Invitación a la Comisión de Economía, Fomento y Desarrollo de la Cámara de Diputados

Operación del Sistema PIN Pass en Tarjetas de Crédito

Presentación del Superintendente de Bancos e Instituciones Financieras,
Sr. Carlos Budnevich Le-Fort

(Valparaíso, martes 8 de junio 2010)

I. Antecedentes recientes

En el transcurso del año 2009, esta Superintendencia tomó conocimiento de diversos proyectos adoptados por parte de los bancos y sociedades de apoyo al giro, referidos a la implantación de medidas mitigadoras de fraude con tarjetas de crédito, entre los que se encontraba el PIN Pass. Al respecto, esta Institución comunicó formalmente a la banca que la implementación final de dicho proyecto fuera realizada con la mayor coordinación entre los bancos y las sociedades de apoyo al giro involucradas, teniendo especial cuidado en precaver impactos negativos en los clientes.

II. Normativa aplicable

El marco normativo aplicable a la emisión y operación de tarjetas de crédito está dado, principalmente, por el Capítulo III.J.1 del Compendio de Normas Financieras del Banco Central de Chile, las disposiciones del Título I de la Ley General de Bancos, la Circular N° 17 para Emisores y Operadores de Tarjetas de Crédito y el Capitulo 8-3 de la Recopilación Actualizada de Normas de este Organismo.

En relación con lo anterior, tanto el Capítulo III.J.1 del Instituto Emisor como la Circular N° 17 de esta Superintendencia establecen que los contratos que se celebren entre el Emisor y los Titulares o Usuarios referentes a la utilización de la Tarjeta en su carácter de medio de pago deberán contemplar, en carácter de contenidos mínimos, entre otros: las medidas de seguridad relacionadas con el uso de la Tarjeta y los procedimientos y responsabilidades en caso de robo, hurto, pérdida, adulteración o falsificación de la misma.

Cabe señalar que las disposiciones citadas no optan por alguna modalidad en particular de autentificación de los usuarios en las transacciones ni hacen mención alguna a la forma ni a la tecnología a utilizar. En este sentido, dichas disposiciones son flexibles y neutrales frente a las nuevas tecnologías, bastando para implementar una nueva modalidad de autentificación con que ésta cumpla las exigencias que en materia de seguridad establecen estas normas.

Las modalidades de autentificación que puedan aplicarse son estipuladas en los reglamentos y contratos de los sistemas de las distintas tarjetas de crédito, por lo cual la

implementación del uso de clave secreta no requirió de la modificación de norma alguna ni supuso la necesidad de aprobación de parte de las autoridades regulatorias.

II.1. Exigencias de seguridad

En cuanto a las disposiciones relativas a la seguridad contenidas en el marco normativo citado, se puede señalar:

- El Capítulo III.J.1 del Banco Central dispone que los emisores y operadores deben cumplir con las normas que en materia de gestión y control de riesgos operacionales y tecnológicos, y de requisitos de acceso e información, establezca esta Superintendencia.

- La misma norma del Instituto Emisor dispone que entre los antecedentes requeridos para la inscripción en el registro de emisores y operadores de tarjetas de crédito, debe acompañarse un informe que contenga la descripción y verificación de las políticas de control y gestión de los riesgos operacionales y tecnológicos asociados al giro de Emisor de Tarjetas; los controles internos establecidos para dicho efecto; las características del inventario de las plataformas computacionales; la infraestructura de redes; las aplicaciones comerciales vigentes; los estándares utilizados para la seguridad de la información; el proceso operativo y las condiciones de seguridad para la administración de Tarjetas.

- La Circular N° 17 de la Superintendencia de Bancos e Instituciones Financieras, en su anexo, incluye en la pauta de Evaluación de la Calidad de Gestión y Control de Riesgos Operacional y Tecnológico, el que el emisor cuente con una estructura que permita administrar la seguridad de la información en términos de resguardar su confidencialidad, integridad y disponibilidad, considerando controles para el origen, aprobación, transmisión, y almacenamiento de las transacciones del sistema de pagos utilizado. Lo anterior incluye la implantación de controles de seguridad físicos y lógicos, tales como accesos debidamente autorizados y técnicas robustas de autentificación de tarjeta habientes. Dichos controles, deben restringir el acceso tanto a las aplicaciones, como a las bases de datos del sistema de pagos y deben estar presentes en la emisión de las tarjetas y en la entrega de PIN a los tarjeta habientes.

Adicionalmente, se debe tener presente que las marcas internacionales de tarjetas de crédito tienen establecidos estándares propios que se deben cumplir. El estándar es denominado PCI (Payment Card Industry), aplicable a la industria de tarjetas de pago, y contiene normas de seguridad de datos. Todas las medidas que contempla la norma PCI son parte de las buenas prácticas aplicadas por la industria de las tarjetas y son parte también de otros estándares de seguridad como la norma ISO 27001, que es el modelo que sigue la mayoría de las instituciones financieras. Sólo que la PCI la utilizan para resguardar todo el proceso que involucra el uso de tarjetas.

III. Nueva modalidad de uso de las tarjetas: PIN Pass

Las estadísticas sobre fraudes por uso indebido de las tarjetas mediante suplantación del tarjeta-habiente, han disminuido sistemáticamente durante los últimos años, pese al importante aumento de las transacciones vía tarjeta de crédito. A mayor abundamiento, la empresa Transbank ha informado a la Superintendencia de Bancos e Instituciones Financieras que no ha detectado fraudes provenientes del uso indebido del PIN Pass durante el período en que ha estado en operaciones. A la fecha, Transbank ha recibido dos reclamos de tarjeta-habientes que han indicado su disconformidad con el nuevo sistema y ninguno de establecimientos comerciales. Ello indicaría que hasta el momento el fraude no sería un fenómeno masivo que ocasione inseguridad en el uso de la tarjeta de crédito.

El medio de pago a través de tarjeta de débito utiliza, desde hace varios años, el mecanismo de clave como forma de autentificación de la transacción. A la fecha, no se han presentado aumentos de fraudes y las estadísticas no revelan que éste fenómeno sea relevante. Según información aportada por Transbank sólo 1 de cada 50.000 transacciones efectuadas por Redcompra (0,002% de transacciones anuales por Redcompra de un total anual de 360 millones de transacciones) presenta reclamos.

En lo que respecta a los niveles de seguridad de la modalidad de autentificación anteriormente vigente, la Superintendencia observó que en ella la responsabilidad de autentificar al usuario de la tarjeta estaba entregada a los establecimientos de comercio. El proceso de autentificación consideraba dos exigencias: 1) la identificación del usuario de la tarjeta mediante la exhibición de su cédula de identidad o pasaporte y 2) la firma del comprobante de la transacción por parte del usuario.

Respecto de la primera, que en muchos casos no se observaba, su cumplimiento se acreditaba mediante la anotación del número de RUT del titular en el voucher respectivo. Esta medida podía ser vulnerada debido:

- a la imposibilidad material del comercio de determinar la autenticidad del documento de identificación que se le exhibía;
- al hecho de que en la mayoría de los casos era el propio usuario quien anotaba el número de RUT (y anotado el número correcto se presumía que se había exhibido la cédula de identidad, aun cuando en la práctica podría haberse omitido la presentación de dicho documento, haberse presentado uno falso o incluso el de un tercero);
- a que los terminales más modernos extraían el número de RUT de los datos de la tarjeta y lo imprimían directamente en el voucher;

En relación al segundo requisito, la práctica mostró que los contratos no exigían a los usuarios utilizar la misma firma estampada en su cédula y que los comercios no tenían acceso al registro de firmas, lo cual se traducía en la imposibilidad de validar la firma estampada en el voucher. Como consecuencia de esto, la circunstancia de que la firma

plasmada en el comprobante difiriera visiblemente de la de la cédula de identidad del tarjetahabiente no bastaba por si sola para invalidar una transacción.

Ahora bien y en lo que se refiere a los estándares de seguridad de la modalidad de autentificación mediante el uso de la clave bancaria PIN Pass, se debe mencionar que:

- La clave bancaria secreta corresponde a un mecanismo de firma electrónica, el cual tiene el mismo valor que una firma manuscrita. Esto ya está reconocido desde el año 2002 en nuestra legislación (Ley Nº 19.799), que dispone que los actos suscritos por medio de firma electrónica producen los mismos efectos que los celebrados en soporte de papel, produciendo plenos efectos en el mundo de los negocios y en el judicial.

- La firma electrónica mediante clave permite que el acto de autentificación que estaba entregado a los dependientes de los establecimientos de comercio se traslade a los emisores de las tarjetas quienes son los responsables de mantener sistemas robustos de firma electrónica.

- Los emisores disponen de mecanismos para resguardar las claves, por lo que el uso indebido de ella, normalmente, se origina en violaciones de seguridad originadas en el lado del tarjeta-habiente.

- Esta modalidad de autentificación se encuentra ampliamente probada, tanto en el plano internacional como en el nacional, toda vez que esta clave no es distinta de la usada para operar en la red de cajeros automáticos y en el sistema de débito denominado Redcompra.

- De acuerdo a información entregada por Transbank, la principal defensa frente a un robo de la clave mediante fuerza, es el bloqueo de la tarjeta, lo que es similar a lo que sucede con las tarjetas de cajeros automáticos y de débito.

- En caso de obtención indebida de la tarjeta y de su clave secreta, el tarjeta habiente tiene la responsabilidad de avisar al emisor de la tarjeta del hecho. El tarjeta habiente es responsable por las transacciones efectuadas hasta el momento en que da el aviso y se bloquea la tarjeta. Sin embargo, ciertos emisores han establecido fondos de fraude y seguros para atender estos casos.

- También es preciso recordar que los propios sistemas de los emisores y de la empresa Nexus cuentan con detectores de comportamientos de transacciones anormales que permiten bloquear dicho tipo de transacciones.

IV. Observaciones Finales

La violación de seguridad en el caso de transacciones vía PIN Pass parece ser más difícil que en el caso sin PIN Pass, puesto que requiere el concurso de más hechos. En efecto, se requiere, además del robo o hurto de la tarjeta de crédito, acceder al PIN Pass, lo que no ocurría en el caso en que no se operaba con PIN Pass.

El contrato firmado por el tarjeta-habiente con el emisor considera, dentro de las cláusulas pertinentes, las responsabilidades de cada uno de ellos respecto de su uso. La responsabilidad de verificar la identidad del tarjeta-habiente se ha trasladado del comercio al banco emisor, lo que ha sido informado por Transbank a los comercios.

Lo que es cierto, es que con el PIN Pass, el medio de prueba de una transacción fraudulenta se hace más difícil para el tarjeta-habiente, porque se trataría de la "prueba de un hecho negativo". En consecuencia, es posible que aumente la probabilidad de que el impacto recaiga en el tarjeta-habiente. Sin embargo, esto no debería ocurrir si los bancos adoptan políticas y procedimientos adecuados.

La Superintendencia de Bancos e Instituciones Financieras advirtió específicamente a los bancos que, con motivo de la implantación del sistema de PIN Pass, deberían tomar precauciones especiales a fin de precaver impactos negativos en los clientes. Por ello, esta materia será monitoreada estrechamente para velar por el buen funcionamiento del sistema y en caso de detectarse deficiencias, esta Superintendencia adoptará las medidas correctivas que correspondan.