

Florida Statutes

Title XLVI – Crimes

Chapter 817 – Fraudulent Practices

Part 1 – False Pretenses and Frauds, Generally

§ 817.5681 Breach of security concerning confidential personal information in third-party possession; administrative penalties.

(1) (a) Any person who conducts business in this state and maintains computerized data in a system that includes personal information shall provide notice of any breach of the security of the system, following a determination of the breach, to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification shall be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3) and paragraph (10)(a), or subject to any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system. Notification must be made no later than 45 days following the determination of the breach unless otherwise provided in this section.

(b) Any person required to make notification under paragraph (a) who fails to do so within 45 days following the determination of a breach or receipt of notice from law enforcement as provided in subsection (3) is liable for an administrative fine not to exceed \$500,000, as follows:

1. In the amount of \$1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, \$50,000 for each 30-day period or portion thereof for up to 180 days.

2. If notification is not made within 180 days, any person required to make notification under paragraph (a) who fails to do so is subject to an administrative fine of up to \$500,000.

(c) The administrative sanctions for failure to notify provided in this subsection shall apply per breach and not per individual affected by the breach.

(d) The administrative sanctions for failure to notify provided in this subsection shall not apply in the case of personal information in the custody of any governmental agency or subdivision, unless that governmental agency or subdivision has entered into a contract with a contractor or third-party administrator to provide governmental services. In such case, the contractor or third-party administrator shall be a person to whom the administrative sanctions provided in this subsection would apply, although such contractor or third-party administrator found in violation of the notification requirements provided in this subsection would not have an action for contribution or setoff available against the employing agency or subdivision.

(2) (a) Any person who maintains computerized data that includes personal information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable, but no later than 10 days following the determination, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The person who maintains the data on behalf of another business entity and the business entity on whose behalf the data is maintained may agree who will provide the notice, if any is required, as provided in paragraph (1)(a), provided only a single notice for each breach of the security of the system shall be required. If agreement regarding notification cannot be reached, the person who has the direct business relationship with the resident of this state shall be subject to the provisions of paragraph (1)(a).

(b) Any person required to disclose to a business entity under paragraph (a) who fails to do so within 10 days after the determination of a breach or receipt of notification from law enforcement as provided in subsection (3) is liable for an administrative fine not to exceed \$500,000, as follows:

1. In the amount of \$1,000 for each day the breach goes undisclosed for up to 30 days and, thereafter, \$50,000 for each 30-day period or portion thereof for up to 180 days.

2. If disclosure is not made within 180 days, any person required to make disclosures under paragraph (a) who fails to do so is subject to an administrative fine of up to \$500,000.

(c) The administrative sanctions for nondisclosure provided in this subsection shall apply per breach and not per individual affected by the breach.

(d) The administrative sanctions for nondisclosure provided in this subsection shall not apply in the case of personal information in the custody of any governmental agency or subdivision unless that governmental agency or subdivision has entered into a contract with a contractor or third-party administrator to provide governmental services. In such case, the contractor or third-party administrator shall be a person to whom the administrative sanctions provided in this subsection would apply, although such contractor or third-party administrator found in violation of the nondisclosure restrictions in this subsection would not have an action for contribution or setoff available against the employing agency or subdivision.

(3) The notification required by this section may be delayed upon a request by law enforcement if a law enforcement agency determines that the notification will impede a criminal investigation. The notification time period required by this section shall commence after the person receives notice from the law enforcement agency that the notification will not compromise the investigation.

(4) For purposes of this section, the terms "breach" and "breach of the security of the system" mean unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person. Good faith acquisition of personal information by an employee or agent of the person is not a breach or breach of the security of the system, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

(5) For purposes of this section, the term "personal information" means an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:

- (a) Social security number.
- (b) Driver's license number or Florida Identification Card number.
- (c) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

For purposes of this section, the term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

(6) For purposes of this section, notice may be provided by one of the following methods:

- (a) Written notice;
- (b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. s. 7001 or if the person or business providing the notice has a valid e-mail address for the subject person and the subject person has agreed to accept communications electronically;
or
- (c) Substitute notice, if the person demonstrates that the cost of providing notice would exceed \$250,000, the affected class of subject persons to be notified exceeds 500,000, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - 1. Electronic mail or e-mail notice when the person has an electronic mail or e-mail address for the subject persons.
 - 2. Conspicuous posting of the notice on the web page of the person, if the person maintains a web page.
 - 3. Notification to major statewide media.

(7) For purposes of this section, the term "unauthorized person" means any person who does not have permission from, or a password issued by, the person who stores the computerized data to acquire such data, but does not include any individual to whom the personal information pertains.

(8) For purposes of this section, the term "person" means a person as defined in s. 1.01(3). For purposes of this section, the State of Florida, as well as any of its agencies or political subdivisions, and any of the agencies of its political subdivisions, constitutes a person.

(9) Notwithstanding subsection (6), a person who maintains:

(a) The person's own notification procedures as part of an information security or privacy policy for the treatment of personal information, which procedures are otherwise consistent with the timing requirements of this part; or

(b) A notification procedure pursuant to the rules, regulations, procedures, or guidelines established by the person's primary or functional federal regulator,

shall be deemed to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with the person's policies or the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security of the system.

(10) (a) Notwithstanding subsection (2), notification is not required if, after an appropriate investigation or after consultation with relevant federal, state, and local agencies responsible for law enforcement, the person reasonably determines that the breach has not and will not likely result in harm to the individuals whose personal information has been acquired and accessed. Such a determination must be documented in writing and the documentation must be maintained for 5 years.

(b) Any person required to document a failure to notify affected persons who fails to document the failure as required in this subsection or who, if documentation was created, fails to maintain the documentation for the full 5 years as required in this subsection is liable for an administrative fine in the amount of up to \$50,000 for such failure.

(c) The administrative sanctions outlined in this subsection shall not apply in the case of personal information in the custody of any governmental agency or subdivision, unless that governmental agency or subdivision has entered into a contract with a contractor or third-party administrator to provide governmental services. In such case the contractor or third-party administrator shall be a person to whom the administrative sanctions outlined in this subsection would apply, although such contractor or third-party administrator found in violation of the documentation and maintenance of documentation requirements in this subsection

would not have an action for contribution or setoff available against the employing agency or subdivision.

(11) The Department of Legal Affairs may institute proceedings to assess and collect the fines provided in this section.

(12) If a person discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at a single time, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.