

GOBIERNO DE PUERTO RICO

20^{ma.} Asamblea
Legislativa

1^{ra.} Sesión
Ordinaria

SENADO DE PUERTO RICO

P. del S. 375

27 de febrero de 2025

Presentado por la señora *Soto Aguilú*

Referido a la Comisión de lo Jurídico

LEY

Para enmendar los artículos 221, 228 y 229 de la Ley 146-2012, según enmendada, conocida como el “Código Penal de Puerto Rico”, a los fines de aumentar de ocho (8) a quince (15) años, la pena por la comisión de ciertos delitos contra la seguridad en las transacciones comerciales.

EXPOSICIÓN DE MOTIVOS

Existen diversos métodos de fraude relacionados a las tarjetas de crédito y débito, entre las cuales se configura el “skimming” o lectura de la información codificada. Esta conducta consiste en el hurto de la información de una tarjeta de crédito o débito con el objetivo de plasmarla en una tarjeta falsa para realizar transacciones fraudulentas. Este tipo de hurto se realiza utilizando un apartado electrónico para leer y almacenar los datos codificados en las bandas magnéticas en la parte reversa de una tarjeta de crédito o débito. Ejemplos típicos de esta actividad ocurre en los restaurantes, en las máquinas de cajeros automáticos (conocidas como “ATM”), y en las bombas de las gasolineras.

Por ejemplo, en ocasiones se utilizan los aparatos de escaneo y cámaras de micro video que se colocan en las ATM o en las bombas de gasolina para leer y obtener no solo la información de la banda magnética sino el número identificación (conocido como “PIN number”).

Algunas de estas transacciones fraudulentas presentan una variación en el nombre del tarjetahabiente, el cual ha sido alterado para que tanto en la banda magnética, como en el plástico coincidan. Típicamente, este tipo de actividad criminal comienza a través de la participación de un empleado deshonesto de un lugar comercial legítimo. Según se sabe, este empleado adquiere la posesión de la tarjeta de la víctima, cuando la misma se dispone a pagar por algún servicio recibido. Es en ese momento que el empleado aprovecha y pasa la tarjeta por un aparato electrónico que se le conoce como “aparato de escaneo”, el cual copia la información que contiene dicha tarjeta.

Este dispositivo puede ser tan pequeño, que se puede esconder en la palma de la mano con facilidad y puede tener una gran capacidad de almacenamiento, hay por ejemplo uno con capacidad de un (1) gigabyte puede almacenar la información de hasta dos mil cuarenta y ocho (2,048) tarjetas. Los escenarios más comunes donde puede ocurrir este tipo de actividad son restaurantes y los conocidos “pubs”, debido a que el delincuente puede tener la posesión de la tarjeta fuera de la vista del tarjetahabiente, el tiempo suficiente para copiarla.

Las instituciones financieras que emiten tarjetas de crédito o débito experimentan, al menos, tres tipos de pérdidas: (1) los costos asociados a la reemisión de las nuevas tarjetas; (2) los costos relacionados al monitoreo de las cuentas sujetas al fraude; y (3) las pérdidas directas ocasionadas por el fraude. Asimismo, esto conlleva un severo impacto para el cliente de la institución financiera, a saber: (1) Cada transacción tiene que ser evaluada para examinar la posibilidad de una falsificación, por lo tanto muchas de las transacciones grandes son rechazadas o referidas como consecuencia de esta evaluación, lo que afecta el servicio al cliente; (2) Las tarjetas de crédito tienen que ser sustituidas para los clientes, si se detecta un fraude, lo que tiene un impacto adverso para este; (3) Cientos de clientes son objeto de bloqueo en sus cuentas por sospecha de fraude; y (4) la impunidad, si no es atacada severamente en el esquema de fraude, es lo peor que puede pasar, ya que genera mucha más actividad organizada de fraude.

En atención a las consecuencias de este tipo de conducta delictiva, tanto a nivel federal como local, se han aprobado diversas medidas dirigidas a prevenirla y

encausarla. Desde el año 2001, sobre una treintena de jurisdicciones estatales de los Estados Unidos de América han aprobado legislación dirigida a tipificar esta conducta.

Respecto a Puerto Rico, el Código Penal indica que será sancionada con pena de reclusión por un término fijo de ocho (8) años, toda persona que, con el propósito de defraudar a otra, utilice un aparato de escaneo para acceder, leer, obtener, memorizar o almacenar, temporera o permanentemente, información codificada o contenida en la cinta magnética de una tarjeta de crédito o débito o de cualquier otra índole sin la autorización de su legítimo dueño o usuario.

Igualmente, es sancionada con pena de reclusión por un término fijo de ocho (8) años, toda persona que, con el propósito de defraudar a otra, utilice un codificador para colocar información codificada en la cinta o banda magnética de una tarjeta de crédito o débito, en la cinta o banda magnética de otra tarjeta o en cualquier otro medio electrónico que permita que ocurra una transacción sin el permiso del usuario autorizado de la tarjeta de crédito o débito de la cual se obtuvo la información codificada.

Sin embargo, en tiempos recientes, hemos visto como los medios de comunicación han dado cuenta de que el Negociado de la Policía de Puerto Rico investiga diversas querellas de fraude radicadas por varias víctimas de este acto. De hecho, personal de la División de Robos a Bancos del mencionado Negociado ha indicado que, conforme a sus investigaciones preliminares, se entiende que al parecer los sujetos son integrantes de una organización del estado de la Florida.

En los pasados meses, se han recibido varias querellas relacionadas a este tipo de delitos. Estas personas llegan a un comercio, entretienen a la cajera en lo que el otro monta el artefacto en el terminal del comerciante. Existen hasta varios videos que así lo evidencian.

Ciertamente, es nuestra contención que, aunque en el presente el robo de información de tarjetas de crédito o de tarjetas de débito está tipificado en el Código Penal, entendemos que podría tener un efecto disuasivo mayor si para dicha conducta se establecen penas más severas. A tales efectos, se propone enmendar los artículos 221,

228 y 229 de la Ley 146-2012, según enmendada, conocida como el “Código Penal de Puerto Rico”, a los fines de aumentar de ocho (8) a quince (15) años, la pena por la comisión de ciertos delitos contra la seguridad en las transacciones comerciales.

DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

1 Sección 1.- Se enmienda el Artículo 221 de la Ley 146-2012, según enmendada, para
2 que se lea como sigue:

3 “Artículo 221.-Lavado de dinero.

4 Será sancionada con pena de reclusión por un término fijo de **[ocho (8)]** *quince (15)*
5 años toda persona que lleve a cabo cualquiera de los siguientes actos:

6 ...”

7 Sección 2.- Se enmienda el Artículo 228 de la Ley 146-2012, según enmendada, para
8 que se lea como sigue:

9 “Artículo 228.-Utilización o posesión ilegal de tarjetas de crédito y tarjetas de débito.

10 ...

11 Será sancionada con pena de reclusión por un término fijo de **[ocho (8)]** *quince (15)*
12 años, toda persona que con el propósito de defraudar a otra o para obtener bienes y
13 servicios que legítimamente no le corresponden, utilice una tarjeta de crédito o una
14 tarjeta de débito, a sabiendas de que la tarjeta es hurtada o falsificada, la tarjeta ha sido
15 revocada o cancelada, o el uso de la tarjeta de crédito o débito no está autorizado por
16 cualquier razón. Si la persona convicta es una persona jurídica será sancionada con
17 pena de multa hasta treinta mil dólares (\$30,000).

18 ...”

1 Sección 3.- Se enmienda el Artículo 229 de la Ley 146-2012, según enmendada, para
2 que se lea como sigue:

3 “Artículo 229.- Utilización de aparatos de escaneo, *lectores* o codificadores.

4 Será sancionada con pena de reclusión por un término fijo de **[ocho (8)]** *quince (15)*
5 años, toda persona que, con el propósito de defraudar a otra, utilice un *lector de tarjetas*,
6 aparato de escaneo o *codificadores* para acceder, leer, obtener, memorizar o almacenar,
7 temporera o permanentemente, información codificada o contenida en la cinta
8 magnética de una tarjeta de crédito o débito o de cualquier otra índole, o *información*
9 *almacenada de cualquier otra forma en tales tarjetas*, sin la autorización de su legítimo
10 dueño o usuario.

11 Será sancionada con pena de reclusión por un término fijo de **[ocho (8)]** *quince (15)*
12 años, toda persona que, con el propósito de defraudar a otra, utilice un *lector de tarjetas*,
13 *aparato de escaneo o un* codificador para colocar información codificada en la cinta o
14 banda magnética de una tarjeta de crédito o débito, en la cinta o banda magnética de
15 otra tarjeta o en cualquier otro medio electrónico que permita que ocurra una
16 transacción sin el permiso del usuario autorizado de la tarjeta de crédito o débito de la
17 cual se obtuvo la información codificada.

18 ...”

19 Sección 4.- Esta Ley comenzará a regir inmediatamente después de su aprobación.