CARLTON FIELDS

Florida Governor Signs Florida Information Protection Act

June 25, 2014

On April 30, the Florida House of Representatives unanimously passed the Florida Information Protection Act of 2014, Senate Bill 1524. On June 20, 2014, Governor Rick Scott signed the bill into law. The bill becomes effective July 1, 2014. The Act aims to protect Floridians from identity theft by requiring business and governmental entities to protect personal information and report data breaches. Of significant import, the Act requires businesses and governmental entities to report data breaches to the Florida Department of Legal Affairs, and to consumers sooner than previously required. Specifically, the Act requires business and governmental entities to take reasonable measures to protect personal information and to report significant data breaches to the Florida Attorney General's office and to consumers within 30 days, unless good cause is shown for a 15-day extension. The Act also contains provisions to authorize enforcement actions for statutory violations under the Florida Deceptive and Unfair Trade Practices Act (FDUTPA). The civil penalties for FDUTPA violations could be up to $1,000 per day for the first 30 days and $50,000 for each subsequent 30-day period, not to exceed a total of $500,000. "Covered entities" in Florida will need to update their breach policies and procedures to ensure compliance. **Changes To Existing Law: Prior Statute Governing Security Breaches To Be Repealed** Florida's existing data breach statute, section 817.5681, Florida Statutes, requires any person or company that conducts business in Florida and maintains computerized data in a system that includes "personal information" to provide notice of any breach of the security of the system to any Florida resident whose unencrypted "personal information" was, or is reasonably believed to have been, acquired by an unauthorized person. The Florida Information Protection Act of 2014 repeals section 817.5681 and replaces it with a new statute: section 501.171, under the Consumer Protection Chapter of the Florida Statutes. Section 501.171 materially differs from section 817.5681 in several ways. First, the new statute expands the definition of "personal information." The current statute defines "personal information" as an individual's first name, first initial and last name, or any middle name and last name, in combination with a Social Security number, driver's license or Florida Identification Card number, or account, credit card, or debit card number in combination with any required security, access, or passcode allowing access. **The new statute expands the definition of "personal information" to include health insurance policy or subscriber numbers, information regarding an individual's medical history, financial information, and online user names or email addresses in combination**

with their associated passwords or security questions and answers to permit account access. Another important change relates to the timing for reporting the breach to affected individuals. Florida's data breach statute requires notification of the breach to be provided to any affected individuals within 45 days after a breach has been determined. This notice is to be provided in the event it is merely suspected that the information has been acquired by an unauthorized individual. Failure to provide adequate notice could result in administrative fines not to exceed $500,000. **The new statute requires notice to be provided to affected individuals within 30 days. In addition, notice must now be provided to the Florida Department of Legal Affairs for any breach affecting 500 or more individuals within 30 days of the breach unless good cause is provided to the department in writing for an additional 15-day delay. The new statute authorizes the Florida Office of Attorney General to bring enforcement actions under FDUTPA for any statutory violations, but does not create private rights of action for affected individuals.** Additionally, the new statute requires notification to the Department of Legal Affairs of almost every event related to notification or delay of notification to affected persons. For instance, the notification currently required by Florida's data breach statute must be made unless, after an appropriate investigation or after consultation with relevant federal, state, and local law enforcement agencies, the company reasonably determines that the breach has not and will not likely result in harm to the individuals whosand will not likely result in harm to the individuals whose personal information has been acquired and accessed. **The new statute still provides that affected individuals need not be notified if there is a determination that the breach was not harmful; however, it requires that this determination be made after consultation with relevant federal, state, or local law enforcement agencies, and that a copy of that determination be provided to the Florida Department of Legal Affairs within 30 days of the determination.** The new statute also limits the use of a law enforcement delay. Florida's current data breach statute also has an exception to its reporting requirements if a law enforcement agency determines that reporting would impede a criminal investigation. **While the new statute also provides for this sort of law enforcement-related delay in reporting to affected individuals, the Department of Legal Affairs must still be notified of the breach within the prescribed 30 days.** Florida's current data breach statute allows companies to comply with notification procedures pursuant to the rules, regulations, procedures, or guidelines established by the company's primary or functional federal regulator, in lieu of the notification procedures provided in Florida's existing data breach statute. **While notice can still be provided pursuant to a covered entity's primary or functional federal regulator's rules, the new statute also requires a copy of that notice to be provided to Florida's Department of Legal Affairs.**

Related Practices

Business Transactions
Health Care
Cybersecurity and Privacy
Technology

Related Industries

Health Care
Technology

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.