SQUIRE SANDERS

FLORIDA REVAMPS DATA SECURITY AND DATA BREACH STATUTES

May 2014

On April 30, 2014, the Florida House of Representatives followed the Senate in passing a pair of bills (SB 1524 & 1526) that, unless vetoed by Governor Rick Scott, will replace the state's current data breach notification statute, §817.5681, Fla. Stat., with a new section in the civil code, §501.171, that will include a new exemption from Florida's broad public records law. Governor Scott is expected to sign the new Florida Information Protection Act of 2014 (Act), which will then become effective on July 1, 2014. Essential provisions of the Act are briefly highlighted below.

While generally comparable to a growing number of data breach notification laws in other states, the Florida Act, mirroring a 2013 federal bill (S. 1193), is among the minority of such laws expressly imposing an affirmative duty to "take reasonable measures to protect and secure data in electronic form containing personal information." (§501.071(2)) Literally read, the Act applies to most businesses, wherever located, and to Florida government.

Florida Information Protection Act of 2014 – Essential Provisions

The Act imposes three basic duties and empowers the Florida Department of Legal Affairs (Department), which the Attorney General leads, to enforce them.

Three Duties

1. Protect and Secure: The first duty is that each covered entity maintaining personally identifiable information "shall take reasonable measures to protect and secure [such] data in electronic form." (§517.171(2)) The personal information covered by the Act is significantly expanded to include all medical and health insurance related information. As with the prior statute, there is a safe harbor exclusion for encrypted data.

2. Prompt Notice: The second duty is to provide prompt notice of any data breach, unless a data breach will not result in identity theft or financial harm. (§§501.571(3)-(6)) A business may be required to provide written notices to four distinct persons:

(1) the Department,
(2) all affected individuals,
(3) credit reporting agencies and
(4) third-party agents.

Any potentially harmful breach involving 500 or more Floridians must be reported to the Department, and all breaches potentially resulting in harm must be reported to any affected individual. The Act also specifies the content of the notices to be given. Notably, the Act adds that email notice may suffice, and that "substitute notice" by combination of website posting and media publication is permitted if either direct notice would cost more than $250,000 or more than 500,000 people are affected. Also, an entity subject to a "primary or functional federal regulator" may instead give notice per that regulator's requirements. SB 1526 creates an exemption from public records access for information that the Department receives pursuant to a required notice to it or an investigation that it or another law enforcement agency conducts.

3. Disposal of Records: The third distinct duty the Act imposes (§501.171(8)) is that covered entities "take all reasonable measures to dispose of customer records" containing personal information once they are "no longer to be retained."

New Enforcement Powers

The Act confers two distinct enforcement powers on the Department. Under subsection (9)(a), any violation of the new statute "shall be treated as an unfair or deceptive trade practice in any action" and, thus, allows the Department to seek a declaratory judgment, injunction, other equitable remedies or recovery of actual damages against entities violating any part of the new statute. Subsection 9(b) empowers the Department to impose substantial "civil penalties" (fines) on any non-governmental entity that violates any of the notification requirements. The potential penalty depends on the duration of the violation and ratchets up quickly: $1,000 daily for the first 30 days; $50,000 for each subsequent 30 day period; and for violations longer than 180 days, at most $500,000. Such penalties are levied "per breach and not per individual affected."

Finally, the Act "does not establish a private cause of action." (§501.171(10)) Even so, creative plaintiffs' counsel will likely have no trouble identifying causes of action and defining putative classes. Cases have recently been filed against a number of defendants for alleged data breach notice violations where plaintiffs assert, among other things, negligence, violations of federal statutes and violations of Florida's Deceptive and Unfair Trade Practices Act despite the lack of a private cause of action.[1]

[1] See, e.g., *Carsten v. University of Miami*, Case No. 1:14-cv-20497, U.S. District Court, Southern District of Florida.

SQUIRE SANDERS

FLORIDA REVAMPS DATA SECURITY AND DATA BREACH STATUTES

May 2014

For more information on Florida's data security and data breach statutes, please contact any of the Squire Sanders lawyers listed in this publication.

Contact

Gary P. Timin
Partner, Miami
+1 305 577 2860
gary.timin@squiresanders.com

Rafael M. Langer-Osuna
Associate, Miami
+1 305 577 4723
rafael.langerosuna@squiresanders.com

Andrew R. Kruppa
Partner, Miami
+1 305 577 7712
andrew.kruppa@squiresanders.com

Traci H. Rollins
Partner, West Palm Beach
+1 561 650 7256
traci.rollins@squiresanders.com