Publications
June 01, 2014

SECURITY BREACH NOTIFICATION CHART - Puerto Rico

10 L.P.R.A. St § 4051 ***et seq.***

(Scroll down to Ten, Subtitle 3, Chapter 310)

H.B. 1184 (Signed into law Sept. 7, 2005, No. 111).

Effective January 5, 2006

(Scroll down to Ten, Subtitle 3, Chapter 310)

Application. Any entity that is the owner or custodian of a database that includes personal information of residents of Puerto Rico.

Violation of Security System Definition. Any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality, or integrity of the information in the database has been compromised; or when normally authorized persons or entities have had access and it is known or there is reasonable suspicion that they have violated the professional confidentiality or obtained authorization under false representation with the intention of making illegal use of the information.

- This includes both access to the database through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings.

Notification Obligation. Any entity to which the statute applies must notify citizens of any breach of the security system when the breached database contains, in whole or in part, personal information files not protected by encrypted code but only by a password.

Third-Party Data Notification. Any entity that as part of their operations resells or provides access to digital databases that at the same time contain personal information files of citizens must notify the proprietor, custodian, or holder of said information of any violation of the system's security that has allowed access to those files to unauthorized persons.

Timing of Notification. Clients must be notified as expeditiously as possible, taking into consideration the need of law enforcement agencies to secure possible crime scenes and evidence as well as the application of measures needed to restore the system's security.

- Within a non-extendable term of 10 days after the violation of the system's security has been detected, the parties responsible shall inform the Department of Consumer Affairs, which shall make a public announcement of the fact within 24 hours after having received the information.

Personal Information Definition. At least the name or first initial and the surname of a person, together with any of the following data, so that an association may established between certain information with another and in which the information is legible enough so that to access it there is no need to use a special cryptographic code:

- Social Security number;
- Driver's license number, voter identification, or other official identification;
- Bank or financial account numbers of any type with or without passwords or access code that may have been assigned;
- Names of users and passwords or access codes to public or private information systems;
- Medical information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- Tax information; or
- Work-related evaluations.

Neither the mailing nor the residential address is included in the PI, nor is information that is in a public document and is available to the citizens in general.

Notice Required. The notice of the security system breach shall be submitted in a clear and conspicuous manner and should describe the breach in general terms and the type of sensitive information compromised. The notification shall also include a toll-free number and a website for people to use to obtain information or assistance.

Notice may be provided by one of the following methods:

- Written notice; or
- Authenticated electronic means according to 15 U.S.C. § 7001 (E-Sign Act).

Substitute Notice Available. When the cost of notifying all those potentially affected or of identifying them is excessively onerous due to the number of persons affected, to the difficulty in locating all persons, or to the economic situation of the enterprise or entity; or whenever the cost exceeds $100,000 or the number of persons exceeds 100,000, the entity shall issue the notice through the following steps:

- Prominent display of an announcement to that respect at the entity's premises, on the website of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic; and
- A communication to that respect to the media informing them of the situation and providing information as to how to contact the entity to allow for better follow-up. When the information is of relevance to a specific professional or commercial sector, the announcement may be made through publications or programming of greater circulation oriented toward that sector.

Exception. Conflict with preexisting institutional security policies. No provision of this chapter shall be interpreted as being prejudicial to those institutional information and security policies that an enterprise or entity may have in force prior to its effectiveness and whose purpose is to provide protection equal or better to the information on security herein established.

Penalties. The Secretary may impose fines from $500 up to $5,000 for each violation. The fines provided in this section do not affect the rights of the consumers to initiate actions or claims for damages before a competent court.