuant to IND. CODE § 24-4.9-4-2, the Indiana Attorney General may bring an action against any business that violates the Indiana statute to obtain civil penalties of not more than $5,000 per past violation of the statute and obtain an injunction against future violations.[47]

VII. NEVADA

A. SCOPE OF THE NEVADA STATUTE

The Nevada statute, entitled "Security of Personal Information," applies to any "data collector" which the statute defines to include any type of business entity that "for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with non-public personal information" of a Nevada resident.[48]

"Personal information" is defined as:

> 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) Social security number;
>
> (2) driver's license number or identification card number; and

---

44. *Id*. at 2-10.
45. *Id*. at 3-3.5(b).
46. *Id.* at 3-3.5(c).
47. *Id*. at 4-2.
48. NEV. REV. STAT. ANN. § 603A.030 (2015).

> (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.[49]

B. REQUIRED SECURITY MEASURES UNDER THE NEVADA STATUTE

A data collector that maintains records which contain personal information of a Nevada resident must "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification[,] or disclosure."[50] To the extent that a data collector discloses Nevada residents' personal information pursuant to a contract with a third-party, the data collector is obligated to ensure that such a contract includes a provision requiring the third party also "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."[51]

In addition to these security measures, Nevada law requires businesses to proactively dispose of records containing personal information of Nevada residents. Indeed, similar to the Oregon Consumer Identity Theft Protection Act, OR. REV. STAT. § 646A.622(2)(d)(C)(iv) (2015), the Nevada statute mandates that any business that maintains records which contain personal information of a Nevada resident must "take reasonable measures to ensure the destruction of those records" when such a business "decides that it will no longer maintain the records."[52] Nevada defines "reasonable measures to ensure the destruction" as any "method that modifies the records containing the personal information in such a way as to render the personal information contained in the records unreadable or undecipherable, including, without limitation: (1) shredding of the record containing the personal information; or (2) erasing of the personal information from the records."[53]

VIII. OTHER STATE LAWS REQUIRING SAFEGUARDING PERSONAL INFORMATION

Several other states have enacted laws requiring businesses that either operate in those states or that have obtained personal information of residents in these states to implement and maintain reasonable security measures to protect the unauthorized disclosure of or access to such personal information. For example, under Arkansas' Personal

---

49. *Id*. at § 603A.040.
50. *Id*. at § 603A.210(1).
51. *Id*. at § 603A.210(2).
52. *Id*. at § 603A.200(1).
53. *Id*. at § 603A.200(2)(b).

Information Protection Act, a business that "acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[54]

Under Connecticut law, any business "in possession of personal information of another person shall safeguard the data, computer files and documents containing the information from misuse by third parties, and shall destroy, erase[,] or make unreadable such data, computer files and documents prior to disposal," and the failure to do so may expose such a business to a civil penalty of $500 for each violation of the statute, up to a civil penalties not exceed $500,000 for any single event.[55]

Maryland mandates that, in order to protect personal information "from unauthorized access, use, modification, or disclosure," a business that owns or licenses personal information of Maryland residents, must "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."[56] Additionally, under Maryland's data protection statute, a business that uses a nonaffiliated third party as a service provider to perform services for the business and discloses personal information about a Maryland resident:

> (1) A business that uses a nonaffiliated third party as a service provider to perform services for the business and discloses personal information about an individual residing in the State under a written contract with the third party shall require by contract that the third party implement and maintain reasonable security procedures and practices that:
>
> (i) are appropriate to the nature of the personal information disclosed to the nonaffiliated third party; and
>
> (ii) are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure, or destruction.[57]

Rhode Island law contains requirements that are nearly identical as those set forth in the Maryland statute.[58]

---

54. ARK. CODE ANN. § 4-110-104 (2015) (LexisNexis).

55. CONN. GEN. STAT. § 42-471 (2015).

56. MD. CODE, COMM. LAW § 14-3503(a) (2015).

57. *Id*. at § 14-3503(b).

58. R.I. GEN. LAWS § 11-49.2-2(2), (3) (2015); *see also* UTAH CODE § 13-44-201 (2015) ("any person or business that conducts business in the state and maintains personal information to implement and maintain reasonable procedures to (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of

Finally, Delaware recently passed a new law, effective January 1, 2015, requiring the safe disposition of business records containing consumer personal information.[59] The new law requires commercial entities conducting business in Delaware to take reasonable steps to destroy their consumers' "personal identifying information" prior to the disposal of electronic or paper records.[60] The term "consumer" is defined as an individual entering into a transaction "primarily for personal, family, or household purposes" and "personal identifying information" consists of the consumer's first name or first initial and last name in combination with any of the following data elements: (1) a signature; (2) full date of birth; (3) Social Security number or passport number; (4) driver's license or state identification card number; (5) insurance policy number; (6) financial services account number, bank account number, credit card number, or "any other financial information;" or (7) confidential health care information.[61] A consumer's information qualifies as "personal identifying information" if either his or her name or the accompanying data element is unencrypted at the time of disposal.

Under the new Delaware law, when records are "no longer to be retained," commercial entities must "take all reasonable steps to destroy or arrange for the destruction of a consumer's personal identifying information" within those records.[62] The statute explicitly calls for "shredding, erasing, or otherwise destroying or modifying" the consumer personal identifying information in a manner that makes it "entirely unreadable or indecipherable."[63]

The Delaware statute included several enforcement mechanisms, including a private right of action for consumers who incur actual damages as a result of a violation.[64] Significantly, the statute enables aggrieved consumers to seek treble damages, which could quickly add up given that "each record unreasonably disposed of constitutes an individual violation" of the statute.[65] Under certain circumstances, the Delaware Attorney General and Division of Consumer Protection of the Department of Justice also may bring enforcement actions for violations of the statute.[66]

---

business; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person or business).

59. DEL. CODE ANN. tit. 6 § 5001C-04C.

60. *Id*. at § 5002C.

61. *Id*. at § 5001C(3).

62. *Id*. at § 5002C.

63. *Id*.

64. *Id*. at § 5003C.

65. An Act to Amend Title 6 of the Delaware Code Relating to Commerce and Trade and the Safe Destruction of Documents Containing Personal Identifying Information, H.B. 295 § 50C-103(a), 147th Gen. Assembly (Del. 2014) (enacted); DEL. CODE ANN. tit. 6 § 5003C(b).

66. *Id*. at § 50C-103(c). Note, that the Delaware statute carves out several exemp-

tions for regulated entities, including financial institutions subject to the privacy and security requirements of the Gramm-Leach-Bliley Act, consumer reporting agency subject to the FCRA, and certain covered entities subject to HIPAA's privacy and security requirements. *Id*. at § 50C-104.