Boletín N° 11.078-03

Proyecto de ley, iniciado en moción de los Honorables Senadores señor Ossandón, señora Pérez San Martín y señor Tuma, que modifica la ley N° 20.009, que limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas, en lo relativo a la responsabilidad del usuario y del emisor en casos de uso fraudulento de estos medios de pago.

Fundamentos e ideas matrices

El 1 de abril de 2005 fue publicada la ley 20.009, que crea un marco jurídico de exención de responsabilidad para el tarjetahabiente respecto de los robos, extravíos y hurtos de sus tarjetas de crédito o débito, en cuanto el propio usuario denunciara tal hecho al emisor.

Esta mecánica permite al tarjetahabiente desligarse de los montos cargados o girados de la tarjeta a partir del minuto de la denuncia presentada frente al emisor, trasladando la responsabilidad a este último para la persecución de las operaciones que pudiesen realizarse con posterioridad a ese instante.

Si bien este mecanismo ha funcionado de forma adecuada desde la publicación de la ley, cumpliendo el objetivo de desligar al usuario de la responsabilidad, actualmente podemos identificar algunas derivadas que hacen imperioso ajustar la ley al escenario presente.

De especial interés del proyecto de ley en estudio es el gran aumento de delitos de uso fraudulento de tarjetas, que entre 2014 y 2015 se duplicó, pasando de 17.300 a 34.300[1].

En el escenario internacional existen variadas cifras, de acuerdo a las agencias policiales de la Unión Europea, anualmente el fraude con tarjeta genera 1,5 billones de Euros en pérdidas[23], mientras que en los Estados Unidos con se reportan pérdidas para los emisores por más de 10,9 billones de Dólares, principalmente en fraudes con tarjeta de crédito (71%), seguidos de fraudes con tarjetas de débito (25%) y las tarjetas de prepago (0,5%)[4].

A pesar de contar con complejas cifras, el fraude con tarjeta -al menos a nivel internacional- no ha generado cambios radicales en la forma en la que funcionan y autorizan las operaciones, a tal punto, que algunos especialistas señalan que esto se debería a que los montos involucrados en el fraude son una fracción muy menor de lo que costaría cambiar el sistema para hacerlo más seguro, lo que se debería en parte a que son los comercios quienes absorben gran parte de las pérdidas[5].

Fraudes con o sin tarjeta

La literatura técnica sobre la materia reconoce, principalmente, dos grandes categorías de fraude para el interés del presente proyecto: Fraudes con tarjeta presente, y fraudes sin tarjeta presente.

A la primera categoría corresponden los delitos definidos en el artículo 5º, letras a), b), c) y f) de la ley 20.009, mientras que a la segunda corresponden las letras d) y e) del mismo artículo.

El fraude con tarjeta presente corresponde a las transacciones efectuadas mediante una tarjeta encontrada, hurtada o robada; o bien por medio de una tarjeta falsificada que cuenta con información de pago válido en su banda magnética o chip electrónico, en un escenario en el que el defraudador presenta físicamente la tarjeta al comercio que recibirá el pago.

Por otro lado, el fraude sin tarjeta presente se da, normalmente, en el comercio electrónico o las ventas telefónicas, en cuanto el uso fraudulento no requiere que la persona presente físicamente la tarjeta para la inspección del vendedor, sino que sólo deberá entregar los datos necesarios para operarla, como el número, nombre del titular, fecha de vencimiento y el código CVV (Card Verification Value).

Es en este espacio donde la ley 20.009 no contempló un régimen que regulara la responsabilidad del emisor y el tarjetahabiente, en cuanto todos los supuestos de la ley respecto de la responsabilidad recaen en escenarios donde se extravía, roba o hurta físicamente una tarjeta y el tarjetahabiente notifica al emisor de tal hecho.

Derecho Comparado

El régimen de responsabilidad del emisor y el tarjetahabiente tiene diferentes aproximaciones en el derecho comparado.

En el Reino Unido, el usuario es responsable de las operaciones realizadas fraudulentamente con sus tarjetas hasta $50 libras, cuando dichos fraudes ocurren por extravío, hurto o robo de la tarjeta y no notifica al emisor de tal hecho, o cuando falla en proteger las medidas personalizadas de seguridad -normalmente la clave- de la apropiación por parte de terceros[6].

Asimismo, el usuario en el Reino Unido no será responsable en ningún caso cuando haya realizado la notificación al emisor del extravío, hurto o robo de la tarjeta; cuando el emisor no haya puesto a disposición del usuario un método para notificar el extravío, hurto o robo; y cuando el medio de pago ha sido utilizado en “un contrato a distancia”, es decir, a través de medios no presenciales como el comercio electrónico o la contratación telefónica[7].

En España la Ley 16/2009 de Servicios de Pago cuenta con un régimen de exención de responsabilidad del usuario, distinguiendo entre operaciones autorizadas y no autorizadas por el titular[8].

En general, la ley española contiene grandes similitudes con el régimen inglés, en cuanto hace responsable al emisor de todas las operaciones no autorizadas por el tarjetahabiente, y lo obliga a restituir los montos defraudados al usuario, dependiendo del caso. Asimismo, hace responsable al usuario hasta €150 euro por las operaciones realizadas con tarjetas extraviadas, hurtadas o robadas, a menos que éste notifique al emisor.

Finalmente, la ley española hace responsable al tarjetahabiente por el total de las pérdidas en caso de haber actuado fraudulenta o negligentemente[9].

En Estados Unidos, el régimen aplicable difiere si se trata de tarjetas de crédito o débito, pero comparten similitudes con la legislación comparada del Reino Unido y España. En este sentido, el tarjetahabiente es responsable de las pérdidas hasta por US$50 en casos en que se realizan transacciones no autorizadas por el titular, pero habiendo sido notificado el emisor del extravío, hurto o robo[10]. En aquellos casos en los que no se notifica, el tarjetahabiente será responsable por hasta US$500.

Perú por su parte, posee un marco regulatorio bastante específico dictado en 2013[11] que abarca desde medidas de seguridad en las comunicaciones realizadas con motivo de las operaciones de tarjetas, así como reglas sobre el manejo de datos, hasta medidas de seguridad para los comercios, por nombrar algunas.

Al respecto, la normativa peruana reconoce que el usuario no podrá ser tomado como responsable de las transacciones que no ha autorizado, y menciona explícitamente que opera de la misma forma cuando las tarjetas hayan sido clonadas[12]. Reproduce, además, la mecánica de notificación ya vista en otros casos de derecho comparado.

Nuevos sistemas de pago

Además de los medios de pago basados en tarjetas, como la de crédito o débito, en el último tiempo se ha iniciado un extenso proceso para ampliar el catálogo de medios disponibles en el país. Dentro de los más relevantes se encuentran las tarjetas de pago con provisión de fondo emitidas por bancos, instituciones financieras o entidades no bancarias[13].

Asimismo, se ha autorizado a la empresa METRO S.A. a emitir tarjetas de pago con provisión de fondos para permitir la utilización no solo del transporte público, sino también el pago de bienes y servicios de cualquier tipo utilizando el mismo instrumento[14], lo anterior se agrega a la existencia de la ya vetusta tarjeta BIP!, que corresponde a una tarjeta de pago con provisión de fondos restringida al pago en el sistema de transporte.

También es relevante la llegada al país de algunas funcionalidades de sistemas de pago como PayPal[15] de la mano de MultiCaja que permite, a través de transferencias bancarias a MultiCaja, el uso de PayPal en cualquier parte del mundo para el pago de bienes y servicios; o la llegada de Mercadopago[16] que, entre otras funciones, permite recolectar dinero a través del sistema.

En otro tipo de servicios atingentes, podemos encontrar a RecargaFácil[17] -también de Multicaja- para el pago por recargas de servicios telefónicos o de TV de Pago; Khipu[18] que opera facilitando transferencias bancarias entre cada cliente; PagoRUT[19] del BancoEstado que permite realizar y recibir pagos por medio de la aplicación, utilizando los saldos disponibles en la Cuenta RUT del banco; o Pagoclick[20] de Copec para el pago de combustible pero utilizando tarjetas de crédito sobre la infraestructura de WebPay OneClick de Transbank[21].

Similar a PagoRUT de BancoEstado, encontramos una serie de otros sistemas basados en el pago vía aplicaciones móviles, como BBVA Wallet[22] que permite el pago contra la tarjeta de crédito del banco; de BancoChile se encuentra disponible la app Mi Pago[23], también orientada a la realización o recepción de pagos mediante códigos QR o sistemas NFC. En general, existe un amplio catálogo de soluciones ofrecidas por los bancos, pero siempre de manera propietaria y circunscrita a los servicios del banco.

Fuera de la categoría del pago bancario, es necesario hacer mención de los revolucionarios medios de pago basados en monedas criptográficas con modelo distribuido[24], en las que solo la oferta y demanda por dichas monedas fija su valor, sin necesidad de contar con el control de un Banco Central.

Tal es el caso de Bitcoin, y variantes similares que podemos encontrar funcionando en Chile en muy menor escala, pero que han iniciado la llamada “Revolución de la Cadena de Bloques” (Blockchain Revolution), y que ha comenzado a permear distintas industrias con el modelo descentralizado y distribuido de la Cadena de Bloques para cosas tan diferentes como la autenticación de identidades, hasta la trazabilidad de bienes en el mercado[25].

Ciertamente, a pesar de aún contar con una matriz de pago cuyos principales exponentes siguen estando basados en el intercambio a través de tarjetas de crédito o débito, existe mayor variedad de servicios que no funcionan con la lógica de las tarjetas, que las que igualmente pueden ser objeto de fraude y donde corresponde, de la misma forma, analizar la responsabilidad del usuario y el emisor en tales casos.

Responsabilidad del usuario y el emisor

Actualmente, la ley 20.009 contempla un régimen de excepción de responsabilidad para el tarjetahabiente frente al uso fraudulento de las tarjetas, basado en un sistema de notificación al emisor el cual deberá -a partir de tal notificación- tomar las providencias del caso para prevenir el mal uso de la tarjeta o la información que ésta posee.

Esta fórmula funciona bajo el supuesto que el tarjetahabiente conoce del uso fraudulento de la tarjeta, o al menos de la amenaza de uso fraudulento ya sea porque la tarjeta se ha extraviado, ha sido hurtada o robada, por lo que carga sobre su persona la obligación de notificar al emisor para eximirse de la responsabilidad de las transacciones efectuadas a partir de ese momento[26].

El problema que presenta esta lógica es la relativa indefensión en la que queda el tarjetahabiente -o el usuario de otros medios de pago- cuando la operación fraudulenta ocurre bajo la total ignorancia del titular, frecuentemente como resultado de la clonación del instrumento u otros métodos similares. El tarjetahabiente o el usuario solo se notifica de tales operaciones cuando recibe los cargos en el balance de la tarjeta o de su cuenta.

En tal escenario, el tarjetahabiente no tiene oportunidad de notificar de nada sospechoso al emisor, por lo que las providencias de la ley 20.009 no se ejecutan.

A pesar de esto, parece ser justo mencionar que el mercado ha actuado de forma relativamente razonable con este tipo de casos, cubriendo el emisor las operaciones efectivamente fraudulentas y liberando al titular de tales cargas, como parte de un sistema de negociación pública entre las autoridades y la industria[27].

Sin embargo, subsisten prácticas altamente discutibles, las cuales son también objeto del proyecto en discusión.

Desde el punto de vista judicial, podemos encontrar pronunciamientos específicos de la justicia respecto de la responsabilidad tanto del emisor como del tarjetahabiente basados en las disposiciones de la ley 19.496 sobre protección de los derechos de los consumidores. De especial interés resulta la querella infraccional presentada contra el Banco de Chile por autorizar operaciones no realizadas por el tarjetahabiente, incluso luego de haber sido bloqueada la tarjeta de débito del actor[28].

El actor describe la situación típica que se encuentra en estudio: se realizan cargos a su cuenta corriente por medio de su tarjeta de débito, utilizando los datos de la banda magnética y su clave personal, por lo que el banco los autoriza, sin embargo, alega que tales operaciones nunca fueron realizadas por el tarjetahabiente.[29]

En segunda instancia la Corte de Apelaciones de Santiago acogió la querella infraccional contra el Banco de Chile (o Banco Edwards) por no tomar las medidas de seguridad necesarias para determinar si quien operó la tarjeta de débito del demandante fue realmente éste, en el escenario típico de un fraude por clonación de la banda magnética de la tarjeta.

Los argumentos de la Corte señalan “[...]que en el presente caso se incurrió efectivamente en infracción a lo dispuesto en el artículo 23 de la Ley N° 19.496, al no emplearse las medidas de seguridad y resguardo necesarios en el uso y manejo de la tarjeta de débito/crédito, que permitiesen comprobar que la persona que efectuó los

giros de dinero realmente haya sido la legítimamente autorizada, en este caso, el actor.”[30].

Agrega además “[...]el solo hecho que las transacciones denunciadas figuraran aparentemente como efectuadas por el titular, no permite liberar a la institución bancaria que cursó los giros de la obligación de actuar con la debida diligencia, responsable y cuidadosamente, impidiendo la materialización de sucesivas transacciones mientras no se verificara la legitimidad de las operaciones, máxime si se tiene en consideración que este modus operandi corresponde precisamente a una de las formas clásicas de fraudes por clonación de tarjetas de débito y crédito.”[31].

Se hace evidente que la ley 20.009 no resuelve por medio del sistema de notificaciones al emisor el escenario antes descrito, por lo que los particulares y los tribunales de justicia han recurrido a la ley de protección del consumidor para fijar la obligación del emisor en estos casos, consistente en medidas de seguridad suficientes para garantizar que quien realiza las operaciones con las tarjetas sea, efectivamente, el tarjetahabiente; superando de esta forma -y tal como lo desarrolla la Corte de Apelaciones- el modelo de notificaciones y bloqueo de los medios de pago como medida de exención de responsabilidad del emisor o del usuario según corresponda.

De este escenario nacen situaciones perjudiciales tanto para el consumidor o usuario de los medios de pago, como para el mercado retail y financiero.

El proyecto en estudio propone abordar los plazos en los que deberán los emisores retornar los importes pagados en operaciones fraudulentas[32], la inducción a la contratación de seguros para cubrir los montos defraudados y las cláusulas contractuales que liberen de responsabilidad al emisor, o que la distribuyan o trasladen a otros miembros de la cadena de pago.

Delitos relacionados con el uso de medios de pago

La literatura científica reconoce una amplia variedad de delitos asociados al uso de tarjetas de crédito o débito[33]. Los más relevantes actualmente, además del siempre presente robo o hurto de la tarjeta, corresponden al phishing, pharming y skimming por un lado, la clonación de tarjetas, y la generación de tarjetas virtuales, también llamada carding, por otro.

El phishing se vale del uso de correos electrónicos o sitios web especialmente confeccionados para otorgar apariencia de legitimidad simulando la marca o presencia en línea de un banco o institución financiera, y de esta forma, obtener del titular los datos necesarios para la realización de operaciones bancarias[34].

Al respecto de este tipo, la jurisprudencia está dividida, dando lugar a variados fallos absolutorios[35] en favor del banco[36], que contrastan con aquellas posiciones tendientes a la protección del consumidor frente a las estafas realizadas o facilitadas por este medio.

El llamado skimming corresponde al hurto de los datos almacenados en las bandas magnéticas de las tarjetas a través de un dispositivo (skimmer) que registra la información al ser deslizada la tarjeta a través de él[37].

El uso del skimmer se genera normalmente en lugares donde se facilita la tarjeta a un tercero para su operación en un Terminal de Punto de Venta (o POS por sus siglas en inglés), como un restaurante o una estación de combustibles; o incluso son instalados en cajeros automáticos y la clave de usuario es capturada por medio de microcámaras de video alojadas sobre el teclado del dispositivo.

A continuación, el autor del hurto cuenta con algunos de los datos más importantes de la tarjeta para poder clonarla y darle uso, por ejemplo, a través del comercio electrónico, o incluso retirando dinero desde los cajeros automáticos antes que el tarjetahabiente o el emisor se den por notificados de la estafa.

Propuestas y estructura del proyecto

Los delitos descritos anteriormente, al igual que la clonación de las tarjetas, pueden ser abordado a través de las normas del Código Penal o la ley de delitos informáticos 19.223[38], según corresponda, o la propia ley 20.009 que establece penas a distintos hechos punibles relacionados con el uso fraudulento de tales instrumentos. Desde el punto de vista infraccional y la responsabilidad del emisor, la jurisprudencia ha encasillado este tipo de comportamientos en el artículo 23 de la ley de protección del consumidor, respecto de la seguridad en el consumo que debe ser garantizada por el proveedor, como ya lo hemos visto anteriormente.

Sin embargo, el tratamiento de la responsabilidad del tarjetahabiente respecto de los delitos realizados con técnicas como la clonación, el skimming, o en general, todos aquellos en que el fraude se realiza sin conocimiento del titular, no cuenta con reglas especiales como sí cuentan el robo o hurto de la tarjeta de crédito o débito en la ley 20.009.

Para el establecimiento de un régimen especial de responsabilidad del usuario y emisor de los medios de pago, el proyecto en estudio propone una serie de modificaciones a la ley 20.009 para incorporar el concepto de “medio de pago” como objeto genérico en el que pueda identificarse no solo a las tarjetas de crédito como en el régimen vigente, sino también a otros sistemas que permitan la compra y venta de bienes y servicios, por ejemplo, a través de transacciones electrónicas que no involucren tarjetas.

Asimismo, el proyecto incorpora en el artículo 5º a las tarjetas con provisión de fondos emitidas por instituciones autorizadas de acuerdo a la legislación vigente, en cuanto son objeto del mismo tipo de delitos que las tarjetas de crédito o débito. Incorpora, además un nuevo literal al artículo para penar la suplantación del usuario frente al emisor para conseguir datos que permitan operar un medio de pago.

Las modificaciones al artículo 5º no incorporan otros medios de pago distintos de las tarjetas, en cuanto la responsabilidad por delitos relacionados con la irrupción en sistemas de tratamientos de información ya se encuentran penados en la ley 19.223 que tipifica figuras penales relativas a la informática.

El proyecto propone, también, un aumento en las penas para quienes incurran en los delitos descritos en el artículo 5º.

A continuación, agrega tres nuevos artículos que detallan el régimen de exención de responsabilidad del usuario frente a los fraudes realizados sin que éste pueda estar en conocimiento de tal hecho, como en los casos de la clonación de una tarjeta o la sustracción de credenciales que permitan operar un medio de pago electrónico desde un banco de datos.

De la misma forma, fija un plazo de 24 horas a los emisores para la devolución de los importes, si corresponde, en los casos de fraude, la prohibición de requerir el cumplimiento de condiciones para tales devoluciones, como la contratación de seguros (ampliamente presentes en el mercado[39]), u otras medidas burocráticas.

Finalmente, el proyecto propone la obligación para el emisor de contar con medidas adecuadas de protección para el medio de pago, siguiendo la pauta fijada por el artículo 23 de la ley sobre protección de los derechos de los consumidores, pero haciendo responsable al emisor de los perjuicios causados por las deficiencias en este campo, en cuanto es de opinión de los autores del proyecto que la facilidad con la que hoy es posible defraudar los medios de pago como las tarjetas de crédito y similares, se debe a las escasas o insuficientes medidas de seguridad con las que cuentan, y no necesariamente a un actuar particular del titular, sin dejar de reconocer la complejidad que este sistema plantea a la hora de mantener un mercado de pago dinámico, de simple utilización y, a su vez, seguro.

POR LO TANTO,

Venimos en someter a discusión el siguiente

PROYECTO DE LEY

ARTÍCULO ÚNICO

Modifícase la ley 20.009 que limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas, de la siguiente forma:

1. Reemplázase el título de la ley por el siguiente: “Establece un régimen de limitación de responsabilidad en casos de fraude para emisores y usuarios de medios de pago”

2. Reemplázanse los artículos 1º y 2º por los siguientes:

“Artículo 1º.- Definiciones. Para los efectos de la presente ley, sin perjuicio de la normativa bancaria o financiera vigente; y de lo señalado en la ley 19.496 que establece normas sobre los derechos de los consumidores, los siguientes conceptos se entenderán de la forma en que se señala:

a) Usuario: El tarjetahabiente de tarjetas de crédito, débito, de pago con provisión de fondos, emitidas por las entidades autorizadas por la ley; el titular de una cuenta que permita el pago por medios electrónicos, aunque este no conste de un instrumento físico como una tarjeta magnética o un dispositivo electrónico; en general, la persona que sea titular de un medio de pago distinto del dinero en efectivo, cheque o vale a la vista; o tenedor de éste cuando se tratare aquellos emitidos al portador.
b) Emisor: La empresa que disponibiliza o pone en circulación el medio de pago autorizado por la ley, cuando corresponda; aquella que afilia a los comercios para la utilización de un medio de pago; o aquella que procesa operaciones realizadas con los medios de pago
c) Comercio: El establecimiento que recibe pagos del usuario y que se encuentra afiliado, mediante actos o contratos, con el emisor o sus representantes.
d) Medio de pago: Cualquier sistema distinto del dinero en efectivo, el cheque o vale a la vista, que permita el pago de bienes y servicios en los comercios afiliados por o para el emisor, retiros de dinero u otras operaciones a través de los canales ofrecidos por el emisor.”

Artículo 2º.- Los usuarios podrán limitar su responsabilidad en los términos establecidos por esta ley, en caso de hurto, robo o extravío del medio de pago o de las credenciales que permiten operarlo, dando aviso pertinente al emisor.

El emisor deberá proveer al usuario servicios de comunicación, de acceso gratuito y permanente, que permitan recibir y registrar los referidos avisos. Por el mismo medio de comunicación, y en el acto de recepción, el emisor deberá entregar al usuario un número o código de recepción del aviso y la fecha y hora de su recepción.

Los medios de pago por los que el usuario haya dado aviso de extravío, hurto o robo, serán bloqueados de inmediato por el emisor.”

3. Reemplázanse en el artículo 3º la expresión “las tarjetas sean operadas” por “los medios de pago sean operados”; y la palabra “tarjetahabiente” por “usuario” en las dos ocasiones en las que aparece.

4. Reemplázase en el artículo 4º la palabra “tarjetahabiente” por “usuario”.

5. Reemplázase el artículo 5º por el siguiente:

“Artículo 5º.- Las siguientes conductas constituyen delito de uso fraudulento de tarjeta de crédito, de pago con provisión de fondos o débito:

a) Falsificar tarjetas de crédito, de pago con provisión de fondos o débito.
b) Usar, vender, exportar, importar o distribuir tarjetas de crédito, con provisión de fondos o débito falsificadas o sustraídas.
c) Negociar, en cualquier forma, con tarjetas de crédito, de pago con provisión de fondos o débito falsificadas o sustraídas.
d) Usar, vender, exportar, importar o distribuir los datos o el número de una tarjeta de crédito, de pago con provisión de fondos o débito, haciendo posible que terceros realicen operaciones de compra o de acceso al crédito, los fondos o al débito que corresponden exclusivamente al titular.

---

[1] La Tercera, "Fraudes con tarjetas bancarias casi se duplicaron en 2015", 20 de enero de 2016. Disponible en http://www.latercera.com/noticia/fraudes-con-tarjetas-bancarias-casi-se-duplicaron-en-2015/

[2] EUROPOL, "Payment Card Fraud in the European Union. Perspective of Law Enforcement Agencies". 20 de septiembre de 2012. Disponible en https://www.europol.europa.eu/sites/default/files/documents/1public_full_20_sept.pdf

[3] También Cfr. Banco Central Europeo. "Fourth report on card fraud". 15 de julio de 2015. Disponible en https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

[4] Consultora Rippleshot, "State of Card Fraud: 2016", *white paper*, pp. 3-4. Disponible en http://info.rippleshot.com/blog/chip-pin-emv-wont-stop-fraud-heres

[5] Al respecto, "*So why is the U.S. so far behind? It seems to come down to money. The losses for banks do not yet exceed the costs of a switch-over, although merchants say that's because they usually shoulder much of the cost burden from fraud.*". Consumer Reports "House of Cards". Consumer Reports Magazine, edición de julio de 2011. Artículo disponible en http://www.consumerreports.org/cro/magazine-archive/2011/june/money/credit-card-fraud/overview/index.htm

[6] "The Payment Services Regulations" de 9 de febrero de 2009, sección 62, parr. 1. Disponible en http://www.legislation.gov.uk/uksi/2009/209/pdfs/uksi_20090209_en.pdf

[7] Ibid. Sección 62, parr. 3.

[8] Ley 16/2009 de Servicios de Pago, artículo 26, número 1, disponible en https://www.boe.es/buscar/act.php?id=BOE-A-2009-18118

[9] Ibid. Art. 32, número 2.

[10] Federal Trade Commission, "Disputing Credit Card Charges". disponible en https://www.consumer.ftc.gov/articles/0219-disputing-credit-card-charges

[11] Resolución SBS 6523-2013, disponible en http://busquedas.elperuano.com.pe/normaslegales/aprueban-el-reglamento-de-tarjetas-de-credito-y-debito-resolucion-n-6523-2013-1008675-1/

[12] Ibid. art 23, inciso segundo, número 3.

[13] Cfr. Ley 20.950, de 29 de octubre de 2016.

[14] Ibid. art. 13.

[15] BioBio Chile "Ahora tu CuentaRUT podrá pagar internacionalmente tras convenio PayPal-MultiCaja". 17 de febrero de 2015. Disponible en http://www.biobiochile.cl/noticias/2015/02/17/ahora-tu-cuentarut-podra-pagar-internacionalmente-tras-convenio-paypal-muticaja.shtml

[16] OhMyGeek, "Presentaron en Chile al sistema de pago online 'MercadoPago'". 27 de mayo de 2015. Disponible en http://www.ohmygeek.net/2015/05/27/mercadopago-en-chile/

[17] Cfr. https://www.recargafacil.cl/#info

[18] La Segunda, "Khipu: Una forma segura y eficiente de pagar en línea". 14 de abril de 2015. Disponible en http://www.lasegunda.com/Noticias/Economia/2015/04/1004429/Khipu-Una-forma-segura-y-eficiente-de-pagar-en-linea

[19] Cfr. https://www.bancoestado.cl/imagenes/_personas/servicios/app-movil/descarga.asp

[20] Cfr. http://ww2.copec.cl/pagoclick

e) Negociar, en cualquier forma, con los datos o el número de la tarjeta de crédito, de pago con provisión de fondos o débito, para las operaciones señaladas en la letra anterior.
f) Usar maliciosamente una tarjeta bloqueada, en cualquiera de las formas señaladas en las letras precedentes.
g) Suplantar la identidad del usuario frente al emisor para obtener autorización para realizar transacciones con una tarjeta de crédito, de pago con provisión de fondos o débito.

---

[21] Cfr. https://www.transbank.cl/public/personas/todo-sobre-tus-medios-de-pago/webpay-oneclick/

[22] Cfr. https://www.bbva.cl/personas/bbva-wallet/; Wayerless, "BBVA lanza en Chile aplicación para pagar con tu smartphone", 23 de abril de 2015. Disponible en https://www.wayerless.com/2015/04/bbva-wallet-chile/

[23] Cfr. https://ww3.bancochile.cl/wps/wcm/connect/personas/portal/canales/movil/mi-pago

[24] Cfr. https://bitcoin.org/bitcoin.pdf

[25] Bit2Me "¿Qué es la Cadena de Bloques (Blockchain)?". Disponible en http://blog.bit2me.com/es/que-es-cadena-de-bloques-blockchain/

[26] Cfr. Ley 20.009, art. 1º.

[27] Servicio Nacional del Consumidor, "Bancos se harán responsables por problemas que afectaron a consumidores tras clonación de tarjetas", 23 de agosto de 2012. Disponible en http://www.sernac.cl/bancos-se-haran-responsables-por-problemas-que-afectaron-a-consumidores-tras-clonacion/

[28] Primer Juzgado de Policía Local de Providencia, "Wilson Goldsmith, Patricio vs Banco de Chile", sentencia de Primera Instancia pronunciada el 20 de enero de 2016, disponible en http://www.pjud.cl/documents/396729/0/BANCO+EDWARS+POLICIA+LOCAL.pdf/c6299675-b372-414c-acac-afb2a4b2da8b

[29] Ibid.

[30] Corte de Apelaciones de Santiago, Causa Rol P-36855-2014 "Wilson Goldsmith, Patricio vs Banco de Chile", sentencia de segunda instancia pronunciada el 12 de septiembre de 2016, a fojas 617, visto Séptimo.

[31] Ibid. visto Quinto.

[32] CONADECUS, "Clonación de tarjetas: 'Qué hacer y cómo protegerse'" 1 de septiembre de 2014. Disponible en http://www.conadecus.cl/conadecus/?p=8718

[33] Cfr. Veres Ferrer, Ernesto y otros, "El mercado de las tarjetas bancarias en España: Una panorámica". Tribuna Económica, Revista ICE, número 876, edición enero-febrero de 2014, pp. 172-176. Disponible en http://www.revistasice.com/CachePDF/ICE_876___1C260E4ED358350AF1D954E815604C8D.pdf

[34] Ibid. Además, Cfr. Panda Security. "Phishing". Disponible en http://www.pandasecurity.com/ecuador/homeusers/security-info/cybercrime/phishing/

[35] Corte de Apelaciones de Puerto Montt, causa rol 35-2011, "Weisser Modinger, Enrique contra Banco Santander Chile", sentencia de segunda instancia pronunciada el 3 de agosto de 2011.

[36] Corte de Apelaciones de Chillán, causa rol 5302-2011, "Marta Torres Muñoz contra Banco Corpbanca", sentencia de segunda instancia pronunciada el 23 de mayo de 2012.

[37] Cfr. BBVA, "Skimming: la estafa de la clonación de tarjetas", disponible en https://www.bbva.com/es/cl/noticias/ciencia-tecnologia/tecnologia/skimming-la-estafa-la-clonacion-tarjetas/; https://es.wikipedia.org/wiki/Skimming_(fraude); La Tercera, "Fábrica de clonadores de tarjetas bancarias operaba en el centro de Santiago", 17 de abril de 2013. Disponible en http://www.latercera.com/noticia/fabrica-de-clonadores-de-tarjetas-bancarias-operaba-en-el-centro-de-santiago/

[38] Oxmán, Nicolás. "Estafas informáticas a través de Internet: acerca de la imputación penal del 'phishing' y el 'pharming'", 29 de julio de 2013. Disponible en http://www.scielo.cl/scielo.php?

La pena por este delito será de presidio menor en su grado medio a máximo, multa correspondiente al triple de lo defraudado, y el comiso de los bienes adquiridos por medio del ilícito, los que serán dispuestos para la compensación del emisor en los casos en que corresponda.

Esta pena aumentará en un grado, si la acción realizada produce perjuicio a terceros."

6. Agréganse los siguientes artículos 6º, 7º y 8º, nuevos:

"Artículo 6º.- El usuario no se tendrá por responsable en las operaciones realizadas sin su autorización, cuando el ilícito corresponda a la utilización de los datos necesarios para realizar una operación con el medio de pago sin que el usuario haya podido conocer tal hecho. De esta forma, la sustracción de los datos de una tarjeta de crédito desde el banco de datos de un comercio; la clonación de los datos de una tarjeta de débito a través de medios electrónicos, magnéticos o radiantes; la obtención por medios fraudulentos de las credenciales necesarias para operar un pago a través de una plataforma electrónica, entre otras conductas de similar naturaleza, no podrán ser imputables al usuario cuando éste no estuviese en conocimiento de su acaecimiento, sin perjuicio de la responsabilidades que deberá perseguir el emisor respecto de las personas que participen en la comisión del delito.

Será deber del emisor probar que el usuario se encontraba en conocimiento de las operaciones fraudulentas o que actuó sin la debida diligencia para el manejo del medio de pago.

Artículo 7º.- El emisor no podrá imponer condiciones ni requerir medidas anexas al usuario para la cancelación de los cargos realizados sin su autorización, o la devolución de los importes si correspondiera y, en ambos casos, deberá realizar dichas operaciones dentro de las 24 horas hábiles siguientes al momento en que fueran detectadas o notificadas. Tampoco podrá imputarlos al comercio en el que fueron realizados los pagos, excepto en los casos en que pueda ser comprobada la negligencia del comercio en la custodia o manejo de los datos del medio de pago necesario para la transacción, o su actuar fraudulento en los términos señalados por el artículo 5º.

Las cláusulas contractuales entre el emisor o sus personas relacionadas y el comercio que hagan responsable a éste último por las pérdidas en las operaciones realizadas mediante algún medio fraudulento, se tendrán por no escritas, correspondiendo siempre al emisor asumirlas, sin perjuicio del derecho a demandar el pago de quien resultare responsable del delito.

---

script=sci_arttext&pid=S0718-68512013000200007

[39] Al respecto, prácticamente todas las instituciones bancarias ofrecen seguros contra el fraude o robo de tarjetas. Cfr. BancoEstado, http://www.bancoestado.cl/imagenes/_personas/productos/seguros/tarjetas-y-cuentas/seguro-fraude-tarjeta.asp; Banco BCI, https://www.bci.cl/corredora-de-seguros/seguros/seguro-multiproteccion/multiproteccion-plan-preferencial; Banco Falabella, https://www.segurosfalabella.cl/web/seguros/full-proteccion-documentos; solo por mencionar algunos.

Artículo 8º.- El emisor procurará contar con medidas de seguridad suficientes para impedir la comisión de ilícitos como aquellos desarrollados en el artículo 5º, resguardando la prestación segura del servicio en los términos señalados por el artículo 23 de la ley 19.496; y será responsable de los perjuicios que se produzcan por las deficiencias en la protección de los sistemas tecnológicos del medio de pago.”