

INFORME DE LA COMISIÓN DE ECONOMÍA recaído en el proyecto de ley, en primer trámite constitucional, 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.

BOLETÍN N° 11.078-03.

HONORABLE SENADO:

Vuestra Comisión de Economía tiene el honor de informar respecto del proyecto de ley de la suma, en primer trámite constitucional, iniciado en moción de los Honorables Senadores señores Ossandón, señora Pérez San Martín y señor Tuma.

La iniciativa ingresó a tramitación en el Senado con fecha 10 de enero de 2017, pasando a la Comisión de Economía.

Cabe hacer presente que, no obstante tratarse de un proyecto de artículo único, la Comisión de Economía lo discutió y aprobó solo en general, y propone a la Sala proceder del mismo modo.

A una o más de las sesiones en que la Comisión estudió el proyecto asistieron, especialmente invitadas, las siguientes personas:

De la Superintendencia de Bancos e Instituciones Financieras (SBIF): el Director Jurídico, señor Andrés Prieto, y el Director de Comunicaciones y Asuntos Internacionales, señor Erick Rojas.

De la Asociación de Bancos e Instituciones Financieras (ABIF): el Presidente, señor Segismundo Schulin-Zeuthen, y el Fiscal, señor Juan Esteban Laval.

De la Corporación Nacional de Consumidores y Usuarios (CONADECUS): el Vicepresidente, señor Álvaro Gallegos.

De la Universidad de Chile, del Departamento del Centro de Estudios en Derecho Informático de la Facultad de Derecho: el abogado, representante, señor Renato Jijena.

De VISA International Ltda.: el Vicepresidente de Relaciones Gubernamentales de VISA para América Latina y el Caribe,

señor Salvador Pérez Galindo, y la Gerente General de VISA Chile, Servicios VISA International, señora Paola Ledezma.

Del Servicio Nacional del Consumidor (SERNAC): el Jefe de División de Consumo Financiero, señor Rodrigo Romo; la Jefa del Departamento de Análisis y Cumplimiento de Normativas Financieras, señora Gabriela Millaquén, y la asesora Legislativa, señora Paola Jhon.

También asistieron:

De la Secretaría General de la Presidencia (SEGPRES), la señora Verónica Pinilla y el señor Daniel Portilla.

Los asesores de Parlamentarios, señores Eduardo Faúndez (Honorable Senadora señora Lily Pérez), Eduardo Barros y Claudio Flores (Honorable Senador señor Eugenio Tuma), señoras Kareen Herrera y Andrea Gómez (Honorable Senador señor Jorge Pizarro), señor Héctor Mery (Honorable Senador señor Iván Moreira), señora Melissa Mallega (Honorable Senador señor Rabindranath Quinteros), señores Arturo Du Monceau, José Huerta (Honorable Senador señor Manuel José Ossandón) y Nickolás Mena (Honorable Senador señor Bianchi).

De la Fundación Jaime Guzmán, los analistas, señor Diego Vicuña, y señoras Mikaela Romero y Teresita Santa Cruz.

De la Biblioteca del Congreso Nacional, el abogado señor James Wilkins.

El periodista del Senado, señor Francisco Ramdohr.

La analista señora Javiera Campos.

NORMAS DE QUÓRUM ESPECIAL

No hay.

OBJETIVOS DEL PROYECTO

Modificar 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, fortaleciendo el régimen especial de responsabilidad del usuario y emisor de medios de pago, proponiendo entre otras, las siguientes medidas:

- Ampliar al uso fraudulento de nuevos medios de pago, el régimen de limitación de responsabilidad que actualmente establece para el caso del uso fraudulento de tarjetas de crédito o débito;

- Ampliar el catálogo de conductas que constituyen el delito de uso fraudulento de tarjetas de crédito, de pago con provisión de fondos o débito, y aumentar las penas;

-Establecer un régimen de exención de responsabilidad para el usuario frente a fraudes realizados sin que él pueda estar en conocimiento de tal hecho, como en el caso de clonación de una tarjeta;

- Fijar un plazo de 24 horas a los emisores para la devolución de los importes, si corresponde, en los casos de fraude, y establecer la prohibición de requerir el cumplimiento de condiciones para tales devoluciones, como la contratación de seguros u otras medidas burocráticas.

- Consagrar como responsabilidad del emisor de un medio de pago, el contar con medidas de seguridad suficientes para evitar la comisión de ilícitos, y ser responsable de los perjuicios que se produzcan por deficiencias en la protección de los sistemas tecnológicos del medio de pago.

- - - - -

ANTECEDENTES

Para el debido estudio de esta iniciativa de ley, se han tenido en consideración, entre otros, los siguientes:

A. ANTECEDENTES JURÍDICOS

- Ley N° 20.009, que limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas.

- Ley N° 19.496, sobre protección de los derechos del consumidor.

- Ley N° 20.950, que autoriza emisión y operación de medios de pago con provisión de fondos por entidades no bancarias.

B. ANTECEDENTES DE HECHO

La moción que dio origen a este proyecto.

- FUNDAMENTOS.

En sus **fundamentos**, la moción comienza señalando que el 1 de abril de 2005 fue publicada la ley N° 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.

Este mecanismo ha cumplido su objetivo y funcionado de forma adecuada desde la publicación de la ley, pero actualmente podemos identificar algunas situaciones que hacen imperioso ajustar la ley al escenario presente.

La moción da cuenta del gran aumento de delitos de uso fraudulento de tarjetas, que entre 2014 y 2015 se duplicó en nuestro país, pasando de 17.300 a 34.300 casos. 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, mientras que en Estados Unidos 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%).

Los autores de la moción llaman la atención que, 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. 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, ya que en alguna medida son los comercios quienes absorben gran parte de las pérdidas.

- CATEGORÍAS DE FRAUDE.

La moción luego aborda **dos categorías de fraude** en esta materia: fraudes con o sin tarjeta.

En efecto, 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 N° 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). Los autores precisan que es en este espacio donde la ley N° 20.009 no contempló un régimen que regulara la responsabilidad del emisor y el tarjetahabiente, pues 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.

La moción aborda el **Derecho Comparado** en este tema, y afirma que 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 el monto de \$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. El usuario 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.

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. 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 por hasta €150 euros 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.

En Estados Unidos, el régimen aplicable es distinto tratándose 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. 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, 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. Reproduce además la mecánica de notificación ya vista en otros casos de derecho comparado.

- NUEVOS SISTEMAS DE PAGO.

El texto de la moción continúa refiriéndose a los **nuevos sistemas de pago**, que hacen necesario actualizar nuestra legislación.

Los autores de la moción ponen de relieve que, 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 fondos emitidas por bancos, instituciones financieras o entidades no bancarias.

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. Lo anterior se agrega a la existencia de la 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, 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 que, entre otras funciones, permite recolectar dinero a través del sistema.

En otro tipo de servicios atingentes, podemos encontrar a RecargaFácil, también de Multicaja, para el pago por recargas de servicios telefónicos o de TV de Pago; Khipu aqsque opera facilitando transferencias bancarias entre cada cliente; PagoRUT 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 de Copec para el pago de combustible, pero utilizando tarjetas de crédito sobre la infraestructura de WebPay OneClick de Transbank .

Agregan que, similar a PagoRUT de BancoEstado, encontramos una serie de otros sistemas basados en el pago vía aplicaciones móviles, como BBVA Wallet que permite el pago contra la tarjeta de crédito del banco; de BancoChile se encuentra disponible la app Mi Pago, 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, 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 que van desde la autenticación de identidades hasta la trazabilidad de bienes en el mercado.

En conclusión, los autores afirman que 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, los 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.

El texto de la moción consigna que actualmente, la ley N° 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.

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 toman conocimiento 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 N° 20.009 no se ejecutan.

Los autores de la moción estiman justo mencionar

que, no obstante el vacío legal, 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. 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 respecto de la responsabilidad, tanto del emisor como del tarjetahabiente, basados en las disposiciones de la ley N° 19.496 sobre protección de los derechos de los consumidores.

De especial interés resulta la querrela 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. 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.

En segunda instancia la Corte de Apelaciones de Santiago acogió la querrela 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.”. 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.” .

La ley N° 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.

El proyecto en estudio propone abordar los plazos

en los que deberán los emisores retornar los importes pagados en operaciones fraudulentas, 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.

A continuación, el texto de la moción se refiere a los **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. Los más relevantes actualmente, además del siempre presente robo o hurto de la tarjeta, corresponden al phishing, pharming y skimming, por un lado, y a la clonación de tarjetas, y 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. En esta materia, la jurisprudencia está dividida, dando lugar a variados fallos absolutorios en favor del banco, 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. 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 micro cámaras de video alojadas sobre el teclado del dispositivo. De este modo, 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 autores de la moción presentan a continuación las **propuestas y estructura del proyecto**.

Señalan que los delitos mencionados, al igual que la clonación de las tarjetas, pueden ser abordados a través de las normas del Código Penal o la ley de delitos informáticos N° 19.223 , según corresponda,

o la propia ley N° 20.009 que establece penas a distintos hechos punibles relacionados con el uso fraudulento de tales instrumentos. Desde el punto de vista infraccional y de la responsabilidad del emisor, como ya se ha señalado, 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.

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 en la ley N° 20.009, como sí cuentan el robo o hurto de la tarjeta de crédito o débito.

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 referida ley N° 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 5° 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 5° 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 N° 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 5°.

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 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), 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.

DISCUSIÓN EN GENERAL

La Comisión inició la discusión general del proyecto, en sesión de 12 de julio de 2017, escuchando la exposición de distintos invitados.

SUPERINTENDENCIA DE BANCOS E INSTITUCIONES FINANCIERAS

El Director Jurídico de la Superintendencia, señor Andrés Prieto, luego de agradecer la invitación y excusar la asistencia del Superintendente de Bancos e Instituciones Financieras, se refirió a esta moción parlamentaria cuyo objeto es modificar la ley N° 20.009, de 2005, que limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas, ley vigente que aborda el tema.

Como elementos de contexto a tener en consideración, manifestó que la ley N° 20.009 creó un marco jurídico de exención de responsabilidad para el tarjetahabiente respecto de los robos, extravíos y hurtos de sus tarjetas de crédito, 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 aviso al emisor. El emisor asume la responsabilidad de la persecución de las operaciones que pudiesen realizarse con posterioridad al aviso.

La moción en estudio es fundada largamente, afirmó. De esos fundamentos, destacan principalmente tres elementos:

- Aborda 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. Al respecto, llamó la atención que, probablemente, el tarjetahabiente recién se entere cuando le llegue la cartola mensual, y ese momento puede ser muy tarde para dar el curso que exige la ley.

- Señala que el tarjetahabiente no tiene oportunidad de notificar de nada sospechoso al emisor, por lo que las providencias de la ley N° 20.009 no se ejecutan.

- Reconoce que el mercado ha actuado bien en estos casos, cubriendo las operaciones fraudulentas y liberando al titular de tales cargas, como parte de un sistema de negociación pública entre las autoridades y la industria. A modo de ejemplo de lo anterior, el señor Prieto se refirió a lo ocurrido el año 2012, año en que hubo una clonación masiva de tarjetas, y en esa oportunidad fueron los emisores los que asumieron el costo de lo ocurrido.

El señor Prieto abordó las principales modificaciones propuestas en la iniciativa en comento:

1.- Amplía los instrumentos.

Comprende a los medios de pago en general (tarjetas de crédito, y se suman las de débito, provisión de fondos, cuentas que permitan el pago por medios electrónicos y en general, cualquier medio de pago distinto del dinero en efectivo, cheque o vale a la vista). La redacción deja abierta la puerta a nuevos medios de pago que puedan crearse en el futuro.

2.- Sujeto responsable:

El emisor del medio de pago, así como el operador y el que realiza el rol adquirente (afilia comercio).

3.- Delitos:

Incorpora la figura de suplantación de identidad del usuario frente al emisor para obtener autorización para realizar transacciones con las tarjetas.

4.- Aumento de penas:

Aumenta la sanción mínima privativa de libertad. Sigue siendo presidio menor, pero grado medio a máximo, y elimina el grado mínimo, dejando un margen más estrecho para el juez. También incorpora una sanción pecuniaria (multa) y decomiso de bienes adquiridos por medio del ilícito.

5.- Exclusión de responsabilidad.

El usuario no será responsable cuando ocurra:

- Utilización de datos necesarios para realizar una operación con el medio de pago sin que el usuario haya podido conocer tal hecho. Destacó que este punto es relevante porque es primera vez que se desvincula a la tarjeta de la operación que se haga, por ejemplo, con los datos.

- Sustracción de los datos de una tarjeta de crédito desde el banco de datos de un comercio.

- Clonación de los datos de una tarjeta de débito a través de medios electrónicos magnéticos o radiantes.

- Obtención por medios fraudulentos de las credenciales necesarias para operar un pago a través de una plataforma electrónica.

- Otros de similar naturaleza.

6.- Transfiere la carga de la prueba del usuario al emisor. El señor Prieto hizo presente que hoy día el sistema diseñado distingue según se trate con anterioridad o posterioridad al aviso. En el proyecto, dadas ciertas condiciones, es el emisor quien debe probar.

7.- El emisor debe 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.

8.- El emisor debe asumir las obligaciones económicas derivadas del uso fraudulento del medio de pago, pudiendo demandar el pago al responsable del delito.

9.- Incorpora un plazo de 24 horas hábiles para la reversa o devolución de cargos sin autorización del usuario, desde que las operaciones fueron detectadas o notificadas.

En este punto, el señor Prieto hizo notar que la moción da vuelta la hipótesis que actualmente consagra la ley. Ahora existirá un plazo para el banco. Esto no significa en caso alguno que en 24 horas quede zanjado el tema de la responsabilidad.

10.- El emisor debe contar con medidas de seguridad suficientes para impedir la comisión de ilícitos con sus productos, resguardando la prestación segura del servicio en los términos establecidos en el artículo 23 de la ley N° 19.496, sobre Protección de los Derechos del Consumidor.

Continuando con su exposición, el Director Jurídico de la SBIF formuló algunos comentarios. Por una parte, hay que considerar que los usuarios de los medios de pago carecen de los elementos probatorios para revertir la presunción de mal uso del instrumento. El control no lo tiene el usuario, y por lo tanto no tiene modo de revertir una presunción de mal uso. Además, efectivamente los sistemas a través de los cuales se opera el medio de pago, son administrados en forma habitual por terceros relacionados al emisor o contratados por éste.

Desde el punto de vista de la responsabilidad de los actores, el señor Prieto puso de relieve que el Banco Central acaba de publicar, el 30 de junio pasado, la normativa relativa a la ley de medios de pago, manteniendo conceptos de emisor y operador, y creando además el de Proveedor de Servicios para Procesamiento de Pagos (PSP). El PSP, sin ser un operador propiamente tal, puede prestar servicios de afiliación al

comercio. Surge en este punto la duda si va a quedar considerado dentro de las hipótesis de la ley.

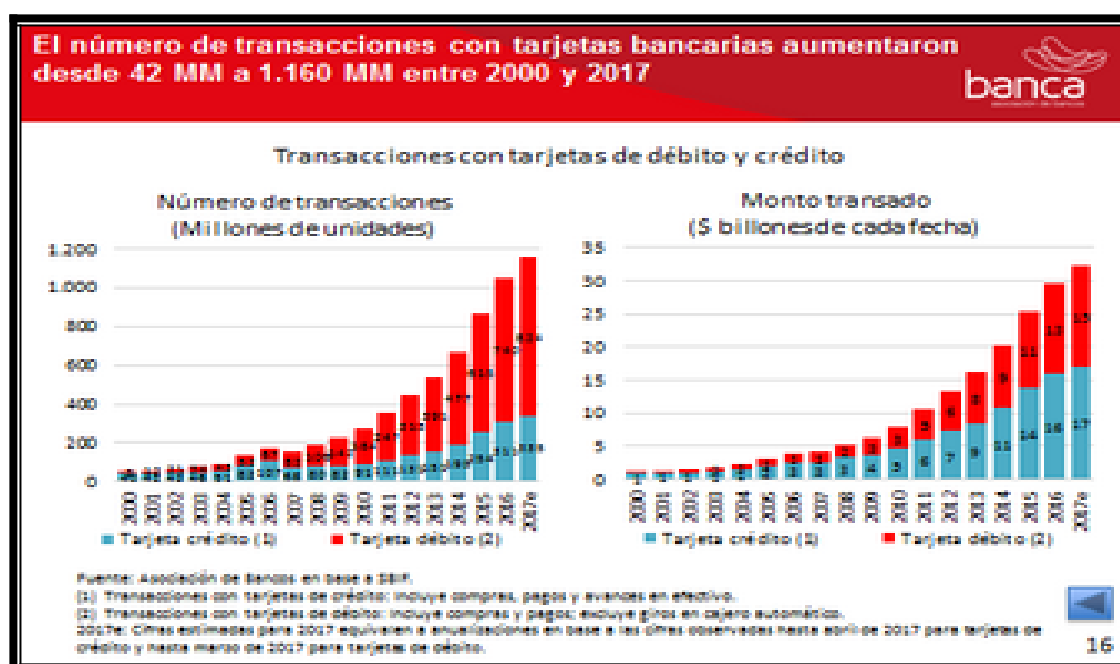
No obstante, de acuerdo a esta normativa, la responsabilidad por la seguridad operacional de las actividades encomendadas a dichos terceros debe ser asumida por el emisor y operador frente a los usuarios de tarjetas, lo que no resulta coincidente con la moción. Esto sin perjuicio que eventualmente se pueda perseguir la responsabilidad del tercero.

Finalmente, el señor Prieto subrayó que el artículo 5° no incluye fraudes que se pudiesen realizar con otros medios de pago incluidos en la definición, distintos de las tarjetas, como las transferencias electrónicas. Esta figura quedaría fuera del proyecto.

ASOCIACIÓN DE BANCOS E INSTITUCIONES FINANCIERAS

El señor Segismundo Schulin-Zeuthen, Presidente de la ABIF, realizó un análisis del contexto en que propone legislar la moción en estudio, y el marco general de las tarjetas de pago.

Comenzó señalando que la confianza en los medios de pago, especialmente en las tarjetas de pago, es un objetivo esencial para los reguladores y para la banca, considerando que un porcentaje importante del consumo de los hogares se paga con tarjetas (IEF 1er semestre 2016: 17,4% en 2009 a 27,3% en 2015). Hay un aumento que representa la siguiente gráfica:



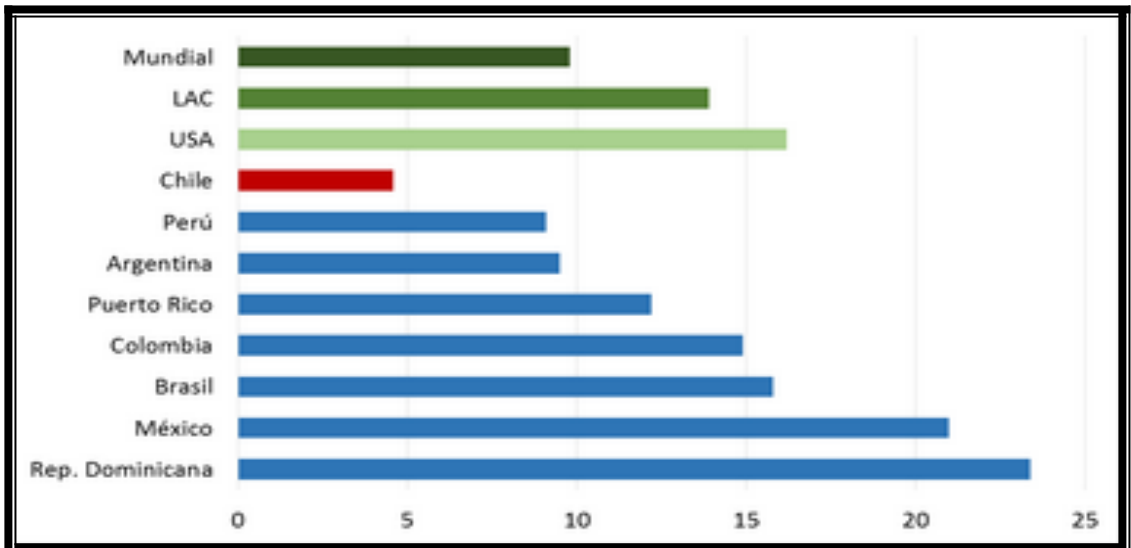
Las funciones y roles de cada agente determinan su responsabilidad en la cadena de pagos.



En su parecer, la moción tiende a fijar mucho la responsabilidad sólo en el emisor.

Por otra parte, el Presidente de ABIF declaró que es imposible suprimir totalmente el uso fraudulento de los medios de pago y, en especial, de las tarjetas de pago. En su opinión, esa es una realidad que no se puede negar, lo que debe hacerse es tratar de mitigarla.

Destacó que Chile presenta tasas de fraudes inferiores al promedio mundial y latinoamericano:



La banca realiza constantes esfuerzos de innovación e inversiones para mitigar el uso fraudulento de los medios de pago. Dio algunos ejemplos de los esfuerzos realizados:

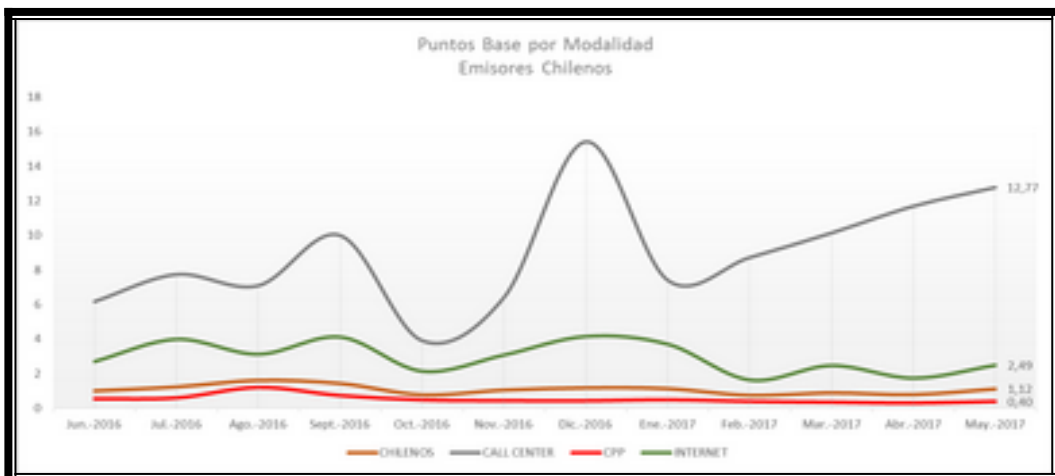
- Incorporación del chip en las tarjetas de crédito y débito emitidas a contar del 1 de abril de 2017. Esto, producto de un acuerdo de la industria.

- Implementación del perturbador magnético para proteger el uso de la banda en las tarjetas. Esto es necesario atendido que no se puede eliminar el uso internacional de la tarjeta, y hay varios países que no tienen chip.

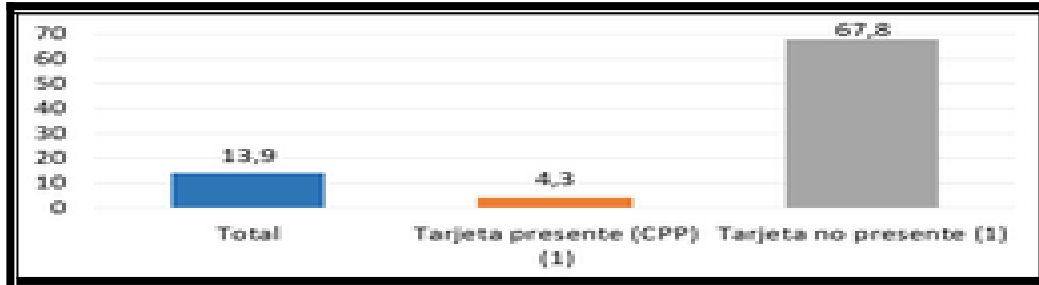
- Incorporación de clave secreta en transacciones presenciales con tarjeta de crédito (PinPass).

- Incorporación de autenticación robusta en compras por internet (Web Pay Plus). En este punto, hizo presente que hay grandes comercios que han decidido no operar por este sistema y asumir ellos esa responsabilidad y ese riesgo.

El señor Schulin-Zeuthen destacó que la incorporación de nuevas tecnologías y el desarrollo de la banca digital han provocado una disminución en el uso presencial de las tarjetas de pago y un aumento en las transacciones no presenciales. Y el uso fraudulento de las tarjetas de pago es mayor en las compras no presenciales, siendo las tarjetas emitidas en el exterior por entidades extranjeras las que presentan un mayor porcentaje de fraudes. En efecto, a nivel mundial, cerca de un 70% del fraude es con tarjeta no presente, como lo muestran estas gráficas:



Tasas de fraude por modalidad en Latinoamérica (Puntos base)



Cualquier regulación no puede desconocer la existencia de reglamentación internacional de las marcas, porque si no la aceptación quedaría limitada.

Intervino luego el Fiscal de la ABIF, señor Juan Esteban Laval, quien en primer término formuló una sistematización del contenido de la ley N° 20.009, vigente en la materia:

- El titular puede limitar su responsabilidad, dando aviso al emisor en caso de extravío, hurto o robo de tarjetas de crédito.

- El emisor debe mantener un servicio permanente y gratuito para que el titular dé aviso y se bloquee de inmediato la tarjeta.

- El emisor es responsable por las operaciones que se realicen luego que la tarjeta sea bloqueada, salvo que se pruebe que las operaciones fueron realizadas por el titular o adicionales.

- Se tienen por no escritas las cláusulas que impongan el deber de prueba en el titular.

- Se establece un catálogo de delitos por el uso fraudulento de las tarjetas.

- La ley N° 20.009 es consistente con el estándar de responsabilidad en las relaciones de consumo.

En efecto, el estándar de responsabilidad en las relaciones de consumo se traduce:

- En materia de fraudes, el estándar de responsabilidad se traduce en que el proveedor es responsable en los casos en que, actuando con negligencia, causa un menoscabo al consumidor (artículos 3 letra d), 12 y 23 de la ley N°19.496).

- Sin embargo, la ley N° 19.496 establece también el deber que tiene el consumidor de evitar los riesgos que puedan afectarle.

- Para determinar la responsabilidad en casos de fraude, al día de hoy se recurre a un criterio subjetivo. Los tribunales ponderan, a través de la prueba, la diligencia empleada por cada uno de los intervinientes en la relación de consumo.

El señor Laval abordó a continuación los principales aspectos del proyecto de ley:

1.- Amplía el alcance de la ley a todo medio de pago con excepción del dinero, cheque y vale vista.

2.- Agrega un nuevo delito, cuyo tipo penal sería 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.

3.- Establece que el usuario no será responsable por 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. Este es, en su parecer, el punto más complejo.

4.- Dispone que será deber del emisor probar que el usuario se encontraba en conocimiento del fraude o que actuó sin la debida diligencia en el manejo del medio de pago.

5.- Establece que el emisor no podrá condicionar ni requerir medidas para cancelar o devolver la suma cargada al usuario en un plazo de 24 horas, salvo que se pruebe la negligencia.

6.- Dispone que el emisor no podrá imputar al comercio los cargos realizados a menos que pruebe su negligencia en el manejo de los medios de pagos.

7.- Consagra que las cláusulas contractuales en dicho sentido se tendrán por no escritas correspondiendo al emisor asumir los perjuicios.

8.- Crea la obligación del emisor de contar con medidas de seguridad suficientes para evitar la comisión de delitos y que será responsable por las deficiencias en la protección de los sistemas de medios de pago.

Puntualizados los principales aspectos de la iniciativa en estudio, el señor Laval realizó algunos comentarios a la normativa propuesta. En síntesis, el proyecto, en su visión, incrementa el riesgo moral y desincentiva el cumplimiento de las obligaciones que corresponden a los demás actores.

En primer lugar, incrementa el riesgo moral. Este efecto se debería a que la iniciativa radica la responsabilidad únicamente en el emisor del medio de pago, incrementando el riesgo moral, lo que promueve el auto-fraude, especialmente en transacciones no presenciales, y desincentiva la adopción de medidas de seguridad por parte del comercio.

Las hipótesis para eximirse de responsabilidad son impracticables (una verdadera “prueba imposible”). Se exige probar que:

a) El usuario conocía las operaciones que se realizaron con su medio de pago: el conocimiento es inmaterial y su existencia depende de la declaración del usuario.

b) El usuario actuó sin la debida diligencia: dificultad para probar la falta de diligencia, especialmente en casos de auto-fraude.

El combate contra el fraude sólo será eficaz en la medida que los emisores, los operadores, el comercio, los usuarios y las marcas, tomen medidas para salvaguardar el correcto uso de los medios de pago. Y no radicándolo exclusivamente en uno de los intervinientes como, en su parecer, ocurre en este proyecto de ley.

En segundo lugar, el señor Laval afirma que esta iniciativa desincentiva el cumplimiento de las obligaciones que corresponden a los demás actores.

a) Así, serían obligaciones de los adquirentes:

- Poner a disposición del comercio dispositivos que sean capaces de soportar tecnologías seguras para la operación de tarjetas;

- Los cajeros automáticos deben contar con medidas de seguridad para evitar la sustracción de información de las tarjetas y claves de los usuarios; y

- Deben capacitar a los comercios en la operación de terminales para evitar el mal uso de las tarjetas de crédito, evitar duplicidades, extracción de información, etcétera.

- Velar por la seguridad de las transacciones (en el tramo POS hasta sus sistemas)

b) Son obligaciones de los comercios:

- Contar con el conocimiento y protocolos de identificación de usuarios de tarjetas para evitar la suplantación, especialmente en las compras no presenciales.

- En algunos modelos de venta, los comercios autentican las transacciones. Esto ocurre, por ejemplo, en los hoteles.

- Contar con condiciones de seguridad para evitar la sustracción de información de los tarjetahabientes.

- Capacitar e instruir a su personal respecto de la operatoria del sistema.

c) Son obligaciones de los clientes:

- Mantener en lugar seguro sus medios de pago y productos;
- No divulgar los datos de sus tarjetas, para protegerlas de un mal uso (esto aplica para transacciones presenciales y no presenciales).
- Dar aviso oportuno e inmediato sobre eventos de fraude que los afecten.
- Aportar los antecedentes al emisor y concurrir antes las autoridades competentes (Ministerio Público, PDI).

d) Son obligaciones del emisor:

- Autenticación del tarjetahabiente cuando este rol está radicado en el emisor (firma electrónica simple – PIN-).
- Proveer sistemas de bloqueo y seguridad de las transacciones (en el tramo adquirente-emisor).

Por otra parte, la nueva regulación del Banco Central en materia de tarjetas de pago, establece que la responsabilidad de pago en el caso de tarjetas emitidas en el extranjero, corresponde al operador local con el que contrató el emisor.

En cuanto a los fraudes cometidos en compras realizadas en comercios o plataformas tecnológicas extranjeras, se encuentran regulados en las condiciones generales de las marcas internacionales de medios de pagos. Por ello, las normas del presente proyecto en ningún caso pueden aplicar a dichas transacciones.

El Fiscal de la ABIF, señor Laval, formuló las siguientes conclusiones en relación al texto en estudio:

La moción, en la práctica, establece la responsabilidad objetiva del emisor, dado que supone la obligación de cancelar o devolver la suma cargada al usuario en 24 horas; esto a diferencia de lo que ocurre con la responsabilidad subjetiva consagrada en la ley vigente, que se establece actualmente por los tribunales. De acuerdo al proyecto, se puede excepcionar: “Salvo que se pruebe la negligencia”. Cabe preguntarse si es posible probar la negligencia en 24 horas. Y es una disposición contraria al legítimo derecho de defensa.

Asimismo, como ya señaló, la moción incrementa el riesgo moral, dado que invita al auto-fraude, especialmente en transacciones no presenciales (por ejemplo, compra de cupo en dólares).

También desincentiva el cumplimiento de las obligaciones que corresponden a los intervinientes en el mercado, especialmente la adopción de medidas de seguridad por parte del comercio. Y desincentiva la persecución de la responsabilidad penal de los autores del fraude.

La responsabilidad debe asignarse de acuerdo con el rol que los distintos actores desempeñan en el mercado de tarjetas de pago. Esto debería consagrarse como un principio en esta materia.

Agregó que, con este proyecto se favorece a ciertos comercios que privilegian tasas de abandono menores sobre medidas de seguridad estrictas. Esto ocurre cuando ciertos comercios advierten que en una compra no presencial, mientras más capas de seguridad, mayor posibilidad de que el cliente abandone el proceso de compra. Y por tanto privilegian tasas de abandono menores.

Finalmente, afirmó que alterar el estándar de responsabilidad en los términos propuestos, importa un mayor riesgo para el emisor que no puede traducirse en un mayor precio, atendido que desde abril de 2013, los precios de los contratos sobre productos financieros se encuentran congelados, luego que se derogaran las normas que establecían los criterios sobre proposición y aceptación de modificaciones de contratos.

El Fiscal de la ABIF consideró pertinente realizar algunos comentarios específicos, para el caso de mantenerse la intención de legislar en esta materia. Tales son los siguientes:

1.- No resulta necesario determinar conceptos ya definidos en la regulación específica que corresponde al Banco Central en uso de sus atribuciones legales (Capítulo III.J.1 del Compendio de Normas Financieras), considerando su objeto de velar por el normal funcionamiento del sistema de pagos. En este punto, se sugiere hacer un reenvío a la normativa del Banco Central.

2.- El plazo de reintegro de fondos de 24 horas a los clientes por parte del emisor, no permite realizar una investigación seria para determinar responsabilidades. El plazo para llevar a cabo dicha investigación debería ser suficiente para investigar el caso, especialmente en transacciones en el extranjero. En su parecer, se debería poder determinar la diligencia de cada uno de los intervinientes.

3.- Evaluar establecer un mecanismo de abonos provisorios, al menos para montos por sobre las UF 25, para permitir al emisor y al adquirente realizar las investigaciones que correspondan, y autorizar el reintegro del abono provisorio en caso que se determine la responsabilidad del cliente, con el interés máximo legal.

4.- Se debe permitir expresamente contra cargar al comercio los montos reclamados por los clientes, cuando el comercio haya sido negligente en el cumplimiento de sus obligaciones, facilitando el fraude. En caso de haber responsabilidad del comercio, es el adquirente el que debe

realizar las gestiones respectivas para contra cargar o compensar en la liquidación respectiva.

5.- Crear un tipo penal que sancione al cliente que efectúe declaraciones falsas en esta materia.

6.- Modificar el tipo penal propuesto, eliminando la expresión frente al emisor, ya que existen modelos de venta en que la autenticación la realiza el comercio, como es el caso de los hoteles.

7.- Establecer expresamente el derecho del emisor, el adquirente o el comercio que devuelve al usuario el monto defraudado, a subrogarse para recuperar el monto abonado y perseguir las responsabilidades pertinentes.

8.- Contemplar la posibilidad de que las cláusulas de responsabilidad entre el comercio, en especial el de gran tamaño y el electrónico, y los emisores, sea determinada por la autonomía contractual de las partes.

CORPORACIÓN NACIONAL DE CONSUMIDORES Y USUARIOS (CONADECUS).

El señor Álvaro Gallegos, Vicepresidente de Conadecus, expuso la opinión de esta organización en relación al proyecto de la referencia.

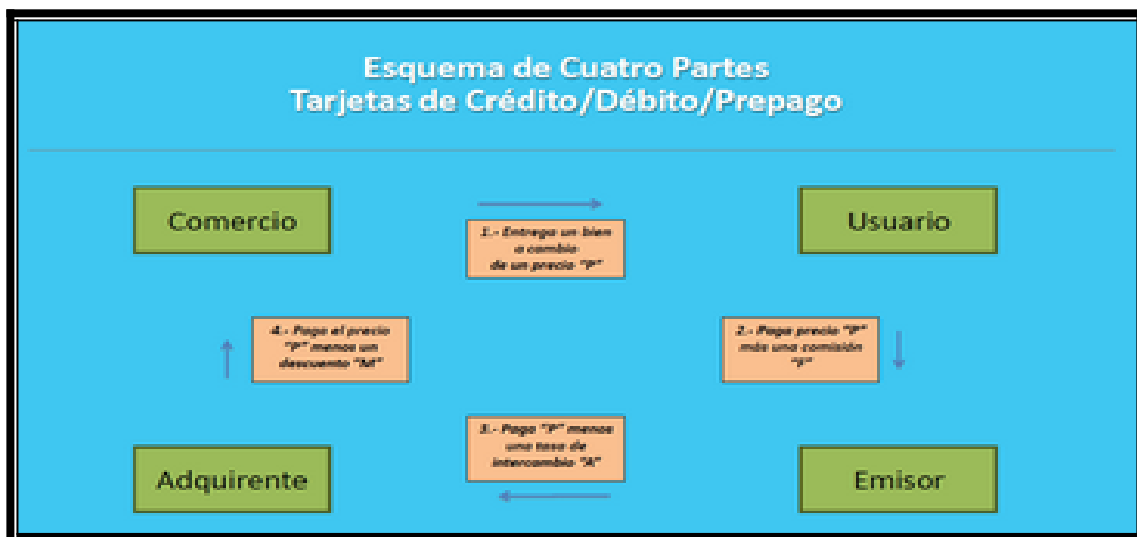
Recordó que Conadecus es una organización privada sin fines de lucro, constituida por un centenar de personas naturales, mayoritariamente profesionales, que trabajan para elevar el estándar en materia de protección al consumidor y defenderlo frente a los abusos. Participa en representación de los consumidores en varios Consejos de la Sociedad Civil, presidiendo varios de ellos, como por ejemplo los de la Superintendencia de Insolvencia y Reemprendimiento SIR y el del Servicio Nacional del Consumidor SERNAC.

Los principales objetivos de Conadecus son: contribuir a la construcción de una sociedad que respete los derechos de los ciudadanos que emanan de su condición de consumidores y usuarios de servicios públicos y privados; informar, orientar y educar a los consumidores y usuarios a través de todos los canales disponibles (sitio web, redes sociales, vía telefónica y presencialmente en su local ubicado en Valentín Letelier #16, Santiago de Chile), y asumir la defensa y representación de los consumidores y usuarios en el marco de la ley e institucionalidad.

El señor Gallegos puso de relieve que, en los últimos años, ha existido un crecimiento explosivo de las tarjetas. Esto se produce porque hay más consumidores dispuestos a ocupar estos medios de pago, y aprecian tener a su disposición los medios de pago que se ofrecen. Estos medios de pago deben contar con medios de seguridad suficientes; y

ojalá sus costos ser menores, pues actualmente tenemos un costo altísimo, que es por ejemplo 10 veces superior respecto de países como Australia.

Mostró el siguiente esquema:



Manifestó que las tres tarjetas son medios de pago, aunque operen de forma distinta respecto del momento en que se entrega el dinero. En relación a cada una de ellas, los emisores establecen reglas para evitar fraudes.

Coincidió con lo señalado en cuanto a que las funciones de emisor y adquirente son radicalmente distintas.

Luego de estas reflexiones, el señor Gallegos presentó la opinión de Conadecus sobre la iniciativa en estudio.

Indicó que Conadecus valora positivamente la modificación legal que limita la responsabilidad de los usuarios de tarjetas de crédito, débito y prepago (en adelante TCDP) por extravío, hurto, robo y operaciones fraudulentas.

Las TCDP son productos que emiten los bancos y otras empresas, como las del llamado retail financiero, para ser puestos a disposición de sus clientes a fin de ser utilizadas por éstos como medio de pago.

El uso de las TCDP por parte de los usuarios sin duda que les facilitan las transacciones respecto de otros medios como el efectivo y el cheque, pero es un hecho que cada vez que una transacción se realiza mediante una TCDP se originan ingresos en beneficio del emisor.

En consecuencia, respecto del usuario, no puede ser más que el emisor el responsable de la seguridad del sistema de transacciones que alberga y regula el uso de las TCDP, tal como es la

práctica en todo sistema de medios de pago, incluidos el efectivo y el cheque.

En relación a este último punto, el señor Gallegos hizo un matiz. Hay un ámbito en que esos riesgos pueden ser responsabilidad del adquirente y no del emisor, por no tomar las medidas necesarias en ciertos casos en que interactúa directamente con el comercio.

Continuando con su exposición, señaló que la modificación propuesta en el proyecto de ley viene a poner al día a Chile respecto de la práctica de mercado de países desarrollados en los que rigen las reglas de seguridad y protección del usuario de las empresas de tarjetas.

Esas empresas de tarjetas aplican políticas de seguridad denominadas Cero Responsabilidad para el cliente. Dio como ejemplo de casos en que los que el tarjetahabiente no asume responsabilidad alguna, por política de la empresa, lo que ocurre en el caso de VISA. La política de Cero Responsabilidad de VISA protege al usuario de usos no autorizados de su tarjeta tanto en las transacciones presenciales como en las no presenciales, eliminando la responsabilidad del consumidor respecto de transacciones fraudulentas.

En el caso de MasterCard, el usuario no tendrá responsabilidad respecto de transacciones no autorizadas si ha cuidado razonablemente su tarjeta de extravío, robo o hurto y ha dado oportuno aviso al emisor del eventual extravío, robo o hurto.

Expuestas las consideraciones anteriores, formuló algunas observaciones puntuales al texto propuesto:

1.- En el nuevo artículo 1°:

- En su letra b), es necesario corregir la definición de emisor, por cuanto incluye entre sus funciones la afiliación de comercios, actividad que corresponde al adquirente y no al emisor.

Sugirió incluir dentro de este artículo 1° la definición del "Adquirente".

- En la letra c) debe reemplazarse la expresión "con el emisor" por "con el "adquirente", pues el comercio no tiene relación contractual con el emisor.

- Del mismo modo, en la letra d) corresponde reemplazar la palabra "emisor" por "adquirente".

2.- En el nuevo artículo 6°, inciso primero, en su parecer no corresponde hacer la diferencia que allí se establece respecto de tarjetas de crédito o débito, puesto que ambos tipos de tarjeta pueden ser objeto de las conductas fraudulentas señaladas. Del mismo modo, habría que incluir en este artículo a las tarjetas de prepago o tarjetas con provisión de fondos, tal como se hace en el nuevo artículo 5°.

3.- Las referencias al "emisor" en el inciso segundo, del nuevo artículo 7°, no son aplicables a éste sino al adquirente, lo que sugirió corregir.

Finalizadas las exposiciones de los invitados a la sesión, los Honorables Senadores presentes formularon preguntas y comentarios.

La **Honorable Senadora señora Pérez** expresó que ha sido positivo oír estas exposiciones, cada una de las cuales aporta bastante.

Preguntó al Fiscal de la ABIF el por qué, frente a los ataques cibernéticos, particularmente del último tiempo, los bancos ofrecen a sus clientes un seguro con costo adicional para protegerse, dando a entender que de otro modo el banco no responde.

El mismo planteamiento lo realiza respecto de los casos de clonación de tarjetas. En muchos casos a las personas no les roban la tarjeta sino que se las clonan o extraen los datos. Se ha expuesto debidamente lo relativo a las capas de seguridad, pero aun así surge la misma duda, porque el cliente, para quedar protegido, tiene la necesidad de tomar un seguro adicional.

En el mismo sentido se pronunció el **Honorable Senador señor Tuma**. El tarjetahabiente puede extravíar la tarjeta, pero hay barreras para que no cualquiera la pueda usar, como la exigencia de claves o pinpass. Pero no se entiende por qué, para resultar protegido, el usuario tiene que pagar un seguro al banco a quién le entregó su dinero precisamente para que se lo cuidara.

El Presidente de ABIF, señor Segismundo Schulín-Zeuthen, dio respuesta a las inquietudes planteadas. Señaló que los seguros que se ofrecen son para todos los productos y básicamente son para cubrir situaciones previas al momento en que el cliente da a conocer al emisor la pérdida. Ese período hoy es tierra de nadie en Chile.

En relación a los fraudes con tarjeta presente, reiteró que se han ido adoptando una serie de medidas y resguardos.

El gran problema está en los fraudes de tarjeta no presente. Es un tema muy complejo, en el que se han ido adoptando y cada vez se toman más medidas. Por ejemplo, algunos bancos avisan al titular de la tarjeta apenas se realiza una transacción, incluso en algunos casos al celular. Cuando una transacción se sale de las pautas de comportamiento de un cliente, se encienden las alarmas, pero los hackers también empiezan a aprender las pautas de comportamiento. También están los casos de robo de bases de datos.

Reiteró que los seguros adicionales que se

ofrecen son para cubrir aquellos períodos que hoy están en tierra de nadie. Y puso de relieve que también hay una responsabilidad como usuario de cuidar sus medios de pago.

La **Honorable Senadora señora Pérez** manifestó que, no obstante la explicación, en su parecer el banco debiera proteger a sus clientes sin necesidad de un seguro adicional, y adoptar todas las medidas posibles, como los mensajes de texto al celular cuando se realiza una transacción, en forma gratuita, no es posible que este tipo de servicios se cobren aparte, como ocurre en muchos casos.

Asimismo declaró que es inaceptable que, al momento de presentarse un proyecto como el que se discute ya se anuncie por parte de ABIF que debería subirse el costo a los usuarios. Le preocupa que siempre se hagan advertencias de este tipo, y que, en definitiva, iniciativas que buscan favorecer al consumidor, por este tipo de medidas terminan perjudicándolo.

El **Honorable Senador señor Tuma** compartió lo señalado.

En respuesta, el Presidente de ABIF expresó que el negocio de los bancos es el manejo de riesgos, y si existen mayores riesgos, se generan mayores costos. En su opinión, sería ilustrativo invitar a representantes de algunas de las marcas como VISA o MasterCard. No comparte la afirmación que siempre el responsable es el emisor.

El **Honorable Senador señor Pizarro** abordó un tema distinto. Recordó que el Fiscal de la ABIF expresó que esta normativa podría aumentar el riesgo de auto-delito, y en esa línea consultó si existe información de cuantos son los auto-delitos de los tarjetahabientes. En su parecer es un punto importante.

Por otra parte, en relación a las cifras y gráficos dados a conocer por el Presidente de la ABIF, conforme a los cuales en Chile se producen menos fraudes que el promedio internacional, consultó a qué se atribuyen estas cifras, si hay una menor cantidad de tarjetas, un mayor cuidado al entregarlas, mayor responsabilidad de los usuarios, o que otro factor puede incidir en estos resultados.

El señor Schulin-Zeuthen señaló que desconoce estadísticas, pero analizándolo por el lado de los reclamos que presentan los clientes por supuestos fraudes (por giros que dicen no haber hecho, transferencias u otros), se puede afirmar que en la gran mayoría de los casos son resueltos.

En relación al por qué el fraude es menor en nuestro país, le parece que la respuesta se encuentra en un conjunto de factores. Se han hecho trabajos importantes en seguridad, la banca también lo ha hecho, y la gran mayoría de las personas tiene cuidado al usar sus medios de pago.

Por su parte, el Vicepresidente de Conadecus, señor Gallegos, reiteró que en materia de responsabilidad, empresas como VISA tienen una política de cero responsabilidad. Agregó que tanto las empresas de tarjetas como también los emisores, hacen un esfuerzo enorme y eso se valora. Las compañías de tarjetas tienen todas las herramientas necesarias para detectar una operación sospechosa. Los bancos en Chile, aunque han avanzado bastante, deben hacer una mayor inversión en esta materia. El banco debe conocer a sus clientes y su comportamiento.

El Presidente de ABIF, en relación a lo señalado por el señor Gallegos, puntualizó que se está exponiendo sesgadamente la política de VISA en relación a la “responsabilidad cero”.

Por otra parte, si bien es efectivo que el banco debe “conocer a su cliente”, esa afirmación hoy día ya no es una realidad, basta pensar por ejemplo en lo que ocurre con las Cuentas Rut, en que solo por ser chileno mayor de 14 años se puede ser titular de una cuenta. Se ha ido perdiendo el “*know your client*” con la bancarización, y con la cada vez mayor disposición de medios de pagos.

VISA INTERNACIONAL LTDA

El Vicepresidente de Relaciones Gubernamentales de VISA para América Latina y el Caribe, señor Salvador Pérez Galindo, luego de agradecer la invitación a participar en esta sesión de la Comisión, puso de relieve que el tema que aborda el proyecto en estudio es de gran importancia.

Agregó que sin duda es necesario actualizar la ley N° 20.009 vigente en la materia, que data del año 2005, atendido que la industria ha experimentado una gran transformación en estos años. En ese sentido, celebró el trabajo de la Comisión y su esfuerzo en tal sentido, en un marco normativo tan importante como este.

Se refirió brevemente a lo que es VISA y cómo se define. VISA no es una entidad financiera, sino una empresa de tecnología de pagos. Se trata de una de las primeras *fintech* (desarrollo de servicios financieros basados en innovación tecnológica) que nació hace más de 50 años en Estados Unidos, cuando se empezó a electrificar el tema de los pagos. Está presente en Chile hace casi tres décadas y actualmente tiene su base de operaciones para Cono Sur en nuestro país.

Señaló que Chile es un país que va a la vanguardia en materia de pagos electrónicos en la región. Destacó asimismo el dinamismo de su economía y las innovaciones que se están llevando a cabo, razón por la que es muy importante para VISA.

Luego, el señor Pérez Galindo realizó una exposición que tituló “La seguridad en los medios de pago: una responsabilidad compartida”, apoyado en un power point. Su presentación tiene tres objetivos principales:

1.- Explicar la evolución reciente en medios de pago y sus implicaciones para la seguridad.

2.- Compartir su visión de la seguridad como una responsabilidad compartida de todos los participantes en la cadena pagos. En su parecer, la iniciativa en estudio enfatiza mucho el rol del emisor de la tarjeta, estimó que sin duda ahí hay una responsabilidad importante pero no es la única.

3.- Compartir consideraciones finales sobre el proyecto de modificación a la ley N° 20.009.

Expresó que el primer gran mensaje de su presentación es que en la industria el ambiente de compras está cambiando. La distinción histórica entre pagos en el mundo físico (fundamentalmente usando una tarjeta en un punto de venta) y el digital (no presencial, usando algún canal electrónico) se está borrando cada vez más rápidamente. Es cada vez más difícil de distinguir. Dio el siguiente ejemplo: presencialmente efectúo un pago mediante una aplicación de mi celular, ¿es una transacción presencial o digital?

El mundo de pagos digital presenta un desafío importante en seguridad, y la industria está invirtiendo para proteger esos nuevos canales de hacer pagos.

En efecto podemos encontrar:



Agregó que todos los dispositivos vinculados a internet son potenciales terminales puntos de ventas (POS). En ese sentido, se dice que el POS está en todos lados:



Algunos de estos ejemplos son más futuristas que otros. En efecto, al día de hoy ya se puede pagar por medio de celulares, cuyo crecimiento ha sido explosivo y es así como hoy en el mundo hay más celulares, tablets y varios otros dispositivos electrónicos afines, que habitantes. Se estima que para el año 2020 habrá cincuenta mil millones de dispositivos conectados a internet. En un futuro habrá, por ejemplo, refrigeradores que mantendrán por sí solos el inventario de lo que se necesita e inclusive harán transacciones digitales pidiendo los artículos que hagan falta.

Las transacciones digitales son el vehículo del crecimiento en consumo y un reto para el comercio. El canal de crecimiento futuro es precisamente el canal digital. En la lámina se observa que estamos hablando de crecimiento de dos dígitos en el mundo digital:



En China, el 75 % del comercio electrónico es a través de un dispositivo móvil, se ha transformado en el nuevo canal de comercio.

Sobre el rol de VISA.

En primer término, el señor Pérez Galindo puntualizó que VISA no tiene relación con los comercios ni con los consumidores. VISA es un intermediario y una plataforma tecnológica. Como VISA, les interesa que esa plataforma logre:

- Generar confianza y conveniencia al realizar pagos electrónicos. Afirmó que la experiencia de pago debe ser sencilla y el consumidor debe quedar tranquilo.

- Maximizar la seguridad de los pagos electrónicos independientemente del dispositivo o canal.

- Ampliar la inclusión financiera mediante mayor acceso y uso de pagos electrónicos entre consumidores y comercios. Todavía hay un porcentaje de la población que no tiene acceso a estos medios de pago y le parece fundamental, ya no es un lujo tener estos medios de pago electrónicos, es una necesidad.

Sostuvo que la seguridad en los pagos es una responsabilidad compartida entre los múltiples actores en la cadena de pagos.

Distinguió entre los siguientes actores en la cadena de pagos:

- 1. Adquirente:** Institución que afilia y vincula a los comercios al sistema VISA, les procesa transacciones y les realiza liquidaciones financieras. En Chile se utiliza también el término operadores. Es la entidad que se vincula con el comercio, son entidades independientes y muchas veces tienen responsabilidades diferentes según el rol que asuman.

- 2. Procesador Adquirente:** Realiza servicios de procesamiento para los adquirentes.

- 3. Proveedor de Servicios para Procesamiento de Pagos:** Provee servicios de valor agregado y conectividad a las redes de pago para los comercios. Se trata de una figura nueva que ha llegado a Chile recientemente con la modificación de la normativa sobre tarjetas del Banco Central. Es una figura crecientemente importante en todo el mundo, y que VISA reconoce y la tiene normada.

- 4. Comercio:** Provee bienes y servicios a cambio de pago. Para aceptar tarjetas, los comercios deben de ser validados y mantener una relación con un adquirente.

5. Emisor: Institución que emite tarjetas y mantiene una relación financiera con el tarjetahabiente.

6. Procesador Emisor: Realiza servicios de procesamiento para los emisores.

7. Tarjetahabiente: Portador de una cuenta VISA.

El señor Pérez Galindo explicó que estos actores participan en el modelo de pago de tipo abierto (tipo VISA):



Subrayó que todos estos actores tienen una responsabilidad en la seguridad. Si alguno de ellos fallara con sus protocolos, la manera de proteger la información, se va a generar un problema de seguridad. Y en la visión de VISA todos tienen que asumir su responsabilidad y hacer lo que les corresponde para minimizar los riesgos de fraude.

Cuatro Pilares de la visión de VISA en materia de la seguridad.

Se trata de ejemplos concretos de las responsabilidades que se le asignan a cada uno de los actores o jugadores.

Los cuatro pilares que explicará son:

- Devaluar la información sensible, que se traduce en no exponer esta información. Las herramientas son: chip para las transacciones comerciales (EMV) y la tokenización, que es la réplica del chip para el mundo digital.

- Aprovechar tecnologías de datos (*"Big Data"*). Poder tomar decisiones de fraude en tiempo real con la información disponible, incluso poder por ejemplo declinar una transacción en el punto de venta.

- Proteger los sistemas de información. Lo anterior atendido que el robo de bases de datos, los *hackers*, están cada día más presentes. La industria ha establecido ciertos estándares, como por ejemplo que evitar almacenar información sensible a nivel comercio, que puede ser robada y usada para cometer fraude en el mundo físico o digital.

- Proteger e involucrar al consumidor. Que el consumidor asuma un rol proactivo en la prevención, con más control sobre sus transacciones. Para esto se cuenta con herramientas tales como alertas SMS o email, y se formula el principio o regla de “cero responsabilidad”.

El señor Pérez Galindo expresó que ilustrará cada uno de los pilares.

Pilar N° 1. Devaluación de información – Chip:

Este tema es importante para entender lo que ha pasado hasta el momento, y como el riesgo de clonación de una tarjeta ha bajado mucho en los últimos años. Ha existido una gran inversión de la industria para reemplazar tarjetas, terminales, puntos de venta y cajeros automáticos.

El chip de la tarjeta permite validar cada transacción, generando un criptograma único, lo que significa que cada transacción es única y no se puede copiar la información. Eso protege la transacción presencial en puntos de venta y cajeros automáticos.

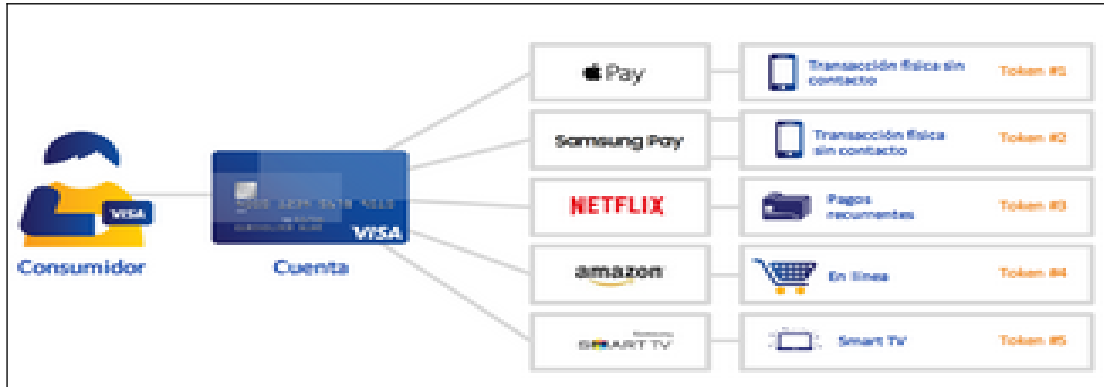
Se establece una regla de cambio de responsabilidad, conforme a la cual la parte que ha hecho la inversión esté protegida del fraude. Así, desde octubre de 2014, y a nivel global internacional, el emisor o el adquirente que no haya invertido y migrado a chip es responsable por el fraude. Lo anteriormente expuesto queda a nivel entre emisor y adquirente, el tarjetahabiente tiene la relación con el emisor.

Aplica en POS/ ATM, y cubre transacciones nacionales e internacionales

Agregó que el gran reto es el canal no presencial, el comercio electrónico. Se han hecho varios esfuerzos, siendo el más sólido, ambicioso y que más tiempo va a llevar es el de tokenización.

Pilar N°1 Devaluación de información –
Tokenización.

Lo graficó de la siguiente forma:



El token ya existe para la banca en línea, todos lo usamos cuando queremos hacer una transferencia bancaria. El concepto llevado a la industria de las tarjetas es sustituir los 16 dígitos que hay en una tarjeta por un nuevo número, también de 16 dígitos, que es el token. Esa sustitución se hace en una bóveda en la nube, y VISA y el emisor de la tarjeta van a tener la información. Ese token se puede acotar para que sólo sirva para un dispositivo, un teléfono celular, un computador, para un comercio (por ejemplo Netflix o Amazon), y no se puede usar ese token fuera de ese dispositivo o comercio. El mejor ejemplo es el de los celulares con el Apple Pay y el Samsung Pay. Esta es la solución de seguridad que se tiene para el mundo digital hasta el momento.

Pilar N°2, el Uso de Herramientas Anti-Fraudes

Continuando con su presentación, el señor Salvador Pérez señaló con respecto del pilar N°2, es decir, el uso de herramientas anti-fraudes, que existe una regla reciente de parte de VISA, de acuerdo a la que a partir de julio de 2018 todos los emisores de tarjetas VISA estarán obligados a tener herramientas de monitoreo de fraude, en tiempo real. El Big Data permite proveer mejores tomas de decisión y, también, en materia de fraudes minimizar la posibilidad de su ocurrencia gracias a las herramientas que ofrece la tecnología de la información.

Pilar N°3, Salvaguardia de la Información.

El pilar N°3, Salvaguardia de la Información, es muy importante. Mencionó el Caso Target en los Estados Unidos, como un ejemplo de los riesgos de robos de información a nivel de comercios. Destacó la política de las marcas, porque esta es una regla de la industria, es evitar el almacenamiento de información que no necesita el comercio. Para eso hay estándares internacionales conocidos como PCI-DSS, por sus siglas en inglés, *Payment Card Industry – Data Discernation Standards*, que dan una serie de orientaciones y educación a los comercios de cómo administrar el manejo de la información, tanto para el mundo presencial como para el

digital.

Pilar N° 4, “Involucrar al Tarjetahabiente”.

El último pilar, el N° 4, cual es “Involucrar al Tarjetahabiente”, es uno de los más importantes porque está referido al rol del consumidor. Recordó que ya mencionó lo relativo a las alertas y se centró en la “Regla de Cero Responsabilidad”. Explicó que es un principio que se ha expandido en el tiempo, y que en América Latina recién lo implantaron en agosto del año 2016. Si bien el principio es muy conocido en los Estados Unidos, porque lleva mucho tiempo allá, es un tema nuevo en nuestros países y que han estado socializando con sus bancos.

El principio o regla de “cero responsabilidad” es el beneficio al tarjetahabiente consistente en que no es responsable por cargos no autorizados, concepto que sugiere que el proyecto lo incorpore. Cargo no autorizado es aquél en el que el tarjetahabiente no tuvo participación en autorizar la transacción; no se benefició de recibir un bien o servicio y no participó en la operación.

El alcance de este mecanismo de protección es robo, extravío o fraude. Cualquier transacción que no haya autorizado el tarjetahabiente. Cubre puntos de venta; cajeros automáticos; transacciones locales o internacionales. Hay excepciones en ciertos productos, como son las tarjetas comerciales y las corporativas o el prepago anónimo. Respecto de este último, hizo presente que la nueva normativa del prepago en Chile distingue entre prepago anónimo e identificable. A nivel de reglas, no hace sentido proveer protección respecto del prepago anónimo.

Por el lado del emisor, la obligación es realizar un abono provisional dentro de cierto plazo de tiempo del tipo de producto. La ley habla de reembolsar el monto de la transacción realizada. Sin embargo, a nivel de regla de la marca, VISA prefiere hablar de un abono provisional, que es algo que sugiere que lo considere también el proyecto. En relación al plazo, estima que este debe ser razonable. En este punto, indicó que 24 horas es un tiempo muy reducido y complica que tal reembolso efectivamente se realice, especialmente si hay días feriados o fines de semana. En tal sentido, considera que el plazo de 24 horas no es realista para poder realizar tal operación de reembolso. VISA tiene un plazo de hasta 5 días, lo que ha variado en el mundo, porque no existe una regla única. La propuesta de VISA respecto de este punto es que se amplíe también el referido plazo, y que llegue a 5 días.

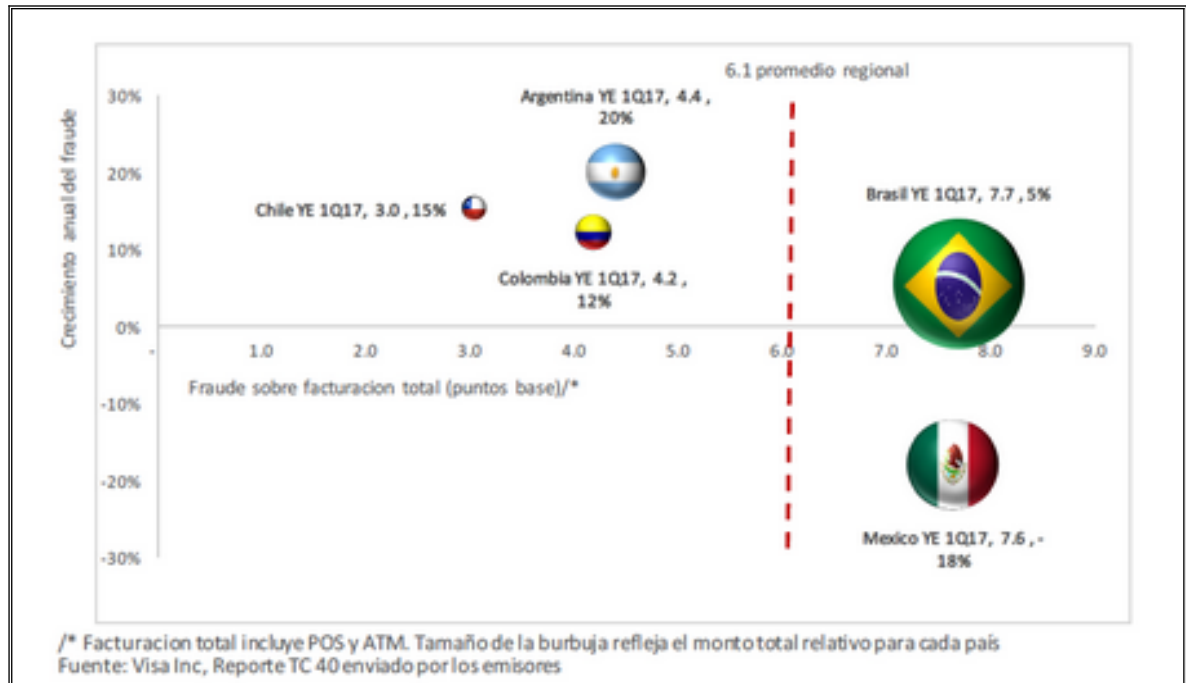
Lo anteriormente expuesto es sin perjuicio de la investigación que generará la situación. Obviamente el tarjetahabiente estará sujeto a confirmar que efectivamente no autorizó la transacción; que no hubo una participación suya. Esto tiene por finalidad evitar que se realicen auto fraudes, porque siempre existe ese riesgo. Reconoce que, dentro de este contexto, el concepto de “cero responsabilidad” puede ser mal entendido.

Tal investigación puede tomar entre 90 a 120 días, dependiendo de si el fraude es nacional o internacional. Indicó que en el

caso chileno los fraudes tienen un alto componente internacional.

Destacó que el reto de la seguridad en los pagos son tanto la conveniencia como la seguridad para el cliente.

Respecto de las estadísticas de fraude, se limitó a dejar en claro que nuestro país no es de los cuales VISA esté preocupado, tal como demuestra la siguiente gráfica comparativa.



Consideraciones finales.

-Actualmente hacer pagos de manera electrónica es más seguro y conveniente.

-VISA y sus emisores y adquirentes invierten sumas crecientes en materia de tecnología y herramientas de seguridad.

-Las reglas y protocolos que establecen van dirigidas a generar incentivos para que todas las partes involucradas en la cadena de pagos asuman su responsabilidad.

-El principio de "cero responsabilidad" para el consumidor es un beneficio que conlleva obligaciones de un uso responsable del medio de pago.

-El proyecto de reforma a la ley N° 20.009 busca ampliar la protección del consumidor financiero pero es importante hacerlo de manera integral y atendiendo responsabilidades para todos los participantes.

Sugerencias.

-Diferenciar rol emisor del rol adquirente u operador en línea, con las definiciones de la nueva normativa de tarjetas de pago del Banco Central de Chile.

Hizo presente que en la terminología chilena adquirente es básicamente la figura del operador. Así lo dispone la normativa del Banco Central. Sin embargo, resultado de esa normativa habrá cambios en la estructura de la industria en Chile, Aunque históricamente ha habido sólo una empresa realizando esta función a nombre y cuenta de los emisores, esta cambiará, y habrá nuevos actores que no estarán haciendo eso necesariamente a nombre y cuenta de un emisor. Le parece importante dejar en claro el rol del operador o adquirente como entidad responsable de la vinculación con el comercio (afiliación, interconexión, liquidación de transacciones, etcétera.).

-Respecto del artículo 6° establecer que "El usuario no se tendrá por responsable en las operaciones realizadas sin su autorización, *siempre y cuando dicha operación se le haya previamente reportado al emisor (...)*. Celebra que el usuario no se tenga por responsable en las operaciones realizadas sin su autorización, pero la ley debe dejar bien establecida su obligación de reportar cualquier cargo no reconocido. Actualmente la ley establece la exigencia de reportar el robo o extravío de la tarjeta, pero no la obligación de reportar la transacción no reconocida. Además, siempre es posible que sea el tarjetahabiente el primero que se dé cuenta que ha sido víctima de un fraude.

-En relación al artículo 7° del proyecto, hizo dos sugerencias:

(a) incorporar el concepto de "abono provisional" sujeto a los resultados de la investigación, en lugar de "cancelación de los cargos" o "devolución de los importes", y

(b) considerar un plazo que no exceda de cinco días en lugar de 24 horas.

En el caso del comercio, establecer obligaciones de salvaguardar y proteger la información de los usuarios, así como de colaborar en las investigaciones. En su parecer, el proyecto deja muy abierta la responsabilidad que pueda tener el comercio en los casos de fraude. Por lo anterior, es importante incluso considerar la obligación de que tengan que salvaguardar y proteger la información de los usuarios, pues el comercio siempre la estará manejando.

Por su parte, Paola Ledezma destacó que el objetivo de la presentación es complementar el proyecto en discusión y manifestó su disposición a apoyar el trabajo legislativo en lo que fuere pertinente.

**DIRECTOR CEDI UNIVERSIDAD DE CHILE
PROFESOR RENATO JIJENA**

El profesor Renato Jijena agradeció la invitación a exponer en relación a esta materia.

Señaló que analizará el boletín N° 11.078 desde la perspectiva de la “seguridad de sistemas”, comprendiendo la seguridad de los sistemas bancarios en general y la de las tarjetas de crédito en particular. Se trata de un contexto que se construye y regula con las normas generales del derecho, con estándares especiales ISO, con normas oficiales del INN como la 27001-2013 y con normas administrativas de la SBIF.

Propone salir del contexto del artículo 23 de la ley N° 19.496 que obliga a que el proveedor garantice la seguridad en el consumo, aunque, en definitiva, se arribe a la misma conclusión.

Expuso un caso concreto: una cuentacorrentista del Banco de Chile se entera sólo a posteriori que le fueron emitidas y usadas tres tarjetas de crédito electrónicas, con las cuales unos ciudadanos peruanos, perfectamente identificados, compraron pasajes a Lima. Y el banco responsabiliza, incluso judicialmente, a la cliente. Ni siquiera hubo algún llamado de la ejecutiva de cuenta al cliente, advirtiéndole esta operación. Ese es el estándar que se está aplicando al día de hoy.

Esto es claramente una negligencia grave en materia de seguridad de sistemas en general y de autenticación electrónica en particular. Y la responsabilidad asociada en este caso del emisor, por haber permitido estas operaciones, en la línea de lo que establece el proyecto, es importante que sea regulada, explicitada y precisada.

Otro caso de negligencia por no verificación de identidad se produce en el caso de phishing, donde los bancos se escudan en la cláusula que establece que todo lo relacionado con mal uso de la clave será siempre de responsabilidad exclusiva del titular. Declaró que esta cláusula sin duda es abusiva y debe prohibirse legalmente, o al menos dirigirse por ley, y acá el proyecto está en la línea correcta cuando propone tenerla por no escrita. Este último punto es, judicialmente, un tremendo avance.

Los bancos ya han sido condenados judicialmente por no tomar las medidas necesarias para evitar fraudes o delitos informáticos que afectan a los consumidores, en concreto tratándose del uso de las claves que ellos consideran y determinan contractualmente como de responsabilidad exclusiva de los clientes.

Dice mucho que en el pasado reciente la banca y el comercio hayan tenido que escalar o aumentar los niveles de seguridad en sus plásticos, pasando del uso de bandas magnéticas a los chips. Se trata de

un cambio que era indispensable implementar. La obligación de ser diligentes es principalmente de los emisores de las tarjetas, lo que se traduce en establecer sistemas preventivos de autenticación y seguridad de los plásticos. De nada sirve la seguridad a posteriori.

En el contexto de la seguridad de información, la SBIF hablaba, en junio de 2016, de enfatizar la necesidad de tomar medidas de control para disminuir los riesgos operacionales, y de mejorarse la gestión preventiva de los riesgos operacionales.

A pesar de que hace unos años nos acercamos al tema defendiendo a la banca ante demandas colectivas concretas de los consumidores, hoy no podemos sino estar de acuerdo con el contenido esencial del proyecto de ley. La ley debe adecuarse a la realidad presente, o dicho de otra forma, las definiciones o los estándares de seguridad y de responsabilidades asociadas a los riesgos de robo, hurto, extravío o clonación deben actualizarse y precisarse. La ley N° 20.009 tiene que ser actualizada y el proyecto va en esa línea.

Si se determina que a esta fecha los emisores de tarjetas han sido negligentes adoptando medidas de seguridad y previniendo, entonces limitar la responsabilidad de los usuarios o tarjetahabientes es un estándar necesario.

La ley vigente dice que los avisos o noticias en caso de hurto, robo o extravío deben hacerse mediante sistemas de comunicación de acceso permanente y que el bloqueo por el emisor debe ser inmediato; así se materializa la eximente de responsabilidad para el usuario a contar desde el aviso, y caemos en el ámbito de una operación o transacción bancaria oportunamente "no autorizada por el titular" y a la obligación de que se le restituyan los montos defraudados. El gran problema es que esta norma no sirve para el mundo de los pagos electrónicos. Precisó que, por cierto, si un titular no notifica el extravío, hurto o robo, él también debe ser responsable en alguna medida, y esa responsabilidad puede cuantificarse, y si un emisor no establece un procedimiento idóneo de notificación o aviso también puede explicitarse su responsabilidad. Ahora bien, en el caso de las clonaciones, cuando el titular nunca supo del delito previo y el fraude posterior y no pudo notificar o avisar, cabe preguntarse a quién responsabilizamos.

Preguntas relevantes: ¿Por qué entonces a veces los emisores responsabilizan a los tarjetahabientes por las operaciones fraudulentas realizadas por terceros dolosamente, y se niegan a realizar los contra cargos y reembolsar lo defraudado? Hay una acción dolosa de un tercero y hasta ahora se responsabiliza al tarjetahabiente.

¿Por qué en el hecho se les obliga a contratar un seguro complementario (se les induce o engaña), que solo tiene un fin de lucro para la entidad financiera que emite el plástico? Estimó que no hay justificación jurídica para ello, la obligación de ser diligente nace por el vínculo contractual con el tarjetahabiente, no porque se tome un determinado seguro.

Nuevamente en el contexto de la seguridad de sistemas: ¿son idóneos los mecanismos de autorización de las operaciones, de manera tal que el carácter fraudulento quede de manifiesto antes de realizarse y se bloquee preventivamente la operación, sea presencialmente con plásticos (con tarjeta presente en la mayoría de los casos clonada) o mediante Internet? ¿Cómo pudo ocurrir entonces el caso del Banco de Chile referido al inicio, que autorizó operaciones no realizadas por el tarjetahabiente, si no es por negligencia del banco en la implementación de sus mecanismos de autenticación o de verificación de identidad? Reiteró que se trata de una cláusula abusiva.

A continuación, el señor Jijena formuló algunos comentarios respecto del texto del proyecto.

Expresó que el proyecto propone utilizar el término "medios de pago" para aludir a tarjetas y transacciones electrónicas sin tarjeta. Le parece una cuestión semántica de muy poca importancia, porque esas transacciones electrónicas siempre se hacen en base a asientos electrónicos contables que corresponden a la cuenta corriente, al débito o al crédito.

En cuanto a las propuestas de definiciones, le parecen innecesarias porque el mercado y la industria no caen en confusiones conceptuales.

Respecto de los plazos de reembolsos ante fraudes, le parece un poco breve que sea en 24 horas hábiles desde que sean detectadas, porque internamente se realizan procesos de verificación que pueden ser más largos. En ese sentido, está de acuerdo con lo planteado por los representantes de VISA, en cuanto a que se trata de un plazo no realista.

Por otra parte, rechazó una vez más la inducción a la contratación de seguros antifraudes adicionales como condición para los contra cargos, y se manifestó de acuerdo en que se restrinja. Destacó que este es un punto muy importante.

En relación a las normas eximentes de responsabilidad, compartió las que se proponen, por ejemplo, para el caso de donaciones dolosas no conocidas o ignoradas totalmente por el tarjetahabiente, que nunca podrían serle imputadas, como se hizo en el caso del Banco de Chile, salvo que durante la investigación posterior se determine que hubo aprovechamiento. Y el traslado de la carga de la prueba al emisor para probar que él si las conocía o fue negligente.

o o o o o

Finalizadas las exposiciones de los invitados a la sesión, intervinieron los Honorables Senadores presentes.

La **Honorable Senadora señora Pérez** agradeció las exposiciones. Manifestó estar orgullosa de ser una de las autoras de la moción, que claramente es una necesidad en nuestro país. Agregó que las exposiciones fueron claras y concretas.

Le resulta gratificante escuchar opiniones informadas y positivas, particularmente luego que en la sesión anterior se advirtieran por parte de algunos invitados, ciertos peligros inminentes de una iniciativa como la en estudio, como, por ejemplo, encarecer los costos.

Declaró que la situación actual en este ámbito es inaceptable. Son inexplicables situaciones como las que se exija el pago adicional de un seguro frente a los ciber ataques o que la carga de la prueba sea de cargo del cliente, entre otras.

Este proyecto es un clamor de la gente, y es absolutamente transversal, afecta tanto a quienes tienen recursos como a aquellos que no, porque hoy prácticamente todo se compra con tarjetas.

El **Honorable Senador señor Pizarro** pidió al representante de VISA algunas aclaraciones respecto de la forma como opera el Pilar N°1, específicamente en lo relativo a la tokenización, y si los 16 números distintos de los de la tarjeta que utilice, por ejemplo, el Apple Pay, se van a poder usar sólo en un tipo de comercio, y será necesario tener un número distinto para cada compra, o bien con ese número se podrá comprar en cualquier comercio que cuente con el sistema.

El **Honorable Senador señor Quinteros** agradeció y felicitó las exposiciones. Afirmó que se trata de un muy buen proyecto que hace falta en nuestro país. Hay muchísimos ejemplos de los abusos que se producen en esta materia.

En respuesta al Honorable Senador señor Pizarro, el señor Pérez Galindo explicó que el token puede ser para un comercio, por ejemplo Netflix, caso en el cual se sustituyen los 16 dígitos de la tarjeta que serán únicos para hacer una transacción ahí. Ahora bien, si se trata de un token para un dispositivo, por ejemplo con Apple Pay, el token es sólo para el dispositivo de que se trata.

SERVICIO NACIONAL DEL CONSUMIDOR (SERNAC)

El Jefe de División de Consumo Financiero de SERNAC, señor Rodrigo Romo, intervino en representación del organismo. Anunció que SERNAC tiene una opinión favorable a esta iniciativa de ley, que es sin duda muy necesaria. Asimismo manifestó la disponibilidad de SERNAC para participar en la tramitación y perfeccionamiento de este proyecto.

Realizó luego una exposición en power point que aborda los siguientes puntos:

I. Breve descripción del Mercado Financiero en Chile.

II. Ranking sub-mercado: Banca y Tarjetas de Crédito relacionadas al retail.

III. Actual regulación.

IV. Acciones.

V. Jurisprudencia.

VI. Comentarios al proyecto.

I. Breve descripción del mercado financiero en Chile.

La industria financiera está integrada por distintos tipos de entidades. Abarca aquellas que brindan servicios de ahorro e inversión, crédito, entre otros.

Desde el punto de vista de los reclamos, al SERNAC llegan reclamos de consumidores principalmente contra la banca, el retail financiero y las cajas de compensación.

Respecto a los productos o servicios más reclamados en el mercado financiero por los consumidores, durante el segundo semestre de 2016, se encuentran las tarjetas de multitiendas (32,8%), los créditos de consumo (14,1%) y las cuentas corrientes (8%).

II. Ranking sub-mercado: Banca y Tarjetas de Crédito relacionadas al retail.

El señor Romo expresó que cada semestre SERNAC realiza un ranking en relación a los sub mercados financieros más reclamados.



Hizo presente que los bancos y las tarjetas de crédito relacionadas al retail representan más del 80% de los reclamos.

En cuanto a los principales motivos de reclamos en la banca, indicó:

PRINCIPALES CAUSAS DE RECLAMOS	% DE RESPECTO AL TOTAL DE RECLAMOS CONTRA LA BANCA	
	2º SEMESTRE 2015	2º SEMESTRE 2016
FRAUDE: CONSUMIDOR NO RECONOCE TRANSACCIÓN POR CLONACIÓN Y/O SUPLANTACIÓN	13,9%	18,2%
NO REVERSA CARGOS MAL EFECTUADOS	14,4%	14,0%
DINERO NO ENTREGADO PARCIAL O TOTAL	9,7%	9,2%

COBROS EXCESIVOS POR INTERESES Y COMISIONES	10,5%	8,0%
COBRANZA EXTRAJUDICIAL: PROCEDIMIENTOS QUE NO CORRESPONDEN Y COBROS EXCESIVOS	6,8%	7,0%

Destacó que la causal más reclamada es precisamente el fraude, aquellos casos en que el consumidor no reconoce la transacción por clonación y/o suplantación.

En relación a los principales motivos de reclamos contra las tarjetas de crédito relacionadas al retail, mostró los siguientes datos:

PRINCIPALES CAUSAS DE RECLAMOS	% RESPECTO AL TOTAL DE RECLAMOS CONTRA TARJETAS DE CRÉDITO RELACIONADAS AL RETAIL	
	2° semestre 2015	2° semestre 2016
Cobranza extrajudicial no corresponde	16,83%	19,14%
No reversa cargos mal efectuados	16,89%	17,96%
Cobros excesivos o duplicados	10,35%	8,49%
Fraude: consumidor no reconoce transacción por clonación y/o suplantación	4,58%	7,43%
Cobro de seguros no contratados	7,56%	6,89%

Aquellos casos en que el consumidor no reconoce la transacción por clonación y/o suplantación, si bien no constituyen la causal más reclamada, tienen bastante prevalencia.

Concluyó que los datos expuestos revelan que la materia que aborda este proyecto es un tema que está presente de manera importante en el mercado financiero.

III. Actual regulación.

El señor Romo manifestó que la normativa vigente contiene varias normas que han permitido construir una cierta interpretación en esta materia:

A) Ley N° 19.496 sobre Protección de los Derechos de los Consumidores:

- El artículo 3° inciso primero letra a), reconoce como derecho básico del consumidor la libre elección del bien o servicio y señala que el silencio no constituye aceptación en los actos de consumo.

- El artículo 3° inciso primero letra d), establece el derecho a la seguridad en el consumo de bienes o servicios.

- El artículo 12 dispone que todo proveedor de bienes o servicios estará obligado a respetar los términos, condiciones y modalidades conforme a las cuales se hubiere ofrecido o convenido con el consumidor la entrega del bien o la prestación de servicio.

- El artículo 23 consagra el deber de profesionalidad de los proveedores, que conlleva la obligación de prestar el servicio de manera de no causar menoscabo al consumidor.

Puso de relieve que la norma central es el artículo 23, que junto con el artículo 3° letra d) permiten configurar una obligación de los proveedores de servicios financieros de entregar este servicio de manera segura.

B) Ley N° 20.009 sobre extravío, robo o hurto de tarjetas:

- Artículo 3°. “En el caso que las tarjetas sean operadas con posterioridad al aviso de extravío, hurto o robo, corresponderá al emisor probar que las operaciones fueron realizadas por el tarjetahabiente titular o los adicionales autorizados por éste”.

- Artículo 4°. “El tarjetahabiente no tendrá responsabilidad por las operaciones realizadas con posterioridad al aviso o noticia entregada al emisor, sin perjuicio de la responsabilidad penal que corresponda”.

El señor Romo puntualizó que esta ley no establece que la responsabilidad previa al aviso es necesariamente del tarjetahabiente.

IV. Jurisprudencia.

En este punto, el Jefe de la División Consumo Financiero de SERNAC, señor Rodrigo Romo, presentó dos sentencias de la Corte de Apelaciones de Santiago que recogen la interpretación del SERNAC:

1. Rol Ingreso de Corte N° 342-2016 (Ilustrísima Corte de Apelaciones de Santiago):

Hizo referencia a los principales considerandos que abordan este punto:

“SEGUNDO: Que, la impugnación efectuada en el recurso alude esencialmente a una cuestión que dice relación con la

suficiencia de la prueba rendida para los efectos de establecer si la entidad bancaria desplegó las medidas de seguridad racionalmente esperables a objeto de evitar la vulneración de un adecuado servicio prestado en sus tarjetas de crédito”.

“TERCERO: Que, esta cuestión resulta de suyo compleja, pues no es posible analizar este conflicto desde la óptica del derecho civil tradicional, sino que debe ponderarse en conformidad a la normativa especial contenida en la Ley N°19.496”.

“CUARTO: (...) En este caso, el servicio consiste en el otorgamiento por el BANCO ...de tarjetas de crédito, lo que supone que la entidad bancaria preste el servicio ofrecido sin fallas o deficiencias en cuanto, en lo que aquí interesa, a la seguridad, no solamente cuando se celebra el contrato entre las partes, sino en la relación que se establece después, a propósito de su utilización (...)”.

“QUINTO: (...) un problema adicional es aquel relativo a la carga probatoria. Desde el momento en que el proveedor niega haber incurrido en alguna deficiencia, falla o error de cualquier tipo en la provisión del servicio, se hace cargo de la obligación de probar tal aserto, esto es, planteado en términos positivos, deberá acreditar el debido cuidado, la diligencia, la actuación del proveedor conforme a los estrictos términos del servicio inmaculado ofrecido. Y ello es así, atendido el carácter protector del derecho del consumidor, unido a la circunstancia de la mayor disponibilidad y facilidad probatoria que normalmente acompaña a las entidades proveedoras de servicios (...)”.

2. Rol Ingreso de Corte N° 1796-2015 (Ilustrísima Corte de Apelaciones de Santiago):

“TERCERO: La conclusión lógica que se obtiene de lo acontecido, es que siendo responsabilidad de la denunciada acreditar la efectividad de la operación financiera en virtud de la cual hacía cobros a la denunciante, pues tenía todos los medios a su alcance, no cumplió con tal carga. En consecuencia, sólo cabe concluir que la operación financiera cuestionada no fue realizada por la consumidora, a la que se trató de darle apariencia de legítima, sirviéndose de sus antecedentes personales, que estaban en poder de la denunciada”.

“CUARTO: (...) los artículos 3° letra d) y 23 de la ley 19.496.

El primero de los textos legales citados, dispone que es un derecho del consumidor, la seguridad en el consumo de bienes y servicios, norma que ha sido vulnerada pues en el presente caso, la falta del cuidado y resguardo de la denunciada, dio lugar a que usándose los datos personales de la denunciante se le atribuyera una deuda que no contrajo, provocándosele un menoscabo en los términos establecidos en la segunda de las disposiciones legales antes mencionadas.

Hizo presente que presenta estos fallos pues ilustran que jurisprudencialmente se ha establecido el principio que este proyecto viene a consagrar en la ley.

V. Acciones.

El SERNAC ha adoptado ciertas acciones en relación a este tema:

CONTEXTO – RECLAMOS RELACIONADOS CON LA CLONACIÓN DE TARJETAS DE CRÉDITO Y DÉBITO:		
<u>A junio de este año</u>	→	1.244
• Respondidos favorablemente	→	39,6%
• No fueron acogidos	→	60,2%
<u>En el año 2016</u>	→	3.144
• Respondidos favorablemente	→	44,40%
• No fueron acogidos	→	51,18%

En este punto, el Honorable Senador señor Moreira consultó cuáles fueron las razones por las que no fueron acogidos los reclamos.

El señor Romo señaló que las razones fueron variadas. El principal argumento es que se le imputa la carga de la prueba al consumidor.

Continuando con su exposición, manifestó que en lo que va del año 2017 se han interpuesto 17 denuncias en contra de entidades financieras y del mercado de retail por infringir la ley en materia de seguridad de productos, deber de profesionalidad y negligencia en la prestación de sus servicios.

Se iniciaron 13 mediaciones colectivas a nivel nacional referentes a cláusulas abusivas que buscan limitar anticipadamente la responsabilidad de estas empresas en caso que los consumidores sufrieran conductas fraudulentas realizadas por terceros, la mayoría de las mediaciones avanzan bien. Sin embargo ante la falta de disposición de llegar a acuerdo en la mediación colectiva por parte de Itaú Corpbanca, ésta se cerró negativamente y se presentó una demanda colectiva en junio de 2017.

Agregó que desde el año 2015 a la fecha suman 74 denuncias contra entidades financieras. Los proveedores con más denuncias son: Banco Estado con 23 (31%), Tarjeta Cencosud con 10 (13,5%) y Banco de Chile con 9 (12,1%). Precisó que estas cifras se relacionan también con la masividad de los citados proveedores.

VI. Comentarios al proyecto.

El señor Romo formuló algunas observaciones y comentarios al texto en estudio:

- La ley N° 20.009 no resuelve la totalidad de los problemas asociados a las operaciones financieras, principal razón por la que se ha recurrido a la Ley sobre Protección de los Derechos de los Consumidores.

- En ese sentido, este proyecto de ley es un avance, en cuanto especifica y explicita obligaciones que hoy día el SERNAC desprende de normas actualmente vigentes en la LPC.

- Al disponerse que “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”, se subsana el error de suponer que el tarjetahabiente siempre conoce del uso fraudulento de la tarjeta, o al menos de la amenaza de uso fraudulento.

- El tarjetahabiente o el usuario muchas veces sólo se notifica de las operaciones fraudulentas cuando recibe su estado de cuenta. Por lo que estas operaciones ocurren muchas veces a espaldas del consumidor y sólo se entera cuando ya ha transcurrido mucho tiempo.

- SERNAC siempre ha estimado que aun cuando el consumidor no haya dado aviso al emisor del robo, hurto o extravío de tarjeta de crédito (por desconocimiento, porque se trata de una tarjeta clonada, entre otros) es el emisor quien debe probar que estas transacciones fueron realizadas con autorización del cliente, punto del que el proyecto se hace cargo de manera explícita.

- En efecto, el proyecto reafirma que el emisor y no el consumidor tiene la carga de la prueba, y que los emisores no pueden supeditar la respuesta oportuna y adecuada a estas situaciones a la contratación de seguros o a la imposición de otras condiciones.

- Por otro lado, parece adecuado que se establezca un plazo (el proyecto propone 24 horas hábiles) para que los emisores efectúen las devoluciones de dinero que correspondan. En opinión del señor Romo, este es un aspecto muy relevante, sin perjuicio que se pueda discutir sobre la duración de ese plazo. Hoy en día el tratamiento que se da en los casos en que el consumidor cuenta con seguro y aquellos en que no ha contratado seguro es muy distinto, siendo que la responsabilidad es la misma, aquel consumidor con seguro recibe el reembolso de su dinero a los pocos días, es un incentivo perverso a contratar el seguro. Además muchas veces los emisores extienden el plazo para resolver esta materia, por tanto tiempo que prescribe la acción infraccional para el consumidor.

- Es un acierto que se establezca que el emisor procure contar con medidas de seguridad suficientes para impedir la comisión de ilícitos, cuestión que debiera consagrarse como un deber.

- Finalmente, y ante el pronto funcionamiento de las tarjetas de prepago, se modifica la referencia a tarjetas de crédito y débito, y se extiende también el alcance de la ley N° 20.009 a otros medios de pago, lo que también es positivo.

-- Sometida a votación la idea de legislar en la materia, el proyecto fue aprobado en general por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señor Tuma (Presidente), señora Pérez, y señores Pizarro y Quinteros. (Unanimidad, 4X0).

Aprobado en general el proyecto, y conforme lo permite el artículo 127 el Reglamento de la Corporación por tratarse de un proyecto de artículo único, la Comisión procedió al análisis particular del proyecto. Sin embargo, en una sesión posterior, el señor Presidente recabó el acuerdo de la Comisión para despachar el proyecto sólo en general, dado que la complejidad de la materia amerita que sea puesta en conocimiento del Senado para que, una vez se apruebe la idea de legislar, se abra un espacio de tiempo para que se presenten indicaciones que permitan mejorar la iniciativa.

Tal proposición fue aprobada por la unanimidad de los miembros presentes, Honorables Senadores señores Tuma (Presidente), señora Pérez y señores Moreira y Quinteros. (Unanimidad, 4X0).

Asimismo, en esta última oportunidad, la Comisión también acordó, con la misma votación, dejar constancia de las materias que fueron abordadas en forma específica y respecto de las cuales deberían presentarse indicaciones para corregir errores u omisiones, haciendo presente que otros aspectos del proyecto no fueron tratados por la Comisión por haber decidido, en definitiva, despecharlo sólo en general.

Las materias que fueron abordadas en forma específica y respecto de las cuales deberían presentarse indicaciones para corregir errores u omisiones, fueron las contenidas en el numeral 1 y el numeral 2, respecto de las letras a) y b) del artículo 1° de la ley N° 20.009, que el artículo único del proyecto propone reemplazar.

N° 1

El proyecto propone reemplazar 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".

El Presidente de la Comisión, **Honorable Senador señor Tuma**, propuso sustituir el título propuesto por el siguiente: "Establece

un régimen de limitación de responsabilidad para los usuarios de medios de pago”. Los miembros presentes de la Comisión estuvieron de acuerdo con la modificación propuesta, pues refleja mejor el objetivo y texto del proyecto.

N° 2

Este numeral propone reemplazar los artículos 1° y 2° de la ley N° 20.009.

La Comisión analizó los conceptos de usuario y de emisor, contenido en las letras a) y b) del artículo 2°, respectivamente.

El artículo 1° del proyecto consagra definiciones.

“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.”.

El **Honorable Senador señor Tuma** consideró que la definición de usuario debe quedar consagrada de la manera más amplia posible, en el entendido que siempre van apareciendo nuevas formas de pago y la idea es que el usuario de cualquier forma de pago que no sea el dinero efectivo quede protegido por esta ley. En el mismo sentido se pronunció la **Honorable Senadora señora Pérez**, en cuanto no debe restringirse el concepto de usuario sólo al tarjetahabiente. El **Honorable Senador señor Quinteros**, por su parte, recordó las aprensiones hechas valer por invitados a las sesiones anteriores, respecto a las definiciones que establece el proyecto, particularmente en cuanto a que serían términos ya definidos por la normativa del Banco Central. Finalmente, el **Honorable Senador señor Pizarro** consideró que debe ser una definición que englobe adecuadamente a todos los medios de pago distintos del dinero efectivo, y también el vale vista y el cheque, que tienen un régimen especial.

La Comisión estimó que texto de la letra a) debería quedar, en su oportunidad, de la siguiente manera:

“a) Usuario: 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.”.

Respecto del concepto emisor, contemplado en la letra b. El texto del proyecto es del siguiente tenor:

“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.”.

La Comisión recordó las intervenciones de los distintos invitados a las sesiones en que la Comisión ha tratado el proyecto, quienes pusieron de relieve la necesidad de distinguir la figura del emisor de la del adquirente. Esta definición de la letra b) las confunde.

El Honorable Senador señor Tuma consideró que las definiciones propuestas por VISA son un buen punto de referencia.

El asesor del Honorable Senador señor Ossandón, señor Huerta, expresó que desde el punto de vista del usuario no existen figuras distintas, sólo existe el banco con el que contrató, y para él debiera ser indiferente donde se comete el fraude. Pero, efectivamente, son diversos frentes de la cadena donde puede ocurrir el fraude.

La Comisión consideró que será necesario, en su momento, separar la definición contenida en la letra b) en dos distintas, de emisor y adquirente, cada una en una letra diferente, en los siguientes términos:

“b) Emisor: Institución que emite medios de pago y mantiene una relación financiera con el tarjetahabiente.”.

“c) Adquirente: Aquella institución que afilia a los comercios para la utilización de un medio de pago; o aquella que procesa operaciones realizadas con los medios de pago.”.

TEXTO DEL PROYECTO APROBADO EN GENERAL

Se inserta a continuación el texto del proyecto que la Comisión de Economía propone aprobar en general.

PROYECTO DE LEY:

“Artículo único. Modifícase 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, 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 1° y 2° por los siguientes:

“Artículo 1°.- Definiciones. Para los efectos de la presente ley, sin perjuicio de la normativa bancaria o financiera vigente; y de lo señalado en la ley N° 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 2°.- 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.

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.

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.

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 N° 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.”.

Acordado en sesiones celebradas los días 12 de julio, 2, 9 y 15 de agosto de 2017, con la asistencia de los Honorables Senadores señor Eugenio Tuma Zedán (Presidente), señora Lily Pérez San Martín y señores Iván Moreira Barros, Jorge Pizarro Soto y Rabindranath Quinteros Lara.

Sala de la Comisión, a 15 de agosto de 2017.

PEDRO FADIC RUIZ
Abogado Secretario de la Comisión

RESUMEN EJECUTIVO

INFORME DE LA COMISIÓN DE ECONOMÍA RECAÍDO EN EL PROYECTO DE LEY, EN PRIMER TRÁMITE CONSTITUCIONAL, 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.

BOLETÍN N° 11.078-03.

I. PRINCIPALES OBJETIVOS DEL PROYECTO PROPUESTO POR LA COMISIÓN: Modificar 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, fortaleciendo el régimen especial de responsabilidad del usuario y emisor de medios de pago, proponiendo entre otras, las siguientes medidas:

- Ampliar el régimen de limitación de responsabilidad que actualmente establece para el caso del uso fraudulento de tarjetas de crédito o débito, al uso fraudulento de nuevos medios de pago;
- Ampliar el catálogo de conductas que constituyen el delito de uso fraudulento de tarjetas de crédito, de pago con provisión de fondos o débito, y aumentar las penas;
- Establecer un régimen de exención de responsabilidad para el usuario frente a fraudes realizados sin que él pueda estar en conocimiento de tal hecho, como en el caso de clonación de una tarjeta;
- Fijar un plazo de 24 horas a los emisores para la devolución de los importes, si corresponde, en los casos de fraude, y establecer la prohibición de requerir el cumplimiento de condiciones para tales devoluciones, como la contratación de seguros u otras medidas burocráticas.
- Consagrar como responsabilidad del emisor de un medio de pago, el contar con medidas de seguridad suficientes para evitar la comisión de ilícitos, y ser responsable de los perjuicios que se produzcan por deficiencias en la protección de los sistemas tecnológicos del medio de pago.

II. ACUERDOS: Aprobado en general (4x0).

III. ESTRUCTURA DEL PROYECTO APROBADO POR LA COMISIÓN:

El proyecto consta de un artículo único, que en sus seis numerales, propone modificaciones a la citada ley N° 20.009.

IV. NORMAS DE QUÓRUM ESPECIAL: No hay.

V. URGENCIA: No tiene.

VI. ORIGEN INICIATIVA: Moción de los Honorables Senadores señores Ossandón, señora Pérez San Martín y señor Tuma.

VII. TRÁMITE CONSTITUCIONAL: Primer trámite.

VIII. INICIO TRAMITACIÓN EN EL SENADO: Con fecha 10 de enero de 2017 ingresó al Senado, pasando a la Comisión de Economía.

IX. TRÁMITE REGLAMENTARIO: Primer informe.

X. LEYES QUE SE MODIFICAN O QUE SE RELACIONAN CON LA MATERIA:

- Ley N° 20.009, que limita la responsabilidad de los usuarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, hurtadas o robadas.

- Ley N° 19.496, sobre protección de los derechos del consumidor.

- Ley N° 20.950, que autoriza emisión y operación de medios de pago con provisión de fondo por entidades no bancarias.

PEDRO FADIC RUIZ
Abogado Secretario de la Comisión

ÍNDICE

	PÁGINA N°
CONSIDERACIONES PRELIMINARES.....	1
ASISTENCIA.....	1
OBJETIVOS DEL PROYECTO.....	2
ANTECEDENTES.....	3
DISCUSIÓN EN GENERAL.....	11
<i>Invitados:</i>	
<i>Superintendencia de Bancos e Instituciones Financieras (SBIF).....</i>	<i>11</i>
<i>Asociación de Bancos e Instituciones Financieras (ABIF).....</i>	<i>14</i>
<i>Corporación Nacional de Consumidores y Usuarios (CONADECUS)</i>	<i>22</i>
<i>VISA International Ltda.</i>	<i>27</i>
<i>Abogado señor Renato Jijena, del Departamento del Centro de Estudios en Derecho Informático de la Facultad de Derecho, Universidad de Chile.....</i>	<i>36</i>
<i>Servicio Nacional del Consumidor (SERNAC).....</i>	<i>40</i>
APROBACIÓN EN GENERAL.....	48
TEXTO DEL PROYECTO.....	51
SESIONES.....	54
RESUMEN EJECUTIVO.....	55