INFORME DE LA COMISIÓN DE ECONOMÍA, FOMENTO, MICRO, PEQUEÑA Y MEDIANA EMPRESA, PROTECCIÓN DE LOS CONSUMIDORES Y TURISMO RECAÍDO EN EL PROYECTO DE LEY 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° 11078-03 (S).

HONORABLE CÁMARA:

La Comisión de Economía, Fomento, Micro, Pequeña y Mediana Empresa, Protección de los Consumidores y Turismo pasa a informar el proyecto de ley referido en el epígrafe, de origen en una moción del senador señor Manuel José Ossandón y de los ex senadores, señor Eugenio Tuma, y señora Lily Pérez, en segundo trámite constitucional y primero reglamentario, sin urgencia.

Durante el análisis de esta iniciativa legal la Comisión contó con la colaboración de las siguientes personas, señoras y señores:

El senador Manuel José Ossandón.

En representación del Ministerio de Economía, Fomento y Turismo, la jefa de asesores Michele Labbé; y las asesoras, señoras Cecilia Flores y Ximena Contreras.

El Director de la Unidad Especializada en Lavado de Dinero, Delitos Económicos Medioambientales y Crimen Organizado (ULDDECO) de la Fiscalía Nacional del Ministerio Público, Mauricio Fernández.

El Director Nacional del Servicio Nacional del Consumidor, Sernac, Lucas del Villar.

El Presidente de Banco Estado, Arturo Tagle y la Fiscal Isabel Margarita Cabello.

El Vicepresidente del Banco Central, señor Joaquín Vial, el Fiscal Juan Pablo Araya y la Gerente de la División de Política Financiera Solange Berstein.

El Superintendente de Bancos e Instituciones Financieras, SBIF, Mario Farren, el Jefe de Gabinete, Gabriel Acuña, y el Director Jurídico, Cristián Carmona,

El Vicepresidente Ejecutivo de Retail Financiero, Claudio Ortiz, y el colaborador Sergio Rodríguez.

En representación de la Policía de Investigaciones de Chile ,PDI, el Jefe de la Brigada Investigadora de Delitos Económicos, Bridec, Subprefecto Cristian Lobos y el Jefe de la Brigada Investigadora del Cibercrimen Metropolitana, Subprefecto Rodrigo Figueroa.

En representación de Transbank S. A., el Gerente General, Alejandro Herrera, y el Fiscal, Rodrigo Undurraga Ossa, el Presidente, Fernando Cañas, y el Gerente de Asuntos Corporativos, Raúl Muñoz.

La profesora de Derecho Civil de la Universidad de Talca, señora Erika Isler Soto.

El Presidente de la Corporación Nacional de Consumidores y Usuarios, CONADECUS, Hernán Calderón.

El Presidente de la Organización de Consumidores y Usuarios, ODECU, Stefan Larenas.

El Presidente de la Asociación de Bancos e Instituciones Financieras de Chile A. G., Segismundo Schulin-Zeuthen, y el Fiscal, Juan Esteban Laval.

I. CONSTANCIAS REGLAMENTARIAS PREVIAS.

1.- La idea matriz o fundamental del proyecto.

La idea central del proyecto tiene por propósito 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, para lo cual propone las siguientes medidas.

i.- 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.

ii.- 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.

iii.- 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;

iv.- 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.

v.- 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.

2.- **NORMAS DE CARÁCTER ORGÁNICO CONSTITUCIONAL Y DE QUÓRUM CALIFICADO.**

Cabe destacar que este proyecto de ley no contiene normas con el carácter de ley orgánica constitucional ni de quórum calificado.

3.- **NORMAS QUE REQUIEREN TRÁMITE DE HACIENDA.**

No hay disposiciones que requieran ese trámite.

4.- **APROBACIÓN DEL PROYECTO.**

El proyecto fue **aprobado, en general, por la unanimidad** de la diputada y de los diputados integrantes, señores Alejandro Bernales, Sofía Cid, Renato Garín, Amaro Labra (en reemplazo del diputado señor Boris Barrera) Joaquín Lavín, Miguel Mellado, Jaime Naranjo, Hugo Rey (en reemplazo del diputado señor Harry Jürgensen), Alexis Sepúlveda (Presidente), Enrique Van Rysselberghe, y Pedro Velásquez (11x0x0).

5.- **DIPUTADO INFORMANTE.**

Se designó como Diputado Informante al señor **JAIME NARANJO ORTIZ**.

II. ANTECEDENTES.

A) Fundamentos del proyecto.

Se expone, a título de fundamento, 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 sistema, agregan los autores, ha cumplido su objetivo y funcionado de forma adecuada desde la publicación de la ley, pero actualmente se pueden 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 patrocinantes de esta iniciativa 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 se 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.

Luego, la moción aborda dos categorías de fraude en esta materia: los 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 solo deberá

entregar los datos necesarios para operarla, como el número, nombre del titular, fecha de vencimiento y el código CVV (*Card Verification Value*). Se precisa 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.
- 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 que 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 o 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 patrocinantes 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 querella infraccional presentada contra el Banco de Chile por autorizar operaciones no realizadas por el tarjetahabiente, incluso luego de haber sido bloqueada la tarjeta de débito del actor. 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 querella infraccional contra el Banco de Chile (o Banco Edwards) por no tomar las medidas de seguridad necesarias para determinar si quien operó la tarjeta de débito del demandante fue realmente éste, en el escenario típico de un fraude por clonación de la banda magnética de la tarjeta. Los argumentos de la Corte señalan “[...] que en el presente caso se incurrió efectivamente en infracción a lo dispuesto en el artículo 23 de la ley N° 19.496, al no emplearse las medidas de seguridad y resguardo necesarios en el uso y manejo de la tarjeta de débito/crédito, que permitiesen comprobar que la persona que efectuó los giros de dinero realmente haya sido la legítimamente autorizada, en este caso, el actor.”. 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.

B) Legislación comparada.

Cabe consignar que el proyecto en estudio trata el derecho comparado en esta temática y constata que el régimen de responsabilidad del emisor y el tarjetahabiente tiene diferentes aproximaciones en la legislación comparada.

Así 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

C) Leyes que se modifican o que se relacionan con la materia;

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; la ley N° 19.496, sobre protección de los derechos del consumidor, y la ley N° 20.950, que autoriza emisión y operación de medios de pago con provisión de fondos por entidades no bancarias.

III. RESUMEN DEL CONTENIDO DEL PROYECTO APROBADO POR EL SENADO.

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

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

A continuación, agrega tres nuevos artículos que detallan el régimen de exención de responsabilidad del usuario frente a los fraudes realizados sin que éste pueda estar en conocimiento de tal hecho, como en los casos de 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, la moción 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.

IV. SÍNTESIS DE LA DISCUSIÓN GENERAL EN LA COMISIÓN Y ACUERDOS ADOPTADOS.

El **senador señor Manuel José Ossandón** hace mención al “lobby” que ha sido objeto en relación con la iniciativa en estudio, tanto del retail, como los bancos e instituciones financieras.

Relata los hechos que dieron origen al proyecto, fundado en una clonación de tarjeta bancaria que ocurrió a un ciudadano que tuvo que probar el robo y debió asumir los gastos necesarios para recuperar lo robado después de un tiempo prolongado. Considera que se produce una asimetría entre los derechos del cliente y la institución.

Plantea que con el proyecto se reemplaza la responsabilidad del cliente a la entidad bancaria que debe, además, asumir la prueba del hecho. En la actualidad las medidas de seguridad necesarias no se adoptan y el peso de la prueba recae en el cliente.

El **diputado señor Renato Garín** coincide con el señor senador, dejando ver los incentivos del sistema para que el cliente use de los avances en efectivo que al final endeudan exageradamente al cliente. Destaca la modificación de la responsabilidad penal a una de carácter objetiva y también, en cuanto se extiende a las compras electrónicas.

Hace hincapié, sin embargo, en la demora de Chile en incorporar las Normas de Basilea III al tratamiento de esta problemática, lo cual nos coloca en posición desventajosa en relación con otros países.

Manifiesta que estaría de acuerdo con la iniciativa, introduciéndole algunas modificaciones.

El señor **Joaquín Vial, Vicepresidente del Banco Central**, explica que el mandato que tiene el Banco Central es velar por el normal funcionamiento de los pagos internos y externos y en ese contexto, el banco emite normas sobre emisión y operación de tarjetas de pago, un elemento que calza en su mandato.

Relata que el fraude con tarjetas de crédito y medios electrónicos de pago es una preocupación de los reguladores a nivel internacional y del que se están haciendo cargo en Chile donde los niveles de fraude de esta naturaleza son relativamente bajos, comparados con otros países.

Opina que a nivel global es una situación que aumenta en el tiempo, pero que tiende a una cierta estabilización en los últimos años, lo que se ha logrado en parte al uso de tecnologías que permiten alertar al usuario de la tarjeta respecto de la ocurrencia de transacciones anómalas, lo que se hace mediante el envío de mensajes de texto, lo que ha permitido el control de volumen y número de operaciones de fraude.

Respecto de las acciones para poder controlar estos ilícitos, señala que en casi todas las jurisdicciones, el fraude después de que se ha dado aviso por el usuario, por pérdida o extravío, la responsabilidad recae en el emisor. Esta es una situación que la legislación contempla y no hay mayor problema.

Reconoce la existencia de un vacío legal entre el momento en que ocurre el evento hasta su aviso, pero la experiencia internacional es que se tiende a eximir de responsabilidad al dueño de la tarjeta, pero la regla general es que hay límites, lo que en los seguros se conoce como deducibles con lo que se busca desincentivar el fraude que podría hacer el propio dueño de la tarjeta respecto del emisor.

Explica que otro hecho que ha ido ocurriendo es que las propias marcas de tarjetas han asumido condiciones de eximir de responsabilidad al usuario de tarjeta, pero en forma voluntaria, sin perjuicio que, después de realizado los reembolsos se encuentran evidencias de fraude por el usuario de la tarjeta ejerzan las acciones legales correspondientes para efectuar la restitución.

Manifiesta que es necesario tener claridad respecto del estado de la situación al día de hoy, antes del proyecto de ley. Existe un vacío legal que es donde apunta el proyecto de ley y que tiene que ver con las transacciones realizadas antes de notificar al emisor de la tarjeta, observando que la actual legislación sólo se refiere a las tarjetas de crédito, no se aplica a los otros medios de pago, lo que es importante porque son tecnologías en constante cambio y evolución, por ello advierte que se debe ser cuidadoso con regular sólo las tarjetas de crédito y advierte que se debe buscar una figura lo suficientemente amplia para cubrir esas nuevas tecnologías de medios de pago.

Respecto del proyecto de ley, señala que tienen una buena impresión respecto de aquel y lo consideran necesario puesto que viene a llenar un vacío legal.

Algunos de los aspectos que se observan, es que debe haber consistencia de la definición con aquellas contenidas en la normativa del Banco Central, que se amplíe a pagos electrónicos en general, se debe reconocer el principio de que todos los actores involucrados en el sistema de pagos deben adoptar medidas de seguridad, es decir, el usuario, el comercio etc., también se debe incorporar la obligación del tarjetahabiente de informar al emisor las transacciones no reconocidas y fijar un fijar un plazo razonable para la restitución de fondos.

Precisa que este es un tema sensible. Hace un tiempo trascendió la filtración de información sensible de tarjetas de crédito de emisores locales y que podría haber afectado a usuarios de tarjetas de crédito.

Al respecto, señala que la información filtrada correspondía en su mayoría a tarjetas vencidas, y los emisores bloquearon las vigentes, dando aviso a sus clientes y las filtraciones tendrían su origen en comercios donde las tarjetas fueron utilizadas, y no en instituciones financieras.

A nivel internacional, ha habido eventos de filtración masiva de información, no solo de tarjetas, sino de bases de datos completas. Algunas, como *Heartland Payment Systems*, afectó a 134 millones de tarjetas en el año 2008, *Cathay Pacific* afectó a 9,4 millones de tarjetas en 2018, por mencionar algunos casos.

Señala que este proyecto incentiva que los emisores envíen alertas de fraude a los tarjetahabientes afectados, sin perjuicio que también exige que éstos informen al emisor

cuando tomen conocimiento de un fraude. Mientras mejores y más masificados estén los mecanismos de alerta de transacciones, las pérdidas por transacciones fraudulentas debieran ser más acotadas.

De haber existido cargos en las tarjetas, éstos tendrían que haber sido absorbidos por los emisores. Lo anterior no obsta al derecho de los emisores de tarjetas para perseguir la posible responsabilidad de los comercios desde los cuales se hubiera producido la filtración.

Acerca de posibles perfeccionamientos al proyecto de ley, indica que se podrían incorporar más medidas para mitigar el riesgo moral. La moción exige al titular o usuario dar cuenta al emisor de las transacciones no autorizadas de que tome conocimiento, pero sin precisar el efecto derivado del cumplimiento o incumplimiento de dicho deber.

Se debe establecer umbrales por sobre los cuales se haga efectiva la exención de responsabilidad, tal como existe en otros países.

El proyecto de ley impone obligaciones indistintamente a Emisores u Operadores (adquirentes), aun cuando sus relaciones contractuales, en la práctica, se estructuren de manera diferente.

Los emisores u operadores deberían enviar alertas de fraude, demostrar que una operación fue autorizada por el titular (art. 6°); cancelar cargos o restituir fondos de transacciones no autorizadas (art. 7°); y adoptar medidas de seguridad para prevenir comisión de ilícitos descritos en la ley.

Los consumidores tienen relaciones contractuales con los Emisores, por los que son éstos quienes deberían enviar alertas de fraude y cancelar cargos o restituir fondos de transacciones.

Se debería analizar la conveniencia de distinguir entre los roles y obligaciones asignadas, señalando explícitamente que éstas son sin perjuicio del derecho de los Emisores a perseguir las responsabilidades que correspondan, luego de la restitución de los fondos.

Las obligaciones del proyecto de ley son extensivas a las tarjetas “cerradas”, es decir de uso sólo en comercios relacionados con el emisor, si bien éstas no son fiscalizadas por la SBIF. Ello supone una dificultad para la fiscalización de este aspecto de la ley.

Es conveniente resguardar la coherencia entre los diversos artículos de este proyecto de ley, de manera que su ámbito de aplicación alcance efectivamente a todas las transacciones electrónicas y no solo a los pagos con tarjetas. Por ejemplo, dada la redacción de los artículos 6° y 7°, sería conveniente aclarar cómo se haría efectiva la exención de responsabilidad del titular y la restitución de fondos en una operación como una transferencia electrónica de fondos, en la que no hay emisores u operadores involucrados.

Asimismo, señala que es necesario asegurar la consistencia legislativa entre este proyecto de ley y el de Ciberdelincuencia.

En conclusión, la prevención del fraude es un esfuerzo permanente y requiere que todos los agentes involucrados en el sistema de pagos minoristas tengan incentivos correctos, por ejemplo, para usar e incorporar tecnologías (emisores y operadores), y para tener un comportamiento diligente (comercios y usuarios).

El Banco Central de Chile valora positivamente esta moción parlamentaria y los perfeccionamientos que se le introdujeron durante el primer trámite constitucional, Chile tiene niveles relativamente bajos de fraude en tarjetas. Advierte que es importante que esa situación se mantenga y que esta moción parlamentaria contribuya a ello.

En relación con los denominados umbrales de responsabilidad, explica que en el caso de la Unión Europea, los primeros 50 euros del fraude, corren por cuenta del dueño de la tarjeta, pero a partir de esa cifra en más, es responsabilidad del emisor de la tarjeta. En el Reino Unido esa cifra es de 35 libras esterlinas y en estados Unidos es de 50 dólares, cifra que aumenta si no se notifica al emisor, de manera que hay diferentes incentivos para el cuidado de las tarjetas.

Sobre el porcentaje de inversión de los bancos en ciberseguridad en Chile y el nivel de ella, señala que esa información debe tenerla la Superintendencia de Bancos como supervisores del sistema bancario, pero este proyecto de ley incentiva al emisor para que haga las inversiones necesarias en esta materia. Destaca que en cualquier caso lo importante es la política y el cuidado que tengan las instituciones en estas materias, según lo demuestra la experiencia del propio Banco Central, lo que se da por el propio cuidado y entrenamiento de la gente de la institución respectiva.

La Ley General de Bancos contiene elementos importantes para efectos de hacer exigencias de capital en caso que no haya un buen manejo del riesgo operacional, dentro de los cuales se contempla la ciberseguridad. Cuando la citada ley se encuentre totalmente implementada, porque hay una gradualidad para su vigencia, habrá aún mejores condiciones en esta materia respecto de lo que se estaba hace poco tiempo.

Precisa que no hay un parámetro que recomiende la OCDE, sino más bien tiene una estimación de los gastan de los distintos países en este tema.

El señor **Mario Farren, Superintendente de Bancos e Instituciones Financieras, SBIF**, expresa que no han participado en la discusión del proyecto de ley, sin perjuicio de haber entregado su opinión mediante un oficio de julio de 2017, cuando la moción se encontraba en el primer trámite constitucional.

Advierte que hay mucha coincidencia de conceptos con lo expresado por los representantes del Banco Central. El concepto fundamental en esta materia es la confianza del usuario respecto de los productos y servicios de acceso a su dinero y por ello es tema de preocupación de la SBIF.

Señala que esto tiene que ver con objetivos estratégicos como el acceso y riesgo operacional y la ciberseguridad y aplicación de la nueva ley de Bancos con los estándares de la Convención de Basilea III e integración del CMF.

Informa que el número de transacciones web es de 449 por cada cheque presentado a pago, el número de transacciones realizadas a través de cajeros automáticos y tarjetas de pago superan largamente las realizadas por medio de cheques, sin embargo sigue siendo importante en relación a los montos de pagos en efectivo.

A partir del año 2014 hay un aumento muy significativo de las operaciones de débito por canales digitales, lo que pone de relieve la importancia de discutir sobre el fraude y ciberseguridad atendida la masificación de estos medios.

Agrega que existen 11,4 millones de operaciones diarias, lo que comprende todo tipo de acciones como entrar a la página web para ver un saldo o realizar operaciones de transferencia a través de tarjetas, los pagos son 4,5 millones de operaciones, pero las operaciones totales son más de 11 millones al día.

Expone acerca del trabajo de la SBIF en materia de transición digital, apunta a diversos objetivos, tales como acceso y ciberseguridad, seguridad de medios de pago, disponibilidad de canales y el tratamiento de los fraudes por las instituciones fiscalizadas.

Respecto a lo que sucede cuando un usuario reclama a su emisor desconociendo un pago, hay un proceso que ocurre casi en simultáneo, desde que se efectúa el reclamo, éste ingresa y se procesa en el sistema con lo que se abre un expediente, mientras se bloquean los productos involucrados en el reclamo y se provisiona el monto. Luego se inicia

una investigación y el banco debe determinar si autoriza o no la devolución de los montos afectados, en un proceso que puede llegar a demorar meses.

Aduce que en algunos casos, con tarjetas de crédito el plazo de reposición o devolución del cargo en la tarjeta de crédito puede demorar hasta 120 días y en el caso de las tarjetas de débito puede demorar hasta 41 días, período de incertidumbre para el cliente, que involucra al emisor que puede ser un banco, comercio o emisores no bancarios.

El levantamiento hecho por la SBIF y con la aplicación de las nuevas leyes que contemplan nuevos elementos ya referidos anteriormente por la exposición del representante del Banco Central, muestra que el 53 por ciento de las instituciones realiza abonos provisorios en las tarjetas de débito, aun cuando la ley les reconoce plazos amplios para realizar esa acción. En el caso de las tarjetas de crédito, este abono provisorio alcanza el 92 por ciento. Aclara que en todo caso, estos datos corresponden a una encuesta hecha entre bancos.

Opina que la sola tramitación de este proyecto ha enviado una señal que ha sido adoptada por el mercado en dirección al estándar que se quiere regular, porque quien resuelve en un primer momento es el emisor de la tarjeta.

Ilustra a la Comisión señalando que la ley actualmente se hace cargo de una pequeña porción del problema, en un universo donde hay tarjetas de crédito y de débito, tarjetas de prepago, otros medios de pago como la transferencia electrónica o acciones que se realizan a través de teléfonos celulares. La ley se hace cargo de transacciones presenciales, transacciones post aviso, ciertos delitos que se encuentran regulados y la carga de la prueba es asumida en la actual ley por el usuario o tarjetahabiente, en circunstancias que todas estas se dan en el mercado, pero que la nueva ley asumiría todos estos elementos, todos los medios de pago, presenciales o no, antes y después del aviso y presenta un nuevo catálogo de delitos específicos, con lo que aparece que se legisla en el sentido correcto.

Se valora la ampliación del perímetro de aplicación de la ley a todos los medios de pago y a las transacciones electrónicas, se aborda la relativa indefensión del usuario para los casos de operaciones fraudulentas, presenciales y no presenciales. Es posible observar positivamente la inversión de la carga de la prueba para los casos previos al aviso de fraude, en consideración a que el usuario carece de elementos probatorios del mal uso, lo que sí pose la marca el emisor y la red de adquirencia.

Propone que en el proyecto de ley debiera habilitarse al emisor a subrogarse en las acciones del cliente para perseguir las responsabilidades correspondientes.

Hoy existe la tecnología para reducir los fraudes a su mínima expresión, sin que esto implique mayores costos para las personas. Hay un sistema en que el emisor asume toda la responsabilidad, desde su conocimiento y lo pagan inmediatamente. Aprecia que ese sistema genera incentivos perniciosos, no hay incentivos como lo sería el uso del deducible, para generar responsabilidades por parte del usuario de los medios de pago. Este caso es tan pernicioso como si se apuntara a la responsabilidad exclusiva del tarjetahabiente, se debe tener un cierto sentido de proporcionalidad que permita a los productos convivir con las tecnologías y su evolución y que evite la desbancarización.

Observa que históricamente el fraude en el sistema es bajo y es un objetivo deseable de política mantener esta situación. El proyecto avanza en esta materia, pero advierte que hay espacios de perfeccionamiento en desarrollar el mecanismo de restitución y cancelación para evitar el riesgo moral.

Explica que debe transcurrir un procedimiento judicial completo para determinar la existencia o no de un autofraude y proceder a dejar sin efecto la cancelación o restitución de fondos.

Sugiere precisar el alcance del artículo 8 para fortalecer la supervisión de las autoridades competentes referidas a las medidas de seguridad y determinación de responsabilidades contenidas en el mismo.

Luego, aclara que la OCDE no es prescriptiva en cuanto a porcentajes o gasto en ciberseguridad, pero la información que disponen muestra que los porcentajes oscilan entre un 7 y un 15 por ciento de los gastos de información y tecnología. Han hecho una encuesta que los fijaría en un rango medio del estándar OCDE, sin perjuicio que se destaca la forma en que se hace ese gasto, que implica acciones distintas como regular conductas, entrenamientos, asegurarse con los directorios se aseguran del cumplimiento de esas conductas seguras para evitar el contagio de las redes institucionales, lo que se llama la ciberhigiene.

Precisa que es necesario distinguir entre los productos bancarios. Explica que la tarjeta de débito asume que el tarjetahabiente dispone de los fondos contra los que se carga el monto y que es distinto de la situación de los créditos, independiente del caso de la tasa máxima convencional y los informes que se han hecho después de la entrada en vigencia de la tasa máxima convencional, muestran una correlación de que en el período hay más o menos 275.000 personas que habrían salido del mercado, pero no hay una relación de causalidad directa y única, es decir, se hizo el estudio que señala y exige la ley, pero además han ocurrido otras cosas en ese período que no permiten determinar una causa única a esa situación.

Agrega también que las tarjetas de débito generan bancarización en cuanto hay gente que tiene acceso a productos bancarios que les permiten manejar sus finanzas con independencia y eso es bueno, pero eso no significa necesariamente un producto de crédito, como sí lo es la tarjeta de crédito.

El señor **Cristián Carmona, Director Jurídico de la SBIF**, realiza algunas observaciones al proyecto de ley como propuestas para mejorar la normativa.

El artículo 1° establece el ámbito de aplicación de la iniciativa, el cual es más amplio que el comprendido en la nueva denominación de la ley al principio (art. único N° 1).

La iniciativa hace referencia a “emisores” y “operadores” de tarjetas de pago. Estos conceptos no solo comprenden entidades fiscalizadas SBIF y reguladas por el Banco Central de Chile de acuerdo al artículo 2, por lo que cabría precisar estos conceptos.

El artículo 1 extiende el ámbito de aplicación de la iniciativa tanto a “tarjetas de pago” como a “transacciones electrónicas”. Sin embargo, varias disposiciones circunscriben su alcance sólo a lo primero.

Señala que el artículo 4 hace referencia a un nuevo concepto denominado “servicios similares”; pide precisar la redacción del inciso primero del artículo 7 y verificar si corresponde incluir al “operador” dentro de esa obligación, adicional al “emisor” que es el proveedor del servicio financiero.

El señor **Claudio Ortiz, Vicepresidente Ejecutivo del Retail Financiero**, señala que en la industria de los medios de pago, como indicador, tienen cerca de 220.000.000 de transacciones al año. Representa a todos los emisores no bancarios y a la sociedad y apoyan al giro bancario emisor; hay operaciones de fusión que dan origen a un nuevo marco jurídico de manera que representan al emisor no bancario tradicional, como por ejemplo, Abcdin, Hites o Corona y algunas sociedades de apoyo al giro bancario CAT Cencosud con Scotiabank, CMR Falabella con el banco Falabella, Wallmart que se encuentra en fusión con el banco BCI para formar una sociedad de apoyo al giro bancario emisor.

Señala que este mayor desarrollo de los medios de pago hace necesario perfeccionar el marco legal, con lo que se muestran de acuerdo.

Destaca que los medios de pago electrónico descritos son de uso universal, geográficamente, a nivel doméstico e internacional, y también desde un punto de vista multisectorial, porque opera no solo en este estadio del mercado financiero sino también dentro de la economía, lo que es importante si se consideran las principales acciones de fraude y de ciberataque, estos han sido más del ámbito internacional que local, a la vez que es importante diferenciar los usos que se hacen de los medios de pago cuando se hacen transferencias dentro del mismo mundo financiero o de cuando se usa ese medio para hacer, por ejemplo una reserva de hotel, en que se entregan todos los datos de la tarjeta y lo que se denomina el túnel de seguridad que contempla el sistema para esas operaciones puede tener problemas que dejen expuesto el medio de pago.

Opina que el proyecto de ley amplía el alcance de la legislación al abordar todos los medios de pago y es un avance importante; se mejora y amplía la tipificación de los delitos; se perfecciona el régimen sancionatorio, aun cuando lo consideran insuficiente, establece reglas y procedimientos en materia de responsabilidad ante situaciones conscientes de extravío, hurto o robo que sufre el titular.

Destaca que es necesario mejorar el proyecto de ley, destacando la necesidad de clarificar las reglas y la responsabilidad ante transacciones que desconoce el titular sin existir la condición de extravío, hurto o robo; reglamentar las condiciones y acotar periodo de desconocimiento y restitución de las transacciones pasadas, de manera de evitar una innecesaria incertidumbre. En el régimen sancionatorio es importante fortalecer las sanciones tratándose de reincidencia, casos de asociación ilícita u organizaciones delictuales y es necesario abordar los perfeccionamientos que desincentiven el autofraude.

El señor **Sergio Rodríguez, secretario técnico de la comisión de ciberseguridad del Retail Financiero**, explica que existe un fraude doméstico que ocurre en Chile, lo que se denomina *Crossborder,* es lo que sucede fuera de Chile. La transacción en el extranjero puede ser o no presencial y es esta modalidad la que queda expuesta al fraude.

Desde el punto de vista de la seguridad, al usar una tarjeta, cualquiera sea el emisor, la mayoría de ellas incluyen un chip que no permite su clonación y que al ser usada a través de internet o el comercio en Chile, hay una serie de mecanismos de seguridad con factores de autentificación, lo que es una barrera contra los fraudes, pero esas condiciones, fuera de Chile no están presentes y los mecanismos de seguridad de *e-commerce* son muy bajos y por ello el 80 por ciento de los fraudes se da en esta circunstancia.

Fuera de Chile el fraude se da en el 57 por ciento de las transacciones con tarjeta no presente y un 30 por ciento corresponde a situaciones de tarjeta presente.

Sobre los montos de los fraudes, acumulado al año en Chile es relativamente pequeño en relación con las compras, es decir, Chile tiene el mejor índice fuera de Venezuela, porque el gobierno de Chávez obligó a todas las tarjetas a migrar al sistema de chip, que es algo que también se hace en nuestro país.

A modo de ejemplificar los volúmenes de inversión que implica señala que una tarjeta de banda magnética cuesta cerca de cien pesos, pero la tarjeta con chip tiene un valor cercano a los mil pesos. A ello se agrega el costo de entregarlo al cliente, que es de cerca de catorce dólares, todas estas inversiones se reflejan en los mejores indicadores de América Latina en esta materia.

Explica el funcionamiento del sistema, un cliente de tarjeta con chip finalmente transfiere la información a través de una llave o clave que se abre al final del proceso. Si este túnel de información se rompe, queda expuesta la información y es por donde se puede ingresar para cometer el fraude.

La ley N° 20.009 establece que el tarjetahabiente víctima de robo o extravío debe notificar al emisor de esa circunstancia y desde ese instante la responsabilidad corre por

cuenta del emisor, pero precisa que antes de ese aviso es responsabilidad del cliente tarjetahabiente.

Consideran positivo la ampliación de la ley a todos los “Medios de Pago”, que antes era solo para Tarjetas de Crédito, esto es “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.”.

También es positiva la definición de los principales “conceptos” que se utilizan: Usuario, Emisor, Comercio, Medios de pago.

Con el aviso del extravío, hurto o robo, se define claramente que la responsabilidad se traspasa al emisor para las transacciones futuras, y le da la posibilidad al usuario de reclamar las transacciones pasadas.

Aparece entendible que se amplía el capítulo sancionatorio del fraude.

Es razonable que el proyecto de ley aborde la responsabilidad por las transacciones no presenciales. Sin embargo, consideran fundamental que exista un equilibrio entre la responsabilidad del emisor y la debida diligencia del usuario para evitar riesgos sistémicos.

Explica que ahora se agrega el evento del fraude, que es notificado por el cliente, y el emisor notificado tiene tres días para pagar y el problema es que se concede un período ilimitado para que el cliente pueda impugnar transacciones y ello puede resultar en un incentivo al autofraude, porque el proyecto de ley no plantea que esta situación tenga un límite y así podría desconocer todas las transacciones de los últimos tres años desde que notifica al emisor.

El proyecto de ley debiera para el caso de las transacciones desconocidas por el cliente, con ocasión de aviso de fraude, establecer un plazo máximo de reclamo de 72 horas hábiles si la notificación de la transacción por parte del emisor vía electrónica, y 15 días hábiles para notificación física la del estado de cuenta que suele hacerse impresa en papel y se envía por correspondencia. De esta manera se pueden reclamar o desconocer transacciones incluidas hasta el estado de cuenta anterior al aviso, es decir, un plazo de 30 días hacia atrás.

Proponen tipificar en el artículo 5 el uso malicioso de los medios de pagos por parte del usuario para obtener un provecho ilícito y ese será un incentivo para evitar el autofrude.

Sugieren, finalmente aumentar las penalidades y multas considerando que los delitos en su gran mayoría son cometidos por bandas organizadas, no por personas aisladas u ocasionales.

El señor **Hernán Calderón, Presidente de Conadecus**, manifiesta la importancia de esta discusión porque es muy controvertido en los casos de pérdida, clonación o uso indebido que al usuario le hace perder dinero desde sus tarjetas, sin que después exista una responsabilidad por esos hechos. Agrega que muchas veces, a pesar que se comunica esta situación por el consumidor, hay una tramitación larga para que el consumidor pueda probar que no fue él quien usó la tarjeta de esa manera.

Señala que los emisores tratan de descartar su responsabilidad y traspasarla al consumidor. Este es un proyecto de ley que viene a regular parte de estas controversias, donde los consumidores son afectados permanentemente.

Apunta que hoy no solo existen las tarjetas de crédito, sino también de débito, cuenta rut y un sin número de instrumentos y nuevos medios de pago. Esto significa que los consumidores quedan expuestos cuando los emisores no toman las medidas de resguardo o seguridad para proteger sus bases de datos e instrumentos.

Cuenta que las circunstancias han llevado a crear una comisión de expertos y un encargado en ciberseguridad para enfrentar la acción de ciberdelincuentes que pueden afectar a los consumidores.

Manifiesta que les parece correcto establecer un régimen de limitación para la responsabilidad en caso de fraude para emisores y medios de pago. Aclara que este último concepto incluye otros medios, no solamente las tarjetas de crédito, sino también las de débitos y otras que se usan en el sistema financiero o en la red de cajeros automáticos.

Expresa que le parece adecuado y necesario limitar la responsabilidad del usuario de estos medios de pago, sin perjuicio que el pago por medio electrónicos permite realizar las mismas operaciones con el uso de un teléfono celular, medio que puede ser más riesgoso que el uso de un computador porque es susceptible de clonación, pero como no es una tarjeta, podría considerarse al margen del ámbito de esta ley, lo que amenaza la obsolescencia de la ley antes de su publicación.

Estima que es importante considerar la responsabilidad del emisor y distinguir en relación con el cliente, que se entiende por emisor, por cuanto los bancos y casas comerciales delegan en Redbanc la emisión, en circunstancias que se contrata con una institución determinada, y es ella la que debe responder a través de sus ejecutivos, pero ello debe precisarse, de lo contrario se deja al usuario en la obligación de descubrir quién es el responsable penal de la falta de seguridad contratada.

Algo que se debiera incluir en el proyecto, es que nada se dice respecto de los seguros de fraude que todas las instituciones comerciales que usan estos medios de pago obligan al cliente a contratar, como una forma de eludir su responsabilidad. Al respecto, señala que este proyecto de ley hace que sean innecesarios esos seguros, algo que Conadecus siempre ha dicho respecto del seguro de fraude, que no es necesario porque los emisores son responsables.

Propone que en esta iniciativa parlamentaria se establezca expresamente que no se podrá exigir al usuario que contrate un seguro por fraude para cubrir la responsabilidad que corresponde al emisor y que se contemplen sanciones para que esta ley se cumpla y evitar que se busquen nuevos mecanismos para contratar seguros contra fraudes.

Expresa que se ha hecho un lobby fuerte con esta ley por parte de algunos actores del mercado financiero para poder incorporar la existencia de un deducible lo que debe resultar inaceptable para un usuario que sufre la pérdida, robo o clonación de su tarjeta o en forma virtual.

Aclara que la responsabilidad del emisor es total y no puede ser que el usuario se haga responsable por la falta de medidas de seguridad del emisor del medio de pago.

Observa que es misión del banco dar protección y seguridad a los servicios contratados por un deber de custodia de los recursos, dinero que el cliente le ha entregado y no hay razón para contratar un seguro, por parte el cliente, para que se cubra la falta de seguridad que debe suministrar la institución bancaria.

El deber del cliente es informar el delito o falla o extravío de la tarjeta o clonación, tampoco puede ser objeto de un deducible, porque hay una responsabilidad del emisor. El castigo del usuario irresponsable que no avisa oportunamente es que no se le va a responder, tal como sucede hoy, de manera que no necesita un deducible, tiene que el banco ser capaz de asumir sus medidas de seguridad y si no lo hace debe tener un castigo y responder.

Pregunta cuál es la utilidad del seguro de fraude, cuando hay una responsabilidad que debe ser evidente, si existe el deber de custodia de la entidad sobre los bienes que yo le encargué en un contrato.

Señala que el fraude ocurre en un día preciso, por lo que debe verse como opera la responsabilidad dando el aviso oportuno de ello.

El señor **Stefan Larenas, Presidente de la Organización de Consumidores y Usuarios, ODECU**, recuerda que la ley N° 20.009, a la fecha se ha convertido en una norma que no es suficiente.

Observa que estas situaciones se encuadran en las figuras del robo, robo informático y una situación donde existen muchos medios de pago y la aparición de nuevas formas de pago, lo que produce que haya un sinnúmero de tarjetas en el mercado, donde se hace imposible no hablar de los seguros.

Explica que la protección que el consumidor tiene hoy es el seguro, pero el Sernac ha recibido 1.243 reclamos, cerrados solo 39 por ciento de manera favorable y un 60,2 por ciento no fueron acogidos. Relata que el Servicio mantiene abierta una serie de acciones judiciales con entidades bancarias por cláusulas que limitan su responsabilidad ante fraudes.

Comenta que el Sernac suele realizar alguna acción colectiva, como el caso en la Araucanía, donde los bancos restituyen sumas de dineros tras la mediación del Sernac en un caso de fraude masivo.

En los casos individuales son muy pocos en que el consumidor logra vencer en juicio, porque el principio que asienta el tribunal es que "*de acuerdo al principio de buena fe y de las obligaciones que emanan de la naturaleza del contrato, a tomar todas las providencias que fueren necesarias, para evitar que terceros extraños hicieran uso o se aprovecharan de los fondos custodiados por el banco*….". Al hablar de las providencias necesarias, se refiere al deber de diligencia.

Por su parte, la Corte Suprema acogió un recurso de protección de un cliente de un banco y ordenó a la entidad financiera devolver los fondos que fueron sustraídos de su cuenta corriente por fraude informático. "Asentado lo anterior, no queda más que calificar el actuar de la recurrida como ilegal y arbitrario, puesto que al no asumir el perjuicio económico trasladando los efectos del fraude bancario al actor, afecta directamente el patrimonio de éste, vulnerando así el artículo 19 N° 24 de la Constitución Política".

Estas sentencias son un avance, pero en realidad es el caso de un consumidor que tiene recursos para llegar a la Corte Suprema.

Por otra parte, los contratos de cuenta corriente estipulan clausulas como la siguiente: "*14.- CLAVE SECRETA PARA USO DE CUENTA CORRIENTE:*

La clave secreta es personal e intransferible, al suscribir las Condiciones Particulares o Contrato de Cuenta Corriente el Cliente se obliga a mantener la debida diligencia, sigilo y cuidado en su utilización, siendo de su responsabilidad su divulgación a terceros y asumiendo la responsabilidad por los perjuicios que el mal uso o la utilización errónea de ésta pueda ocasionarle al mismo Cliente, al Banco y/o a terceros, salvo cuando el Cliente hubiere informado personal y previamente al Banco el hecho de la pérdida o sustracción de su clave secreta. El Cliente, en conocimiento de la normativa sobre secreto bancario y de las responsabilidades civiles y penales que pueden derivarse de toda operación bancaria relacionada con la(s) Cuenta(s) Corriente(s), acepta que toda operación efectuada por alguno de estos medios, se presumirá hecha por el propio Cliente.".

Las ofertas de seguro se efectúan pensando en que el cliente no se verá envuelto en ningún problema y quedará cubierto por el seguro en caso necesario. Un ejemplo que expone es el siguiente:

En caso de un asalto en cajero automático, se recibirá protección hasta 2 horas después de realizada la transacción, ya sea que lo obliguen a girar dinero con la tarjeta o le roben el dinero.

Tendrá hasta 48 horas desde ocurrido el siniestro, para denunciar al seguro el robo, hurto, pérdida y/o extravío de la tarjeta.

En caso de falsificación o adulteración de la tarjeta o banda Magnética, la Compañía indemnizará el monto de la pérdida hasta el monto de UF 127.

Quedarán cubiertas las pérdidas ocurridas desde la primera transferencia no reversable y que ocurran dentro del plazo de 120 días antes del momento en que se efectúe el bloqueo de las claves y hasta la hora del bloqueo. El valor del Seguro UF 0,0401

El problema que presenta esta lógica es la relativa indefensión en la que queda el tarjetahabiente -o el usuario de otros medios de pago- cuando la operación fraudulenta ocurre bajo la total ignorancia del titular, frecuentemente como resultado de la clonación del instrumento u otros métodos similares.

El tarjetahabiente, o el usuario, solo se notifican de tales operaciones cuando recibe los cargos en el balance de la tarjeta o de su cuenta.

El seguro no es obligatorio, pero ello no significa que no haya demoras o dilaciones en el ejercicio de la cobertura del seguro, pero el artículo 6 del proyecto de ley, se debe[1] calificar como clave del mismo, porque viene a salvar la situación descrita.

Califica la moción como un avance en la protección del consumidor y el mismo proyecto insiste en el deber de adoptar las medidas de seguridad necesarias para prevenir la ocurrencia de ilícitos descritos.

En todo caso, el proyecto de ley enfrenta un determinado problema del consumidor, puesto que le da mejores plazos para que el consumidor pueda exigir su derecho, exigir la restitución de lo que se le ha robado y obliga a tomar las medidas de seguridad necesarias y pertinentes, es un avance correcto y considera que abordar los seguros es ineludible en este proyecto, porque si bien no hay obligación de contratarlos, la forma de su oferta asó lo hace aparecer.

El señor **Segismundo Schulin-Zeuthen**, **Presidente de la Asociación de Bancos e Instituciones Financieras de Chile A. G.**, reflexiona en primer lugar que el país debe definir qué va a hacer con el efectivo y que los proyectos de ley deben discutirse a la luz de esa definición y dar impulsos a la bancarización.

Opina que este es un proyecto de ley que traba la bancarización porque cualquier medio de pago para ser exitoso, debe distribuir bien los riesgos, que es lo que ha permitido la operación del cheque, pero acá están mal distribuidos los riesgos.

[1] "Artículo 6º.- En los casos a que se refiere el artículo anterior, el titular o usuario no será responsable por las operaciones realizadas con posterioridad al aviso de fraude dado al emisor por las mismas vías establecidas para estos efectos en la presente ley, ni por aquellas operaciones que desconozca haber autorizado efectuadas con anterioridad al aviso de fraude que el titular o usuario reclame dentro de los treinta días corridos siguientes a la expedición de dicho aviso o que haya tenido conocimiento de ellas. Para estos efectos, y en relación con el conocimiento de la existencia de operaciones no autorizadas, se considerará especialmente la circunstancia que el emisor u operador haya enviado una alerta de fraude y que exista constancia de su recepción por parte del titular o usuario.
En los casos en que el titular o usuario desconozca haber autorizado una operación, corresponderá al emisor u operador demostrar que la operación fue autorizada por el titular o usuario y registrada con exactitud.

El registro de la utilización de las tarjetas de pago no bastará, necesariamente, para demostrar que la operación fue autorizada por el titular o usuario, ni que éste actuó de manera fraudulenta o con negligencia inexcusable. En todo caso, cuando el titular o usuario tome conocimiento de alguna de las conductas del artículo anterior deberá dar cuenta al emisor en los términos señalados en el inciso primero.
En ningún caso se aplicará la exención de responsabilidad señalada, si se prueba que el titular o usuario tuvo participación en los delitos descritos en el artículo 5°, que obtuvo un provecho ilícito o que actuó con dolo o negligencia inexcusable facilitando su comisión.
El titular o usuario soportará el total de las pérdidas que afronte como consecuencia de operaciones que sean fruto de su actuación fraudulenta.". boletín N° 11.078-03.

Señala que en el caso de los medios de pago bancarios, el uso de tarjetas y transferencias van en un rápido aumento, si a ello se agrega todos los medios de pago no bancarios que emergen de manera importante y que no están regulados, las cifras serían muchos mayores, porque hay un problema con los medios de pago no regulados, porque este proyecto se debe entender referido a los medios de pago más que a las tarjetas de crédito.

Las cifras de fraude en Chile comparadas con otros países, siguen siendo bajas. Por cada millón de pesos, se defrauda en 460 pesos, lo que a nivel mundial estaría en el orden de los mil pesos, 1.400 pesos en Latinoamérica, 1.600 pesos en EEUU.

Advierte que hay un problema en las transferencias, porque es ahí donde están aumentando fuertemente los fraudes y el 84 por ciento se concentra en las primeras transferencias. Observa que aquí aparece otro problema, el de las bandas criminales que mediante engaños obligan a las personas a pagar sumas de dinero mediante transferencias, que siendo instantáneas, es casi imposible restituir el dinero.

Respecto de clientes que han tenido problemas con productos financieros, se focalizan, básicamente, en tarjetas de crédito, no afecta a cuentas corrientes y en las transferencias, es un número muy bajo.

Explica el sistema de operación, porque señala que es allí donde se encuentran las responsabilidades.

El modelo de cuatro partes, que es el que funciona en el mundo y que el Banco Central ha sancionado, pero que en Chile opera el modelo de tres partes aunque ello cambiará pronto.

En primer lugar se encuentra el emisor, que puede ser o no un banco y que es al que se le atribuye finalmente la responsabilidad en el proyecto de ley. A continuación está el adquirente, Transbank, que en realidad es más que un adquirente. En tercer lugar el tarjetahabiente y en cuarto lugar, el comercio.

Precisa que cada uno tiene responsabilidades en el proceso, lo que no obsta para decir que el cliente debe entenderse con cada responsable, porque el cliente siempre se entenderá con el emisor.

Pregunta quién es responsable el emisor si el tarjetahabiente usa un computador de un *cyber* café, por ejemplo donde la información queda muy expuesta, si el sistema de transacciones de un comercio es *hackeado.*

Recuerda el caso de la filtración de 25 mil tarjetas a una empresa pública, donde se robó a un proveedor la información de tarjetahabientes, había indicios de dónde se produjo el problema, pero hubo que denunciar al Ministerio Público y se perdieron dos meses hasta que se reconoció que les habían robado la información y poder bloquear la tarjeta de los clientes. El problema es que esos datos se almacenan y no se usan de inmediato.

Informa que hay comercios que deciden no emplear sistemas de seguridad, porque hay un proceso relativamente lento de validación y pierden muchas transacciones en ese proceso, como *webpay* o líneas aéreas*.*

Si se autoriza una compra con una tarjeta de crédito que se encuentra bloqueada, autorizada por el procesador, ¿es responsable el emisor en este caso? Posiblemente sí, porque hay un contrato con ese procesador

Si el cliente da aviso de bloqueo de la tarjeta y el emisor procesa igualmente una transacción de esa tarjeta de crédito, el emisor es claramente responsable de esa transacción.

Sobre el proyecto de ley, observa que el marco legal debe ser aplicable a emisores bancarios y no bancarios, porque estos últimos no están regulados.

El proyecto de ley, respecto de operaciones anteriores y de las posteriores al aviso, no se establece un plazo para el rechazo de las operaciones, lo que deja la incertidumbre respecto del plazo anterior.

Señala que se deben devolver o reintegrar los cargos dentro de tres días hábiles, lo que plantea el problema de la resolución definitiva en ese breve plazo, por parte de un tribunal.

La investigación requiere de un tiempo prudente, no pueden ser 3 días hábiles. Expresa que las marcas para efecto de las contra cargas internacionales, toman ente 75 y 120 días.

En cuanto a las posibilidades de información del cliente, acota que se ha referido siempre a la notificación del estado de cuenta. Sin embargo, señala que hoy, casi todos los bancos informan vía mail o SMS las transacciones que se hacen por vía de tarjetas de crédito o transferencias, se pueden revisar los estados de cuenta y además, se puede considerar cuando llega el estado de cuenta. Por ello considera que rechazar operaciones sin un plazo hacia atrás es un exceso, porque ha tenido todas esas alternativas para tomar conocimiento de sus transacciones.

En la práctica, el proyecto radica la responsabilidad únicamente en el emisor, lo cual dista radicalmente de los estándares internacionales. Esto genera consecuencias, cuya magnitud si bien no es cuantificable, pero que claramente limitará sustancialmente el desarrollo de la industria, estableciendo además claras oportunidades de arbitraje regulatorio; incrementa el riesgo moral, ya que facilita el auto-fraude, especialmente en transacciones no presenciales. En el caso de las TEF, esto se agrava aún más por el requisito de instantaneidad; se 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; 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.

Precisa que a partir de la idea de riesgo se pueden entender varias situaciones consultadas.

Recuerda que este es un negocio en que intervienen cuatro partes, donde cada uno tiene sus responsabilidades y así, por ejemplo son claros los casos en que el emisor es responsable, pero también el tarjetahabiente es responsable.

Cita a modo de ejemplo el caso de la ley de cheques, que dice que el documento se debe pagar, salvo que la firma sea notoriamente disconforme, pero donde además hay la obligación de dar cuenta del extravío del documento o su robo, lo que ha permitido su funcionamiento por muchos años.

Revela que hay un problema de riesgo moral que se debe evitar. Reponer los fondos en los 3 días siguientes, desde el punto de vista del emisor, si la marca de la tarjeta que debe hacer los contracargos, se demora 150 días y al cabo de ese plazo se demuestra que la transacción se hizo efectivamente, significa que hubo crédito gratis por 150 días.

Si se pone toda la responsabilidad en el emisor, sistemáticamente el comercio dejará de usar los sistemas que minimizan riesgos, como *webpay*. Si en definitiva el responsable es el emisor, se pregunta para qué adoptar los cuidados necesarios respecto de las bases de datos o aceptar tarjetas y sin poner mayores cuidados.

En cuanto a la posible desbancarización, señala que ello afectaría principalmente al Bancoestado con su cuenta Rut, donde se puede abrir la cuenta y tener

tarjeta, a partir del rut, sin más antecedentes. Puntualiza que si es que se quiere poner toda la responsabilidad en el emisor, la banca privada no tendrá alicientes para bancarizar.

Respecto de la inversión en seguridad indica que el problema no es cuanto se invierte, sino cuan eficiente es en la inversión. Indica que hay un serio problema adicional en el país, que es que no hay cultura de seguridad. Señala que en los dos casos en que se ha robado a los dueños del banco, aclara que no a sus clientes, las fallas estuvieron en acciones del personal que no tiene cultura de ciberseguridad, donde en un caso una ejecutiva cotizaba sus viajes de vacaciones desde su estación de trabajo y a partir de allí se infectó a todo el banco. Esto se aplica también a nivel de clientes y hay una campaña comunicacional para educar al cliente en el uso de medios de pago. A ello agrega que se debe educar a los clientes.

Señala que hay muchos medios de pagos nuevos, producto del avance tecnológico, las llamadas *fintech (financial technologies),* pero el gran problema hoy son las *bit tech como Applepay o googlepay o Alipay,* esta última de origen chino que ha crecido absolutamente sin regulación. Opina que el proyecto de ley debe regular estos medios también, pero ello pasa por que la Comisión de Mercados Financieros, que ha declarado que los regulará, lo efectúe porque de lo contrario la ley será inútil y habrá migración hacia medios no regulados.

El señor **Mauricio Fernández, Director de la Unidad Especializada en Lavado de Dinero, Delitos Económicos Medioambientales y Crimen Organizado (ULDDECO) de la Fiscalía Nacional**, destaca en primer lugar cómo desde la perspectiva penal y procesal penal vinculada a tarjetas de crédito y débito y a los delitos informáticos en general que ha sido el parlamento quien ha impulsado leyes en esta materia, la ley de delitos informáticos, N°19.223 y la ley N° 20.009.

Estas son leyes que han tenido una aplicación importante y son herramientas que se usan para conseguir sanciones respecto del uso fraudulento de tarjetas de crédito y débito, de manera que constituye una legislación penal bien aplicada.

Precisa que solo se referirá a un artículo de la ley propuesta que es el artículo con incidencia panal o procesal penal.

En relación con el artículo 5° del proyecto de ley, opina que ella es una iniciativa valiosa que amplía el objeto material del uso fraudulento de tarjetas en general, con lo que se reconoce explícitamente los avances en medios de pago.

Es relevante la incorporación de un nuevo literal g) en el artículo 5° que establece el uso fraudulento de tarjetas de pago, que extiende la posibilidad de sanción incluso a otros ámbitos, más allá del plástico, de la tarjeta misma.

El proyecto, en el inciso segundo de la letra g) establece la posibilidad de sancionar criminalmente con las mismas penas del uso fraudulento de tarjetas de pago, al que mediante cualquier engaño o simulación, obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de depósitos a la vista, de provisión de fondos, tarjetas de pago o cualquier otro sistema similar, última frase que propone mejorar en cuanto señale o se refiera a cualquier otro medio de pago, de manera de poder reconocer la punibilidad de otros medios de pago que pudieran tener en la evolución de estos, de manera que el proyecto de ley se hace cargo no solo de las tarjetas, sino de los pagos que se hacen por vías no físicas.

Señala que este proyecto es una oportunidad para que se aborde un tema que se ve recurrentemente en la práctica investigativa y de enjuiciamiento que es la detección, sólo en Chile, del sujeto que presta su cuenta para la recepción del monto defraudado, a quien no se le puede imputar la comisión del delito de fraude.

Sugiere que se debe estudiar la posibilidad de establecer un delito de receptación, sancionar a quien presta conociendo o no pudiendo menos que conocer que esto proviene de un ilícito cometido por un tercero, generalmente desde el extranjero. Aclara que

esto establecerá un desincentivo para cooperar con estas acciones a cambio de un porcentaje o comisión, que por los tiempos de la colaboración internacional, hacen muy difícil poder perseguir al delincuente que actúa desde el extranjero.

Comenta que debieran incorporarse los delitos de la ley N° 20.009 en el artículo 27 de la ley N°19.913, que crea la unidad de análisis financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos, porque se debe dar una señal en términos que la obtención de recursos importantes que se entienden por vía de la defraudación de tarjetas de crédito y débito o en general de cualquier medio de pago, en la medida que se actúa ocultando ese origen ilícito, debiera ser incorporado, como lo han sido otras figuras, como delito base de lavado de dinero, porque ello abre las posibilidades de cooperación.

Explica que en el caso de lo ocurrido en el Banco de Chile, lo que investiga Hong Kong y la denuncia que se hace, es por lavado de dinero asociado a defraudaciones, estas ya están incorporadas en la ley de lavado de dinero como delito base de lavado de dinero, pero que debieran considerarse los delitos de la ley N° 20.009 como delitos base, lo que potenciaría la persecución penal, especialmente cuando hay recursos importantes comprometidos.

Señala que hay un aumento de la penalidad, lo que le parece prudente y proporcional, la ley N° 20.009 parte en 61 días y se queda ahí o baja, porque la práctica es quedarse en el grado inferior. El proyecto innova aumentando en ese sentido con la pena de presidio menor en su grado medio, 541 días, lo que parece como proporcional y adecuado.

Ante la consulta de cuándo actúa y a requerimiento de quién actúa la Unidad de Lavado de Activos, responde que ellos no son la Unidad de Análisis Financiero, que depende del Ministerio de Hacienda, que se relacionado con privados y que tienen obligación de reportarle operaciones calificadas como sospechosas y algunos de esos reportes, cuando se confirman, pasan a ser de conocimiento del Ministerio Público.

Acota que no es el único ámbito de investigación de oficio que tiene la Fiscalía y puede iniciar sus propias investigaciones, sin perjuicio de lo cual resalta que estando incorporando el mundo de las infracciones a las tarjetas ya los medios de pago como delito base de lavado implica que se le hacen exigible todos los mecanismos del sistema de prevención, detección y sanción del lavado que implica mucho más refuerzo en la prevención y en la sanción de los delitos asociados a las tarjetas y medios de pago. Ello refuerza el cumplimiento de la ley y la respuesta del Estado a una forma de delito que es muy rápido, que tienen conexiones internacionales, con la banca o de operadores extranjeros que trabajan desde otros países, sin perjuicio de considerar las criptomonedas como mecanismos de pago en el extranjero.

El **señor Arturo Tagle, presidente del Consejo de Banco Estado**, expone que Banco Estado tiene 10,8 millones de cuenta rut, de las cuales 8 millones efectúan transacciones todos los meses y si se observan en 6 meses, son más de 9 millones de tarjetas activas en cuenta rut.

Informa que además tienen cerca de 600.000 tarjetas de crédito, que en materia de transacciones de estas tarjetas no es una gran participación la del Banco, pero que en tarjetas de débito más del 60 por ciento de las transacciones que se hacen por Redcompra, cuenta rut, son de Banco Estado.

Los datos que entregan demuestran que es de la máxima relevancia para el Banco esta discusión.

Plantea que el proceso de bancarización que ha ido realizando Banco Estado ha tenido un gran valor para el desarrollo de la economía en Chile y también para facilitar la vida a las empresas y a las personas del país. Además de los ahorros de costos y facilitar las transacciones, se hace más seguro del efectivo y de los salarios que reciben las personas, pero también esa bancarización permite dejar huella de las transacciones que se efectúan y hacer

un *track* en distintas materias como delitos, áreas tributarias que permiten decir que avanzar en la bancarización es de un gran valor para Chile y poder avanzar como lo hacen los países desarrollados.

Advierte que países más avanzados miran hacia la eliminación del efectivo como un aporte a bajar los costos de transacción y hacerlas más seguras y aunque falta mucho para ello, Banco Estado cree que es ese el camino a seguir, tener menos transacciones en efectivo y más transacciones con dinero plástico o por transacción electrónica, lo que marcará la relevancia de una legislación que regule esos medios de pago.

Explica que la bancarización tiene mecanismos variados y complejos que no implica mantener el *status quo* sino que, por el contrario la tecnología ha avanzado tanto que se hace necesario revisar permanentemente la regulación, siendo adecuados algunos pasos que se han dado como la regulación del Banco Central de la tarjeta de pre pago o en el caso de dispositivos móviles, que eliminan la tarjeta, pero que tienen sus propios riesgos.

En materia de fraude y seguridad se necesita que la regulación se vaya adaptando porque el fraude innova permanentemente nuevas formas de hacer caer nuevas víctimas y la tecnología va cambiando, por lo que estima conveniente que se entregue a una autoridad, como la Superintendencia de Bancos por ejemplo o el Banco Central, las atribuciones suficientes para tener las medidas que se deben exigir a los bancos en seguridad.

Opina que poner todo el peso de la responsabilidad en un solo lado en las transacciones de medios de pago, como lo hace este proyecto, es peligroso. Ejemplifica con el caso del cheque, que de a poco va quedando obsoleto en su uso, pero que fue un medio de pago muy exitoso por cerca de 50 años y ello porque parte de la responsabilidad se pone en el Banco, con el cuidado de dinero y la emisión de los talonarios, que los cheques sean seguros y cuidar los fondos depositados, pero pone el cuidado del talonario y de la firma e manos del titular de la cuenta corriente, de manera que el Banco responde cuando la firma es notoriamente disconforme. Señala que este es un ejemplo de administración equilibrada del riesgo y quien lo administra.

Apunta a que el proyecto carga mucho la mano en el banco en cuanto debe responder ante la insinuación o información del cliente que desconoce una transacción.

Añade que Banco Estado recibe una cifra mensual de reclamos cercana a los 2.300 sobre los 10 millones de tarjetas de débito y crédito que maneja el Banco. De esos reclamos el Banco restituye el dinero en cerca del 40 por ciento de los casos, sea porque existen seguros o porque el Banco considera que algunos de los dispositivos o medios provistos por el banco, tienen alguna debilidad, como si por ejemplo se demuestra que la clonación de la tarjeta se ha producido en uno de los cajeros del banco o en alguno de los que tiene interconexión o cuando se prueba que el medio en el que se hizo la clonación es en el mecanismo de pago y ello porque es el banco quien dispone de los dispositivos técnicos y es ahí donde el banco responde tenga o no seguros.

En el otro 55 por ciento de los casos, un tercio del total, el caso termina en una aclaración cuando el banco señala al cliente que el comercio a que se refiere la información es, por ejemplo, la estación de servicio tal, de tal lugar, porque a veces el nombre legal del establecimiento comercial no corresponde con el nombre de fantasía del mismo.

En el 27 por ciento de los casos que restan, es el cliente el que pierde el reclamo porque no hay un patrón de fraude o se han usado todas las claves y dispositivos que el Banco entrega al cliente y este no los ha cuidado debidamente.

Manifiesta el temor que el proyecto, en los términos en que se encuentra redactado, signifique aumentar los montos al sistema y que ellos terminen traspasados al consumidor y sean una dificultad para la apertura de la cuenta que es más flexible y fácil de abrir que es la cuenta Rut y que implique que muchas de las víctimas de estos fraudes se

encuentren en el Banco Estado y defraudar a un banco con esta ley será mucho más fácil y ello generará más requisitos para abrir la cuenta en el banco.

Relata que el Banco Estado procesa al mes trescientos millones de transacciones, sólo Caja Vecina procesa 34 millones de transacciones al mes; 8 millones de cuentas usaron servicios Banco Estado al mes. Ante estos números, la cantidad de fraudes son un porcentaje mínimo, pero se debe mantener la vista respecto del cliente individual que resulta afectado.

En cuanto a las inversiones en seguridad tecnológica, el Banco está invirtiendo del orden de 8.500 millones de pesos en seguridad tecnológica, pero ello es muy amplio, siendo este año lo más importante las protecciones anti *hackeo* que ataca solo un aspecto de la seguridad. Otra protección adicional es la protección de los cajeros automáticos, donde se ha sufrido mucha clonación.

Dentro de las medidas de actualización, el banco pronto empezará a notificar vía mensaje de texto las operaciones que se realicen en las cuentas, lo que es una medida que ayudará a evitar los fraudes.

Respecto del número de tarjetas clonadas, señala que no son pocas, aunque siendo millones de tarjetas podría decirse que es porcentualmente menor, considerando que son 12 millones de tarjetas en el mercado que tiene banco Estado de las cuales se presentan 2300 reclamos al mes, una fracción de los cuales son clonaciones las que han bajado mucho en número, pero han derivado hacia otras formas de engaño para obtener las claves de internet, además el banco está cambiando sus tarjetas actuales a tarjetas que incorporan *chip* y que es un compromiso asumido con la SBIF y que se espera en tres años completar el reemplazo en las tarjetas de cuenta rut.

Advierte que en los casos de venta internacional no hay claves en las tarjetas, el *pin pass* es un invento chileno que se está empezando a usar en otras partes, pero tampoco se usa en empresas nacionales que se han convertido en regionales como Latam.

Respecto de la necesidad del seguro, explica que se debe entender que la clave es la firma y que la SBIF exige desde hace cuatro años una segunda firma, a ello se agrega las exigencias que hace cada banco a las primeras transferencias e incluso software para identificar sitios falsos. Si a un cliente le imitan la firma responde el seguro, en algunos casos de imitación de las firmas o de robo de cheques sueltos, respondía el seguro.

Tampoco están de acuerdo que en los casos de los clientes que han sido engañados para entregar sus claves no se aplica el seguro, porque para eso fue contratado. Si el cliente no tuviera seguro, el banco no responde, esa es la forma en que lo ha entendido la banca y el 10 por ciento de las cuentas rut tienen seguros.

Los plazos son largos para dar respuestas, pero no desconoce espacios para mejoras. Banco Estado ha mejorado sus procedimientos para procesar los reclamos, pero el mayor plazo está dado por los fraudes internacionales, porque las marcas tienen sus propios plazos y procedimientos, son 90 días para dar respuesta al reclamo en estos casos y eso alarga muchos los plazos a clientes que necesitan su dinero.

Comenta que le han asignado un valor al seguro y que si este se masifica debiera ser más barato por economías de escala y que será más atractivo para las compañías de seguros.

En la revisión de procedimientos se ha identificado que hay cierta información que se puede no pedir, por ejemplo, las cartolas cuando ellas ya estaban en poder del banco. Sin perjuicio que algunos dispositivos son de Transbank, no es el cliente quien los contrata, es el banco que contrata con Transbank y ante una falla del aparato que provee esa marca, el banco asume que es su responsabilidad y es el banco el que paga.

Explica que se sabe cuándo hay clonación y donde porque no se clona solo una tarjeta, se clonan muchas. La información, a través de un mecanismo desarrollado, se junta en la asociación de bancos y ello le permite efectuar la identificación de las clonaciones que se hacen en dispositivo POS de Transbank y el banco lo asume. Si el patrón no existe, o son casos extraños, se entiende que es responsabilidad del cliente.

La señora **Isabel Margarita Cabello, Fiscal del Banco Estado**, señala que desde el punto de vista del banco, se considera que desde que el cliente da aviso el banco tiene responsabilidad por todas las operaciones que se efectúen con posterioridad a ese aviso, porque la obligación del banco es bloquear esa tarjeta o las transferencias que se hayan hecho.

Manifiesta que les preocupa el traspasar el peso de la prueba a los bancos cuando el cliente se refiere a operaciones anteriores al aviso, porque ello sería entregar la responsabilidad al banco y se dejaría al cliente con una responsabilidad que debiera responder por culpa grave o gravísima, es decir, debería actuar de manera dolosa o negligente, de manera inexcusable para hacerse responsable de una situación que no necesariamente es de responsabilidad del banco.

Cuando se habla del hurto, robo o extravío de la tarjeta, hoy se dice que el banco es responsable desde el momento en que se le da el aviso y para todas las operaciones posteriores, lo que es claro y lógico. Señala que les preocupa cuando se hace responsable al banco también de todas aquellas operaciones que el cliente desconozca después del aviso y hasta cinco días después, porque basta que el cliente dé aviso para que cualquier situación ocurrida el cliente la pueda desconocer y el banco no tiene un plazo razonable para saber qué es lo que ocurre, si se trata de una clonación, de fraude o un phising, etc., es el análisis que se hace después que un cliente da el aviso.

Preocupa también la situación de los fraudes, en que se dice que una vez que se da el aviso de fraude hay un plazo de 30 días para desconocer las operaciones anteriores a la fecha del aviso, situación que deja al banco en indefensión ante el cliente, que puede desconocer todas las operaciones anteriores al aviso por no tener claridad de cuando las hizo, por ejemplo.

Hay que dar más equivalencia entre las partes y las responsabilidades. Es importante que el consumidor en este caso tenga responsabilidad como buen padre de familia y se pueda establecer requisitos para los clientes que cumplan con ciertas obligaciones.

En los sitios privados se ofrece a los clientes ciertas medidas de seguridad, como el uso de softwares que los protege de eventos de *phishing* o *pharming* que son las maneras comunes de defraudación a través de imitación de las páginas del banco o hacen creer que uno se encuentra en el banco.

Estas son medidas que buscan que el cliente pueda cuidar sus productos bancarios y eliminar estas exigencias en vez de beneficiar la bancarización y el desarrollo de la banca, harán que el cliente actué con excesiva ligereza y decida desconocer las operaciones porque no tiene ningún riesgo en ello.

Apunta que se busca seguir avanzando en la bancarización y desarrollo de lo que es la banca para toda la población, sin hacer irresponsables a los clientes por el uso de los productos, se trata que además el cliente debe ser cuidadoso en el uso de sus claves, productos que debe evitar caigan en manos de terceros.

Precisa que se conoce la existencia de gente que se dedica a los fraudes y los engaños, pero la preocupación del banco está en educar a su gente, en ofrecer herramientas de protección, pero eliminar absolutamente la responsabilidad del cliente cuentacorrentista o del tarjetahabiente es un perjuicio a la bancarización que se busca. Señala que no es posible que el cliente en esta caso sea irresponsable, que pueda solo hacer el denuncio y si es cierto o no, ello no se cuestiona y el banco estará obligado a reembolsar en el

plazo de 3 días y que para que el banco pueda excusarse debe acreditar una negligencia inexcusable o doble, es decir, hay un peso de la prueba que recae sobre las instituciones bancarias que no tiene contrapeso en lo que se exige al cliente para el cuidado de sus productos.

Estima que sin perjuicio de establecer una responsabilidad clara al momento del aviso por robo, hurto o extravío o fraude, que la banca se haga responsable por las operaciones posteriores, no es posible que cualquier acto anterior pueda quedar cubierto sin necesidad que se pruebe, a lo menos, que existe algún patrón o fraude, de lo contrario quedan entregados al uso irresponsable e indebido de estas facultades de reclamar y poder obtener un pago.

Solicita que se considere la revisión de los plazos que se establece y se consagren requisitos que signifiquen una mayor responsabilidad para el dueño de los productos bancarios, porque no solamente con el aviso se puedan desconocer las operaciones anteriores, que puede significar incurrir en un perjuicio a la bancarización y a la enseñanza en el uso de los productos bancarios.

Explica que se hizo un análisis del tiempo promedio que se requiere de estudio y es de entre 7 y días 10 días, según la información que se encuentre disponible. Recalca que el banco es consciente que los medios que se ponen a disposición de los clientes es responsabilidad del banco que sean seguros y estima que ello no está en discusión. Precisa que cuando es claro que hubo una clonación, ello se reembolsa con o sin seguro, pero lo complejo es entrara a hablar de formas más complejas de fraude, como el denominado “cuento del tío” donde el fraude consiste en conseguir las claves mediante engaños Hay una responsabilidad de educar a la gente en cuanto a no entregar sus claves.

Las situaciones requieren un análisis y sostiene que entre 7 y 10 días es un plazo razonable para analizar, por ejemplo si existe un patrón de fraude, sin perjuicio que a veces se encuentran patrones que resultan desconocidos, pero que resultan ser nuevas formas de defraudar.

El señor **Lucas del Villar Director Nacional del Servicio Nacional del Consumidor, Sernac**, expresa que durante el año 2018, el SERNAC ha recibido 5.454 reclamos en materia de fraude considerando banca y retail. De estos, se han recibido 3.084 reclamos en contra de entidades bancarias relacionadas con clonación-suplantación, de los cuales, 2077 casos (67por ciento) corresponden a suplantación. En otras palabras, los casos ingresados por clonación en banca llegan a un 33 por ciento.

Aclara que el Sernac recibe cerca de 340.000 reclamos al año. Los reclamos por definición son una insatisfacción al consumidor financiero en este caso, por la cual la empresa no da una respuesta directa en la mayoría de los casos, pero el Sernac recibe el reclamo aunque las personas no hayan concurrido directamente a la institución.

Del total de reclamos 2018 relacionados con suplantación, un 66% no fueron acogidos y un 25 por ciento sí se acogen. El resto está en tramitación, fue derivado, no procede, no existían antecedentes suficientes para tramitar, o no fueron respondidos.

Durante el mismo año 2018, el SERNAC recibió 2.370 reclamos en contra tarjetas de crédito relacionadas al retail, por clonación-suplantación, de los cuales, 1623 casos (68,5 por ciento) corresponden a suplantación, siendo CMR Falabella la entidad más reclamada, con un 28.2 por ciento de casos este año.

El año 2017, el SERNAC recibió 3.127 reclamos en contra de entidades bancarias relacionadas con clonación-suplantación. Del total de reclamos en 2017, 1290 casos (41 por ciento) fueron por suplantación y 1.837 (59 por ciento) corresponden a clonación. En cuanto a las tarjetas de crédito relacionadas al Retail, se recibieron 2.462 reclamos, de éstos, 1.285 casos (52 por ciento) fueron por suplantación y por lo tanto 1.177 reclamos fueron por clonación.

Entre el año 2016 y octubre del 2018, el SERNAC ha interpuesto más de 320 denuncias de interés general (JIG), en contra de entidades financieras, por fraudes (clonación, suplantación, no reconocimiento de deuda, entre otros) relacionados a distintos productos financieros, tanto en el retail como en la banca.

Del total de denuncias, Banco Estado concentró el 26 por ciento de ellas, seguido por CAR (Ripley) con una participación de un 14 por ciento.

En el mes de septiembre de 2018, SERNAC presentó una demanda colectiva, en contra de Banco Itaú-Corpbanca, el propósito de esta acción es que la entidad bancaria responda a un grupo de consumidores que señalan haber sido defraudados con hasta 12 millones de pesos en algunos casos.

A través de 100 reclamos, los consumidores indicaron al SERNAC que habían sido víctimas de transacciones fraudulentas, mediante la aprobación automática de créditos, avances en tarjeta de crédito, utilización de dineros depositados y líneas de crédito, entre otros, por montos que posteriormente eran transferidos a cuentas de desconocidos. Operaciones, que los consumidores aseguran no haber efectuado y de las que se enteraron cuando revisaban sus estados de cuentas, y solo en casos aislados, se efectuaron avisos, a sus teléfonos móviles o correos electrónicos.

Este servicio, en la demanda iniciada, cuestiona el uso de mandatos amplios e indeterminados en los contratos, que habrían permitido que se extendieran a otros productos de forma automática y sin resguardos, dejando espacio para que se realizaran transferencias u otorgamientos de créditos no autorizados.

Por otra parte, tampoco actuaron los mecanismos internos para controlar acciones fraudulentas, como cotejar el historial del cliente; avisar de una transferencia o actividad inusual, o comprobar que el titular era quien estaba tomando créditos por altos montos, o realizando otro tipo de transacciones.

En este caso, se busca resguardar el derecho de los consumidores a servicios financieros seguros, y, el deber de profesionalidad de los proveedores de productos y servicios financieros, relativos a tomar todos los resguardos necesarios para cuidar, el patrimonio confiado por los consumidores.

A través de esta demanda, SERNAC ha solicitado se declare: la nulidad de las transacciones, el cese de las gestiones de cobranza y se otorguen las restituciones e indemnizaciones, derivadas todas y cada una, de las operaciones electrónicas no reconocidas, de los cargos y de los cobros que se han realizado, a los consumidores afectados.

Respecto del proyecto de ley señala que se amplía el ámbito de aplicación de la ley N° 20.009, la actual ley resulta aplicable a operaciones realizadas con tarjetas de crédito; el proyecto incorpora el concepto de “medio de pago”, como objeto genérico, en el que puedan identificarse no sólo las tarjetas de crédito, 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. Así también, incluye a las tarjetas de pago con provisión de fondos, y tarjetas de débito.

Se propone una ampliación del tipo penal y el aumento en las penas relacionadas a delitos de uso fraudulento de tarjetas de pago.

Se introducen modificaciones al actual régimen de exención de responsabilidad del usuario frente a los fraudes, abarcando todos aquellos supuestos en que el usuario o tarjetahabiente no ha tomado conocimiento del fraude, como lo son los supuestos de clonación de tarjetas o sustracción de credenciales para operaciones de pago electrónicas. A través, de la introducción de una nueva conducta tipificada como delito de uso fraudulento de tarjeta de pago (artículo 5, letra g).

Respecto al régimen de exención, de responsabilidad, es necesario que el consumidor, al momento de dar aviso del fraude bancario o a más tardar dentro de los 5 días hábiles siguientes al aviso, en caso de robo, hurto o extravío desconozca las operaciones que no fueron realizadas por él, plazo que, en el caso de fraude, es de 30 días corridos, siguientes a la expedición del aviso o que haya tenido conocimiento de estas transacciones.

Además, establece una alteración al régimen de carga de la prueba, ya que, respecto de las operaciones desconocidas realizadas con anterioridad al aviso de extravío, robo o hurto, es el proveedor quien tiene que probar que no fueron realizadas por el consumidor.

Establece un plazo de tres días hábiles para la devolución de los importes, en casos de fraude e impone al proveedor la obligación de contar con medidas adecuadas de protección para el medio de pago, y lo hace responsable de todos los perjuicios causados por las deficiencias en sus mecanismos o sistemas de seguridad.

Observa en relación al desconocimiento de operaciones producto del extravío, hurto o robo de tarjetas de pago o servicios similares, el artículo 4° inciso 2° dispone: "*Tratándose de las operaciones anteriores a dicho aviso, el titular o usuario deberá reclamar al emisor aquellas que desconoce su autorización, en el mismo acto del aviso o hasta cinco días hábiles siguientes a su expedición"*.

Resulta necesario aclarar, la naturaleza del plazo establecido en el texto del proyecto, señalando expresamente, si producirá la caducidad, inoponibilidad o la prescripción, de la posibilidad de desconocer operaciones y que estas sean inmediatamente canceladas o bien se proceda a la restitución inmediata de los fondos, en plazo de 3 días establecido en el artículo 7° inciso primero del proyecto en comento.

Se recomienda indicar la procedencia de la caducidad del mismo, en relación únicamente a la restitución legal dispuesta. Lo anterior, sin perjuicio de los plazos para interponer las acciones de la ley N° 19.496. Así también, y en concordancia, con lo dispuesto en el artículo 6° inciso 1°, del proyecto, se propone que el plazo de 5 días hábiles, establecido en el artículo 4° inciso 2°, sea computado "desde que el titular o usuario haya tenido conocimiento de las transacciones que desconoce". Lo anterior en virtud de los derechos que asisten al consumidor, como el artículo 17A de la Ley de Protección de los Derechos de los Consumidores, que dispone: "*Los proveedores de bienes y servicios cuyas condiciones estén expresadas en contratos de adhesión deberán informar en términos simples el cobro de bienes y servicios ya prestados, entendiendo por ello que la presentación de esta información debe permitir al consumidor verificar si el cobro efectuado se ajusta a las condiciones y a los precios, cargos, costos, tarifas y comisiones descritos en el contrato. Además, toda promoción de dichos bienes y servicios indicará siempre el costo total de la misma*.".

Así también, aquellos derechos incorporados por la ley N° 20.555, que incorpora, a través del artículo 17D a la ley N° 19.496, la posibilidad de solicitar información a proveedores de servicios financieros, la cual debe ser otorgada en 3 días hábiles, y se refuerza en el reglamento N° 44-2012 ,"Sobre información al consumidor de tarjetas de crédito bancarias y no bancarias" del Ministerio de Economía Fomento y Turismo, que en su artículo 25 inciso 2° señala: "*En el plazo de tres días hábiles desde la fecha de la solicitud presencial o desde la recepción en caso que se haya efectuado por otro medio de comunicación, el Emisor deberá entregar la información requerida con el contenido y la presentación indicada en el artículo 22, actualizada hasta la fecha de emisión de documento que contiene la información requerida."*. Finalmente cabe hacer presente que el referido artículo 22, contiene el detalle pormenorizado de información, que debe ser otorgada al consumidor, incluyendo cupo total, compras en cuotas y avances en efectivos realizados, con el producto tarjeta de crédito.

Se propone incorporar en el artículo 8°, una referencia que indique la posibilidad de ejercer acciones por parte de los titulares o usuarios, en los plazos contemplados por la Ley Sobre Protección a los Derechos de los Consumidores N°19.496. Así también al

respecto, es relevante tener a la vista los nuevos plazos y mecanismos de prueba que se incorporan en materia de consumo, con la entrada en vigencia de la Ley 21.081, que fortalece al Servicio Nacional del Consumidor, aumentando los plazos de prescripción de las acciones derivadas de aquellas conductas infraccionales, y permiten la utilización de un modelo de carga dinámica de la prueba, que permitirá sostener procesos judiciales más equitativos en esta materia, en donde la mayor cantidad de antecedentes probatorios, constan en poder de los proveedores que interactúan en toda la cadena de uso y disposición de fondos, a través de diversos medios de pago.

La señora **Michele Labbé, jefa de asesores del ministerio de Economía**, señala que el ejecutivo piensa que este proyecto apunta en el sentido correcto, hay un vacío legal importante en términos a la forma en que se están tratando los fraudes de tarjetas de crédito y medios de pago en general y no solo las tarjetas de crédito, de manera que es necesario cubrir una serie muy amplia de situaciones, 8 tipos de fraudes respecto de los cuales sólo se ha tipificado uno.

Manifiesta que es necesario buscar un balance entre la protección de los tarjetahabientes y que no haya un riesgo moral de considerar que no hay alicientes para que tenga el debido cuidado.

Acota que las presentaciones han hecho importantes aportes como la SBIF que hace un punto respecto que el proyecto de ley menciona solo la situación de dos actores, el emisor y el tarjetahabiente sin considerar al tercero que es intermedio y al que no se menciona. Por ello es necesario, por ejemplo que se consideren todas las partes que menciona el Banco Central.

Estima necesario distinguir las situaciones de robo y hurto de aquellas situaciones fraudulentas porque corresponden a delitos distintos y además se debe tipificar la situación del proveedor de los medios para realizar los fraudes.

Para evitar el riesgo moral es necesario distinguir las fechas de aviso respecto de las fechas de transacciones anteriores, los períodos objetados, el proyecto de ley no pone límite en el tiempo a los plazos hacia atrás para reclamar. El tarjetahabiente tiene la obligación de chequear su cuenta cuando le llega, de modo que podría pensarse que un plazo razonable es el de un mes atrás contado desde la fecha de facturación respectiva, pero debe considerarse los casos en que la información no llega o no está disponible para el cliente o no le es posible acceder a ella.

Así también debe considerarse los 3 días que establece el proyecto como plazo, pero una forma de acercarse el tema es pensar en una restitución provisoria de fondos, con lo que se puede dar un plazo suficiente para analizar la situación del supuesto fraude.

Expone que es necesario considerar en la redacción del proyecto, que no sea cerrado en la descripción de los delitos, de manera que pueda ser posible incluir nuevas formas de defraudación o que se aplique a nuevos medios de pago que puedan aparecer.

La señora **Erika Isler**, **profesora de Derecho Civil de la Universidad de Talca**, indica que estas son materias reguladas por la ley N° 20.009 que se considera un progreso en la protección del consumidor, aunque estima que se necesitan algunas modificaciones y esa es una materia en que el proyecto de ley avanza.

En cuanto a su ámbito de aplicación, esto es a qué tipo de actos jurídicos se aplica la ley actual y el proyecto de ley, el régimen de la ley N° 20.009, se avoca a los aspectos principales, que son restringidos- En primer lugar se habla solamente de tarjetas y en particular de tarjetas de crédito; en segundo lugar, en cuanto a las operaciones ilícitas se refiere al hurto, robo o al extravío.

Precisa que en los antecedentes del proyecto de ley se abordan correctamente los supuestos fácticos a los que se aplica esta legislación especial, es decir, no

sólo a las tarjetas de crédito, sino también a las de débito y otros medios de pago, lo que parece correcto porque los actos ilícitos por los que se involucran cargos no consentidos son más amplios que su relación con las tarjetas de crédito y, en la medida que se puedan establecer supuestos más amplios implicará que la ley no deberá estarse reformando cada que aparezca un nuevo tipo de acto ilícito.

Señala que lo mismo ocurre respecto de los supuestos ilícitos que actualmente se refieren solo al robo, hurto o extravío y que el proyecto de ley amplía a otros ilícitos que no estarían cubiertos por esta ley, aunque sí estarían cubiertos por la ley del consumidor, como por ejemplo los casos de clonaciones.

Es sabido que los delincuentes recurren constantemente a nuevas técnicas para sustraer dineros de ciertas cuentas, por ello vale también aquello de mantener una norma amplia para no tener que reformarla continuamente.

Hace presente que por estar dentro del ámbito de la responsabilidad civil no se exige el estricto principio de tipicidad que es propio de la norma penal.

Advierte que es necesario ajustar las normas, porque el artículo 1, al establecer el ámbito de aplicación lo amplía a cualquier medio de pago y a cualquier operación ilícita, pero los artículos 2 y 3 aluden solamente al robo, hurto o extravío y no considera la situación de supuestos más amplios que se plantea en el artículo anterior.

En cuanto a la responsabilidad propiamente tal, tanto la legislación actual como el proyecto de ley distinguen entre las operaciones realizadas con anterioridad a un aviso y las que se realizan después de este.

El consumidor, cliente o tarjetahabiente una vez que advierte los cargos no consentidos o el hurto, robo o extravío de la tarjeta da aviso a la entidad financiera y partir de ese momento se bloquean las operaciones futuras. Hace presente que en cuanto a la exigencia del aviso no hay cambio, de manera que se mantiene el régimen anterior y el posterior al aviso.

Una vez que el consumidor da aviso se puede limitar su responsabilidad, lo que significa que es de cargo del emisor acreditar el consentimiento del cargo y que fue realizado por el consumidor- En estos términos, se establece una presunción simplemente legal, es decir, una presunción que el cargo no fu consentido, pero el proveedor puede acreditar que ello no fue así.

El proyecto de ley establece la responsabilidad directa del proveedor después del aviso, pero llama la atención y propone clarificar la idea de que el artículo 2 vuelve a indicar que el consumidor puede limitar su responsabilidad, cuando parece ser correcto técnicamente establecer directamente la responsabilidad del proveedor porque si se dice que el consumidor puede limitar su responsabilidad, se podría interpretar erróneamente que se requiera de algún tipo de clausula para que el consumidor limite su responsabilidad. Agrega que también deben ajustarse los supuestos normativos, más allá del robo, hurto o pérdida.

Respecto de la diligencia que se debe exigir al consumidor, se puede homologar la idea del aviso a que el cargo que se produce por negligencia inexcusable puede ser atribuido al consumidor.

En cuanto a las situaciones de cargos anteriores al aviso, el régimen actual nada señala, hay un silencio del legislador y aquí hay dos posiciones. Una que defiende al proveedor que no quiere hacerse cargo de los cobros no consentidos y que señala que el cargo de antes del aviso es de costo del consumidor. La otra tesis, que aparece como correcta y ha sido asumida mayoritariamente por los tribunales, entiende que los cargos anteriores al aviso no son automáticamente de cargo del consumidor, sino que el emisor debe acreditar en este caso la falta de diligencia. Si por ejemplo se está ante una firma claramente disconforme, es una falta de diligencia del proveedor, si no se solicita la cédula de identidad en algunos

supuestos o la tarjeta está a nombre de un varón y es presentada por una mujer, son casos de manifiesta falta de diligencia del proveedor.

En cuanto a la legitimidad pasiva, a quien se puede demandar, la ley actual habla del emisor, aunque el proyecto de ley habla del emisor y lo amplía al operador lo que se encuentra de acuerdo con la ley de protección de los consumidores que atribuye responsabilidad también al intermediario.

Acerca de la legitimidad activa, la ley actual habla del tarjetahabiente, pero el proyecto de ley habla del tarjetahabiente o usuario, que es concordante con una moderna concepción del consumidor, en que no se requiere que la persona haya celebrado un contrato de consumo para ser considerado consumidor.

En el ámbito de las clausulas de modificación convencional de responsabilidad, hay que entender que existen clausulas de limitación, que disminuyen la responsabilidad y otras de exoneración si se expresa que el proveedor no va a responder.

La ley actual se refiere solo a los casos posteriores al aviso, al igual que el proyecto de ley, ambos señalan que si existe una clausula que invierte la carga de la prueba en perjuicio del consumidor, por ejemplo, se establece que el cliente debe acreditar la negligencia del proveedor, en esos casos esa cláusula se tendrá por no escrita, lo que nos alude a la inexistencia.

Señala su opinión en cuanto parece aconsejable clarificar el tipo de ineficacia a que se refiere la expresión “se tendrá por no escrita”. Si es una inexistencia, opera de pleno derecho y no prescribe, pero aconseja aclara el sentido de aquello para efectos de una interpretación uniforme.

Nada se dice antes del aviso y pregunta qué pasaría en los casos de contratos de adhesión como de tarjeta de crédito o débito. Todos los cargos anteriores al aviso de hurto, extravío o robo serán de cargo del consumidor, pero este supuesto no es sancionado expresamente ni por la ley ni por el proyecto de ley, ni con algún tipo de ineficacia, pero como se encuentran contenidas en un contrato por adhesión, se trataría de una clausula que se debe someter al control de fondo según los establece la ley de protección de los derechos de los consumidores, artículo 16, letras c) y d), cuando se invierte la carga de la prueba en perjuicio del consumidor.

Comenta que es importante clarificar cómo actuará esta ley con la de protección de los derechos de los consumidores y el derecho común, porque si bien esta ley regula quien debe cargar con estos cobros no consentidos, no es menos cierto que se trata de una relación de consumo y aun cuando no estuviere regulado por esta ley, se podría derivar la responsabilidad del proveedor, a partir del deber de diligencia del proveedor, que se consagra en los artículos 23, sobre incumplimiento contractual y el deber de seguridad genérico que se establece en el artículo 3, sin perjuicio de lo cual observa que le parece correcto que se dicte una ley especial para evitar dudas respecto de la responsabilidad del proveedor.

En este sentido, sostiene que cualquier seguro que se exija al consumidor sobre cargos no consentidos, es un seguro que no cumple con el cargo de utilidad. El Código de Comercio establece expresamente la idea que el seguro debe ser útil, de manera que, si se ofrece un seguro a un consumidor por un asunto que ya se encuentra regulado en cuanto a los cargos no consentidos, sería un cargo no útil.

Conviene clarificar la relación con la ley del consumidor y si la infracción a esta ley especial puede ser sancionada en sede del derecho que protege a los consumidores, por ejemplo, mediante una denuncia ante un juzgado de policía local, en invocación del artículo 23 y considerando además, que el artículo 2 bis de la ley del consumidor establece expresamente su aplicabilidad en casos que haya silencio de la ley especial cuando el interés difuso o colectivo sea comprometido o la norma especial no establece un estatuto indemnizatorio.

Cree, además, que sería conveniente agregar el régimen supletorio al que se pueda recurrir en caso de silencio supletorio de esta ley, que en el caso de la responsabilidad civil sería el régimen común y eventualmente en las cláusulas abusivas, la ley de protección de los derechos de los consumidores.

Explica en cuanto al régimen de diligencia que por tratarse de un contrato oneroso en materia de consumidores, no necesariamente debe ser conmutativo en los términos del derecho común y los estándares resultan distintos.

No obstante tratarse de un contrato de consumo, oneroso, la diligencia se exige a ambas partes y a ambas se exige una mediana diligencia, el Código Civil establece que la culpa será leve en los contratos onerosos, para ambas partes y por ello es una diligencia media.

En materia de consumo, si en ambos casos hay negligencia mediana, la diligencia mediana exigida al proveedor es superior a la exigencia mediana que se exige al consumidor, porque el proveedor es un individuo acostumbrado a estas operaciones o negocios, es un profesional y por conocer el negocio se genera una posición asimétrica, es él quien dispone de los dispositivos tecnológicos, los cajeros automáticos, las páginas web y el consumidor sólo usa lo que dispone por el proveedor.

La jurisprudencia a la que se ha referido, es respecto a lo que ocurre antes del aviso y en ese caso la jurisprudencia dice que no se puede indicar que la responsabilidad sea automática del consumidor, sino que se invierte la carga de la prueba y de esa manera el consumidor debe acreditar la negligencia del proveedor o que el cargo no ha sido consentido.

En cuanto a los plazos, el artículo 6° señala que el titular no es responsable por las operaciones posteriores al aviso, si desconoce haber realizado estas operaciones con anterioridad al aviso de fraude tiene un plazo de 30 días siguientes a la expedición del aviso o que haya tenido conocimiento. Puede ocurrir que transcurra un plazo importante hasta darse cuenta que se han hecho estos cargos. Observa que ese plazo *dies aquo* es subjetivo, porque señala como referencia “el darse cuenta de algo” y será objetivo si se cuenta desde un día que resulte cierto, como la fecha de celebración del contrato, desde la entrega del producto, etc.

El *dies aquo* como técnica legislativa, favorece la certeza jurídica, pero *dies aquo* subjetivo favorece la justicia y es este el que propone el proyecto de ley. Sin embargo, este plazo subjetivo debe ir asociado a un plazo máximo, que es algo que no propone el proyecto de ley. ¿Debe esperarse eternamente que una persona se dé cuenta que le han robado sus tarjetas o debemos establecer un plazo máximo de caducidad asociado al *dies aquo* subjetivo? Esta última parece ser la tesis correcta, es decir, se debe asociar a un plazo máximo de caducidad pero de inicio objetivo.

En cuanto al plazo de reintegro, se entiende que es sin perjuicio que se pueda solicitar la devolución de ese reintegro, una repetición en que el proveedor pueda solicitar la restitución si por ejemplo, se acredita que el cargo fue consentido o que hubo algún fraude del consumidor.

El señor **Rodrigo Figueroa, Jefe de la Brigada Investigadora del Cibercrimen Metropolitana, Subprefecto** informa en primer lugar que desde el 2010 a 2018 respecto del uso fraudulento de las tarjetas de crédito y de débito hay un aumento considerable de ellos, respecto de las órdenes de investigar e instrucciones particulares recibidas por la PDI coinciden con ese aumento.

Se refiere a un estudio hecho por el Banco Central según antecedentes proporcionados por SBIF y la ABIF, respecto de los medios usados en el comercio donde se aprecia un aumento en las transferencias electrónicas de fondos.

En relación con los *modus operandi* que se han conocido, precisa en primer lugar que se viene a tipificar algunas de las formas de operación fraudulenta que se han conocido, porque hay denuncias por uso fraudulento de tarjetas que se pueden tomar como un sabotaje informático o espionaje informático o como estafas y otras defraudaciones y uso fraudulento de tarjetas de crédito.

En casos de sabotaje informático, está el llamado *skimming* que es la instalación de dispositivos usados para extraer información de tarjetas de crédito al momento de realizar una transacción y que puede ser usado en cajeros automáticos o en locales comerciales donde se clona la tarjeta al entregarla para pagar.

En caso de espionaje informático está la modalidad de *carding* que es la extracción de datos de las tarjetas de crédito para hacer compras fraudulentas. Se encuentran en la *Deep web* o *dark web*.

En las estafas y otras defraudaciones contra particulares, se encuentra el traspaso de créditos a cuentas de víctimas, es la obtención de datos de las víctimas para transferir datos desde sus tarjetas, líneas de crédito o realizar préstamos a su nombre para que luego, mediante engaño, la víctima transfiera el dinero a otra cuenta. Explica que es el caso del falso ejecutivo y que se da con bastante frecuencia.

Respecto del proyecto de ley, observan que el artículo 2 se refiere a los titulares o usuarios de tarjetas de pago o de cualquier otro sistema similar podrán limitar su responsabilidad derivada del uso de los mismos en los términos establecidos por esta ley, en caso de hurto, robo o extravío de la tarjeta de pago, dando aviso oportuno al emisor, pero no se incluye el fraude, que es lo que señala a continuación en el proyecto.

Sobre la responsabilidad, el artículo 5 establece que las siguientes conductas constituyen delito de uso fraudulento de tarjeta de crédito, de pago con provisión de fondos o débito:

“b) Usar, vender, exportar, importar o distribuir tarjetas de pago falsificadas o sustraídas.”.

Sugiere que en este literal se incluya el porte de tarjetas o elementos conocidos para la comisión de este delito, similar a lo que señala el artículo 445 del código penal, cuyo objetivo es poder incautar los elementos usados para cometer el delito.”

Aclara que se han detectado casos de personas que han intentado ingresar a Chile con elementos conocidos para adulterar cajeros automáticos, pero la actual legislación no permite incautar las especies, solo se prohíbe el ingreso pero es posible que la persona pueda delinquir en otro país, pero el espíritu es poder neutralizar la capacidad delictiva de esas personas. Igualmente ocurre cuando en algunos controles se ha detectado a personas con dispositivos POS, de pago electrónico, adulterados o con dispositivos para adulterar cajeros electrónicos, similar a lo que ocurre en el citado artículo que se refiere a elementos para la comisión del delito de robo, pero no para otros delitos.

En la letra d) de la iniciativa, “d) Usar, vender, exportar, importar o distribuir los datos o el número de tarjetas de pago, haciendo posible que terceros realicen pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de las mismas.”

En este caso se sugiere sancionar el almacenamiento en cualquier forma o medio de los números o datos de tarjetas de pago y en que una persona no puede justificar su almacenamiento o procedencia. Sugieren que no se use la palabra “terceros” para no excluir al tenedor de manera que se refiera “haciendo posible que se realicen operaciones…”.

Explica al respecto que han tenido situaciones en que se ha encontrado en poder de sujetos, libretas que contienen números de tarjetas de crédito y las respectivas claves. Los mismos antecedentes se han encontrado en un computador.

Sobre la letra g), párrafo tercero; “g) Suplantar la identidad del titular o usuario frente al emisor, operador o comercio afiliado para obtener autorización para realizar transacciones con una tarjeta de pago.

Asimismo, incurrirá en el delito y sanciones que establece este artículo el que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas.

La pena señalada en el inciso primero aumentará en un grado, si cualquiera de las conductas tipificadas en este artículo produce perjuicio a terceros.”.”

Sugiere en este caso que se aplique la misma pena para quien simule ser empleado de algún emisor, operador o comercio afiliado de tarjetas de pago o similares y que provoque algún perjuicio al titular o usuario.

Este es el caso del falso ejecutivo bancario, modalidad en que se desbarató una organización criminal hace poco tiempo, que se dedicaban a estafas reiteradas y fraudes, asociación ilícita que usaba la figura del falso ejecutivo, sea telefónicamente, donde a la persona se le entregaban una serie de datos sobre su cuenta corriente lo que propiciaba el engaño, e incluso personas que iban a los domicilios para retirar los dispositivos que son usados en las transferencias electrónicas.

Expone que se debe considerar agregar la situación del que facilite los medios para la recepción y/o extracción de los valores obtenidos ilícitamente. Señala que son muchos los casos donde los cuentacorrentistas o propietarios de cuenta rut, facilitan sus cuentas para poder recibir los dineros que se han defraudado a otros clientes, de manera que son retirados por vía de un tercero.

Explica que las organizaciones criminales tienen repartidas sus funciones y dentro de ellos hay quienes se dedican a reclutar personas para usar sus cuentas a cambio de un porcentaje de los dineros obtenidos, generalmente equivalente al 10 por ciento del total de lo obtenido por el ilícito y esto hoy no tienen sanción, salvo algunos casos n que se encauza por el delito de receptación, que es una figura más propia del robo.

Precisa que no poseen el dato del número de tarjetas emitidas y que ello puede ser consultado a las entidades fiscalizadoras de las mismas.

La baja en los delitos a partir de 2013 no es una razón que se haya estudiado, pero hay una tendencia al alza. Aclara que en todo caso hay denuncias que se procesan como sabotaje informático, por ejemplo, y no por uso fraudulento de tarjetas. Una ley más específica podrá ayudar a determinar cuál es el tipo de delito que se va a configurar.

Respecto a la responsabilidad de los propios usuarios en algunas investigaciones, menciona que no tienen esa estadística, pero sí ha llamado la atención el término respecto de la responsabilidad inexcusable y quien la determinará, si es el banco o el órgano jurisdiccional.

El señor **Cristian Lobos Acevedo Jefe de la Brigada Investigadora de Delitos Económicos, Bridec, Subprefecto**, dice acerca del número de tarjetas, que si bien esta es una ley del año 2005, posteriormente el Banco Central emite una comunicación en la que permite a otras entidades financieras o instituciones financieras, la emisión de este tipo de tarjetas, como casas comerciales del *retail* lo que permite que el acceso a tarjetas de crédito, de débito o de pago en general, acceso de personas con un nivel educacional más bajo y ello

es el fundamento también de porqué es en las cuentas rut donde se depositan los dineros que se obtienen de estas operaciones ilícitas.

Agrega que el gran volumen de tarjetas disponibles hace que haya un aumento en un año de la cantidad de delitos.

Hay también casos de bajas en las denuncias o de los delitos, pero ello también puede ser resultado de las campañas que hace la banca o el emisor y las campañas de la PDI que por ejemplo, realiza hacia los adultos mayores en conjunto con Senama.

El señor **Alejandro Herrera Gerente General de Transbank,** informa que durante 2018 se efectuaron 1.500 millones de transacciones, cerca de 59 mil millones de dólares que pasan por su red, se responsabilizan por el pago a los comercios y recaudan los fondos desde los emisores. En diciembre de 2018, que representa un *peak* de transacciones, se espera realizar sobre 375 transacciones por segundo, lo que demuestra una gran inversión y desarrollo tecnológico en este rubro.

Respecto de la evolución del monto de ventas en millones de dólares, ellas se duplican cada 4 años, llegando a los 60.330 millones de dólares al año 2018, en cifras muy similares entre las tarjetas de crédito y débito, cerca del 19,3 por ciento del producto interno bruto y el 31 por ciento del consumo privado.

En cuanto a la penetración de uso en el consumo, señala que alcanza 25 puntos (*ranking* especial), lo que posiciona a Chile por sobre países como Alemania, Japón, Italia o México y por debajo de países como Suiza, Holanda, Estados Unidos o Canadá, que es uno de los países más bancarizados en términos de tarjetas de crédito y débito.

En cuanto a la evolución de las ventas por internet, se espera que en 2018 sean el 18 por ciento de las ventas que se efectúan con tarjetas de crédito y débito. El número de transacciones es de 1500 millones de ellas, mucho más de redcompra, tarjeta de débito que de crédito, en que la relación es de 3,5 a 1.

Algunas cifras indican que en Chile hay aproximadamente 10 millones de tarjetas de crédito, titulares más las adicionales y más de 15 millones de tarjetas de débito otorgadas por instituciones reguladas por la SBIF.

La importancia del medio de pago entre las personas naturales es del 57 por ciento, los cheques han caído al 2,8 por ciento que en 2003 era el 46 por ciento, el *e-banking* o transferencias electrónicas es del 27 por ciento y los giros de ATM, han caído al 19 por ciento.

Tienen una cobertura del 100 por ciento en el territorio nacional, es decir, se encuentran presentes en todas las comunas en los rubros más variados. La cobertura de los POS son 363 mil y 298 mil locales comerciales y 174 mil clientes. En cuanto a los puntos de contacto por cada habitante, que es algo que se discute a nivel de banco mundial e instituciones internacionales, explica que en 2018 cada cien mil habitantes adultos hay 2400 puntos de contacto o POS, lo que pone a Chile sobre países como Rusia, Alemania, México o Perú. En el caso de Brasil, explica que hay una particularidad, porque tiene más de un POS por local comercial.

En cuanto a los fraudes, en lo que se refiere solo a Transbank, detalla que han desarrollado algunas herramientas, plataformas y aplicaciones, páginas web y *Web Pay* a la cual los comercios tienen acceso para vender sus productos por internet, que además les ofrecen el servicio para las transacciones que vienen desde el extranjero y que se hace con las marcas, con alguna particularidad, *verify by Visa* o *Mastercard secure code*, de esta manera, cuando un extranjero viene a comprar a Chile la autorización se va a la marca y los emisores adscritos a estas verificaciones autorizan las transacciones. A ello se suman el pin pass, que se desarrolló en Chile antes que en otros países y la tecnología chip y contact less.

Advierte que una de las razones por la cual puede haber una caída de los delitos de fraude en tarjetas, es porque a partir del año 2012 y parte de 2013, se inicia la migración a las tarjetas con *chip*, lo que tuvo un impacto sobre los fraudes. A continuación, surge una alta emisión de cuentas rut, que, en cuanto plásticos, aún no tienen *chip*, sino solo con tecnología de banda magnética que es más vulnerable al fraude.

De acuerdo con la información que proveen las marcas, el índice de fraude en Latinoamérica y el Caribe, Chile presenta 3,4 puntos base, sobre 10.000, siendo el segundo país en la región con la mejor estadística en esta materia, donde el promedio mundial es de 11,3 puntos base. Precisa que el promedio de Latinoamérica es de 13,5 puntos base. Explica también que hay países que tienen altas cifras de fraude, históricamente, porque los precios en esos países permiten que se cubra el fraude, los precios al comercio, las tasas de intercambio son tan altos que el adquirente o los bancos emisores tienen un margen suficientemente alto para aceptar este fraude y no invierten ni gastan en medidas de seguridad.

Las cifras de fraude en 2015 a 2018, parten con un nivel de fraude bastante alto, 4.23 punto base y terminan con un 2.57, que son niveles de fraudes más bajos que en otros años producto de las medidas que se han adoptado por distintos agentes del sistema. Si se quisiera ver cuánto corresponde a nivel nacional o extranjero, el fraude de tarjetas que provienen del extranjero es más alto producto de la dificultad de verificación, los estándares son diferentes y hay bandas que vienen de otros países y afectan principalmente grandes tiendas con estos fraudes.

Donde más se produce el fraude nacional es en los contact center, luego internet y el presencial es muy bajo.

Respecto del proyecto de ley, hacen presente que este sistema es una cadena de pago, donde hay muchos participantes. Los participantes necesarios son el emisor, el usuario o tarjetahabiente, el comercio y el adquirente, que en este caso es Transbank, que enrola los comercios y realiza los procesamientos. Los participantes eventuales son las marcas internacionales, el procesador emisor, el procesador adquirente, los proveedores de servicios de red (terminales de punto de ventas o plataformas web) y los proveedores de servicio de pago (PSP).

Señala que es de importancia reconocer en el proyecto de ley la responsabilidad de cada uno de estos participantes necesarios y sería un error dejar sin responsabilidad a alguno de ellos.

Hace presente la necesidad de separar lo que es la validación de una tarjeta, que es el plástico físico mismo; la autorización de la transacción significa verificar que el establecimiento está adherido a la red, que la tarjeta está vigente y cuenta con los fondos y la autentificación del usuario dependerá de si se exige firma electrónica o firma física, pin pass, etc.

Es necesario tipificar el delito cuando se suplanta al establecimiento comercial lícito mediante una página web que parece ser de un determinado establecimiento comercial para que los tarjetahabientes efectúen compras, normalmente con ofertas o promociones muy atractivas. El objeto de esta suplantación es obtener información para después hacer uso fraudulento de la información de las tarjetas o que se materialicen transacciones, se abonen ellas y no se entregue el producto o servicio.

Otro elemento es la creación de un establecimiento comercial “lícito” con el objeto de defraudar, sean físicos o virtuales. Generalmente para servicios que se pagan por anticipado o compras virtuales con entrega diferida, como ocurre en el turismo, donde después de realizar el abono se produce la anulación de transacciones, problema que se genera con la marca y los problemas para encontrar a los responsables.

Señala que se debe considerar también, el que uno de los actores de esta cadena voluntariamente acepte responsabilidades que no se encuentran tipificadas, al objeto de tener mayor volumen de transacción y de ventas. Advierte que hay tiendas que están

dispuestas a no pedir verificación o pin pass para no perjudicar su volumen de ventas y están dispuestos a asumir la responsabilidad ante eventuales delitos.

Añade que Transbank tiene mucha relación con los emisores y opina que una de las razones por las que se han logrado estos niveles de fraude tan bajos, es precisamente porque hay una acción conjunta de emisores, adquirentes, tarjetahabientes y policías que han logrado una evolución positiva.

Si bien no tiene las cifras de las inversiones de los bancos, aclara que ellas son considerables y algunas son estratégicas, pero lo califica como un porcentaje relevante respecto al patrimonio de cada institución. Lo que Transbank invierte en ciberseguridad es una cifra sustanciosa.

Recalca la necesidad de que el proyecto de ley considere que cada una de las partes tenga su responsabilidad y dentro de ello, no aparece razonable pedir ciberseguridad al tarjetahabiente, pero ello debe pedirse respecto de los emisores. En el caso de los adquirentes, tienen la obligación y responsabilidad de invertir en ciberseguridad y se les tiene que exigir, al igual que a establecimientos comerciales que operan en internet con porcentaje de sus ventas no presenciales y deben tener páginas web seguras, autenticaciones y asumir las responsabilidades que les corresponden, con mayor razón si ellos están dispuestos a no exigir las medidas de autentificación para evitar fraudes.

Opina que en general el proyecto de ley parece ir en el sentido correcto y les preocupa algún desbalance en la responsabilidad que propone, les parece que no se deja claro especialmente la responsabilidad del tarjetahabiente, porque es importante que ellos cumplan su debida responsabilidad y se evite la negligencia o el posible dolo respecto del medio de pago y de las claves, sea en transacciones presenciales o no presenciales.

Expresa que sería bueno incorporar la tipificación del delito para el caso de los establecimientos comerciales que se crean ilícitamente o lícitamente, pero con el objeto de defraudar.

Finalmente, precisa que dan su opinión en su rol de adquirente y en su relación con los comercios, no representan a los bancos que es a quienes corresponde el rol de emisor.

El señor **Rodrigo Undurraga; fiscal de Transbank**, aclara que el plazo de 30 días aparece como adecuado, porque hay dos controles, uno de esos controles es el aviso. El plazo de 30 días se cuenta desde el aviso o desde que el tarjetahabiente tuvo o debió tener conocimiento de las transacciones, por ello se emiten los estados de cuenta mensual y este contrato de tracto sucesivo, se extingue con esas liquidaciones, de manera que el plazo es suficiente porque, reitera, se dio el aviso o el tarjetahabiente debió tener conocimiento o recibido su estado de cuenta.

Respecto del plazo de tres días, si bien no les corresponde verificar como emisor qué es lo que sucedió con una transacción, desde el punto de vista del adquirente que debe desarrollar una investigación y recabar datos y recurrir a la marca internacional, el plazo de tres días para tener una conclusión, desde el punto de vista del adquirente y que es similar al del emisor, es inadecuado y debiera considerarse un plazo mayor.

Desde el punto de los tipos penales, esta es una ley que protege al consumidor y cambia una serie de principios de las responsabilidades de los consumidores, pero que trata temas penales. Solicitan que dentro de los tipos penales se incorporen aquellos que dicen relación con los establecimientos comerciales, sea por suplantación o por la incorporación de terminales inadecuados o por conductas similares que presentan gran dificultad para acreditar el ilícito ante los tribunales se debe recurrir a las figuras de estafas y defraudaciones.

El señor **Fernando Cañas, presidente de Transbank**, precisa que siendo este un sistema de cuatro partes es muy complejo dejar una de ellas sin responsabilidad y que, en busca del necesario equilibrio, el cliente tarjetahabiente debe tener responsabilidad.

V. DISCUSIÓN PARTICULAR.

Se da lectura al artículo único del texto aprobado por el Senado:

“Artículo único. Modificase 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 la denominación de la ley por la siguiente: “Establece un régimen de limitación de responsabilidad en casos de fraude para emisores y usuarios de medios de pago.”.

2) Antepónese al artículo 1°, el siguiente epígrafe:

“Título I

Del ámbito de aplicación y reglas generales”

3) Reemplázanse los artículos 1º, 2º, 3° y 4°, por los siguientes:

“Artículo 1º.- Ámbito de aplicación. La presente ley regula el régimen de responsabilidad aplicable en los casos de extravío, hurto, robo o fraude de tarjetas de crédito, tarjetas de débito, tarjetas de pago con provisión de fondos, o cualquier otro sistema similar, en adelante conjuntamente, las “tarjetas de pago”, emitidas y operadas por entidades sujetas a la fiscalización de la Superintendencia de Bancos e Instituciones Financieras y a la regulación del Banco Central de Chile. También regula el régimen de responsabilidad en los casos de extravío, hurto, robo o fraude de tarjetas de pago emitidas y operadas por entidades no sujetas a la fiscalización y regulación de los organismos indicados, salvo disposición expresa en contrario.

Asimismo, se aplicará a los fraudes en “transacciones electrónicas”. Para efectos de esta ley, se entenderá por tales aquellas operaciones realizadas por medios electrónicos que originen cargos y abonos o giros de dinero en cuentas corrientes bancarias, cuentas de depósitos a la vista, cuentas de provisión de fondos, tarjetas de pago u otros sistemas similares, tales como instrucciones de cargo en cuentas propias para abonar cuentas de terceros, incluyendo pagos y cargos automáticos, transferencias electrónicas de fondos, avances en efectivo, giros de dinero en cajeros automáticos y demás operaciones electrónicas contempladas en el contrato de prestación de servicios financieros respectivo. Se comprenden dentro de este concepto las transacciones efectuadas mediante portales web u otras plataformas electrónicas, informáticas o telefónicas dispuestas por la empresa bancaria o el proveedor del servicio financiero correspondiente.

Los plazos de días hábiles que establece esta ley no considerarán los sábados, domingos ni festivos.

Artículo 2º.- Los titulares o usuarios de tarjetas de pago o de cualquier otro sistema similar podrán limitar su responsabilidad, derivada de la utilización de los mismos, en los términos establecidos por esta ley, en caso de hurto, robo o extravío de la tarjeta de pago, dando aviso oportuno al emisor.

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

Las tarjetas de pago respecto de las que el titular o usuario haya dado aviso de extravío, hurto, robo o fraude deberán ser bloqueadas de inmediato por el emisor.

Artículo 3º.- En el caso que las tarjetas de pago sean utilizadas con posterioridad al aviso de extravío, hurto, robo o fraude, el emisor será responsable de tales transacciones y sus consecuencias económicas en virtud de lo señalado en el inciso final del artículo anterior.

Las cláusulas de los contratos que impongan el deber de prueba sobre el titular o usuario, por operaciones realizadas con posterioridad al aviso de extravío, hurto, robo o fraude, se tendrán por no escritas.

Artículo 4º.- El titular o usuario de tarjetas de pago o servicios similares no tendrá responsabilidad por las operaciones realizadas con posterioridad al aviso de extravío, hurto o robo dado al emisor, sin perjuicio de la responsabilidad penal que corresponda.

Tratándose de las operaciones anteriores a dicho aviso, el titular o usuario deberá reclamar al emisor aquellas que desconoce su autorización, en el mismo acto del aviso o hasta cinco días hábiles siguientes a su expedición.

En los casos de fraude, se aplicará lo dispuesto en los artículos 5° y siguientes.”.

4) Incorpórase, a continuación del artículo 4°, el siguiente epígrafe:

“Título II
De la responsabilidad por uso fraudulento de tarjetas de pago”

5) Sustitúyese el artículo 5º, por el siguiente:

“Artículo 5º.- Las conductas que a continuación se señalan constituyen delito de uso fraudulento de tarjetas de pago y se sancionarán con la pena de presidio menor en su grado medio a máximo y multa correspondiente al triple del monto defraudado:

a) Falsificar tarjetas de pago.

b) Usar, vender, exportar, importar o distribuir tarjetas de pago falsificadas o sustraídas.

c) Negociar, en cualquier forma, tarjetas de pago falsificadas o sustraídas.

d) Usar, vender, exportar, importar o distribuir los datos o el número de tarjetas de pago, haciendo posible que terceros realicen pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de las mismas.

e) Negociar, en cualquier forma, con los datos o el número de tarjetas de pago, para fines de realizar las operaciones señaladas en el literal anterior.

f) Usar maliciosamente una tarjeta de pago bloqueada, en cualquiera de las formas señaladas en las letras precedentes.

g) Suplantar la identidad del titular o usuario frente al emisor, operador o comercio afiliado para obtener autorización para realizar transacciones con una tarjeta de pago.

Asimismo, incurrirá en el delito y sanciones que establece este artículo el que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas.

La pena señalada en el inciso primero aumentará en un grado, si cualquiera de las conductas tipificadas en este artículo produce perjuicio a terceros.”.

6) Agrégase el siguiente artículo 6º:

“Artículo 6º.- En los casos a que se refiere el artículo anterior, el titular o usuario no será responsable por las operaciones realizadas con posterioridad al aviso de fraude dado al emisor por las mismas vías establecidas para estos efectos en la presente ley, ni por aquellas operaciones que desconozca haber autorizado efectuadas con anterioridad al aviso de fraude que el titular o usuario reclame dentro de los treinta días corridos siguientes a la expedición de dicho aviso o que haya tenido conocimiento de ellas. Para estos efectos, y en relación con el conocimiento de la existencia de operaciones no autorizadas, se considerará especialmente la circunstancia que el emisor u operador haya enviado una alerta de fraude y que exista constancia de su recepción por parte del titular o usuario.

En los casos en que el titular o usuario desconozca haber autorizado una operación, corresponderá al emisor u operador demostrar que la operación fue autorizada por el titular o usuario y registrada con exactitud.

El registro de la utilización de las tarjetas de pago no bastará, necesariamente, para demostrar que la operación fue autorizada por el titular o usuario, ni que éste actuó de manera fraudulenta o con negligencia inexcusable. En todo caso, cuando el titular o usuario tome conocimiento de alguna de las conductas del artículo anterior deberá dar cuenta al emisor en los términos señalados en el inciso primero.

En ningún caso se aplicará la exención de responsabilidad señalada, si se prueba que el titular o usuario tuvo participación en los delitos descritos en el artículo 5°, que obtuvo un provecho ilícito o que actuó con dolo o negligencia inexcusable facilitando su comisión.

El titular o usuario soportará el total de las pérdidas que afronte como consecuencia de operaciones que sean fruto de su actuación fraudulenta.”.

7) Incorpórase, a continuación del artículo 6º, el siguiente epígrafe:

“Título III
De la cancelación de cargos o restitución de fondos”

8) Agréganse los siguientes artículos 7° y 8°:

“Artículo 7º.- El emisor u operador de las tarjetas de pago deberá proceder a la cancelación de los cargos o la restitución de los fondos correspondientes a las operaciones realizadas con posterioridad al aviso de extravío, hurto, robo o fraude, o de aquellas operaciones cuya autorización ha sido desconocida por el titular o usuario dentro de los tres días hábiles siguientes a dicho aviso.

Sólo si se acredita por sentencia firme o ejecutoriada que el titular o usuario ha participado en la comisión del delito, que obtuvo un provecho ilícito o que actuó con dolo o negligencia inexcusable facilitando su comisión, se procederá a dejar sin efecto la cancelación de los cargos o la restitución de fondos, sin perjuicio de las indemnizaciones que correspondan según la legislación y normativa aplicable.

Artículo 8º.- Los emisores y operadores de tarjetas de pago, los comercios y otros establecimientos afiliados a un sistema de tarjetas de pago, así como las demás entidades que intervengan o presten servicios asociados a pagos y transacciones electrónicas, deberán adoptar las medidas de seguridad necesarias para prevenir la comisión de los ilícitos descritos en esta ley, conforme a la legislación y normativa que les resulte aplicable, y resguardando la prestación segura del servicio en los términos señalados por el artículo 23 de la ley N° 19.496. La falta o deficiencia de tales medidas será considerada para la determinación de las responsabilidades correspondientes a cada uno de ellos.”.”.

INDICACIONES.

Se elabora una indicación sustitutiva, que fue trabajada y consensuada entre el Ejecutivo y los diputados miembros de la Comisión y sus asesores.

Se formula la siguiente indicación sustitutiva de la y los diputados Sofía Cid, Boris Barrera, Alejandro Bernales; Renato Garín, Harry Jürgensen, Miguel Mellado, Jaime Naranjo, Alexis Sepúlveda y Enrique van Rysselberghe, para reemplazar el texto del proyecto de ley por el siguiente:

“Artículo primero. - 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 la denominación de la ley por la siguiente: “Establece un régimen de limitación de responsabilidad para emisores y titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude.”.

Puesta en votación, se **aprueba** por unanimidad. Votan la diputada Cid y los diputados Barrera, Garín, Jürgensen, Miguel Mellado, Naranjo, Sepúlveda, Silber, Van Rysselberghe y Pedro Velásquez. (10x0x0).

2) Reemplázanse los artículos 1º al 8º por los siguientes:

Título I

Del ámbito de aplicación y reglas generales

“Artículo 1º.- La presente ley, en adelante la “Ley”, regula el régimen de responsabilidad aplicable en los casos de extravío, hurto, robo o fraude de tarjetas de crédito, tarjetas de débito, tarjetas de pago con provisión de fondos, o cualquier otro sistema similar, en adelante conjuntamente, las “tarjetas de pago”, emitidas y operadas por entidades sujetas a la fiscalización de la Comisión para el Mercado Financiero y a la regulación del Banco Central de Chile, en relación con el respectivo giro de emisión u operación de dichos instrumentos. También regula el régimen de responsabilidad en los casos de extravío, hurto, robo o fraude de tarjetas de pago emitidas y operadas por entidades no sujetas a la fiscalización y regulación de los organismos indicados, salvo disposición expresa en contrario.

Asimismo, se aplicará a los fraudes en transacciones electrónicas. Para efectos de la ley, se entenderá por tales aquellas operaciones realizadas por medios electrónicos que originen cargos y abonos o giros de dinero en cuentas corrientes bancarias, cuentas de depósitos a la vista, cuentas de provisión de fondos, tarjetas de pago u otros sistemas similares, tales como instrucciones de cargo en cuentas propias para abonar cuentas de terceros, incluyendo pagos y cargos automáticos, transferencias electrónicas de fondos, avances en efectivo, giros de dinero en cajeros automáticos y demás operaciones electrónicas contempladas en el contrato de prestación de servicios financieros respectivo. Se comprenden dentro de este concepto las transacciones efectuadas mediante portales web u otras plataformas electrónicas, informáticas, telefónicas o cualquier otro sistema similar dispuesto por la empresa bancaria o el proveedor del servicio financiero correspondiente.

Para efectos de la ley, las tarjetas de pago y sistemas de transacciones electrónicas podrán referirse en forma conjunta como “medios de pago”.

Los plazos de días hábiles que establece esta ley no considerarán los sábados, domingos ni festivos u otros que no correspondan a días hábiles bancarios conforme a lo previsto en el artículo 38 de la Ley General de Bancos.”.

La señora **Michele Labbé** señala que esta indicación ha actualizado el órgano fiscalizador y en atención a la gran velocidad de los cambios tecnológicos, se agregó “operaciones u otros sistemas similares” con ello se busca poder dejar dentro de la regulación nuevos mecanismos de operación de estos productos que aparezcan en el futuro con el desarrollo tecnológico. Además, se incluye la definición del plazo de días hábiles, pensando en la existencia de un feriado especial, como es el feriado bancario de 31 de diciembre.

Puesta en votación, se **aprueba** por unanimidad. Votan la diputada Cid y los diputados Barrera, Garín, Jürgensen, Miguel Mellado, Naranjo, Sepúlveda, Silber, Van Rysselberghe y Pedro Velásquez. (10x0x0).

***

“Artículo 2º.- Los titulares o usuarios de medios de pago, así como los titulares de otras cuentas o sistemas similares que permitan efectuar transacciones electrónicas, en adelante referidos en forma conjunta como los “usuarios”, podrán

limitar su responsabilidad, en los términos establecidos por la Ley, en caso de hurto, robo, extravío o fraude, dando aviso oportuno al emisor.

El emisor o prestador del servicio financiero de pagos electrónicos de dichos medios de pago, en adelante, referidos en forma conjunta como los “emisores”, deberá proveer al usuario, todos los días del año, las 24 horas del día, de canales o servicios de comunicación, de acceso gratuito y permanente, que permitan efectuar 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, código de recepción o identificador de seguimiento; y la fecha y hora del aviso; procediendo de inmediato al bloqueo respectivo del medio de pago, en lo referido a su funcionalidad para efectuar pagos o transacciones electrónicas.

Además, deberá enviar al usuario una comunicación por escrito con la información a que se refiere el inciso anterior, de la manera más expedita. En todo caso, el incumplimiento de esta obligación no afectará la validez o eficacia del aviso recibido.

En todo caso, y bajo su responsabilidad, el emisor podrá encomendar a un operador de medios de pago la provisión de estos canales o servicios de comunicación, así como la realización, en su representación, de las constancias de recepción o bloqueos que procedan.”.

La señora **Michele Labbé** explica que este artículo regula el ámbito de la responsabilidad de los usuarios, en especial con posterioridad al aviso de fraude y al bloqueo inmediato. Se precisa que los canales de comunicación deben estar disponibles todos los días, las 24 horas, es decir, permanentes y además, deben ser gratuitos.

Se agrega el deber de confirmación por escrito y le entrega de un número de seguimiento del aviso, pero se advierte que la falta de notificación por escrito no altera la validez del aviso. Se permite que el banco pueda encomendar los servicios a un tercero, pero el banco mantiene su responsabilidad para bloquear según la orden del aviso que recibe

El **diputado Garín** señala que estas son indicaciones que se recogen de las exposiciones de Bancoestado y Transbank.

Puesta en votación, se **aprueba** por unanimidad. Votan la diputada Cid y los diputados Barrera, Garín, Jürgensen, Miguel Mellado, Naranjo, Sepúlveda, Silber, Van Rysselberghe y Pedro Velásquez. (10x0x0).

***

“Artículo 3º.- En el caso que los medios de pago a que se refiere esta Ley sean utilizados con posterioridad al aviso de extravío, hurto, robo o fraude, el emisor será responsable de tales operaciones y sus consecuencias económicas, en virtud de lo señalado en el artículo anterior.

Por ende, el usuario del respectivo medio de pago quedará liberado de responsabilidad por estos conceptos, sin perjuicio de la responsabilidad penal que pudiere corresponderle con motivo del extravío, hurto, robo o fraude respectivo.

Las cláusulas de los contratos que impongan el deber de prueba sobre el usuario, por operaciones realizadas con posterioridad al aviso de extravío, hurto, robo o fraude, no producirán efecto alguno y se tendrán por no escritas.”.

La señora **Michele Labbé** señala que se introduce una mejoría en relación con la responsabilidad penal, además de una adecuación de la norma que originalmente se contenía en el artículo siguiente.

Puesta en votación, se aprobó por unanimidad. Votan la diputada Cid y los diputados Barrera, Bernales, Garín, Jürgensen, Miguel Mellado, Naranjo, Sepúlveda, Silber y Pedro Velásquez. (10x0x0).

***

“Artículo 4º.- Tratándose de operaciones anteriores al aviso a que se refiere el artículo 2° de esta ley, el usuario deberá reclamar al emisor aquellas operaciones respecto de las cuales desconoce haber otorgado su autorización o consentimiento, en el mismo acto del aviso o hasta cinco días hábiles siguientes a su expedición.

El reclamo solo podrá abarcar operaciones incluidas e individualizadas en la facturación del último estado de cuenta mensual y en todo caso, siempre que no hayan transcurrido más de 30 días desde la fecha de notificación de dicho estado, efectuada en la oportunidad y por los medios pactados al efecto en el contrato de prestación de servicios financieros correspondiente.

En caso de no corresponder el envío de un estado de cuenta, o no encontrarse una o más operaciones no autorizadas incluidas en el último estado de cuenta remitido, el usuario que tenga conocimiento de las mismas por otras vías de información provistas por el emisor podrá igualmente desconocer su autorización, en la medida que su materialización o registro no sea anterior a 30 días contados desde el aviso efectuado por el usuario.

Sin perjuicio de lo anterior, tratándose de operaciones previas al aviso, pero que sean facturadas en un estado de cuenta mensual posterior a dicho aviso, igualmente podrán ser reclamadas en el plazo máximo de 30 días desde la emisión y entrega de dicho estado.

En relación con el conocimiento de la existencia de operaciones no autorizadas, se considerará especialmente la circunstancia que el emisor haya enviado una alerta de fraude al usuario, identificando las operaciones sospechosas, y que exista constancia de su recepción por parte del usuario, conforme al contrato de prestación de servicios financieros correspondiente.

Tan pronto el usuario tome conocimiento de la existencia de operaciones no autorizadas, deberá otorgar el aviso correspondiente conforme a lo previsto en el artículo 2° de esta Ley, salvo en caso de encontrarse impedido por razones de fuerza mayor o caso fortuito, situación bajo la cual deberá efectuar el aviso respectivo dentro del plazo máximo de 5 días hábiles contado desde que se encuentre en condiciones de expedirlo.

En los casos en que el usuario desconozca haber autorizado una operación, corresponderá al emisor demostrar que la operación fue autorizada por el

usuario y que se encuentra registrada a su nombre o respecto del instrumento de pago o cuenta correspondiente.

El registro de dichas operaciones no bastará, necesariamente, para demostrar que la operación fue autorizada por el usuario, ni que éste actuó de manera fraudulenta o con negligencia inexcusable.”.

La señora **Michele Labbé** explica que se regulan las operaciones celebradas con anterioridad al aviso y se establecen tres tipos de reclamos.

El primero es un plazo para operaciones realizadas previamente al aviso, de hasta 5 días hábiles posteriores al aviso por las operaciones facturadas en el estado de cuenta

En segundo lugar, también hay cinco días posteriores para el caso en que se tome conocimiento por otro medio, distinto al del estado de cuenta.

Si después de dar el aviso llega un estado de cuenta, puede haber operaciones que se han facturado antes del estado de cuenta. En este caso el plazo es de 30 días para poder reclamar desde la notificación del estado de cuenta según contrato con el emisor.

Adicionalmente se agrega el caso de fuerza mayor, si la persona se encuentra fuera del país o enferma y no recibe las notificaciones, este plazo comienza a contarse desde que toma conocimiento y cinco días después de esta notificación, puede dar el aviso.

Originalmente bastaba una alerta de fraude para que el banco pudiera limitar su responsabilidad. Ahora se indica que ello no es suficiente, no basta la alerta general, sino que se debe notificar específicamente al cliente respecto de una alerta en sus tarjetas u operaciones, lo que debe realizarse respecto de operaciones no conocidas o sospechosas.

Agrega que se mantiene la carga de la prueba, pero ha cambiado el artículo donde ella se trata.

Puesta en votación, se **aprueba** por unanimidad. Votan la diputada Cid y los diputados Barrera, Bernales, Garín, Jürgensen, Miguel Mellado, Naranjo, Sepúlveda, Silber, Van Rysselberghe y Pedro Velásquez. (11x0x0).

***

Título II

De la cancelación de cargos o restitución de fondos

“Artículo 5º.- El emisor deberá proceder a la cancelación provisional de los cargos o a la restitución provisional de los fondos correspondientes a las operaciones realizadas con anterioridad al aviso de extravío, hurto, robo o fraude, tratándose de operaciones cuya autorización ha sido desconocida por el usuario, dentro de los siete días hábiles siguientes al reclamo. Tratándose de estas operaciones, la restitución provisional de fondos podrá estar afecta a un deducible máximo equivalente a cero coma cinco unidades de fomento de cargo del usuario, para

el total de las operaciones que puedan ser desconocidas en relación al aviso a que se refiere el artículo 2° de esta Ley.

En todo caso, el emisor estará impedido de ofrecer a los usuarios la contratación de seguros cuya cobertura corresponda a riesgos o siniestros y de cobrar comisiones que el mismo deba asumir conforme a esta Ley. Lo anterior, es sin perjuicio de los seguros que el emisor pueda contratar en calidad de beneficiario, a su cargo.

Sólo si se acredita por sentencia firme o ejecutoriada que el usuario ha participado en la comisión del delito, que obtuvo un provecho ilícito o que actuó con dolo o negligencia inexcusable facilitando su comisión, se procederá a dejar sin efecto la cancelación de los cargos o la restitución de fondos, sin perjuicio de las indemnizaciones que correspondan según la legislación y normativa aplicable.”.

La señora **Michele Labbé** observa que en este artículo se agrega la obligación del emisor de restituir provisionalmente, figura que no existía originalmente en el proyecto de ley. Con esto se le entrega el tiempo suficiente a las instituciones financieras para poder investigar la procedencia del fraude, pero pagando los fondos en el plazo de 7 días.

Destaca que otro punto importante es prohibir que los bancos ofrezcan seguros o se contraten por los riesgos que debe cumplirse por esta ley, es decir, ya no se podrán pagar seguros de fraude.

Adicionalmente se entrega a los bancos la posibilidad de poder descontar un deducible, ello como una forma de que las personas no perciban que las coberturas de esta ley pueda ser un incentivo a ser menos cuidadoso en el uso de las tarjetas. Precisa que el banco puede deducir no cobrar el deducible o cobrar hasta 0,5 UF y como deducible es parte del contrato de prestación de servicios.

El **diputado Garín** señala que este era uno de los puntos centrales del proyecto de ley y se coincide en que el banco no puede cobrar como un extra la protección que el banco debe dar a las tarjetas.

Puesta en votación, se **aprueba** por unanimidad. Votan la diputada Cid y los diputados Barrera, Bernales, Garín, Jürgensen, Miguel Mellado, Naranjo, Sepúlveda, Silber, Van Rysselberghe y Pedro Velásquez. (11x0x0).

***

“Artículo 6º.- Los emisores, operadores, comercios y otros establecimientos afiliados a un sistema de tarjetas de pago, así como las demás entidades que intervengan o presten servicios asociados a pagos y transacciones electrónicas, u otros sistemas de características similares, deberán adoptar las medidas de seguridad necesarias para prevenir la comisión de los ilícitos descritos en esta ley conforme a la legislación y normativa que les resulte aplicable, y resguardando la prestación segura del respectivo servicio en los términos señalados por el artículo 23 de la ley N° 19.496.

En el caso de los emisores u operadores, según corresponda, dichas medidas de seguridad deberán considerar, al menos, lo siguiente:

a) Contar con sistemas de monitoreo, que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual del usuario.

b) Implementar procedimientos internos para gestionar las alertas generadas por dichos sistemas de monitoreo.

c) Identificar patrones de potenciales fraude, conforme a las prácticas de la industria y recomendaciones, los que deberán incorporarse al sistema de monitoreo de operaciones.

d) Establecer límites y controles en los diversos canales de atención, que permitan mitigar las pérdidas por fraude. Los referidos límites y controles deberán basarse en consideraciones de riesgo objetivas, generales y no discriminatorias, en relación con la naturaleza del medio de pago y la clase de operaciones que permita efectuar.

El órgano fiscalizador competente a través de la normativa que dicte recomendara lo señalado en las letras a), b), c) y d) respecto de los emisores sujetos a su supervisión.

La falta o deficiencia de tales medidas será considerada para la determinación de las responsabilidades correspondientes a cada uno de ellos, que pudiere perseguir en su contra el usuario u otro afectado.

Lo indicado, es sin perjuicio de la posibilidad que los emisores puedan perseguir el cumplimiento de la obligación de restitución o reembolso que corresponda, por cancelaciones de cargos o devoluciones de fondos, en base a los estándares y procedimientos de seguridad exigibles a cada una de las entidades antes indicadas, de conformidad con la Ley, las demás leyes y regulaciones aplicables, teniendo presente los términos y condiciones contractuales que los vinculen, en cada caso.”.

La señora **Michele Labbé** subraya que en este artículo se han precisado las nuevas medidas de seguridad que deben adoptar los emisores de las tarjetas y medios de pago. La indicación parlamentaria precisa estas cuatro formas mínimas que deben tener las instituciones financieras para realizar los monitoreos, e igualmente se cubre la observación de algunos diputados respecto a la necesidad de invertir para evitar los fraudes en los medios de pago.

Se establece expresamente la posibilidad que las entidades financieras puedan repetir contra aquellas entidades que no den cumplimiento respecto de medidas de seguridad exigidas en su caso por el órgano pertinente.

Puesta en votación, se **aprueba** por unanimidad. Votan la diputada Cid y los diputados Barrera, Bernales, Garín, Jürgensen, Miguel Mellado, Naranjo, Sepúlveda, Silber, Van Rysselberghe y Pedro Velásquez. (11x0x0).

***

Título III

De la responsabilidad por fraude en tarjetas de pago y transacciones electrónicas.

”Artículo 7º.- Las conductas que a continuación se señalan constituyen delito de uso fraudulento de tarjetas de pago y transacciones electrónicas; y se sancionarán con la pena de presidio menor en su grado medio a máximo y multa correspondiente al triple del monto defraudado:

a) Falsificar tarjetas de pago.

b) Usar, vender, exportar, importar o distribuir tarjetas de pago falsificadas o sustraídas.

c) Negociar, en cualquier forma, tarjetas de pago falsificadas o sustraídas.

d) Usar, vender, exportar, importar o distribuir los datos o el número de tarjetas de pago, haciendo posible que terceros realicen pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de las mismas.

e) Negociar, en cualquier forma, con los datos, el número de tarjetas de pago, y claves o demás credenciales de seguridad o autenticación, para efectuar pagos o transacciones electrónicas, con el fin de realizar las operaciones señaladas en el literal anterior.

f) Usar maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, para transacciones electrónicas bloqueadas, en cualquiera de las formas señaladas en las letras precedentes.

g) Suplantar la identidad del titular o usuario frente al emisor, operador o comercio afiliado, según corresponda, para obtener la autorización que sea requerida para realizar transacciones.

Asimismo, incurrirá en el delito y sanciones que establece este artículo el que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas.”.

La **diputada Sofía Cid** pregunta si la figura de autofraude con daño o perjuicio al emisor se considera o no dentro del texto propuesto.

La señora **Michele Labbé** comenta que este artículo no tiene cambios. Agrega que las figuras que se han descrito incluyen la acción de terceros o del propio cliente o tarjetahabiente, así por ejemplo el uso malicioso de la tarjeta incluye el uso malicioso de la propia tarjeta por el tarjetahabiente.

El **diputado Pedro Velásquez** recuerda que la PDI mencionaba que se identificaba a personas que portaban una cantidad considerable de tarjetas, pero como no estaba tipificado no se podía hacer nada y al parecer ese caso no se considera en este artículo.

La señora **Michelle Labbé** señala que esto es totalmente nuevo, son tipos penales que no existían y por eso la PDI no podía actuar en esos casos y estas son acciones que ayudan a materializar el delito.

La **asesora del Ministerio de Economía, señorita Ximena Contreras**, explica que esta tipificación establece ciertos tipos que deben ser presentados por los fiscales una vez advertido que hay una persona con un maletín lleno de tarjetas, eso es lo que hay que hacer calzar dentro del tipo y el solo portar no es un delito, sino que debe establecerse dentro de la figura penal.

Puesta en votación, se **aprueba** por unanimidad. Votan la diputada Cid y los diputados Barrera, Bernales, Garín, Jürgensen, Miguel Mellado, Naranjo, Sepúlveda, Silber, Van Rysselberghe y Pedro Velásquez. (11x0x0).

***

Título IV

De la investigación y sanción de los delitos

Artículo 8º.-(nuevo) Cuando la investigación de alguno de los delitos penados por esta Ley lo hiciere imprescindible y existieren fundadas sospechas, basadas en hechos determinados, de la participación en una asociación ilícita, o en una agrupación u organización conformada por dos o más personas, destinada a cometer estos ilícitos, el Ministerio Público podrá aplicar las técnicas investigativas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas, y siempre que cuente con autorización judicial.

De igual forma, cumpliéndose las mismas condiciones establecidas en el inciso anterior, el Ministerio Público, y siempre que cuente con autorización judicial, podrá utilizar las técnicas especiales de investigación consistentes en entregas vigiladas y controladas, el uso de agentes encubiertos e informantes, en la forma regulada por los artículos 23 y 25 de la Ley N° 20.000, siempre que fuere necesario para lograr el esclarecimiento de los hechos, establecer la identidad y la participación de personas determinadas en éstos, conocer sus planes, prevenirlos y comprobarlos.

Los resultados de las técnicas especiales de investigación establecidas en este artículo no podrán ser utilizados como medios de prueba en el procedimiento cuando ellos hubieren sido obtenidos fuera de los casos o sin haberse cumplido los requisitos que autorizan su procedencia.”.

La señora **Michele Labbé** precisa que este es un artículo nuevo, a propuesta del Banco Central, en que una vez establecidos los tipos anteriores se permite la persecución de los infractores.

Puesta en votación, se **aprueba** por unanimidad. Votan los diputados Barrera, Bernales, diputada Cid, Garín, Jürgensen, Miguel Mellado, Naranjo, Sepúlveda, Silber, van Rysselberghe y Pedro Velásquez. (10x0x0).

***

“Artículo 9º.- (nuevo) Las penas establecidas en el artículo 7° de la Ley se aplicarán sin perjuicio de las eventuales sanciones que también corresponda aplicar por los delitos contemplados en la Ley N° 19.223, o aquella que las modifique, reemplace o sustituya en materia de delitos informáticos o ciberdelincuencia.

La señora **Michele Labbé** expresa que la idea es sancionar a quien oculte o disimule el origen ilícito de bienes que provienen de la perpetración de los delitos descritos en los artículos anteriores.

Puesta en votación, se **aprueba** por unanimidad. Votan la diputada Cid y los diputados Barrera, Bernales, Garín, Jürgensen, Miguel Mellado, Naranjo, Sepúlveda, Silber, Van Rysselberghe y Pedro Velásquez. (11x0x0).

***

Indicación presentada por la y los diputados Sofía Cid, Boris Barrera, Alejandro Bernales; Renato Garín, Harry Jürgensen, Miguel Mellado, Jaime Naranjo,

Alexis Sepúlveda y Enrique van Rysselberghe, para incorporar un artículo 2º, nuevo al texto:

Artículo segundo. - Intercalase en la letra a) del inciso primero del artículo 27 de la Ley 19.913, luego de la expresión “en relación con el inciso final del artículo 467 del Código Penal” lo siguiente: “; el artículo 7° de la Ley N° 20.009”.”.

La **señora Michele Labbé** indica que esta es una referencia adicional para la persecución por lavado de activos. Así, acerca del banco que recibe depósitos y respecto de los cuales no hay una fuente de origen que sean conocidos, la Unidad de Análisis Financiero investiga de inmediato de donde provienen esos recursos y de inmediato se procede a la comprobación del lavado de activos.

Puesta en votación, se **aprueba** por unanimidad. Votan la diputada Cid y los diputados Barrera, Bernales, Garín, Jürgensen, Miguel Mellado, Naranjo, Sepúlveda, Silber, Van Rysselberghe y Pedro Velásquez. (11x0x0).

VI. ARTÍCULOS E INDICACIONES RECHAZADAS POR LA COMISIÓN.

El **artículo único** del texto aprobado por el Senado:

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

2) Antepónese al artículo 1°, el siguiente epígrafe:

“Título I
Del ámbito de aplicación y reglas generales”

3) Reemplázanse los artículos 1º, 2º, 3° y 4°, por los siguientes:

“Artículo 1º.- Ámbito de aplicación. La presente ley regula el régimen de responsabilidad aplicable en los casos de extravío, hurto, robo o fraude de tarjetas de crédito, tarjetas de débito, tarjetas de pago con provisión de fondos, o cualquier otro sistema similar, en adelante conjuntamente, las “tarjetas de pago”, emitidas y operadas por entidades sujetas a la fiscalización de la Superintendencia de Bancos e Instituciones Financieras y a la regulación del Banco Central de Chile. También regula el régimen de responsabilidad en los casos de extravío, hurto, robo o fraude de tarjetas de pago emitidas y operadas por entidades no sujetas a la fiscalización y regulación de los organismos indicados, salvo disposición expresa en contrario.

Asimismo, se aplicará a los fraudes en “transacciones electrónicas”. Para efectos de esta ley, se entenderá por tales aquellas operaciones realizadas por medios electrónicos que originen cargos y abonos o giros de dinero en cuentas corrientes bancarias, cuentas de depósitos a la vista, cuentas de provisión de fondos, tarjetas de pago u otros sistemas similares, tales como instrucciones de cargo en cuentas propias para abonar cuentas de terceros, incluyendo pagos y cargos automáticos, transferencias electrónicas de fondos, avances en efectivo, giros de dinero en cajeros automáticos y demás operaciones electrónicas contempladas en el contrato de prestación de servicios financieros respectivo. Se comprenden dentro de este concepto las transacciones efectuadas mediante portales web u otras plataformas electrónicas, informáticas o telefónicas dispuestas por la empresa bancaria o el proveedor del servicio financiero correspondiente.

Los plazos de días hábiles que establece esta ley no considerarán los sábados, domingos ni festivos.

Artículo 2º.- Los titulares o usuarios de tarjetas de pago o de cualquier otro sistema similar podrán limitar su responsabilidad, derivada de la utilización de los mismos, en los términos establecidos por esta ley, en caso de hurto, robo o extravío de la tarjeta de pago, dando aviso oportuno al emisor.

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

Las tarjetas de pago respecto de las que el titular o usuario haya dado aviso de extravío, hurto, robo o fraude deberán ser bloqueadas de inmediato por el emisor.

Artículo 3º.- En el caso que las tarjetas de pago sean utilizadas con posterioridad al aviso de extravío, hurto, robo o fraude, el emisor será responsable de tales transacciones y sus consecuencias económicas en virtud de lo señalado en el inciso final del artículo anterior.

Las cláusulas de los contratos que impongan el deber de prueba sobre el titular o usuario, por operaciones realizadas con posterioridad al aviso de extravío, hurto, robo o fraude, se tendrán por no escritas.

Artículo 4º.- El titular o usuario de tarjetas de pago o servicios similares no tendrá responsabilidad por las operaciones realizadas con posterioridad al aviso de extravío, hurto o robo dado al emisor, sin perjuicio de la responsabilidad penal que corresponda.

Tratándose de las operaciones anteriores a dicho aviso, el titular o usuario deberá reclamar al emisor aquellas que desconoce su autorización, en el mismo acto del aviso o hasta cinco días hábiles siguientes a su expedición.

En los casos de fraude, se aplicará lo dispuesto en los artículos 5° y siguientes.”.

4) Incorpórase, a continuación del artículo 4°, el siguiente epígrafe:

“Título II
De la responsabilidad por uso fraudulento de tarjetas de pago”

5) Sustitúyese el artículo 5º, por el siguiente:

“Artículo 5º.- Las conductas que a continuación se señalan constituyen delito de uso fraudulento de tarjetas de pago y se sancionarán con la pena de presidio menor en su grado medio a máximo y multa correspondiente al triple del monto defraudado:

a) Falsificar tarjetas de pago.

b) Usar, vender, exportar, importar o distribuir tarjetas de pago falsificadas o sustraídas.

c) Negociar, en cualquier forma, tarjetas de pago falsificadas o sustraídas.

d) Usar, vender, exportar, importar o distribuir los datos o el número de tarjetas de pago, haciendo posible que terceros realicen pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de las mismas.

e) Negociar, en cualquier forma, con los datos o el número de tarjetas de pago, para fines de realizar las operaciones señaladas en el literal anterior.

f) Usar maliciosamente una tarjeta de pago bloqueada, en cualquiera de las formas señaladas en las letras precedentes.

g) Suplantar la identidad del titular o usuario frente al emisor, operador o comercio afiliado para obtener autorización para realizar transacciones con una tarjeta de pago.

Asimismo, incurrirá en el delito y sanciones que establece este artículo el que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas.

La pena señalada en el inciso primero aumentará en un grado, si cualquiera de las conductas tipificadas en este artículo produce perjuicio a terceros.”.

6) Agrégase el siguiente artículo 6º:

“Artículo 6º.- En los casos a que se refiere el artículo anterior, el titular o usuario no será responsable por las operaciones realizadas con posterioridad al aviso de fraude dado al emisor por las mismas vías establecidas para estos efectos en la presente ley, ni por aquellas operaciones que desconozca haber autorizado efectuadas con anterioridad al aviso de fraude que el titular o usuario reclame dentro de los treinta días corridos siguientes a la expedición de dicho aviso o que haya tenido conocimiento de ellas. Para estos efectos, y en relación con el conocimiento de la existencia de operaciones no autorizadas, se considerará especialmente la circunstancia que el emisor u operador haya enviado una alerta de fraude y que exista constancia de su recepción por parte del titular o usuario.

En los casos en que el titular o usuario desconozca haber autorizado una operación, corresponderá al emisor u operador demostrar que la operación fue autorizada por el titular o usuario y registrada con exactitud.

El registro de la utilización de las tarjetas de pago no bastará, necesariamente, para demostrar que la operación fue autorizada por el titular o usuario, ni que éste actuó de manera fraudulenta o con negligencia inexcusable. En todo caso, cuando el titular o usuario tome conocimiento de alguna de las conductas del artículo anterior deberá dar cuenta al emisor en los términos señalados en el inciso primero.

En ningún caso se aplicará la exención de responsabilidad señalada, si se prueba que el titular o usuario tuvo participación en los delitos descritos en el artículo 5°, que obtuvo un provecho ilícito o que actuó con dolo o negligencia inexcusable facilitando su comisión.

El titular o usuario soportará el total de las pérdidas que afronte como consecuencia de operaciones que sean fruto de su actuación fraudulenta.”.

7) Incorpórase, a continuación del artículo 6º, el siguiente epígrafe:

“Título III
De la cancelación de cargos o restitución de fondos”

8) Agréganse los siguientes artículos 7° y 8°:

“Artículo 7º.- El emisor u operador de las tarjetas de pago deberá proceder a la cancelación de los cargos o la restitución de los fondos correspondientes a las operaciones realizadas con posterioridad al aviso de extravío, hurto, robo o fraude, o de aquellas

operaciones cuya autorización ha sido desconocida por el titular o usuario dentro de los tres días hábiles siguientes a dicho aviso.

Sólo si se acredita por sentencia firme o ejecutoriada que el titular o usuario ha participado en la comisión del delito, que obtuvo un provecho ilícito o que actuó con dolo o negligencia inexcusable facilitando su comisión, se procederá a dejar sin efecto la cancelación de los cargos o la restitución de fondos, sin perjuicio de las indemnizaciones que correspondan según la legislación y normativa aplicable.

Artículo 8º.- Los emisores y operadores de tarjetas de pago, los comercios y otros establecimientos afiliados a un sistema de tarjetas de pago, así como las demás entidades que intervengan o presten servicios asociados a pagos y transacciones electrónicas, deberán adoptar las medidas de seguridad necesarias para prevenir la comisión de los ilícitos descritos en esta ley, conforme a la legislación y normativa que les resulte aplicable, y resguardando la prestación segura del servicio en los términos señalados por el artículo 23 de la ley N° 19.496. La falta o deficiencia de tales medidas será considerada para la determinación de las responsabilidades correspondientes a cada uno de ellos.”.”.

****

No hubo indicaciones rechazadas.

VII. INDICACIONES DECLARADAS INADMISIBLES.

No hubo.

VIII. MENCIÓN DE ADICIONES Y ENMIENDAS QUE LA COMISIÓN APROBÓ EN LA DISCUSIÓN PARTICULAR.

De conformidad a lo establecido en el N° 7° del artículo 304 del Reglamento de la Corporación, la Comisión dejó constancia que introdujo las siguientes enmiendas al texto propuesto por el Senado:

Artículo único, que ha pasado a ser artículo 1.

N 1)

Ha reemplazado la denominación de la ley por la siguiente: “Establece un régimen de limitación de responsabilidad para emisores y titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude.”.

***

N°s 2), 3), 4), 5), 6), 7) y 8)

Han sido reemplazados por el siguiente N°2)

2) Reemplázase los artículos 1º al 8º por los siguientes:

Título I

Del ámbito de aplicación y reglas generales

Artículo 1º.- La presente ley, en adelante la “Ley”, regula el régimen de responsabilidad aplicable en los casos de extravío, hurto, robo o fraude de tarjetas de crédito, tarjetas de débito, tarjetas de pago con provisión de fondos, o cualquier otro sistema similar, en adelante conjuntamente, las “tarjetas de pago”, emitidas y operadas por entidades sujetas a la fiscalización de la Comisión para el Mercado Financiero y a la regulación del Banco Central de Chile, en relación con el respectivo giro de emisión u operación de dichos instrumentos. También regula el régimen de responsabilidad en los casos de extravío, hurto, robo o fraude de

tarjetas de pago emitidas y operadas por entidades no sujetas a la fiscalización y regulación de los organismos indicados, salvo disposición expresa en contrario.

Asimismo, se aplicará a los fraudes en transacciones electrónicas. Para efectos de la Ley, se entenderá por tales aquellas operaciones realizadas por medios electrónicos que originen cargos y abonos o giros de dinero en cuentas corrientes bancarias, cuentas de depósitos a la vista, cuentas de provisión de fondos, tarjetas de pago u otros sistemas similares, tales como instrucciones de cargo en cuentas propias para abonar cuentas de terceros, incluyendo pagos y cargos automáticos, transferencias electrónicas de fondos, avances en efectivo, giros de dinero en cajeros automáticos y demás operaciones electrónicas contempladas en el contrato de prestación de servicios financieros respectivo. Se comprenden dentro de este concepto las transacciones efectuadas mediante portales web u otras plataformas electrónicas, informáticas, telefónicas o cualquier otro sistema similar dispuesto por la empresa bancaria o el proveedor del servicio financiero correspondiente.

Para efectos de la Ley, las tarjetas de pago y sistemas de transacciones electrónicas, podrán referirse en forma conjunta como “medios de pago”.

Los plazos de días hábiles que establece esta ley no considerarán los sábados, domingos ni festivos u otros que no correspondan a días hábiles bancarios conforme a lo previsto en el artículo 38 de la Ley General de Bancos.

Artículo 2º.- Los titulares o usuarios de medios de pago, así como los titulares de otras cuentas o sistemas similares que permitan efectuar transacciones electrónicas, en adelante referidos en forma conjunta como los “usuarios”, podrán limitar su responsabilidad, en los términos establecidos por la Ley, en caso de hurto, robo, extravío o fraude, dando aviso oportuno al emisor.

El emisor o prestador del servicio financiero de pagos electrónicos de dichos medios de pago, en adelante, referidos en forma conjunta como los “emisores”, deberá proveer al usuario, todos los días del año, las 24 horas del día, de canales o servicios de comunicación, de acceso gratuito y permanente, que permitan efectuar 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, código de recepción o identificador de seguimiento; y la fecha y hora del aviso; procediendo de inmediato al bloqueo respectivo del medio de pago, en lo referido a su funcionalidad para efectuar pagos o transacciones electrónicas.

Además, deberá enviar al usuario una comunicación por escrito con la información a que se refiere el inciso anterior, de la manera más expedita. En todo caso, el incumplimiento de esta obligación no afectará la validez o eficacia del aviso recibido.

En todo caso, y bajo su responsabilidad, el emisor podrá encomendar a un operador de medios de pago la provisión de estos canales o servicios de comunicación, así como la realización, en su representación, de las constancias de recepción o bloqueos que procedan.

Artículo 3º.- En el caso que los medios de pago a que se refiere esta Ley sean utilizados con posterioridad al aviso de extravío, hurto, robo o fraude, el emisor será responsable de tales operaciones y sus consecuencias económicas, en virtud de lo señalado en el artículo anterior.

Por ende, el usuario del respectivo medio de pago quedará liberado de responsabilidad por estos conceptos, sin perjuicio de la responsabilidad penal que pudiere corresponderle con motivo del extravío, hurto, robo o fraude respectivo.

Las cláusulas de los contratos que impongan el deber de prueba sobre el usuario, por operaciones realizadas con posterioridad al aviso de extravío, hurto, robo o fraude, no producirán efecto alguno y se tendrán por no escritas.

Artículo 4º.- Tratándose de operaciones anteriores al aviso a que se refiere el artículo 2° de esta ley, el usuario deberá reclamar al emisor aquellas operaciones respecto de

las cuales desconoce haber otorgado su autorización o consentimiento, en el mismo acto del aviso o hasta cinco días hábiles siguientes a su expedición.

El reclamo solo podrá abarcar operaciones incluidas e individualizadas en la facturación del último estado de cuenta mensual y en todo caso, siempre que no hayan transcurrido más de 30 días desde la fecha de notificación de dicho estado, efectuada en la oportunidad y por los medios pactados al efecto en el contrato de prestación de servicios financieros correspondiente.

En caso de no corresponder el envío de un estado de cuenta, o no encontrarse una o más operaciones no autorizadas incluidas en el último estado de cuenta remitido, el usuario que tenga conocimiento de las mismas por otras vías de información provistas por el emisor podrá igualmente desconocer su autorización, en la medida que su materialización o registro no sea anterior a 30 días contados desde el aviso efectuado por el usuario.

Sin perjuicio de lo anterior, tratándose de operaciones previas al aviso, pero que sean facturadas en un estado de cuenta mensual posterior a dicho aviso, igualmente podrán ser reclamadas en el plazo máximo de 30 días desde la emisión y entrega de dicho estado.

En relación con el conocimiento de la existencia de operaciones no autorizadas, se considerará especialmente la circunstancia que el emisor haya enviado una alerta de fraude al usuario, identificando las operaciones sospechosas, y que exista constancia de su recepción por parte del usuario, conforme al contrato de prestación de servicios financieros correspondiente.

Tan pronto el usuario tome conocimiento de la existencia de operaciones no autorizadas, deberá otorgar el aviso correspondiente conforme a lo previsto en el artículo 2° de esta Ley, salvo en caso de encontrarse impedido por razones de fuerza mayor o caso fortuito, situación bajo la cual deberá efectuar el aviso respectivo dentro del plazo máximo de 5 días hábiles contado desde que se encuentre en condiciones de expedirlo.

En los casos en que el usuario desconozca haber autorizado una operación, corresponderá al emisor demostrar que la operación fue autorizada por el usuario y que se encuentra registrada a su nombre o respecto del instrumento de pago o cuenta correspondiente.

El registro de dichas operaciones no bastará, necesariamente, para demostrar que la operación fue autorizada por el usuario, ni que éste actuó de manera fraudulenta o con negligencia inexcusable.

Título II

De la cancelación de cargos o restitución de fondos

Artículo 5º.- El emisor deberá proceder a la cancelación provisional de los cargos o a la restitución provisional de los fondos correspondientes a las operaciones realizadas con anterioridad al aviso de extravío, hurto, robo o fraude, tratándose de operaciones cuya autorización ha sido desconocida por el usuario, dentro de los siete días hábiles siguientes al reclamo. Tratándose de estas operaciones, la restitución provisional de fondos podrá estar afecta a un deducible máximo equivalente a cero coma cinco unidades de fomento de cargo del usuario, para el total de las operaciones que puedan ser desconocidas en relación al aviso a que se refiere el artículo 2° de esta Ley.

En todo caso, el emisor estará impedido de ofrecer a los usuarios la contratación de seguros cuya cobertura corresponda a riesgos o siniestros y de cobrar comisiones que el mismo deba asumir conforme a esta Ley. Lo anterior, es sin perjuicio de los seguros que el emisor pueda contratar en calidad de beneficiario, a su cargo.

Sólo si se acredita por sentencia firme o ejecutoriada que el usuario ha participado en la comisión del delito, que obtuvo un provecho ilícito o que actuó con dolo o negligencia inexcusable facilitando su comisión, se procederá a dejar sin efecto la cancelación de los cargos o la restitución de fondos, sin perjuicio de las indemnizaciones que correspondan según la legislación y normativa aplicable.

Artículo 6º.- Los emisores, operadores, comercios y otros establecimientos afiliados a un sistema de tarjetas de pago, así como las demás entidades que intervengan o presten servicios asociados a pagos y transacciones electrónicas, u otros sistemas de características similares, deberán adoptar las medidas de seguridad necesarias para prevenir la comisión de los ilícitos descritos en esta Ley conforme a la legislación y normativa que les resulte aplicable, y resguardando la prestación segura del respectivo servicio en los términos señalados por el artículo 23 de la ley N° 19.496.

En el caso de los emisores u operadores, según corresponda, dichas medidas de seguridad deberán considerar, al menos, lo siguiente:

a) Contar con sistemas de monitoreo, que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual del usuario.

b) Implementar procedimientos internos para gestionar las alertas generadas por dichos sistemas de monitoreo.

c) Identificar patrones de potenciales fraude, conforme a las prácticas de la industria y recomendaciones, los que deberán incorporarse al sistema de monitoreo de operaciones.

d) Establecer límites y controles en los diversos canales de atención, que permitan mitigar las pérdidas por fraude. Los referidos límites y controles deberán basarse en consideraciones de riesgo objetivas, generales y no discriminatorias, en relación con la naturaleza del medio de pago y la clase de operaciones que permita efectuar.

El órgano fiscalizador competente a través de la normativa que dicte, recomendara lo señalado en las letras a), b), c) y d) respecto de los emisores sujetos a su supervisión.

La falta o deficiencia de tales medidas será considerada para la determinación de las responsabilidades correspondientes a cada uno de ellos, que pudiere perseguir en su contra el usuario u otro afectado.

Lo indicado, es sin perjuicio de la posibilidad que los emisores puedan perseguir el cumplimiento de la obligación de restitución o reembolso que corresponda, por cancelaciones de cargos o devoluciones de fondos, en base a los estándares y procedimientos de seguridad exigibles a cada una de las entidades antes indicadas, de conformidad con la Ley, las demás leyes y regulaciones aplicables, teniendo presente los términos y condiciones contractuales que los vinculen, en cada caso.

Título III

De la responsabilidad por fraude en tarjetas de pago y transacciones electrónicas.

Artículo 7º.- Las conductas que a continuación se señalan constituyen delito de uso fraudulento de tarjetas de pago y transacciones electrónicas; y se sancionarán con la pena de presidio menor en su grado medio a máximo y multa correspondiente al triple del monto defraudado:

a) Falsificar tarjetas de pago.

b) Usar, vender, exportar, importar o distribuir tarjetas de pago falsificadas o sustraídas.

c) Negociar, en cualquier forma, tarjetas de pago falsificadas o sustraídas.

d) Usar, vender, exportar, importar o distribuir los datos o el número de tarjetas de pago, haciendo posible que terceros realicen pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de las mismas.

e) Negociar, en cualquier forma, con los datos, el número de tarjetas de pago, y claves o demás credenciales de seguridad o autenticación, para efectuar pagos o transacciones electrónicas, con el fin de realizar las operaciones señaladas en el literal anterior.

f) Usar maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, para transacciones electrónicas bloqueadas, en cualquiera de las formas señaladas en las letras precedentes.

g) Suplantar la identidad del titular o usuario frente al emisor, operador o comercio afiliado, según corresponda, para obtener la autorización que sea requerida para realizar transacciones.

Asimismo, incurrirá en el delito y sanciones que establece este artículo el que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas.

Título IV

De la investigación y sanción de los delitos

Artículo 8º.- Cuando la investigación de alguno de los delitos penados por esta Ley lo hiciere imprescindible y existieren fundadas sospechas, basadas en hechos determinados, de la participación en una asociación ilícita, o en una agrupación u organización conformada por dos o más personas, destinada a cometer estos ilícitos, el Ministerio Público podrá aplicar las técnicas investigativas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas, y siempre que cuente con autorización judicial.

De igual forma, cumpliéndose las mismas condiciones establecidas en el inciso anterior, el Ministerio Público, y siempre que cuente con autorización judicial, podrá utilizar las técnicas especiales de investigación consistentes en entregas vigiladas y controladas, el uso de agentes encubiertos e informantes, en la forma regulada por los artículos 23 y 25 de la Ley N° 20.000, siempre que fuere necesario para lograr el esclarecimiento de los hechos, establecer la identidad y la participación de personas determinadas en éstos, conocer sus planes, prevenirlos y comprobarlos.

Los resultados de las técnicas especiales de investigación establecidas en este artículo no podrán ser utilizados como medios de prueba en el procedimiento cuando ellos hubieren sido obtenidos fuera de los casos o sin haberse cumplido los requisitos que autorizan su procedencia.

Artículo 9º.- Las penas establecidas en el artículo 7° de la Ley se aplicarán sin perjuicio de las eventuales sanciones que también corresponda aplicar por los delitos contemplados en la Ley N° 19.223, o aquella que las modifique, reemplace o sustituya en materia de delitos informáticos o ciberdelincuencia.

***

Artículo 2º, nuevo.

Ha incorporado el siguiente artículo 2º, nuevo:

Artículo segundo. - Intercálase en la letra a) del inciso primero del artículo 27 de la ley N° 19.913, luego de la expresión “en relación al inciso final del artículo 467 del Código Penal” lo siguiente: “; el artículo 7° de la ley N° 20.009”.”.

IX. TEXTO DEL PROYECTO DE LEY TAL COMO QUEDARÍA EN VIRTUD DE LOS ACUERDOS ADOPTADOS POR LA COMISIÓN.

PROYECTO DE LEY

"**Artículo 1.** Introdúcense las siguientes modificaciones en 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:

1. Sustitúyese la denominación de la ley por la siguiente: "Establece un régimen de limitación de responsabilidad para emisores y titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude.".

2. Reemplázanse los artículos 1º.- al 8º.-, por los siguientes:

Título I

Del ámbito de aplicación y reglas generales

Artículo 1º.- La presente ley, en adelante la "ley", regula el régimen de responsabilidad aplicable en los casos de extravío, hurto, robo o fraude de tarjetas de crédito, tarjetas de débito, tarjetas de pago con provisión de fondos, o cualquier otro sistema similar, en adelante conjuntamente, las "tarjetas de pago", emitidas y operadas por entidades sujetas a la fiscalización de la Comisión para el Mercado Financiero y a la regulación del Banco Central de Chile, en relación con el respectivo giro de emisión u operación de dichos instrumentos. También regula el régimen de responsabilidad en los casos de extravío, hurto, robo o fraude de tarjetas de pago emitidas y operadas por entidades no sujetas a la fiscalización y regulación de los organismos indicados, salvo disposición expresa en contrario.

Asimismo, se aplicará a los fraudes en transacciones electrónicas. Para efectos de la ley, se entenderá por tales aquellas operaciones realizadas por medios electrónicos que originen cargos y abonos o giros de dinero en cuentas corrientes bancarias, cuentas de depósitos a la vista, cuentas de provisión de fondos, tarjetas de pago u otros sistemas similares, tales como instrucciones de cargo en cuentas propias para abonar cuentas de terceros, incluyendo pagos y cargos automáticos, transferencias electrónicas de fondos, avances en efectivo, giros de dinero en cajeros automáticos y demás operaciones electrónicas contempladas en el contrato de prestación de servicios financieros respectivo. Se comprenden dentro de este concepto las transacciones efectuadas mediante portales web u otras plataformas electrónicas, informáticas, telefónicas o cualquier otro sistema similar dispuesto por la empresa bancaria o el proveedor del servicio financiero correspondiente.

Para efectos de la ley, las tarjetas de pago y sistemas de transacciones electrónicas, podrán referirse en forma conjunta como "medios de pago".

Los plazos de días hábiles que establece esta ley no considerarán los sábados, domingos ni festivos u otros que no correspondan a días hábiles bancarios, conforme a lo previsto en el artículo 38 de la Ley General de Bancos.

Artículo 2º.- Los titulares o usuarios de medios de pago, así como los titulares de otras cuentas o sistemas similares que permitan efectuar transacciones electrónicas, en adelante referidos en forma conjunta como los "usuarios", podrán limitar su responsabilidad, en los términos establecidos por la ley, en caso de hurto, robo, extravío o fraude, dando aviso oportuno al emisor.

El emisor o prestador del servicio financiero de pagos electrónicos de dichos medios de pago, en adelante, referidos en forma conjunta como los "emisores", deberá proveer al usuario, todos los días del año, las 24 horas del día, de canales o

servicios de comunicación, de acceso gratuito y permanente, que permitan efectuar 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, código de recepción o identificador de seguimiento; y la fecha y hora del aviso; procediendo de inmediato al bloqueo respectivo del medio de pago, en lo referido a su funcionalidad para efectuar pagos o transacciones electrónicas.

Además, deberá enviar al usuario una comunicación por escrito con la información a que se refiere el inciso anterior, de la manera más expedita. En todo caso, el incumplimiento de esta obligación no afectará la validez o eficacia del aviso recibido.

En todo caso, y bajo su responsabilidad, el emisor podrá encomendar a un operador de medios de pago la provisión de estos canales o servicios de comunicación, así como la realización, en su representación, de las constancias de recepción o bloqueos que procedan.

Artículo 3º.- En el caso que los medios de pago a que se refiere esta ley sean utilizados con posterioridad al aviso de extravío, hurto, robo o fraude, el emisor será responsable de tales operaciones y sus consecuencias económicas, en virtud de lo señalado en el artículo anterior.

Por ende, el usuario del respectivo medio de pago quedará liberado de responsabilidad por estos conceptos, sin perjuicio de la responsabilidad penal que pudiere corresponderle con motivo del extravío, hurto, robo o fraude respectivo.

Las cláusulas de los contratos que impongan el deber de prueba sobre el usuario, por operaciones realizadas con posterioridad al aviso de extravío, hurto, robo o fraude, no producirán efecto alguno y se tendrán por no escritas.

Artículo 4º.- Tratándose de operaciones anteriores al aviso a que se refiere el artículo 2° de esta ley, el usuario deberá reclamar al emisor aquellas operaciones respecto de las cuales desconoce haber otorgado su autorización o consentimiento, en el mismo acto del aviso o hasta cinco días hábiles siguientes a su expedición.

El reclamo solo podrá abarcar operaciones incluidas e individualizadas en la facturación del último estado de cuenta mensual y en todo caso, siempre que no hayan transcurrido más de treinta días desde la fecha de notificación de dicho estado, efectuada en la oportunidad y por los medios pactados al efecto en el contrato de prestación de servicios financieros correspondiente.

En caso de no corresponder el envío de un estado de cuenta, o no encontrarse una o más operaciones no autorizadas incluidas en el último estado de cuenta remitido, el usuario que tenga conocimiento de las mismas por otras vías de información provistas por el emisor podrá igualmente desconocer su autorización, en la medida que su materialización o registro no sea anterior a treinta días contados desde el aviso efectuado por el usuario.

Sin perjuicio de lo anterior, tratándose de operaciones previas al aviso, pero que sean facturadas en un estado de cuenta mensual posterior a dicho aviso, igualmente podrán ser reclamadas en el plazo máximo de treinta días desde la emisión y entrega de dicho estado.

En relación con el conocimiento de la existencia de operaciones no autorizadas, se considerará especialmente la circunstancia que el emisor haya enviado una alerta de fraude al usuario, identificando las operaciones sospechosas, y que exista constancia de su recepción por parte del usuario, conforme al contrato de prestación de servicios financieros correspondiente.

Tan pronto el usuario tome conocimiento de la existencia de operaciones no autorizadas, deberá otorgar el aviso correspondiente conforme a lo previsto en el artículo 2° de esta ley, salvo en caso de encontrarse impedido por razones de fuerza mayor o caso fortuito, situación bajo la cual deberá efectuar el aviso respectivo dentro del plazo máximo de cinco días hábiles contado desde que se encuentre en condiciones de expedirlo.

En los casos en que el usuario desconozca haber autorizado una operación, corresponderá al emisor demostrar que la operación fue autorizada por el usuario y que se encuentra registrada a su nombre o respecto del instrumento de pago o cuenta correspondiente.

El registro de dichas operaciones no bastará, necesariamente, para demostrar que la operación fue autorizada por el usuario, ni que éste actuó de manera fraudulenta o con negligencia inexcusable.

Título II

De la cancelación de cargos o restitución de fondos

Artículo 5º. El emisor deberá proceder a la cancelación provisional de los cargos o a la restitución provisional de los fondos correspondientes a las operaciones realizadas con anterioridad al aviso de extravío, hurto, robo o fraude, tratándose de operaciones cuya autorización ha sido desconocida por el usuario, dentro de los siete días hábiles siguientes al reclamo. Tratándose de estas operaciones, la restitución provisional de fondos podrá estar afecta a un deducible máximo equivalente a cero coma cinco unidades de fomento de cargo del usuario, para el total de las operaciones que puedan ser desconocidas en relación al aviso a que se refiere el artículo 2° de esta ley.

En todo caso, el emisor estará impedido de ofrecer a los usuarios la contratación de seguros cuya cobertura corresponda a riesgos o siniestros y de cobrar comisiones que el mismo deba asumir conforme a esta ley. Lo anterior, es sin perjuicio de los seguros que el emisor pueda contratar en calidad de beneficiario, a su cargo.

Solo si se acredita por sentencia firme o ejecutoriada que el usuario ha participado en la comisión del delito, que obtuvo un provecho ilícito o que actuó con dolo o negligencia inexcusable facilitando su comisión, se procederá a dejar sin efecto la cancelación de los cargos o la restitución de fondos, sin perjuicio de las indemnizaciones que correspondan según la normativa aplicable.

Artículo 6º.- Los emisores, operadores, comercios y otros establecimientos afiliados a un sistema de tarjetas de pago, así como las demás entidades que intervengan o presten servicios asociados a pagos y transacciones electrónicas, u otros sistemas de características similares, deberán adoptar las medidas de seguridad necesarias para prevenir la comisión de los ilícitos descritos en esta ley conforme a la normativa que les resulte aplicable, y resguardando la prestación segura del respectivo servicio en los términos señalados por el artículo 23 de la ley N° 19.496.

En el caso de los emisores u operadores, según corresponda, dichas medidas de seguridad deberán considerar, al menos, lo siguiente:

a) Contar con sistemas de monitoreo, que tengan como objetivo detectar aquellas operaciones que no corresponden al comportamiento habitual del usuario.

b) Implementar procedimientos internos para gestionar las alertas generadas por dichos sistemas de monitoreo.

c) Identificar patrones de potenciales fraudes, conforme a las prácticas de la industria y recomendaciones, los que deberán incorporarse al sistema de monitoreo de operaciones.

d) Establecer límites y controles en los diversos canales de atención, que permitan mitigar las pérdidas por fraude. Los referidos límites y controles deberán basarse en consideraciones de riesgo objetivas, generales y no discriminatorias, en relación con la naturaleza del medio de pago y la clase de operaciones que permita efectuar.

El órgano fiscalizador competente a través de la normativa que dicte, recomendara lo señalado en las letras a), b), c) y d) respecto de los emisores sujetos a su supervisión.

La falta o deficiencia de tales medidas será considerada para la determinación de las responsabilidades correspondientes a cada uno de ellos, que pudiere perseguir en su contra el usuario u otro afectado.

Lo indicado, es sin perjuicio de la posibilidad que los emisores puedan perseguir el cumplimiento de la obligación de restitución o reembolso que corresponda, por cancelaciones de cargos o devoluciones de fondos, en base a los estándares y procedimientos de seguridad exigibles a cada una de las entidades antes indicadas, de conformidad con la ley, las demás regulaciones aplicables, teniendo presente los términos y condiciones contractuales que los vinculen, en cada caso.

Título III

De la responsabilidad por fraude en tarjetas de pago y transacciones electrónicas

Artículo 7º.- Las conductas que a continuación se señalan constituyen delito de uso fraudulento de tarjetas de pago y transacciones electrónicas; y se sancionarán con la pena de presidio menor en su grado medio a máximo y multa correspondiente al triple del monto defraudado:

a) Falsificar tarjetas de pago.

b) Usar, vender, exportar, importar o distribuir tarjetas de pago falsificadas o sustraídas.

c) Negociar, en cualquier forma, tarjetas de pago falsificadas o sustraídas.

d) Usar, vender, exportar, importar o distribuir los datos o el número de tarjetas de pago, haciendo posible que terceros realicen pagos, transacciones electrónicas o cualquier otra operación que corresponda exclusivamente al titular o usuario de las mismas.

e) Negociar, en cualquier forma, con los datos, el número de tarjetas de pago, y claves o demás credenciales de seguridad o autenticación, para efectuar pagos o transacciones electrónicas, con el fin de realizar las operaciones señaladas en el literal anterior.

f) Usar maliciosamente una tarjeta de pago o clave y demás credenciales de seguridad o autenticación, para transacciones electrónicas bloqueadas, en cualquiera de las formas señaladas en las letras precedentes.

g) Suplantar la identidad del titular o usuario frente al emisor, operador o comercio afiliado, según corresponda, para obtener la autorización que sea requerida para realizar transacciones.

Asimismo, incurrirá en el delito y sanciones que establece este artículo el que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro

sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas.

Título IV

De la investigación y sanción de los delitos

Artículo 8º.- Cuando la investigación de alguno de los delitos penados por esta ley lo hiciere imprescindible y existieren fundadas sospechas, basadas en hechos determinados de la participación en una asociación ilícita, o en una agrupación u organización conformada por dos o más personas, destinada a cometer estos ilícitos, el Ministerio Público podrá aplicar las técnicas investigativas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas, y siempre que cuente con autorización judicial.

De igual forma, cumpliéndose las mismas condiciones establecidas en el inciso anterior, el Ministerio Público, y siempre que cuente con autorización judicial, podrá utilizar las técnicas especiales de investigación consistentes en entregas vigiladas y controladas, el uso de agentes encubiertos e informantes, en la forma regulada por los artículos 23 y 25 de la ley N° 20.000, siempre que fuere necesario para lograr el esclarecimiento de los hechos, establecer la identidad y la participación de personas determinadas en éstos, conocer sus planes, prevenirlos y comprobarlos.

Los resultados de las técnicas especiales de investigación establecidas en este artículo no podrán ser utilizados como medios de prueba en el procedimiento cuando ellos hubieren sido obtenidos fuera de los casos o sin haberse cumplido los requisitos que autorizan su procedencia.

Artículo 9º.- Las penas establecidas en el artículo 7° de la ley se aplicarán sin perjuicio de las eventuales sanciones que también corresponda aplicar por los delitos contemplados en la ley N° 19.223, o aquella que las modifique, reemplace o sustituya en materia de delitos informáticos o ciberdelincuencia.

Artículo 2.- Intercálase en la letra a) del inciso primero del artículo 27 de la ley N° 19.913, luego de la frase “en relación al inciso final del artículo 467 del Código Penal” lo siguiente: “; el artículo 7° de la ley N° 20.009”.”.

SALA DE LA COMISIÓN, a 15 de enero de 2019.

Tratado y acordado en sesiones de fecha 13, 20 y 27 de noviembre, 10 y 18 de diciembre de 2018 y 15 de enero de 2019, con la asistencia de la y los diputados señores Boris Barrera, Alejandro Bernales, Sofía Cid, Renato Garín, Harry Jürgensen, Joaquín Lavín, Miguel Mellado, Jaime Naranjo, Rolando Rentería, Alexis Sepúlveda (Presidente), Gabriel Silber, Enrique Van Rysselberghe, y Pedro Velásquez.

Reemplazos temporales:

El diputado Barrera, don Boris fue reemplazado por el diputado Labra, don Amaro. (18.12.2018).

El diputado Jürgensen, don Harry fue reemplazado por el diputado Rey, don Hugo. (18.12.2018).



ALVARO HALABI DIUANA
Abogado Secretario de la Comisión