(H.B. 1184)

(No. 111)

(Approved September 7, 2005)

AN ACT

To create the "Citizen Information on Data Banks Security Act," in order to require that any entity that is the proprietor or custodian of a data bank which includes personal information of citizens who reside in Puerto Rico or that provides access to such data banks, must notify said citizens of any violation of the system's security; to define terms and procedures for notification and dissemination, fix penalties and provide for their regulation and effectiveness.

STATEMENT OF MOTIVES

In the past year over 9.3 million consumers were adversely affected by the identity theft phenomenon within United States jurisdictions. This modality of fraud in which the personal information of another, legally or illegally obtained, is used in an intentional act or through negligence in order to obtain by any means, goods or services, or accede to rights or privileges, or incur obligations or make compromising representations or expressions in the name of the person injured, has greatly increased due to recent technological changes. Making any transaction increasingly depends on data banks that contain information on persons or businesses and whose range has been extended to such a degree that if their security mechanisms suffer any vulnerability, unscrupulous persons are able to assume the identity of another to profit or to maliciously harm third parties.

An insidious modality of this practice consists in the fraudulent configuration of enterprises that, with partial information about a certain consumer, contact those agencies or enterprises that collect marketing or credit information and claim that they are conducting a legitimate transaction to thus obtain additional information about that particular consumer. At present the authorities of at least nineteen (19) states are investigating whether their citizens were affected by a situation that arose at Critical Point, Inc., a company victimized by fictitious "entrepreneurs" who passing for businesses negotiating with the clients of Critical Point obtained information about those clients when in reality they had nothing to do with them. Over 35,000 clients in California and 110,000 in the rest of the nation could have been affected by that situation which came to light in great measure because California is provided with a "statute of transparency" under which any entity that detects a possible violation as to the security of its information must promptly notify its clients.

Several states have followed the example of California; Massachusetts already has a similar law and New Hampshire, New York and Texas are considering such a legislation and analogous legislation has been introduced for the federal forum in Congress.

Regardless of the specific legislation about identity theft contained in the Puerto Rico Penal Code, it is greatly useful to give consumers an additional instrument to protect their good name and credit and safeguard the integrity of their personal information. Thus, this Legislature brings to Puerto Rico this instrument for the protection of the consumer.

BE IT ENACTED BY THE LEGISLATURE OF PUERTO RICO:

Section 1.-This Act shall be known as the "Citizen Information on Data Banks Security Act."

Section 2.-For the purposes of this Act:

(a) "Personal information file" refers to a file containing 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 be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code.

1. Social Security Number.
2. Driver's License Number, Voter's Identification or other Official Identification.
3. Bank or financial account numbers of any type with or without passwords or access code that may have been assigned.
4. Names of users and passwords or access codes to public or private information systems.
5. Medical information protected by the HIPAA.
6. Tax information.
7. Work-related evaluations.

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

(b) "Department" refers to the Department of Consumer Affairs.

(c) "Violation of the Security System" means 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 data bank 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 data banks through the system and physical access to the recording media that contain the same and any removal or undue retrieval of said recordings.

Section 3.-Any entity that is the proprietor or custodian of a data bank for commercial use that includes personal information of citizens who reside in Puerto Rico must notify said citizens of any violation of the system's security when the data bank whose security has been violated contains all or part of the personal information file and the same is not protected by a cryptographic code but only by a password.

Any entity that as part of their operations resells or provides access to digital data banks 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.

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 ten (10) days after the violation of the system's security has been detected, the parties responsible shall inform the Department, which shall make a public announcement of the fact within twenty-four (24) hours after having received the information.

Section 4.-The notice of the violation of the system's security must indicate, as far as the need for any investigation or judicial case in course allows, the nature of the situation, the number of clients potentially affected, whether criminal complaints have been filed, what measures are being taken in the matter and an estimate of the time and cost required to rectify the situation. In case it is specifically known how the confidentiality of the information on an identifiable client was violated, said client shall be entitled to know which information was compromised.

To notify the citizens the entity shall have the following options:

1. Written direct notice to those affected by mail or by authenticated electronic means according to the Digital Signatures Act;
2. When the cost of notifying all those potentially affected according to subsection (1) 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 one hundred thousand (100,000) dollars or the number of persons exceeds one hundred thousand, the entity shall issue the notice through the following two steps:
    a. Prominent display of an announcement to that respect at the entities premises, on the web page of the entity, if any, and in any informative flier published and sent through mailing lists both postal and electronic; and
    b. A communication to that respect to the media informing 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 towards that sector.

Section 5.-No provision of this Act 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.

Section 6.-The Department shall draft and proclaim regulations to comply with the provisions of this Act within one hundred and twenty (120) days after its approval.

Section 7.-Should any provision of this Act be declared unconstitutional or null by any court with jurisdiction or competence, or should it be suppressed by federal legislation, the remaining dispositions shall not be affected and the Act thus modified shall continue to have full force and effect.

Section 8.-The Secretary may impose fines of five hundred (500) dollars up to a maximum of five thousand (5,000) dollars for each violation of the provisions of this Act or its Regulations. 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.

Section 9.-This Act shall take effect one hundred and twenty (120) days after its approval, provided that Section 6 shall take effect immediately after the approval of this Act.

CERTIFICATION

I hereby certify to the Secretary of State that the following Act No. 111 (H.B. 1184) of the 1st Session of the 15th Legislature of Puerto Rico:

AN ACT to create the "Citizen Information on Data Banks Security Act," in order to require that any entity that is the proprietor or custodian of a data bank which includes personal information of citizens who reside in Puerto Rico or that provides access to such data banks, must notify said citizens of any violation of the system's security; to define terms and procedures for notification and dissemination, fix penalties and provide for their regulation and effectiveness,

has been translated from Spanish to English and that the English version is correct.

In San Juan, Puerto Rico, today 6th of February of 2006.

Francisco J. Domenech
Director