EDWARDS WILDMAN

CLIENT ADVISORY

edwardswildman.com

June 2014

An Edwards Wildman Privacy & Data Protection Client Advisory

Major Amendments to Florida Breach Notification Statute: Unique Requirements and Short Deadlines Take Effect July 1

By: Karen Booth, Ted Augustinos, Mark Schreiber and Tom Smedinghoff

Florida Governor Rick Scott recently signed the Florida Information Protection Act of 2014 (SB 1524, the "Act") into law, amending Florida's breach notification statute effective July 1, 2014. The amendments are significant, including the first statutory requirement to provide copies of forensic reports and "policies regarding breaches," to the Florida Attorney General upon request, and the shortest deadline for individual notice (30 days) among state general breach notification requirements.

Through the Act, Florida also joins a number of other states in requiring that companies and government agencies subject to the requirements take steps to prevent data breaches through data security measures and secure disposal of personal information. As an immediate response to the amendments, all businesses and government entities that collect personal information of individuals "in Florida" should ensure that they have adopted and implemented an appropriate data security program and incident response plan.

The Act replaces Florida's current breach notification statute (Fla. Stat. § 817.5681) with a new statute (Fla. Stat. § 501.171), which, among other changes: (a) expands the definition of "personal information" triggering breach notification obligations to include an individual's online account credentials (following California's recent amendments described below), and also to include an individual's name in connection with his or her health care or health insurance information; (b) expands the definition of "breach" from "unlawful and unauthorized acquisition" of personal information to "unauthorized access," of such information; (c) reduces the deadline for notifying affected individuals from 45 to 30 days after discovery, marking the shortest deadline for individual notice imposed by general (not industry-specific) state breach notification requirements; (d) requires notification to the Florida Attorney General regarding breaches affecting more than 500 individuals "in Florida"; (e) imposes unique requirements to provide copies of forensic reports, "policies regarding breaches," and other documentation to the Attorney General upon request; (f) requires reasonable data protection and secure disposal of personal information; and (g) retains relatively unique provisions of Florida's current statute imposing daily monetary fines for late notice, and requiring vendors to notify data owners of breaches within 10 days of discovery, while maintaining that the statute creates no private right of action.

Expanded Definition of Personal Information

Following the approach adopted in recent amendments to California's breach notification statute, the Act expands Florida's current definition of "personal information" triggering breach notification requirements to include "a user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account," whether or not combined with the individual's name. Only California and Puerto Rico currently include similar data elements within the definition of "personal information" for purposes of breach notification requirements. Other states may soon follow California's lead on this issue, as they did after it enacted the first U.S. breach notification statute in 2003.

The Act also expands Florida's current definition of "personal information" to include an individual's first name or first initial and last name in combination with: (a) any information regarding the individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care

professional; or (b) the individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. With respect to covered entities and business associates subject to HIPAA, compliance with the HIPAA Breach Notification Rule would appear to satisfy the requirements of the Act, provided that the breached entity provides a copy of its HIPAA-compliant notifications to the Florida AG in a "timely" manner.

30-Day Deadline for Notifying Affected Individuals

The Act reduces the deadline for notifying affected individuals from 45 to 30 days after discovery, marking the shortest deadline for individual notice imposed by general state breach notification requirements. While certain industry-specific deadlines for notifying affected individuals are significantly shorter (e.g., notice to patients pursuant to the California medical breach notification statute is required within 5 business days of discovery), most general state breach notification requirements do not specify the number of days within which notice is required, instead providing that notice is required "without unreasonable delay" or similar language. Only four states (including Florida's current statute) require notice within a specific number of days following discovery of a breach (subject to law enforcement delay), all currently providing for 45 days for such notice. When the Act takes effect July 1, 2014, Florida's deadline will be reduced to 30 days following discovery. The Act provides, "notice to individuals shall be made as expeditiously as practicable and without unreasonably delay…but no later than 30 days after determination of a breach or reason to believe a breach occurred…" subject to law enforcement delay and risk of harm consultation exceptions.

The Act permits the Attorney General to grant breached entities an additional 15 days to notify affected individuals if good cause for delay is provided to the AG in writing within 30 days after determination of the breach or reason to believe a breach occurred.

Notice to Florida Attorney General Required

With the Act, Florida joins nearly half of U.S. states in requiring notice to the state Attorney General or other agency following a data breach requiring notice to state residents. The Act requires breached entities to notify the Florida AG regarding breaches affecting over 500 Florida residents "as expeditiously as practicable, but no later than 30 days after determination of the breach or reason to believe a breach occurred." Notices to the Attorney General must include certain specific content, including a relatively unique requirement to describe, "any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services."

Similar to Connecticut's breach statute, the Act requires consultation with federal, state or local authorities in order to invoke the risk of harm exception. Where the breached entity finds the risk of harm exception to apply, the Act then requires the breached entity to then submit its written determination to the AG, like Alaska and Vermont.

Requires Production of Forensic Reports, "Policies regarding Breaches" and other Documentation to Attorney General

The Act imposes unique requirements to provide copies of the following documents to the Attorney General upon request: "a police report, incident report, or computer forensics report," and "a copy of the policies in place regarding breaches." While it is not uncommon for state attorneys general and other regulators to request a copy of a breached entity's forensic report regarding an incident, and the breached entity's internal privacy and data security policies and procedures following notice of a breach, Florida is the first state to require by statute that breached entities provide such documentation to the Attorney General upon request. As an immediate response to the amendments, all businesses that collect personal information of individuals "in Florida" should prepare or update their incident response plans, and consider implications of the forensic report disclosure requirement with respect to intentions to assert attorney-client privilege over forensic reports.

A companion statute also passed on June 20, 2014, SB 1526, provides for confidentiality of information provided to the Florida AG following data security incidents, including to provide for certain exemptions from the public records law. Subject to certain exceptions, SB 1526 requires confidential treatment of forensic reports, personal information, and information that would reveal weaknesses in the company's data security or reveal its proprietary information.

Expands Notification Trigger from "Unauthorized Acquisition" to "Unauthorized Access"

The Act expands the definition of "breach" from "unlawful and unauthorized acquisition" of personal information to "unauthorized access," of such information. Florida now joins a very small number of states in which notification obligations are triggered by "unauthorized access" alone. Thus, incidents which involve "unauthorized access" to, but not "unauthorized acquisition" of, personal information may trigger notification obligations under Florida law as of July 1.

Requires Reasonable Data Protection and Secure Disposal of Personal Information

Florida joins a number of other states in requiring that companies and government entities maintaining personal information of state residents take steps to protect against data breaches through data security measures as well as secure disposal of personal information. Specifically, the Act requires "reasonable measures to protect and secure data in electronic form containing personal information," as well as "reasonable measures to dispose…of customer records containing personal information within its custody or control when the records are no longer to be retained." The Act specifies that such secure disposal "shall involve shredding, erasing, or otherwise modifying personal information in the records to make it unreadable or undecipherable through any means."

Retention of Unique Provisions in Current FL Statute regarding Penalties for Non-Compliance and Requirements Specific to Vendor Breaches

The Act retains provisions relatively unique to the current Florida statute providing for specific monetary penalties for failure to comply with breach notification obligations of $1,000 per day for the first 30 days following a violation of the individual or AG notification requirements, $50,000 for each subsequent 30-day period thereafter, and, if the violation continues for more than 180 days, an amount not to exceed $500,000. The Act specifies that it does not create a private right of action.

With respect to vendor breaches, the Act requires third-party agents to notify the covered entity on whose behalf they maintain, store or process breached personal information "as expeditiously as practicable, but no later than 10 days following determination of the breach of security or reason to believe the breach occurred." While many other states specify that notice by a vendor to the data owner is required, most do not specify the number of days within which such notice must be provided. The Act also specifies that obligations to notify the AG and affected individuals apply to the data owner following a vendor breach in which the vendor has provided notice to the data owner.

The Edwards Wildman Privacy and Data Protection Group regularly advises clients on cyber risks and data breaches. For further information, please contact the authors or the Edwards Wildman Attorney that handles your matters.

For more information, please contact the authors of this advisory Ted Augustinos, Partner, +1 860 541 7710, taugustinos@edwardswildman.com, Karen Booth, Associate, +1 860 541 7714, kbooth@edwardswildman.com, Mark Schreiber, Partner, +1 617 239 0585, mschreiber@edwardswildman.com, Tom Smedinghoff, Partner, +1 312 201 2021, tsmedinghoff@edwardswildman.com or one of the attorneys listed below:

Mark E. Schreiber, Partner, Chair, Steering Committee, Privacy and Data Protection Group	+1 617 239 0585	Boston	mschreiber@edwardswildman.com
Theodore P. Augustinos, Partner, Steering Committee, Privacy and Data Protection Group	+1 860 541 7710	Hartford	taugustinos@edwardswildman.com
Laurie A. Kamaiko, Partner, Steering Committee, Privacy and Data Protection Group	+1 212 912 2768	New York	lkamaiko@edwardswildman.com
Sarah Pearce, Partner, Steering Committee, Privacy and Data Protection Group	+44 (0) 20 7556 4503	London	spearce@edwardswildman.com

Barry J. Bendes, Partner	+1 212 912 2911	New York	bbendes@edwardswildman.com
Michael P. Bennett, Partner	+1 312 201 2679	Chicago	mbennett@edwardswildman.com
Nicholas Bolter, Partner	+44 (0) 20 7556 4380	London	nbolter@edwardswildman.com
Kenneth Choy, Partner	+852 2116 6653	Hong Kong	kchoy@edwardswildman.com
Mark Deem, Partner	+44 (0) 20 7556 4425	London	mdeem@edwardswildman.com
Howard M. Gitten	+1 561 820 0230	West Palm Beach	hgitten@edwardswildman.com
Ben Goodger, Partner	+44 (0) 20 7556 4188	London	bgoodger@edwardswildman.com
Edwin M. Larkin, Partner	+1 212 912 2762	New York	elarkin@edwardswildman.com
Stephen M. Prignano, Partner	+1 401 276 6670	Providence	sprignano@edwardswildman.com
Ronie M. Schmelz, Partner	+1 310 860 8708	Los Angeles	rschmelz@edwardswildman.com
Lisa Simmons, Partner	+1 312 201 2503	Chicago	lsimmons@edwardswildman.com
Thomas J. Smedinghoff, Partner	+1 312 201 2021	Chicago	tsmedinghoff@edwardswildman.com
David S. Szabo, Partner	+1 617 239 0414	Boston	dszabo@edwardswildman.com
David L. Anderson, Counsel	+1 310 860 8710	Los Angeles	danderson@edwardswildman.com
Patrick J. Concannon, Counsel	+1 617 239 0419	Boston	pconcannon@edwardswildman.com
Karen L. Booth, Associate	+1 860 541 7714	Hartford	kbooth@edwardswildman.com
Zachary Lerner, Associate	+1 212 912 2927	New York	zlerner@edwardswildman.com
Jonny McDonald, Associate	+44 (0) 20 7556 4620	London	jmcdonald@edwardswildman.com
Haley Morrison, Associate	+1 617 239 0818	Boston	hmorrison@edwardswildman.com
Ari Moskowtiz, Associate	+1 202 939 7934	Washington, DC	amoskowitz@edwardswildman.com
Matthew Murphy, Associate	+1 401 276 6497	Providence	mmurphy@edwardswildman.com
Jamie Notman, Associate	+1 617 235 5303	Boston	jnotman@edwardswildman.com
Patrick Peng, Associate	+852 3150 1936	Hong Kong	ppeng@edwardswildman.com
Erin Pfaff, Associate	+1 310 860 8717	Los Angeles	epfaff@edwardswildman.com
Kayla Tabela, Associate	+1 617 239 0734	Boston	mtabela@edwardswildman.com
Nicholas Secara, Associate	+1 212 912 2785	New York	nsecara@edwardswildman.com
Ajita Shah, Associate	+44 (0) 20 7556 4385	London	ashah@edwardswildman.com
Nora A. Valenza-Frost, Associate	+1 212 912 2763	New York	nvalenza-frost@edwardswildman.com

EDWARDS WILDMAN