OVER 65 YEARS EXPERIENCE

CELEBRATING 65 years PAVESE LAW FIRM

EMPLOYMENT LAW NEWSLETTER

DECEMBER 2014

# Florida's Information Protection Act of 2014
## What Businesses Should Know

Effective July 1, 2014, Florida's Consumer Protection Statute was amended to add new Section 501.171 to provide that covered entities must report security data breaches to Florida's Department of Legal Affairs if the data security breach affects 500 or more individuals and it also requires that a written notice be sent to the affected individuals. This article will provide an overview of the new law.

***Key Definitions***

A "covered entity" includes any business, regardless of entity type or sole proprietor status, that acquires, maintains, stores or uses the personal information belonging to another. In other words, any business, including government entities, that collects and electronically stores the type of personal information more particularly described below is covered and required to comply with this new law.

A "breach of security" means any unauthorized access of data in electronic form containing personal information and "personal information" means either of the following:[1]

a. An individual's first name or first initial in combination with any one or more of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) 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 permit access to an individual's financial account;

[1] § 501.171(1)(b) and (1)(g) respectively.

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

***Notice to Florida's Department of Legal Affairs***

The information that must be contained in this notice includes: 1) a synopsis of events describing the data security breach; 2) the number of individuals in Florida who may be affected by the data security breach; 3) a description of the services to be provided by the business at no charge to affected individuals; 4) a copy of the notice that will be sent to the affected individuals; and 5) the complete contact information for the business' point of contact. The law further provides that the Department of Legal Affairs may request additional information from the affected business to include police reports and a description of events to rectify the data security breach.

***Notice to Affected Individuals***

At a minimum, the notice shall include: 1) the estimated date or the actual date of the data security breach; 2) a description of the information that was accessed; and 3) contact information regarding who the individual may contact at the business for future information.

***Timing of the Notices***

The general requirement is that both types of notices must be sent within 30 days from discovery of the data security breach. Under certain circumstances additional time may be granted.[2]

***No Private Cause of Action/Unfair Trade Practice***

Florida's Information Protection Act of 2014 does not create a private cause of action but it does allow the State to levy civil penalties up to $500,000 against a covered entity that fails to comply with the notice requirements and note that a failure to comply is considered an unfair or deceptive trade practice.

[2] § 501.171(3) and (4).

CONTINUED ON NEXT PAGE

***Duty to Protect Information***

Of important note and in addition to the requirements set forth above, a covered entity "shall take all reasonable measures to dispose or arrange for the disposal, of customer records containing personal information within its custody or control when the records are no longer to be retained. Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means." In light of this new law, covered entities should review their practices relating to the electronic storage of personal information and developing a policy that sets forth the procedures to be followed if the covered entity is a victim of a data security breach.

*Questions regarding the content of this article may be e-mailed to Christina Harris Schwinn at christinaschwinn@paveselaw.com. To view past articles written by Ms. Schwinn please visit the firm's website at www.paveselaw.com. Ms. Schwinn is a partner and an experienced community association, employment and real estate attorney with the Pavese Law Firm, 1833 Hendry Street, Fort Myers, FL 33901; Telephone: (239) 336-6228; Telecopier: (239) 332-2243.*