June 23, 2014

Florida Overhauls Security Breach Law with Groundbreaking Amendment

By Nathan D. Taylor

On June 20, 2014, Florida Governor Rick Scott signed into law a package of bills (S.B. 1524 and 1526) repealing the state's security breach law and putting in its place arguably the broadest and most encompassing breach law in this country. These bills also established a requirement for companies to safeguard personal information relating to consumers.

In response to significant and highly publicized breach incidents occurring over the past year, at least 19 state legislatures have introduced or considered security breach legislation in 2014. This year, Kentucky enacted a new breach law (leaving Alabama, New Mexico, and South Dakota as the only states in the country without breach laws). In addition, Iowa amended its breach law to require, among other things, notice to the Iowa Attorney General (AG) of breach incidents. Nonetheless, the new Florida law, effective July 1, 2014, is groundbreaking in its breadth and scope. As discussed below, the Florida law includes new requirements unseen in similar laws throughout the country, as well as some of the most stringent requirements shared by a handful of states. About the only good news for businesses is the fact that the Florida law does not create a private right of action.

SECURITY BREACH NOTIFICATION

S.B. 1524 repealed the state's security breach law and replaced it with a dramatically broader substitute law. The new Florida breach law will require that a company provide notice to consumers when data in electronic form containing personal information relating to those consumers is accessed without authorization. The simplicity of the law, however, comes to a screeching halt at its consumer notice trigger. The new law appears cobbled together from some of the most onerous provisions of the various security breach laws in the country, while even adding some dramatic new wrinkles.

The following list highlights some of the broadest and most onerous requirements of the bill:

- Similar to the recent California amendment, the new Florida breach law will now define covered "personal information" to include a username or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Peter Day (650) 813-4231
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
William L. Stern (415) 268-7637
Nancy R. Thomas (213) 892-5561
David M. Walsh (213) 892-5262

New York
Cindy Abramson (212) 336-4178
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Michael B. Miller (212) 468-8009
Sotirios Petrovas (212) 336-4377
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
Patrick Bernhardt (202) 887-8771
L. Richard Fischer (202) 887-1566
Adam J. Fleisher (202) 887-8781
D. Reed Freeman, Jr. (202) 887-6948
Libby J. Greismann (202) 778-1607
Julie O'Neill (202) 887-8764
Cynthia J. Rich (202) 778-1652
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

EUROPE

Berlin
Hanno Timner 49 30 72622-1346

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364
Alja Poler De Zwart 32 2 340 7360

London
Ann Bevitt 44 20 7920 4041
Amy Collins 44 20 79204180
Susan McLean 44 20 79204045

ASIA

Beijing
Gabriel Bloch 86 10 5909 3367
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Singapore
Daniel P. Levison 65 6922 2041

Tokyo
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

- The Florida law will require notice to consumers as expeditiously as practicable, but no later than 30 days after the determination that there is reason to believe that a breach has occurred. (The repealed Florida law required notice no later than 45 days after such a determination.)
- Similar to the Connecticut law, the new Florida law includes an express risk-of-harm exception, but makes such exception contingent on not only an investigation but also consultation with relevant federal, state, or local law enforcement. The requirement to consult with law enforcement complicates the risk-of-harm analysis after a breach. To take the position that a breach does not trigger notice because there is no risk-of-harm to consumers, a company will be required to first consult with law enforcement.
- Although the Florida law will permit substitute notice to consumers for certain large breaches, the Florida law will require that substitute notice include, among other things, "[n]otice *in* print and to broadcast media, including major media in urban *and rural* areas" (emphasis added). The phrase notice "in" print, as opposed to notice "to" print, could be read to require that a company publish notice in print media, rather than notifying print media, when providing substitute notice.
- Although many states impose a requirement to notify the state AG or other state regulator, Florida has raised the bar with respect to state notification. The Florida law will require not only that companies provide notice to the AG of breaches involving personal information relating to 500 or more Florida residents, but also that a company provide to the AG upon request, among other things, an incident report or computer forensics report and a copy of the company's policies in place "regarding breaches." This is truly groundbreaking. The Florida law will expressly require that companies turn over information to the AG in connection with an AG investigation of a breach.
- The Florida law will require that notice to the AG of a breach indicate whether any free services are being offered to consumers as a result of the breach, such as credit monitoring.
- Moreover, similar to the Alaska and Vermont laws, the new Florida law requires that a company provide notice to the AG if the company experiences a breach but determines that notice is not required because there is no risk of harm to consumers. As a practical matter, companies may be required to justify their risk-of-harm analysis to the Florida AG.
- The Florida law will permit a company's agent that experiences a breach to provide notice to the AG and consumers on behalf of the company. However, the agent's failure to do so will "be deemed a violation" of the company and not the agent.

SAFEGUARDS

The Florida law will also impose certain safeguards requirements on companies (and their third-party agents) that acquire, maintain, store, or use covered personal information. Specifically, the Florida law will require that a company take "reasonable measures to protect and secure data in electronic form containing personal information." In addition, the Florida law will require that a company take "reasonable measures" to dispose of "customer records," in any form, that contain personal information regarding Florida residents.

AG CONFIDENTIALITY

As noted above, the Florida law will require that companies provide very sensitive information to the AG upon request, including, for example, computer forensic reports regarding a breach. In apparent recognition of the sensitivity of the

information that can be compelled by the AG, the package of bills signed into law by the Florida Governor includes provisions that would provide that information provided to the AG in connection with an investigation is exempt from disclosure under the Florida public records law until the investigation is complete or ceases to be active. Moreover, certain sensitive information would continue to be exempt from disclosure following an investigation, including computer forensic reports and information that would reveal weaknesses in a company's data security.

PRACTICAL IMPLICATIONS FOR BUSINESSES

It is important for companies to consider the potential impacts of the Florida law on their businesses.

- The simple fact is that security incidents occur. Companies will continue to experience security incidents that involve personal information relating to Florida residents. It is important to be mindful of the various compliance traps that exist under this new law, including the fact that usernames and passwords are now covered and the requirements that must be met in order to rely on a determination that there is no risk of harm.
- If a company provides notice to the Florida AG of a breach, the company should be cognizant of the AG's expanded authority to demand documents in connection with an investigation of the incident that may follow notice to the AG. Although AG investigations of breaches are common, never has a state been empowered by the breach law itself to demand production of a wide range of documents, including policies and procedures and reports prepared regarding the incident. Moreover, it is not clear the extent to which attorney-client privilege would provide a basis for not providing any documents to which the privilege should extend.

While Florida may be the first state to significantly overhaul its state breach law in such a dramatic manner, it is quite possible that it will not be the last. Businesses should be cognizant of the ever-changing state landscape and, in the event of a breach, determine any applicable requirements.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.