KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

June 30, 2014

Florida Passes New Data Breach Notification Law Requiring Enforcement of Civil Penalties For Untimely Notice

Personal information now includes online account information, health insurance policy numbers, and medical information

Florida Governor Rick Scott signed into law the Florida Information Protection Act of 2014 ("FIPA") and repealed the state's current breach notification law.[1] FIPA, which will take effect on July 1, is arguably one of the strictest breach laws in the country. It expands the definition of personal information, defines a breach as "unauthorized access of data," imposes new long-term duties on nearly all businesses with Florida customers or those businesses that maintain or use personal data about any person in Florida, and confers distinct enforcement powers on the Florida Department of Legal Affairs in the Office of the Attorney General.[2] The new law also requires businesses to notify any Florida residents affected by a breach within thirty (30) days.

Florida's new law follows the expanded definition of "personal information" that was adopted in California's data breach notification law and includes "a user name or e-mail, in combination with a password or security question and answer that would permit access to an online account."[3] Personal information also now includes a first name or first initial and last name in combination with an individual's "medical history, mental or physical condition, or medical treatment or diagnosis by a health professional" or "health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual."[4]

FIPA imposes several new requirements regarding data retention and destruction practices. Commercial and state government entities must now "take all reasonable measures to dispose of customer records," in any form or media, that contain personal information once they are "no longer to be retained."[5] This provision applies to paper as well as electronic records.[6] Customer records must be disposed of by shredding, erasing or "otherwise modifying" personal information to render it "unreadable or undecipherable through any means."[7]

FIPA also includes a requirement that businesses use "reasonable measures" to protect and secure personal information in electronic form, but the law does not provide guidance on what constitutes reasonable measures.[8]

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Sarah E. Statz
+1 404 572 2813
sstatz@kslaw.com

Elizabeth K. Hinson
+1 404 572 2714
bhinson@kslaw.com

King & Spalding
Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

www.kslaw.com

While FIPA does not establish a private cause of action, it directs the Attorney General to pursue any violation of the new statute as "an unfair or deceptive trade practice in any action" by the department under Section 501.208 of the Florida's Unfair and Deceptive Trade Practices Act. FIPA also empowers the Attorney General to impose civil penalties on any business entity up to $500,000 per breach for failure to timely notify the Attorney General in accordance with the Act, which requires written notice to the Attorney General within 30 days if 500 or more Florida residents are affected by the breach.[9]

Clients should take proactive measures to ensure compliance with state data breach notification laws, such as performing a risk analysis to assess potential risks to all personal information, updating privacy policies and procedures, and implementing procedures to identify and respond rapidly to breach events. Clients should also review their data retention and destruction policies and procedures to ensure they are disposing of consumer data in accordance with state laws.

King & Spalding's Data, Privacy and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Data, Privacy & Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 30 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

* * *

---

[1] *See* S.B. 1524, *available at* http://laws.flrules.org/2014/189.
[2] *See id.*
[3] *Id.* § 1(g)(1)(b).
[4] *Id.* § 3(1)(g)(1)(a)(IV)-(V).
[5] *Id.* § 3(8).
[6] *Id.*
[7] *Id.*
[8] *Id.* § 3(8).
[9] *Id.* § 3(9).