Quito 25 de enero de 2011
PE-051-2011

Doctora
YASHIRA NARANJO SÁNCHEZ
Abogada Consumidores y Usuarios de la DNPrT-DDHHN
Defensoría del Pueblo
Quito

Ref. : Expediente DO-DNPrT-YN-2010

De mis consideraciones:

En relación a lo solicitado mediante providencia de 3 de enero de 2011, cumplo con señalarle:

1. **Detalle en qué consiste las medidas y cómo funcionan todos los mecanismos que las instituciones financieras hayan implantado para mejorar las condiciones de seguridad frente a los fraudes electrónicos que se presentan en la realización de transacciones en cajeros automáticos, vía Internet y vía datafast.**

La Banca Privada ha venido adoptando una serie de medidas que tienen por objeto fortalecer las medidas de seguridad de los canales transaccionales que ponen a disposición de sus clientes, en ese sentido:

a. Cajeros Automáticos.- El delito que afecta a las transacciones que se realizan en esos medios principalmente es el denominado skimming, el mismo que consiste en el robo de datos de la banda magnética de una tarjeta de crédito o débito a través de un dispositivo electrónico diseñado para este fin (skimmer) colocado de manera sobrepuesta en el la lectora de la tarjeta del cajero electrónico. Los datos obtenidos son introducidos en una tarjeta con banda magnética virgen con la que se realiza la estafa. Adicionalmente, a través de una cámara colocada en el mismo cajero, se obtiene la clave.

Sin embargo, que actualmente lo más común es la clonación en el cajero automático, también se lo realiza con la tarjeta de crédito al momento de realizar el pago cuando se pierde de vista al dependiente mientras procesa el pago.

Otra modalidad delictiva que afecta a los usuarios es el denominado “cambiazo”, en la cual los delincuentes se acercan a los cajeros automáticos y observan detenidamente a clientes que tienen dificultad con el manejo del cajero para ofrecerles su ayuda, engañarlos y cambiarles la tarjeta de débito por otra similar pero perteneciente a otra persona. El delincuente consigue la clave ofreciendo ayuda para solucionar el problema del cajero.

Para evitar el delito del skimming la Banca Privada ha instalado en el 100% de cajeros afiliados a BANRED los denominados protectores de teclado, los cuales son dispositivos que no permiten la captura de la clave personal y de exclusivo conocimiento del cliente, elemento indispensable junto con la información de la banda magnética para consumar el delito de skimming, adicionalmente se viene instalando dispositivos físicos o de software antiskimming, los dispositivos físicos son elementos (barras de acero) instalados sobre la ranura de ingreso de la tarjeta con el objeto de evitar que sobre él se instale los skimmers, el software que se han instalado por otro lado apaga automáticamente el cajero cuando detecta la instalación de los skimmers sobre la ranura antes señalada.

Adicionalmente, la Banca Privada viene ejecutando el plan denominado “Protegiendo la Red” que consiste el monitoreo, mediante personal propio, aleatorio, por riesgo, y periódico, de los cajeros para verificar su integridad y no instalación de dispositivos ajenos a los ATM.

Por otra parte, la Banca de forma individual y la Asociación gremialmente, impulsan campañas masivas de comunicación de sugerencias de seguridad en las transacciones en cajeros automáticos, de tal suerte que el usuario de un cajero recibe a través de diversos medios de información las precauciones que debe tomar al momento de usar un ATM.

b. Internet.- Las modalidades delictivas que se efectúan a través de Internet no afectan tan solo al Ecuador ni tampoco su incidencia es mayor en el país de lo que es en otros países de la región, de hecho es sensiblemente menor. La delincuencia transnacional (hackers) que opera en esta modalidad, lo hace, por regla general, usando servidores o redes informáticas ubicadas fuera del país y atacan de forma masiva a varias instituciones públicas y privadas con los más diversos fines, para el caso que nos ocupa, perpetrar el delito de apropiación ilícita o fraude informático.

La Banca Privada ecuatoriana cuenta al momento con similares o mejores controles de seguridad que los implementados en otras instituciones del exterior, ha implementado también las mejores prácticas en materia de seguridad, lo que le permite afirmar que la mayoría de eventos delictivos, lamentablemente, son causados frecuentemente por errores propios de los clientes y usuarios del canal transaccional de Internet.

Son varios las acciones realizadas por la Banca en el tema de seguridad, en ese sentido se efectúan de manera periódica auditorías informáticas (Ethical Hacking) con el objeto de que empresas independientes, con frecuencia extranjeras, simulen ataques informáticos en contra de los sistemas bancarios a efectos de identificar fallas, riesgos e implementar correctivos.

De la misma manera se han implementado los denominados “teclados virtuales” que evitan la captura de claves mediante programas maliciosos o dispositivos externos denominados “keyloggers”, ambos, tanto software como hardware, instalados en los computadores del usuario del canal transaccional de Internet. El teclado virtual no permite que el software o hardware (Keylogger) registre las teclas pulsadas al ingresar un clave en Internet, ya por un lado no existe digitación sobre el teclado de manera directa sino en pantalla y por otro en cada transacción el teclado virtual modifica su configuración de números.

Adicionalmente, varios Bancos, tales como Pichincha, de Guayaquil, Produbanco y Bolivariano, han implementado las tarjetas con coordenadas dinámicas, estas tarjetas son únicas y personales del cliente, cuentan con claves/coordenadas que son solicitadas para cada transacción, es decir el Banco jamás solicita el ingreso de dos claves/coordenadas para una misma transacción, la clave solicitada es aleatoria, por lo que, en el entendido de que no se ha difundido mediante ningún medio la tarjeta de coordenadas, es una seguridad prácticamente inviolable.

Las claves dinámicas se suman a la clave de autenticación que es la que permite el acceso al portal transaccional, que también es secreta y de conocimiento exclusivo del cliente.

Otras instituciones financieras utilizan mecanismos conocidos como Tokens, que no son sino dispositivos físicos que tienen similar función que las coordenadas dinámicas ya que éstos

crean para cada transacción un clave de seguridad, que no es siquiera conocida antes de generarse.

Por otra parte, otras entidades, con menor tráfico transaccional, permiten la realización de operaciones en Internet previa la "matriculación" de la cuenta desde la que se realizarán las transacciones y las que recibirán las transacciones, de igual manera existen casos en los que una vez realizada la operación por Internet, el Banco solicita vía otros medios la confirmación de la transacción, estos mecanismos son también efectivos.

c. Datafast.- Los POS (nombre del mecanismo que llama Usted Datafast) son instrumentos que permiten electrónicamente enviar información de una transacción con tarjeta de crédito o débito hacia el centro de autorizaciones de la administradora de la tarjeta, el POS en si no constituye el elemento del que se sirven los delincuentes para capturar la información de las bandas magnéticas de las tarjetas sino que al ser entregadas por el titular de la tarjeta a un tercero éste las "pasa" por otro elemento denominado skimmer, el que captura la información con la cual se clona la tarjeta de crédito o débito posteriormente.

El delito que afecta a esta transacción es similar al de cajeros automáticos, esto es el skimming, para lo cual la primera y más efectiva medida de seguridad es que el usuario no pierda de vista su tarjeta, no la entregue a terceros y solo realice transacciones en lugares confiables y con su supervisión.

El Sistema Bancario ha iniciado un proceso de estudio de sustitución de tarjetas a fin de adoptar aquellas conocidas como "tarjetas inteligentes" o tarjetas con chip, en donde se elimina la banda magnética y en consecuencia la posibilidad de capturar la información, sin embargo este proyecto por los profundos cambios que significan, que pasan por cambio de tarjetas a todos los usuarios, de sistemas de POS, de Cajeros automáticos, de software, etc., será ejecutado a mediano plazo, previo el análisis de los estándares que se adoptarían, ya que existen varios posibles.

En relación a su consulta sobre la implementación del *teclado virtual* en operaciones por Internet, debo indicarle que la mayoría de Bancos lo tienen implementado así por ejemplo Pichincha cuenta con él desde hace 6 años, Bolivariano desde hace 5 años, Internacional desde hace 4 años, Produbanco desde hace 4 años, de la misma forma Banco Pichincha cuenta con tarjetas con coordenadas dinámicas desde hace 6 años, Bolivariano desde hace 5, Produbanco 4 años.

2. **Remita documentación de la campaña que informó difundió en navidad, así también sus impresiones u otras advertencias en canales como ATM e Internet, o difundidas por otras vías si existiese.**

Adjunto, para su conocimiento, ejemplares de los flyers difundidos en las ciudades de Quito, Guayaquil, Cuenca, Manta, Portoviejo, Loja y la provincia de Imbabura, en los meses de diciembre de 2009, mayo, octubre y diciembre de 2010. La información contenida en ellos fue elaborada por la Asociación con la asesoría de sus técnicos miembros del Comité Ecuatoriano de Seguridad Bancaria y la Policía Nacional, la que participó activamente en la difusión de la información.

En diciembre de 2010, la Asociación participó en el "Plan de Capacitación de Seguridad Ciudadana: Ecuador sin violencia educamos para prevenir", el mismo que es coordinado por la Fiscalía General del Estado y con la participación de la Policía Nacional, Ministerio del Interior y Ministerio de Educación, esta campaña llegó a 1700 UPC –Unidad de Policía Comunitaria- en todo el país y fue difundida por los capacitadores de ese Plan.

Adicionalmente la información se ha distribuido como insertos en medios de comunicación masiva tales como Metrohoy, Metroquil, Diario HOY y en lo principales centros comerciales de las ciudades arriba indicadas.

Esos esfuerzos gremiales se complementan con los de los Bancos, los que informan permanentemente a sus clientes a través de varios canales, tales como estados de cuenta (adjunto para ejemplo unos que corresponden a los Bancos Pichincha y Produbanco), Internet (adjunto solo como ejemplo impresiones de las capturas de pantalla de los Bancos Pichincha, Produbanco, Internacional, Bolivariano, Promerica, General Rumiñahui, Unibanco, Loja, en donde se destaca la información de seguridad), correos electrónicos (adjunto la impresión del correo remitido por Banco Pichincha en días recientes por información fraudulenta que estuvo circulando).

3. Explique la limitación de responsabilidad de la Banca frente a la obligación de dotar de seguridad a los servicios financieros que prestan a sus asociados.

En la comunicación PE-136-2010 citada en su providencia la Asociación dijo textualmente: "La Banca no desconoce en ningún momento su obligación de dotar de seguridades a los servicios que presta; sin embargo, como toda responsabilidad ésta tiene límites y su ejercicio es compartido con los propios usuarios del servicio."

El sentido de lo señalado, no fue sino el indicar que todo esfuerzo que pudiera llevar a cabo cualquier entidad para fortalecer su seguridad debe ser acompañada también por acciones propias del usuario del servicio, es decir aún cuando la Banca incorpore toda clase de seguridades alrededor de una transacción, si un cliente no adopta también medidas elementales de seguridad como por ejemplo no prestar o difundir su claves a terceros, instalar un antivirus en su computador y actualizarlo constantemente, hacer caso omiso de mensajes fraudulentos, verificar el uso de su tarjeta de débito o crédito cuando realiza un compra o un pago, etc., ninguna medida será efectiva.

La Banca realiza sus esfuerzos por fortalecer la seguridad e informa a sus clientes las que deberían adoptar para efectuar transacciones seguras.

En el ámbito jurídico es claro que en el Ecuador rige la denominada responsabilidad subjetiva, esto es que la responsabilidad de una persona en un acto que causa daño está ligado a la culpa que pudiera tener en ella, así lo indica el Reglamento a la Ley Orgánica de Defensa del Consumidor: "Art. 27.- De conformidad con lo previsto en el Art. 28, habrá solidaridad en la responsabilidad de pago de las indemnizaciones civiles por daños causados por vicio o defecto de los bienes y servicios prestados, entre todos aquellos que intervengan en la cadena de producción y distribución. **Se liberará a quien demuestre en juicio que la causa del daño le ha sido ajena**."(las negrillas son de la Asociación), la frase resaltada establece en nuestro sistema legal la denominada responsabilidad subjetiva.

Hago propicia la oportunidad para reiterarle mis sentimientos de consideración y estima y suscribo.

Atentamente,

ECON. CÉSAR ROBALINO GONZAGA
Director Ejecutivo

Anexos