

PROYECTO DE LEY

La Honorable Cámara de Diputados y la Honorable Cámara de Senadores de la Nación sancionan con fuerza de ley.

ARTICULO 1º: Incorpórese como artículo 30bis de la ley 25065 el siguiente

"ARTICULO 30bis: CANCELACION DE COMPRA POR ESTAFA ONLINE: Cuando el titular de una tarjeta de crédito informe al emisor de la existencia de una compra online que ha sido consecuencia del delito de estafa, conforme lo establecido en el Capítulo IV del Código Penal de la Nación, y ésta estuviera pendiente de autorización, el emisor cancelará la compra denunciada en el plazo de 24 a 48 horas evitando que la misma impacte en el resumen o cuenta bancaria del titular".

ARTICULO 2º: Incorpórese como artículo 30ter de la ley 25065 el siguiente:

"ARTICULO 30ter: En el caso del artículo 30bis, el emisor deberá inmediatamente comunicar al proveedor que la operación que se ha realizado mediante su sitio web es producto del delito de estafa."

ARTICULO 3º: Incorpórese como artículo 29bis el siguiente:

"ARTICULO 29bis – DEBER DE INFORMACION – En cumplimiento de lo dispuesto por el artículo 4º de la ley 24240, una vez aceptadas las explicaciones dadas por el titular de las tarjetas bancarias o cancelada la compra en el caso del artículo 30bis, la entidad deberá comunicárselo por un medio fehaciente y de manera clara, precisa, teniendo en cuenta las herramientas de conocimiento con las que cuenta el titular, por lo que la comunicación deberá mínimamente contener:

- a) Indicación precisa con montos, fechas, numero de operación y todo otro elemento que resulte necesario para identificar el concepto u operación que ha sido reconocido por la entidad.*
- b) Explicación precisa y clara del mecanismo que se utilizará para la devolución del monto reconocido y como lo verá impactado el titular en su resumen bancario.*

ARTICULO 4º: Los proveedores de tarjetas de compra, deberán adecuar sus sistemas a los fines de lo establecido en la presente ley, en el plazo de 30 días contados a partir de su publicación.

ARTICULO 5º: Comuníquese al Poder Ejecutivo Nacional.

FUNDAMENTOS

Sr. Presidente

Las estafas virtuales mediante el uso de tarjetas de crédito es una realidad innegable que la mayoría de la población ha sufrido y que claramente a pesar de las precauciones que los usuarios toman para evitarlas llegan a concretarse.

La legislación actual es vasta en materia de "ciberseguridad" en cuanto a la existencia de leyes, decretos, resoluciones, disposiciones y decisiones administrativas, por mencionar alguna de las leyes vigentes Ley 23.554 Defensa Nacional, Ley 24.059 Seguridad Interior, Ley 25.506 Firma Digital, Ley 25.326 Protección de Datos Personales, Ley 26.388 Delitos Informáticos, Ley 26.904 Grooming, Ley 27.411 Convenio sobre Ciberdelito del Consejo de Europa.(Convención de Budapest), Ley 27.436 Modificación art. 128 Código Penal, Ley 27.590 Creación del Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra Niñas, Niños y Adolescentes, Ley 27.699 Protección De Las Personas Con Respecto Al Tratamiento Automatizado De Datos De Carácter Personal.

Sin perjuicio de ello, a pesar de todos los esfuerzos normativos, la evolución de internet y la tecnología han abierto nuevas puertas al mundo digital y con ello han dado paso a delitos cibernéticos e infracciones basadas principalmente en estafas a través del uso indebido y fraudulento de las tarjetas de crédito y débito sobrepasando nuestra capacidad legislativa y dejando al descubierto a los consumidores o usuarios de los servicios brindados por las entidades bancarias y los emisores de estas, por lo que resulta necesario adoptar todas las medidas que resulten útiles para brindar mayor protección y continuar adaptando la legislación.

El objeto de normas de ciberseguridad es el resguardo de empresas y usuarios que operan en el entorno digital tratando de salvaguardar los datos digitales en sistemas que se encuentran interconectados y garantizar que las compras de bienes o servicios que se ejecutan usando aplicaciones o páginas web, es decir compras virtuales, resulten seguras.

Distintas son las técnicas utilizadas para llevar adelante las estafas mediante el uso indebido de las tarjetas de crédito o débito, una de las más usadas es hacerse pasar por empresas ficticias o que imitar a una existente para que el usuario, sin darse cuenta, comparta todas sus claves de acceso a la banca online y así poder robarles, otra es la de suplantar la identidad de entidades bancarias para enviar alertas falsas sobre movimientos sospechosos en las cuentas o bloqueos por motivos de seguridad con el objetivo de generar preocupación en el usuario para que este comparta sus datos sin dudarlo.

Se suman a los modos de estafa mencionados precedentemente, el skimming y el shoulder surfing. La primera consiste en robar la información de las tarjetas de crédito o débito, con el fin de clonaras o reproducirlas para un uso fraudulento posterior utilizando un dispositivo tecnológico conocido como "skimmer", el cual es tan pequeño que cabe en el bolsillo del pantalón y está diseñado para leer la banda magnética de la tarjeta utilizada en una transacción y recopilar la información. El segundo conocido como "shoulder surfing" se trata de una técnica que implica robar datos personales observando a la víctima mientras utiliza dispositivos electrónicos en su vida diaria como cajeros automáticos, terminales de pago en comercios, computadoras o celulares.

Por resolución N°424/2020 de la Secretaria de Comercio Interior, las tiendas o páginas web que venden productos o servicios como así también las aplicaciones pago tienen la obligación de contar en sus plataformas digitales lo que se denomina "botón de arrepentimiento", herramienta que le permite al usuario o consumidor cancelar la compra cualquiera fuere el motivo en un plazo de 10 días desde efectuada la compra o celebrado el contrato. Ahora bien, este botón que la mayoría de las veces tiene que ver con una cuestión de elección, voluntad o preferencia subjetiva resulta útil obviamente cuando es el titular de la compra o suscripción el que decide cancelarla, pero situación distinta ocurre cuando un tercero, no titular, realiza fraudulentamente cualquiera de las acciones mencionadas porque claramente no va a desistir de su accionar.

Frente a la realización de una operación virtual que implique la actuación bancaria mediante el uso de las tarjetas sin el consentimiento de su titular y claramente habiendo obtenido sus datos y los de sus tarjetas de manera ilegal e ilegítima, deben activarse los sistemas de seguridad predispuestos por los proveedores o emisores de éstas a los fines de preservar la propiedad patrimonial de los usuarios.

Ante la comisión del delito de estafa "virtual", la primera respuesta de las entidades bancarias o financieras es la contenida en el Capítulo X (arts. 26 y subsiguientes) de la ley N°25065 de "Tarjetas de Crédito" que brinda al cliente la posibilidad de proceder a la "impugnación o cuestionamiento de la liquidación o resumen bancario", lo que vulgarmente conocemos como "desconocimiento de la compra", sin embargo, este remedio provisorio que no solo es engorroso, lento y no puede ser realizado por cualquier usuario porque la mayoría de las veces se trata de adultos mayores que no tiene las herramientas suficientes para ejecutar el reclamo, no evita que la estafa llegue a su fin porque los sistemas de las entidades no permiten cancelar la transacción sino hasta que impacta en el resumen del usuario, lo que sucede dentro de las 24 o 48 de realizada la misma; ello sucede porque es el proveedor del bien o servicio quien puede cancelarla por pedido del usuario, pero es claro que un delincuente no va a solicitarle la cancelación.

Que, en este orden de ideas resulta necesario que los emisores adecuen sus sistemas de manera que les resulte posible cancelar las compras cuando las mismas sean denunciadas como consecuencia o resultado de una estafa antes de que impacten en la cuenta bancaria del titular, debiendo notificar esta situación a los proveedores a los fines de que las acciones sean consecuentes.

Por último, y en estricto cumplimiento de lo dispuesto por el artículo 4 de la ley 24240 (ley de defensa del consumidor) las comunicaciones emitidas por las entidades bancarias o financieras una vez que los conceptos han sido reconocidos no puede solo limitarse a un informe escueto, inentendible, vago y poco preciso sin explicaciones acerca de como ese reconocimiento se verá

reflejado en los próximos resúmenes bancarios del titular, por lo que resulta indispensable que la comunicación contenga al menos información clara y precisa de los montos, fechas de compra, número de operación y todo otro elemento que resulte necesario para identificar el concepto u operación que ha sido reconocido por la entidad, como también una explicación clara del mecanismo que se utilizará para la devolución del monto reconocido y como lo verá impactado el titular en su resumen bancario.

A esos fines, la normativa vigente debe ser modificada en su parte pertinente y por ello es que solicito a mis pares el acompañamiento del presente proyecto.

Yolanda G. Vega

Diputada Nacional