Garantiza la seguridad de las operaciones y establece la obligación de los proveedores en las ventas con tarjetas de crédito o débito, de contar con un sistema biométrico dactilar de verificación de identidad del cliente
Boletín N° 5378-03

VISTOS: Lo dispuesto en los artículos 63 y 65 de la Constitución Política de la República, lo prevenido en la Ley 18.918 Orgánica Constitucional del Congreso Nacional y lo establecido en el Reglamento de la H. Cámara de Diputados.

CONSIDERANDO:

1. Que en nuestro país existen más de 10 millones de clientes de las multitiendas que administran tarjetas de crédito.
2. El sistema funciona a través de una cuenta corriente de crédito cuya expresión física es una tarjeta de plástico con banda magnética que contiene los datos básicos del cliente.
3. Para comprar y usar el crédito aprobado, el cliente solo debe estar en posesión de la tarjeta y de su carné de identidad. Es perfectamente posible comprar sin la tarjeta; es posible que la tienda emita una tarjeta en el mismo momento en que el cliente desea.
4. El gran problema aparece cuando estas tarjetas son robadas o extraviadas y usadas de modo fraudulento. La ley 20.009, publicada en el Diario Oficial el de 1 de Abril de 2005, establece que el cliente podrá limitar su responsabilidad en el evento que su tarjeta sea usada de un modo fraudulento, debido al extravío, hurto o robo de esta, para lo anterior es necesario que el cliente de aviso de pérdida de la tarjeta y solicite el bloqueo de la misma, pero esto sólo funciona si el cliente se da cuenta de inmediato del robo o extravío, pero generalmente esto no sucede y la víctima del robo o hurto lo advierte después de haber pasado algún tiempo, lo que implica un grave riesgo, puesto que en el tiempo que media entre el robo o hurto y el bloqueo de la tarjeta, esta ya ha sido usada de un modo inescrupuloso y fraudulento.

5 Además del uso fraudulento descrito precedentemente, existen otros tipos de fraude, como por ejemplo:

■ *Skiming* que consiste en la clonación de tarjetas de crédito y débito con el empleo de dos dispositivos; uno sobrepuesto en los cajeros automáticos que captura la información de la banda magnética de la tarjeta de crédito o débito y otro dispositivo falso de porta folleto que contiene una micro cámara que captura la clave secreta de la tarjeta y mediante una antena trasmite la información a un receptor ubicado hasta una distancia de 200 metros.

■ *Robo de Identidad o Suplantación* en donde el ladrón se hace pasar por la víctima para usar una tarjeta o una cuenta bancaria existente este tipo de fraude tiene variantes más perniciosas, A) cuando el delincuente se hace emitir tarjetas o cuentas nuevas con el nombre de la víctima (es un fraude difícil de detectar y de solucionar porque suele permanecer sin detectar por largo tiempo); B) cuando los piratas cibernéticos jaquean las redes y roban claves de acceso y números de tarjetas. La velocidad del delito es tal, que cuando los afectados logran descubrirlo suele ser demasiado tarde.

6. El Subcomisario jefe de Análisis Forense Informático, perito judicial informático y académico de la Universidad de Chile, afirma que los principales delitos asociados al dinero plástico son la estafa, falsificación, uso malicioso de instrumento privado mercantil, clonación y usurpación de identidad de usuarios. Señala que: *"existen organizaciones criminales, nacionales e internacionales actuando en el país. Varías de ellas han sido desarticuladas por fuerzas policiales. Sin embargo, no se deben descartar numerosos casos en que existen personas inescrupulosas que efectúan estos crímenes, por descuido de los usuarios en el resguardo de las tarjetas o bien de las que se encuentran en Internet con algún número de tarjeta válido y deciden "probar" si funciona, cometiendo un serio delito"* (1)

7. Cada día aparecen más casos de uso fraudulento de estas tarjetas con consecuencias de gran envergadura para el cliente. En los últimos casos conocidos y difundidos por los medios, el cliente ha debido entrar en un juicio civil y tener que esperar varios años su resolución, con una serie de inconvenientes y costos asociados. Sólo últimamente, la justicia ha venido fallando a favor del cliente.

8. Recientemente se ha detenido un Ingeniero Informático, acusado de apropiarse de una base de datos de mas de 20.000 clientes de la Banca, quien utilizando sus conocimientos y abusando de la confianza de la empresa Transbank (administradora de las tarjetas Visa, Mastercard, Magna, American Express y Diners Club, además del sistema Redcompra) en la que se desempeño como Jefe de Proyectos y de Desarrollo entre 1995 y 2005, clonó cerca de 800 tarjetas de crédito y débito, girando un promedio de 400 mil pesos diarios, fraude que ascienden a más de 2 millones y medio de dólares. Lo anterior comprueba que ningún sistema es 100% seguro, y que es perfectamente posible la existencia de redes de tráfico de tarjetas y datos de éstas, además de concertación fraudulenta entre cajeros y personal de estas empresas para cometer estos ilícitos, dejando al cliente-ciudadano en precarias condiciones y obligándolo a asumir una defensa jurídica engorrosa y costosa. Todo aquello se resuelve con la lectura de la huella digital.

9. Es difícil conocer el volumen total de estas compras fraudulentas, debido a que la Banca en general cuando ocurre un fraude o delito informático, antes de investigar devuelve la cifra afectada al cliente y después investiga, pero nunca entrega el valor total del fraude en pesos, al parecer, para proteger su imagen y no generar desconfianza en sus clientes. De hecho, algunos bancos han creado el seguro contra fraudes en el ciberespacio, el cual se puede obtener por una módica suma mensual, pero obviamente tiene un tope de dinero de cobertura.
Sin embargo es posible inferir que la cantidad de dinero que involucra es enorme así como es enorme la cantidad de personas que deben sufrir estos inconvenientes.

10. Que todos los problemas señalados precedentemente, en especial el uso fraudulento de tarjetas de crédito extraviadas, hurtadas o robadas, no se presentarían si existiera un sistema de reconocimiento del cliente, mediante el cual el vendedor no tenga duda alguna que quien esta enfrente es realmente quien dice ser.

11. Que en esta era digital en la que nos encontramos, en un país dedicado en masa a la actividad del consumo y con ingresos nacionales crecientes, mejorar las medidas de seguridad para las operaciones con tarjetas de crédito es perfectamente posible, ya que hoy en día existe tecnología suficiente para identificar sin ningún tipo de dudas, y en forma instantánea a las personas que utilizan estos servicios.

12. Que la solución propuesta es que se establezca como obligatorio el uso de un sistema de identificación del cliente a través de la huella digital, obligación que estará inserta en el texto de la ley sobre protección a los derechos de los consumidores. Lo anterior, dará seguridad tanto a los clientes como a los proveedores.

13. Que un sistema como el propuesto tiene un sinnúmero de ventajas, ya que las huellas dactilares son únicas, se forman a partir de la sexta semana de vida intrauterina y no varían en sus características a lo largo de toda la vida del individuo. Ellas están constituidas por rugosidades que forman salientes y depresiones. Las salientes se denominan crestas papilares y las depresiones surcos interpapilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella.

14. Que las huellas digitales son únicas e irrepetibles aún en gemelos idénticos, debido a que su diseño no está determinado estrictamente por el código genético, sino por pequeñas variables en las concentraciones del factor del crecimiento y en las

hormonas localizadas dentro de los tejidos. Cabe señalar que en un mismo individuo la huella de cada uno de sus dedos es diferente.

15. Que son diversas las empresas administradoras de créditos que utilizan este sistema en la identificación de sus clientes, por ejemplo Falabella y CMR, en su red de cajeros automáticos, La Polar al momento en que los clientes adquieren la tarjeta. Asimismo, la mayoría de las lsapres utilizan este sistema en la venta de bonos, y ya varios servicios públicos como las Municipalidades utilizan el lector de huella digital para controlar la entrada y salida de sus funcionario/as.

16. Que saber reconocer quien es el cliente es una gestión básica en la venta al crédito. Por ello, se propone que la ley obligue a estas empresas a incorporar esta tecnología en todos sus puntos de venta, de esta manera el sistema se independiza de la tarjeta plástica y este artefacto solo sirve para activar el sistema pero pierde valor como medio de verificación de identidad.

Es por lo anteriormente expuesto que los diputados abajo firmantes venimos en presentar el siguiente proyecto de ley:

Artículo único: Incorpórese al Titulo III, párrafo 4, de la ley 19.946, sobre Protección al Consumidor, el siguiente texto, que pasará a ser artículo 43 B:

"En el caso de compraventas realizadas con tarjetas de crédito o débito, los proveedores deberán utilizar un sistema de identificación del cliente que impida su uso indebido o fraudulento. Este sistema de identificación utilizará la transmisión de datos biométricos que permitan la lectura instantánea de la impresión dactilar del cliente, mediante dispositivos electrónicos dispuestos al efecto en cada caja o punto de venta del proveedor.

Las empresas que emitan tarjetas de crédito o débito podrán crear para ello sus propios sistemas o utilizar los servicios que pueda proporcionar para este efecto el Servicio de Registro Civil e Identificación.

En todo caso, los sistemas utilizados deberán salvaguardar la privacidad de los datos de identidad biométrica dactilar de los clientes, quedando estrictamente prohibida su venta, comercialización o uso para otro efecto, limitándose exclusivamente su utilización para verificar la identidad del portador propietario de la tarjeta de crédito o débito otorgada por la empresa que provea los servicios.

El proveedor que haga uso de los datos de sus clientes en una forma distinta a la señalada en los incisos precedentes, será sancionado con la pena señalada en los artículos 1 ° y 2° de la Ley 19.223, que tipifica figuras penales relativas a la informática, sin perjuicio de las acciones indemnizatorias que corresponda.

El valor que las empresas cobren a los usuarios por el costo de la transmisión de !os datos biométricos de identificación dactilar no podrá superar el 100% del valor UBI que cobra el servicio de Registro Civil e Identificación ,por estos servicios.

Artículo transitorio: *Los proveedores tendrán un plazo máximo de 18 meses, contados desde la promulgación de la presente ley, para implementar el sistema biométrico de verificación de identidad indicado precedentemente.*