PUBLICATION

Act Imposes New Information Security and Management Requirements on All Florida Businesses

Authors: Alisa L. Chestler
June 23, 2014

On June 20, 2014, and in the wake of several high profile data breaches, Governor Rick L. Scott signed into law the Florida Information Protection Act of 2014 (FIPA), which will replace Florida's existing data breach notification law, Fla. Stat. Ann. § 817.5681. FIPA has far-reaching implications for businesses in possession of Floridians' personal information, and it will require businesses to immediately focus on data security and privacy issues within their organizations. Failure to adhere to FIPA's requirements could result in a business facing an enforcement action brought by the Department of Legal of Affairs (the "Department").

Florida has maintained a law regarding notification in the case of breach for years; however, there is renewed interest after several high-profile breaches and attempts by plaintiffs' attorneys to use breaches as a new opportunity for litigation. FIPA shortens the current 45-day breach notification deadline and requires businesses to notify individuals within 30 days. FIPA will also require businesses to notify the Department of breaches affecting 500 or more individuals. And once a breach has been reported, FIPA will require a business to provide, upon request from the Department, relevant incident reports, computer forensics reports, policies and procedures, and post-breach mitigation steps. Note that this assumes that companies maintain such policies and procedures when handling personal information.

In addition to the new breach notification protocol, FIPA will require almost all businesses to take reasonable measures to protect and secure electronic data containing "personal information." Under FIPA, "personal information" is defined to include a first name or first initial and a last name in combination with any of the following data elements:

1. a social security number;
2. a driver's license or ID card number, passport, military ID or similar number issued on a government document used to verify identity;
3. a financial account number or credit or debit card number in combination with any required security code, access code or password that is necessary to access a financial account;
4. any information regarding an individual's medical history, mental or physical condition or medical treatment or diagnosis by a health care professional; or
5. an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify an individual.

"Personal information" is also defined to include a name or email address, in combination with a password or security question and answer that would permit access to an online account. Notably, "personal information" does not include information that has been encrypted, secured or modified in a way that removes elements that personally identify an individual or that otherwise renders the information unusable.

Additionally, FIPA will require businesses to take reasonable measures to dispose of consumer records, in any form, that contain personal information when these records are "no longer to be retained." While no specific length of time is mandated for retention or destruction of records, FIPA requires information to be disposed of

in a way by "shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable."

FIPA grants the Department the power to enforce the statute in two ways. First, any violation of FIPA constitutes an unfair or deceptive trade practice in any action brought by the Department under Fla. Stat. Ann. § 501.207. Second, the Department can levy significant civil penalties against businesses that violate FIPA's notification requirements.

Although FIPA's obligations to secure and dispose of personal information are similar to federal requirements, these obligations will align Florida with a small minority of other states that require comprehensive information security/management programs. FIPA's effective date is July 1, 2014. Accordingly, companies without privacy and security programs should begin making plans to become compliant with FIPA's new requirements, including documentation of certain policies and procedures. Companies with existing programs should also take the opportunity to audit their own policies and procedures to ensure compliance with the new legislation.

Baker Donelson maintains a Privacy and Information Security team ready to assist you. If you have any questions about FIPA or other data security and privacy issues, please contact a member of our Privacy and Information Security Team.