Proyecto de Ley que modifica Ley N°20.009, limitando la responsabilidad del usuario de tarjetas y otros medios en caso de fraude

Comisión de Economía, Fomento; Micro, Pequeña y Mediana Empresa; Protección de los Consumidores y Turismo

Joaquín Vial Ruiz-Tagle

Vice Presidente Banco Central de Chile

20 de noviembre de 2018

Las materias que aborda esta moción inciden en el objeto y competencias legales del BCCh

- Mandato Legal

  Velar por el **normal funcionamiento** de los **pagos** internos y externos

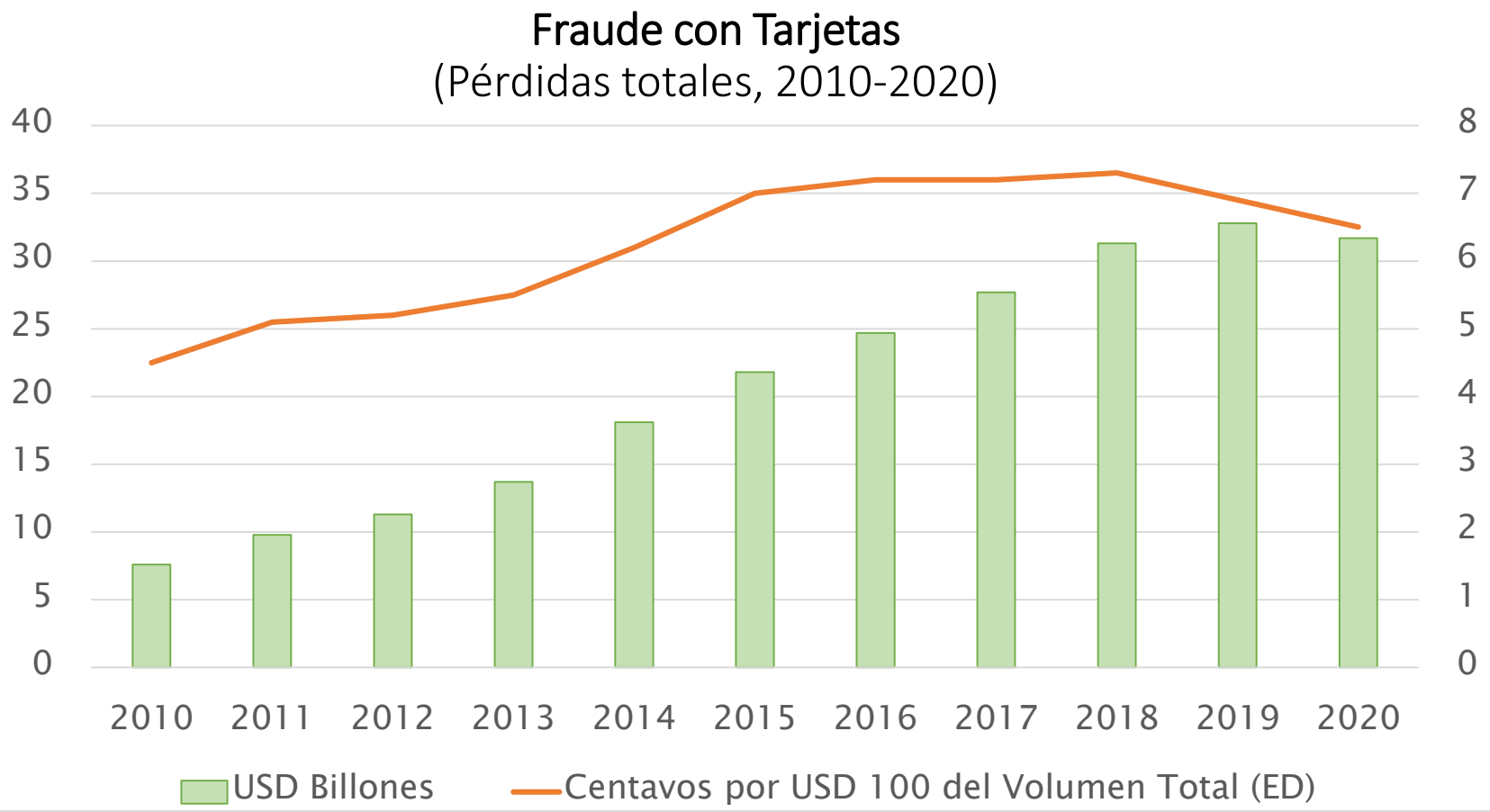
- Normas del Banco Central de Chile (BCCh) sobre Emisión y Operación de Tarjetas de Pago

  - Contienen referencias a seguridad de los medios de pago.
  - Fiscalización Superintendencia de Bancos (SBIF)

- Esta moción no altera la potestad normativa que la legislación le confiere al BCCh en esta materia (LOC del BCCh y Ley N° 20.950).

El fraude con tarjetas es una preocupación de los reguladores y de la industria a nivel internacional

El fraude a nivel global ha aumentado en los últimos años, pero la adopción de mejores estándares tecnológicos debiera contribuir a su mitigación



Fuente: Nilson Report (Octubre 2016)

Varias jurisdicciones contemplan una exención de responsabilidad a partir de ciertos umbrales

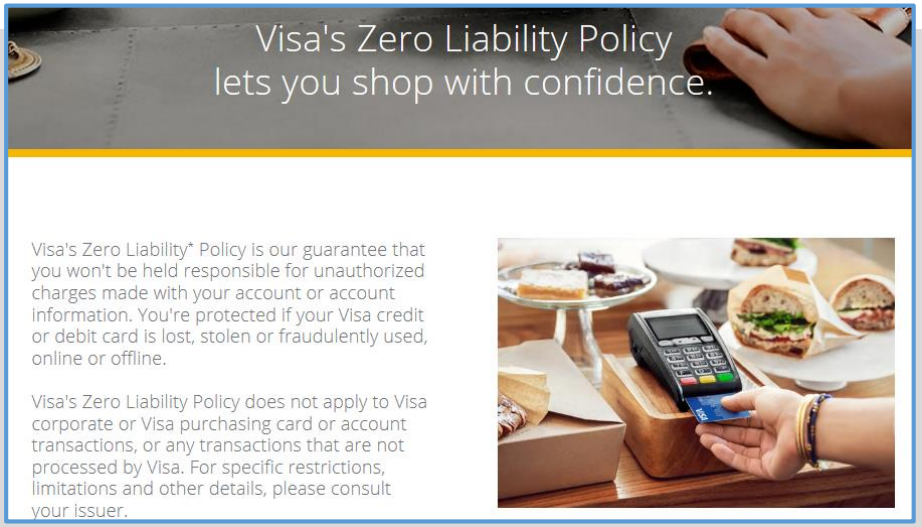
- Eximir a los usuarios de la responsabilidad por transacciones fraudulentas realizadas **después** de dar aviso de pérdida o extravío, como establece Ley N°20.009, es común a nivel internacional.
- Pero existen distintos niveles de protección a los consumidores frente a transacciones fraudulentas (no autorizadas) realizadas **antes** de dar aviso de pérdida.

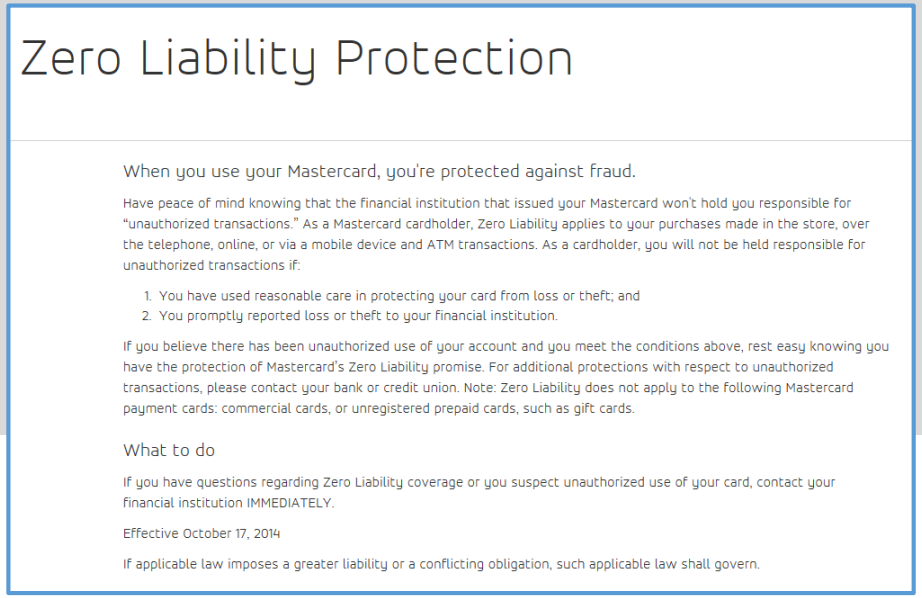
Unión Europea	Reino Unido	EE.UU.	Perú
Consumidor se exime de responsabilidad por transacciones no autorizadas superiores a **50 euros**	Consumidor se exime de responsabilidad por transacciones no autorizadas superiores a **35 libras** (Anexo 1)	Consumidor se exime de responsabilidad por transacciones no autorizadas superiores a **50 dólares**, monto que aumenta hasta **500 dólares** si no notificó al Emisor	Usuario no es responsable en caso de clonación de tarjetas o manipulación de cajeros automáticos.

Fuente: Elaboración propia

Las marcas internacionales de tarjetas han adoptado voluntariamente políticas de “zero liability”

- **“*Zero liability*”:** Bajo algunas condiciones, algunas marcas eximen a los usuarios de las transacciones no autorizadas.
- **“*Liability shifting*”:** entre emisores y adquirentes, la parte que tiene menores estándares de seguridad en sus productos asume las pérdidas de una transacción fraudulenta
- Otras obligaciones contractuales en materia de seguridad para todas las partes involucradas.





Es importante actualizar la Ley N°20.009, pues no aborda temas relevantes en la actualidad

- La Ley vigente regula lo que ocurre con las transacciones que se realizan **después del aviso de robo o pérdida de una tarjeta de crédito**, por lo que para una parte importante de las transacciones electrónicas no hay regulación.

	Notificación al Emisor	
Tipo de Transacción	Transacción anterior	Transacción posterior
Tarjetas de crédito	No regulado	**Regulado en Ley N°20.009**
Tarjetas de débito	No regulado	No regulado
Transferencias Electrónicas de Fondos	No regulado	No regulado
Giros en cajeros automáticos	No regulado	No regulado
Otros	No regulado	No regulado

Fuente: Elaboración propia

Análisis del PdL que modifica la Ley N°20.009

El BCCh presentó su opinión a esta moción parlamentaria en la Comisión de Economía del Senado el año pasado

- El BCCh manifestó una opinión positiva de esta iniciativa

- Elementos específicos comentados e incorporados:
  - Consistencia de definición con las contenidas en normativa del Banco Central
  - Pagos electrónicos en general
  - Reconocer el principio de que todos los actores involucrados en el sistema de pagos deben adoptar medidas de seguridad
  - Incorporar obligación del tarjetahabiente de informar al emisor las transacciones no reconocidas.
  - Fijar un plazo razonable para la restitución de fondos

En los últimos meses se publicó información sensible de tarjetas de crédito de emisores locales

- La información filtrada correspondía en su mayoría a tarjetas vencidas, y los emisores bloquearon las vigentes, dando aviso a sus clientes.

- 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 sólo de tarjetas). Algunos ejemplos:

Empresa	N° tarjetas afectadas	Año
Cathay Pacific	9,4 millones	2018
Home Depot	56 millones	2014
Target	40 millones	2013
Heartland Payment Systems	134 millones	2008

Fuente: Elaboración propia

¿Qué hubiera ocurrido en episodios recientes bajo marco legal propuesto?

- 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.

Posibles perfeccionamientos al PdL

- Se podrían incorporar más medidas para mitigar el riesgo moral:
  - El proyecto 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.
  - Establecer umbrales por sobre los cuales se haga efectiva la exención de responsabilidad, tal como existe en otros países.

Posibles perfeccionamientos al PdL

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

Posibles perfeccionamientos al PdL

- Las obligaciones del PdL son extensivas a las tarjetas “cerradas” (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 PdL , de manera que su ámbito de aplicación alcance efectivamente a todas las transacciones electrónicas (no sólo 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, es necesario asegurar consistencia legislativa entre este PdL y el de Ciberdelincuencia (**Anexo 2**).

Conclusiones

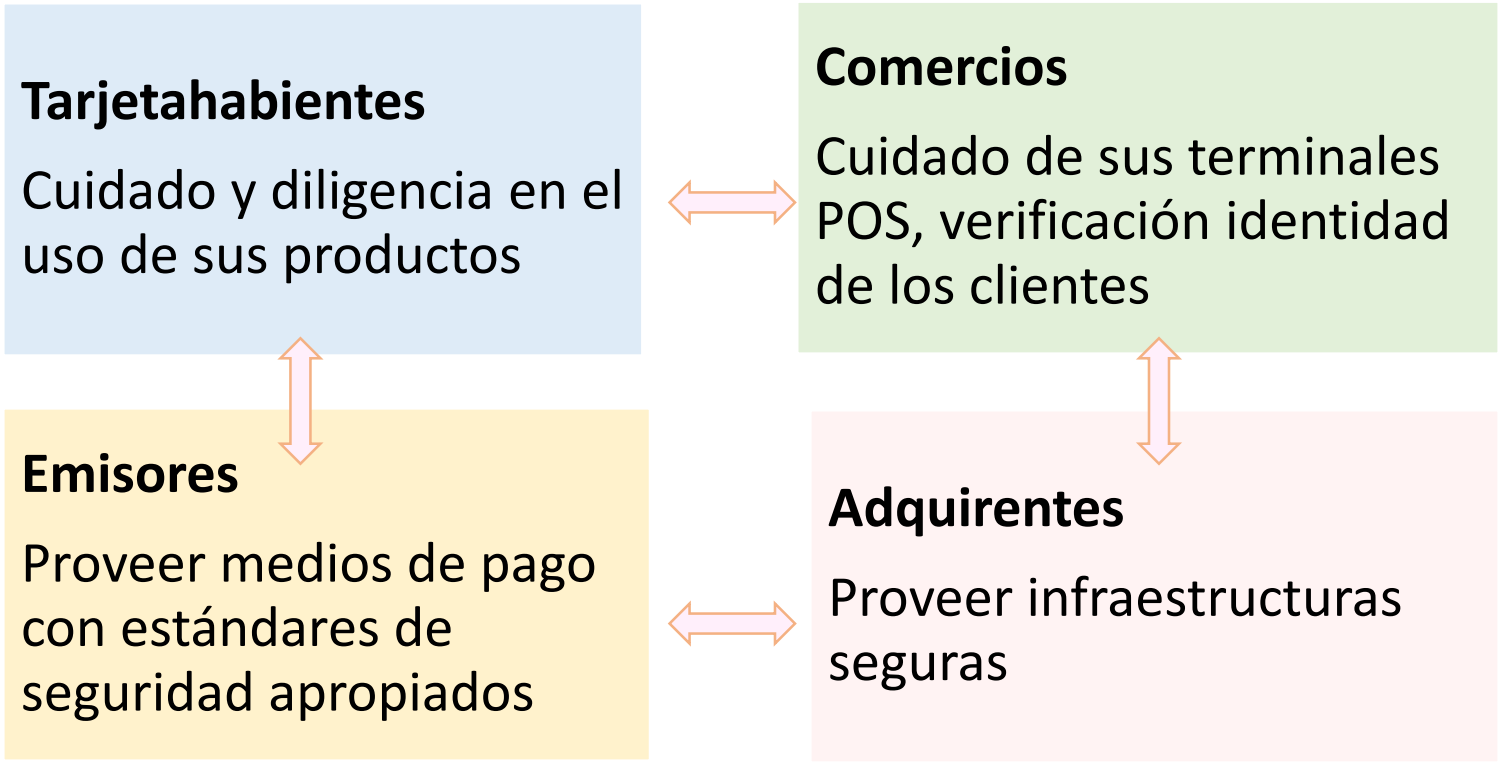
- La prevención del fraude es un esfuerzo permanente y requiere que todos los agentes involucrados en el sistema de pagos minoristas tengan incentivos correctos. Por ejemplo, para usar e incorporar tecnologías (emisores y operadores), y para tener un comportamiento diligente (comercios y usuarios).

- El BCCh valora positivamente esta moción parlamentaria y los perfeccionamientos que se le introdujeron durante el primer trámite.

- Chile tiene niveles relativamente bajos de fraude en tarjetas. Es importante que esa situación se mantenga y que esta moción parlamentaria contribuya a ello.

El buen funcionamiento del sistema de pagos minorista requiere que todos sus participantes tengan los incentivos adecuados

Participantes deben cumplir con medidas de seguridad para prevenir fraudes



Fuente: Elaboración propia

Proyecto de Ley que modifica Ley N°20.009, limitando la responsabilidad del usuario de tarjetas y otros medios en caso de fraude

Comisión de Economía, Fomento; Micro, Pequeña y Mediana Empresa; Protección de los Consumidores y Turismo

Joaquín Vial Ruiz-Tagle

VicePresidente Banco Central de Chile

20 de noviembre de 2018

Anexo 1: Nueva regulación de servicios de pago de Reino Unido (2017) – Reemplaza a la de 2009

http://www.legislation.gov.uk/uksi/2017/752/contents/made

- **Algunos elementos relevantes de esta nueva legislación:**
- La responsabilidad máxima del usuario se rebajó desde 50 a 35 libras, para transacciones no autorizadas derivadas de la pérdida o robo del instrumento de pago o de su apropiación indebida.
- Este umbral no aplica en caso que el usuario haya actuado en forma fraudulenta.
- El usuario debe resguardar sus credenciales de seguridad personalizadas referidas al instrumento de pago. Las otras exigencias ya existentes son emplear el medio de pago de acuerdo a las normas aplicables y notificar sin demora indebida los casos de pérdida o fraude.
- Incorpora criterios expresos relacionados con asignar responsabilidad a los miembros de la cadena de un sistema de pago.

Anexo 2: Relación con PdL que tipifica delitos relacionados con Ciberdelincuencia

1. Con fecha 25 de octubre de 2018, el Ejecutivo presentó un PdL que deroga la Ley 19.223 sobre delitos informáticos y modifica otros cuerpos legales para adecuar su regulación al Convenio de Budapest sobre Ciberdelincuencia.

2. Este PdL tipifica y sanciona un conjunto de figuras penales referidas a la afectación o intervención maliciosa de sistemas informáticos y datos informáticos. Entre ellas, se contempla el delito de abuso de dispositivos, establecido en el artículo 7 de esa iniciativa, que castiga de forma independiente ciertas conductas que sirven de medio para la comisión de otros delitos, dentro de los cuales se encuentran los previstos en el artículo 5° de la Ley 20.009, que esta moción sustituye.

3. Al respecto, y dada la interconexión que puede existir entre las figuras de fraude que sanciona el PdL de Ciberdelincuencia, con los ilícitos de la Ley 20.009, es importante velar por la debida coherencia entre ambas iniciativas, y analizar en su caso la posibilidad de extender las mejoras que el primer PdL incorpora en materia procesal y en cuanto a técnicas especiales de investigación.

Referencias

- Estados Unidos: Fair Credit Billing Act (FCBA) y Electronic Fund Transfer Act (EFTA)
- Perú: Reglamento de Tarjetas de Crédito y Débito (Resolución SBS N°6523-2013).
- Reino Unido: http://www.legislation.gov.uk/uksi/2017/752/contents/made
- Unión Europea: Payment Services (PSD2) Directive 2015/2366
- Mastercard: Zero Liability Protection
- VISA: Zero Liability Policy