

Ley Núm. 111 del año 2005

(P. de la C. 1184), 2005, ley 111

Ley para crear la "Ley de Información al Ciudadano sobre la Seguridad de Bancos de Información"

Ley Núm. 111 de 7 de septiembre de 2005

Para crear la "Ley de Información al Ciudadano sobre la Seguridad de Bancos de Información", a los fines de requerir que toda entidad propietaria o custodia de un banco de información que incluya información personal de ciudadanos residentes en Puerto Rico, o que provea acceso a tales bancos de información, deba notificar a dichos ciudadanos de cualquier violación de la seguridad del sistema; definir términos y procedimientos de notificación y difusión, fijar penalidades y disponer sobre su reglamentación y vigencia.

EXPOSICION DE MOTIVOS

En el pasado año, dentro de las jurisdicciones de los Estados Unidos sobre 9.3 millones de consumidores fueron perjudicados por el fenómeno de la usurpación de identidad. Esta modalidad de fraude en que se usa la información personal ajena, obtenida legal o ilegalmente, por acción intencional o negligencia, para obtener a través de cualquier medio, bienes o servicios, acceder a derechos o privilegios, incurrir obligaciones o hacer representaciones o expresiones comprometedoras a nombre de la persona perjudicada, ha visto un aumento vertiginoso ante los cambios tecnológicos recientes. Cada vez más, la realización de transacciones depende de bancos de información sobre las personas o los negocios, cuya escala ha crecido a tal punto que si surgen vulnerabilidades en sus mecanismos de seguridad, personas inescrupulosas puedan asumir la identidad ajena para lucrarse, o para perjudicar maliciosamente a terceras personas.

Una modalidad insidiosa de esta práctica es la de que se configuren fraudulentamente empresas que, con información parcial sobre un consumidor, acudan a las agencias o empresas que recopilan información de mercado y de crédito so color de estar gestionando una transacción legítima y obtengan así información adicional sobre ese consumidor. En la actualidad, las autoridades de al menos diecinueve (19) estados investigan si sus ciudadanos fueron afectados por una situación en la empresa Critical Point, Inc., víctima de "empresarios" ficticios, que haciéndose pasar por comercios con negocios con los clientes de Critical Point, obtuvieron información sobre esos clientes cuando en realidad no tenían nada que ver con ellos. Sobre 35,000 clientes en California y 110,000 en el resto de la nación pueden haberse afectado por esta situación, que salió a relucir en gran medida porque California dispone de un "estatuto de transparencia" bajo el cual toda entidad que detecte una posible violación de su seguridad de información debe notificar a la clientela con prontitud.

Varios estados han seguido el ejemplo de California; Massachussetts ya tiene una ley similar y New Hampshire, Nueva York y Texas están considerando tal legislación y se ha radicado legislación análoga para el foro federal ante el Congreso.

Independientemente de la legislación específica sobre el delito de usurpación de identidad, contenida en el Código Penal de Puerto Rico, es de gran utilidad darle al consumidor un instrumento adicional para proteger su buen nombre y crédito y salvaguardar la integridad de su información personal. Por tanto, es que esta Asamblea Legislativa procede traer a Puerto Rico este instrumento de protección para el consumidor.

DECRETASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

Artículo 1.-Esta Ley se conocerá como "Ley de Información al Ciudadano sobre Seguridad de Bancos de Información"

Artículo 2.-Para los fines de esta Ley:

(a) "Archivo de información personal" se refiere a un expediente que contenga al menos el nombre o primera inicial y el apellido paterno de una persona, combinado con cualquiera de los siguientes datos de tal manera que se puedan asociar los unos con los otros y en el que la información sea legible sin necesidad de usar para acceder a ella una clave criptográfica especial:

1. Número de Seguro Social
2. Número de Licencia de Conducir, Tarjeta Electoral u otra Identificación Oficial
3. Números de cuentas bancarias o financieras de cualquier tipo, con o sin las claves de acceso que puedan habersele asignado
4. Nombres de usuario y claves de acceso a sistemas informáticos públicos o privados
5. Información médica protegida por la Ley HIPAA
6. Información contributiva
7. Evaluaciones laborales

No se incluye dentro de la información protegida la dirección postal o residencial ni información que sea documento público y esté disponible para la ciudadanía en general.

(b) "Departamento" se refiere al Departamento de Asuntos del Consumidor

(c) "Violación de la Seguridad del Sistema" significa cualquier situación en que se detecte que se ha permitido el acceso de personas o entidades no autorizadas a los archivos de datos de modo que la seguridad, confidencialidad o integridad de la información en el banco de datos quede en entredicho; o cuando haya este acceso por personas o entidades normalmente autorizadas y se sepa o haya sospecha razonable que han violado la confidencialidad profesional u obtuvieron su autorización bajo falsas representaciones con la intención de hacer uso ilegal de la información. Incluye tanto el acceso a los

bancos de información a través del sistema como el acceso físico a los medios de grabación que los contienen y cualquier sustracción o movimiento indebido de dichas grabaciones.

Artículo 3.- Toda entidad propietaria o custodia de un banco de información para uso comercial que incluya información personal de ciudadanos residentes en Puerto Rico, deberá notificar a dichos ciudadanos de cualquier violación de la seguridad del sistema, cuando los bancos de datos cuya seguridad fue violada contuvieran todo o parte de su archivo de información personal y la misma no estuviera protegida con claves criptográficas más allá de una contraseña.

Toda entidad que dentro de sus funciones revenda o provea acceso a bancos de información digitales que a su vez contengan archivos de información personal de ciudadanos deberá notificar al propietario, custodio o tenedor de dicha información de cualquier violación de la seguridad del sistema que haya permitido el acceso a aquellos archivos por personas no autorizadas.

La notificación a la clientela deberá hacerse de la manera más expedita posible, tomando en consideración la necesidad de las agencias del orden público de asegurar posibles escenas de delito y pruebas así como de la aplicación de medidas necesarias para restaurar la seguridad del sistema. Las partes responsables informarán dentro de un plazo improrrogable de diez (10) días de detectarse la violación de la seguridad del sistema al Departamento, el cual hará anuncio público al respecto dentro de veinticuatro (24) horas de recibir la información.

Artículo 4.-La notificación de violación de la seguridad del sistema deberá indicar, hasta donde lo permitan las necesidades de cualquier investigación o caso judicial que se encuentre en curso, la naturaleza de la situación, el número de clientes potencialmente afectados, si se han radicado querellas criminales, qué medidas está tomando al respecto y un estimado del tiempo y costo requerido para rectificar la situación. En el caso que se sepa específicamente en qué se violó la confidencialidad de la información de un cliente identificable, dicho cliente tendrá derecho a conocer qué información quedó en entredicho.

Para notificar a los ciudadanos, la entidad tendrá las siguientes opciones:

1. Notificación escrita directa a los afectados, por vía postal o por vía electrónica autenticada de acuerdo con la Ley de Firmas Digitales;
2. Cuando el costo de notificar a todos los potencialmente afectados de acuerdo al inciso (1) o de identificarlos sea excesivamente oneroso por la cantidad de personas afectadas, la dificultad en localizar a todas las personas, o la situación económica de la empresa o entidad; o siempre que el costo exceda los cien mil (100,000) dólares o el número de personas las cien mil, la entidad llevará a cabo su notificación mediante los siguientes dos pasos:
 - a. Despliegue prominente de un anuncio al respecto en el local de la entidad, en la página electrónica de la entidad, si alguna, y dentro de cualquier volante informativo que publique y envíe a través de listas de correo tanto postales como electrónicas; y

- b. Comunicación al respecto a los medios de prensa, que informe de la situación y provea información sobre cómo comunicarse con la entidad para darle mayor seguimiento. Cuando la información sea de relevancia en un sector profesional o comercial específico, se podrá efectuar este anuncio a través de las publicaciones o la programación orientada a ese sector de mayor circulación.

Artículo 5.-Ninguna disposición de esta Ley se interpretará en perjuicio de aquellas políticas institucionales de información y seguridad que una empresa o entidad tenga en vigor con anterioridad a su vigencia y cuyo efecto sea una protección equivalente o superior a la seguridad de información aquí establecida.

Artículo 6.-El Departamento diseñará y proclamará un reglamento para el cumplimiento de las disposiciones de esta Ley dentro de los ciento veinte (120) días a partir de, su aprobación.

Artículo 7.-Si cualquiera disposición de esta Ley es declarada inconstitucional o nula por algún tribunal con jurisdicción y competencia, o fuere sobreseída por legislación federal, las otras disposiciones no serán afectadas y la Ley así modificada continuará en plena fuerza y vigor.

Artículo 8.-El Secretario podrá imponer multas desde quinientos (500) dólares hasta un máximo de cinco mil (5,000) dólares por cada violación a las disposiciones de esta Ley o de su Reglamento. Las multas dispuestas en este Artículo no afectan los derechos de los consumidores de iniciar acciones o reclamaciones en daños ante un tribunal competente.

Artículo 9.-Esta Ley comenzará a regir ciento veinte (120) días después de su aprobación, disponiéndose que el Artículo 6 tomará efecto inmediatamente después de la aprobación de esta Ley.