El Cuaderno - Escuela de Ciencias Estratégicas Vol 2 N° 4 P. 279-296 (2008)
Medellín - Colombia. Jul - Dic de 2008 ISSN: 2011-0170

El fraude en la actividad bancaria

Nicolás Darío Ramírez Moncada*
nicolasramirez@une.net.co

Eje Temático: Mercados Financieros
Subtema: Bancos

Resumen

La gestión del riesgo operacional en Colombia es un tema de gran actualidad en el sector financiero. A pesar de que las empresas reconocen que factores como fraudes, cambios en las regulaciones, desastres naturales o errores en los sistemas y que ellas representan fuentes de incertidumbre, no existía una concepción de éstos como un conjunto de factores que pueda agruparse bajo una misma categoría denominada Riesgo Operativo.

El riesgo operacional es muy heterogéneo, se asocia con errores humanos, mecánicos, informáticos y de control. Una manera de clasificar el riesgo operacional consiste en seguir el criterio de su causa, que puede estar constituida por:

Sucesos inesperados ajenos al control de la entidad: entre éstos se encuentran desastres naturales, ausencia en el suministro eléctrico, interrupción en las telecomunicaciones, virus informáticos, incendios, robos y otros. **Errores humanos:** son causados por negligencia del personal de la entidad, distracciones, ausencia

* Administrador de Empresas, Universidad Cooperativa de Colombia. Especialista en Gerencia Financera, Universidad Pontificia Bolivariana. Gerente de Zona de Medellín y eje cafetero, GMAC financiera de Colombia S.A.

Artículo recibido el 13 de agosto y aprobado para su publicación el 23 de septiembre de 2008.

de interés o motivación. **Operadores indisciplinados:** se trata de empleados sin escrúpulos, generalmente representados por individuos que no acatan las normas establecidas y que, por tanto, pudieran estar involucrados en acciones inescrupulosas, realizando operaciones no autorizadas que pueden ocasionar pérdidas a la entidad. **Conflicto de intereses:** se producen errores o fallas cuando los gestores, empleados y operadores toman posiciones de riesgo en contra de la estabilidad de la entidad.

Por las características descritas, pretendo presentar las diferentes modalidades de fraude en la actividad bancaria, tomando en cuenta la necesidad de protegerse ante posibles ataques delictivos.

Palabras clave:
Actividad bancaria, cajeros electrónicos, fraudes.

Abstract

The management of the risk operacional in Colombia is a subject of big importance in the financial sector. Although the companies generally recognize that factors like frauds, changes in the regulaciones, Natural disasters or errors in the systems and that they represent sources of important uncertainty, did not exist a conception of these like a group of factors that can agruparse under a same category designated Operative Risk.

The risk operacional is very heterogeneous; associate to human errors, mechanical, informáticos and of control. A way to classify the risk operacional consist in following the criterion of his cause, that can be constituted by:

Sucesos Unexpected extraneous to the control of the entity: Between these find natural disasters, absence in the electrical supply, interruption in the telecommunications, virus informáticos, incendios, thefts and others.human errors: they Are caused by negligence of the personnel of the entity, distractions, absence of interest or motivation. Operators indisciplinados: treat of employees without scruples, generally represented by individuals that no acatan the norms established and that, therefore, could be involucrados in actions inescrupulosas, realizing operations no authorized that they can ocasionar losses to the entity. Conflict of interests: they produce errors or fail when the gestores, employees and operators take positions of risk against of the estabilidad of the entity.

Because of the before described characteristics, pretend with in this report present of the different modalidades of fraud in the activity bancaria taking very in account the need to protect in front of possible attacks delictivos.

Key words:
Activity bancaria, cajeros electronic, frauds.

1.
El fraude en la actividad bancaria

1.1.
El fraude global

Ante los grandes avances tecnológicos el crimen organizado o bandas de delincuencia se han valido de esta herramienta para abrir grietas en la seguridad de los mercados financieros.

Nos enfrentamos a organizaciones criminales profesionales muy complejas y con capacidad tecnológica para desarrollar esquemas de fraude internacional. Desde hace tiempo, la falsificación de billetes dejó de ser un buen negocio para la delincuencia organizada. Y es que los avances tecnológicos son bien aprovechados por los "cerebros" de estas bandas en la producción de cheques y tarjetas de crédito para realizar falsificaciones del más alto nivel.

1.2.
Tipos de fraude

Se considera que hay dos tipos de fraude: el primero de ellos se realiza con la intención financiera clara de malversación de activos de la empresa. El segundo tipo de fraude, es la presentación de infornación financiera fraudulenta como acto intencionado encaminado a alterar las cuentas anuales.

Los fraudes denominados internos son organizados por una o varias personas dentro de una institución, con el fin de obtener un beneficio propio. Los fraudes conocidos como externos son los que se efectúan por una o varias personas para obtener un beneficio, utilizando fuentes externas como son: bancos, clientes y proveedores.

1.3.
Tendencias actuales

Pasemos a analizar las tendencias que han favorecido el desarrollo del fraude.

1.3.1.
Mayor presencia del crimen organizado:

Se trata de pequeñas mafias, dos o tres individuos, cuya actividad empresarial es dedicarse a encontrar objetivos fáciles. En efecto, el crimen

organizado podría ser responsable de la gran mayoría de los fraudes externos. Por ello es preciso recordar que éstos sólo pueden ser exitosos con la participación interna de un empleado corrupto.

1.3.2.
Mayor corrupción de empleados:

Se refiere al empleado que, por una serie de razones éticas y morales, decide que es más fácil ganar dinero de otra forma, ya sea en colaboración con el crimen organizado o por su propia iniciativa.

1.3.3.
La aparición del "tecnofraucrata":

Este término define a aquella gente bien preparada, muy conocedora de los negocios y de los mercados, que considera que lo importante es ganar dinero a costa de lo que sea.

1.3.4.
Desarrollo de técnicas más asequibles de falsificación:

La tecnología ha permitido lograr verdaderas maravillas que no tienen aquel aspecto artesanal de antaño: acciones, bonos, formularios y billetes falsificados.

1.3.5.
Más oportunidades de fraude por errores operativos:

La necesidad de crecer y de ganar nuevos mercados ha llevado a algunas empresas a reducir erróneamente los gastos. Lanzan nuevos productos sin tener buenos procedimientos operativos ni contar con una buena formación de los empleados que van a vender, administrar y procesar esos productos.

1.3.6.
Fraudes multi-jurisdiccionales:

Esa tendencia se viene observando sobre todo en los grandes fraudes en los que intervienen las mafias.

Esto ocurre cuando un fraude se realiza en un país "A" y los fondos son transferidos a un país "B". Frente a esta situación, se deben emprender y coordinar acciones legales en los dos países, lo que es difícil, puesto que, a veces, hay diferencias en el tratamiento y en la penalización de actividades ilícitas.

1.3.7.
Defraudadores dispuestos a presentar batalla legal:

La poca efectividad de la acción legal por parte nuestra hace que el defraudador se salga con la suya. Incluso, a veces, el defraudador se va contra la empresa, alegando daños y perjuicios.

1.3.8.
Mayor velocidad en el movimiento de fondos:

Hoy en día un empleado sólo necesita cinco minutos para cometer un fraude. De ahí la necesidad de que la detección del fraude deje de ser una actividad reactiva y pase a ser un elemento más dentro de la gestión, planeación y estrategia gerencial del empresario moderno.

1.3.9.
¿Quién paga las consecuencias del fraude?

Cuando un fraude o una serie de fraudes suceden en un sector, todos perdemos:

- Los directivos, en múltiples formas, empezando por su reputación y por la pérdida de confianza por parte de los accionistas y de sus mismos colegas.
- Los empleados, quienes se ven afectados por la desmoralización que un fraude genera en un grupo de trabajo.
- Los accionistas, por el efecto de un fraude en los resultados financieros, en el valor de la empresa y en la imagen de la misma en el mercado.
- Los auditores, quienes algunas veces no han podido o no han sabido reconocer los indicios de fraude.
- Las compañías aseguradoras por las indemnizaciones que pagan.
- Los clientes de las entidades financieras que son los más perjudicados
- Por último, todos nosotros, como miembros de la sociedad.

1.3.10.
Modalidades de fraudes

1.3.11.
Fraudes con cheques y tarjetas de crédito.

Son comunes los fraudes con estos dos productos financieros, pero podemos proteger nuestro patrimonio y conocer de qué se valen los estafadores.

1.3.12.
Con cheques

- Comprende la falsificación, adulteración o el uso de cheques en blanco obtenidos ilícitamente. Puede hacer referencia a la falsedad total, aquella en la que el documento es falso y su producción fue realizada por delincuentes. Existe también la falsedad parcial que es aquella en la que se roba el cheque a medio procesar y los falsificadores lo terminan de imprimir. La adulteración de cheques es aquella en la que cambian datos del cheque como borrar el número de cuenta o los roban y los cobran dos veces.

- Falsificación de firma en documentos. El sistema financiero mundial se atiene a una firma autógrafa para el pago de documentos. ¿Es esta una buena medida de seguridad? ¿Existe otra forma más segura para evitar su falsificación? Tenga cuidado al plasmar su firma.

- Alteración de caracteres magnéticos. Hoy día, nuestro sistema financiero utiliza tecnología para facilitar el proceso de captura de la información de los cheques, como lo es la banda de caracteres magnéticos. Si esta misma se llegara a cambiar o alterar, ya no estaríamos hablando del mismo cheque sino de otro distinto.

1.3.13.
Con tarjetas de crédito

En una venta con tarjeta de crédito el comerciante tiene la seguridad de que dicha operación está respaldada por un cupo de crédito otorgado por un banco emisor, quien asume el riesgo y los costos de no pago. Adicionalmente, evita los estudios de solvencia de los clientes y reduce los riesgos de pérdida de cartera. Por otra parte, la seguridad de la tarjeta es mayor frente a la alternativa de manejar efectivo o cheques ya que las posibilidades de fraude con estos medios son mayores. Además, en el caso de los cheques la disponibilidad de recursos para el comerciante no es inmediata, mientras que para muchos comercios en Colombia las consignaciones de las ventas con tarjetas son depositadas automáticamente en sus cuentas al día siguiente de la transacción.

- *Aumento fraudulento de cupos.* El modus operandi de los delincuentes consiste en aumentar el cupo de tarjeta de crédito, a través de modificación de registro de la tarjeta en el sistema de cómputo. A continuación, se presentan avances en efectivo por cajero automático, hasta terminar por completo la cantidad asignada ilícitamente, para entrar de nuevo al sistema en el que se realizan los pagos, los avances y bajan el cupo como se encontraba inicialmente. Esta modalidad se ha preferido en los últimos meses, pues debe haber una persona dentro de la entidad para hacer la

transacción con la cuenta ficticia, y quien por esta operación recibe un porcentaje de comisión.

- *Clonación de tarjetas*. Se han creado mecanismos para robar la información contenida en la banda magnética de la tarjeta. La tarjeta es pasada por el datáfono, desde el mismo sistema se obtiene el contenido de la banda magnética que es "quemado" en otra banda. Hacen una plaqueta con la información de la tarjeta que es utilizada para hacer grandes compras o avances de dinero en efectivo.

- *Tarjeta caliente*. Es el fraude que se efectúa con tarjetas de crédito recientemente robadas y que no tienen ningún tipo de bloqueo.

- *Tarjeta alterada*. Adulteración que se realiza a las tarjetas emitidas por las entidades financieras, a las que les suelen modificar la información numérica y alfabética haciéndolas coincidir con tarjetas vigentes.

- *Falsificación integral de la tarjeta*. Sucede cuando se utiliza un plástico al que, mediante procesos de impresión y de realce de información, se le da características iguales a las legítimamente emitidas por una entidad financiera.

- *Falsificación de la banda magnética*. Se presenta cuando se utilizan plásticos auténticamente emitidos por entidades financieras, a los que se les incluye información en la banda magnética.

- *Comprobantes previamente elaborados*. Otro nombre que se le da a esta modalidad de fraude es el de comprobantes falsos o lavado de comprobantes. Consiste en imprimir los comprobantes con elementos diferentes a los de la tarjeta, se distribuyen en comercios autorizados y pasan como auténticos. Por desgracia, algunos comerciantes se prestan para realizar la transacción fraudulenta: por ejemplo: el delincuente se presenta con un comprobante falso diligenciado por USD1.000, mientras que el comerciante, desde su casa, pide la autorización, y acto seguido le da al antisocial el 60% del dinero.

- *Fraudes por telemercadeo*. Este es un fraude muy común. El delincuente llama a una de las empresas de telemercadeo y hace el pedido de un artículo con cargo a la tarjeta de crédito. Toda la información que suministran es verdadera, incluso los sitios de recepción de la mercancía; sin embargo, esta información se ha suministrado en muchas ocasiones por personas que trabajan con las entidades financieras, pero luego de confirmar los datos correctos, el delincuente cambia la dirección para el envió de la mercancía, en este caso el que termina perdiendo es el establecimiento de comercio que acepta la venta. Este delito se combate haciendo firmar

contratos especiales a los comerciantes, en los que se responsabilicen por los fraudes que ocurran en dicha modalidad. En los países latinoamericanos se ha disminuido este sistema, las entidades financieras se han preocupado por tener claridad en los contratos con estas empresas, mientras que en Estados Unidos y Europa, el porcentaje de fraude es alto.

- *Suplantación de la razón social.* Hace referencia al fraude realizado cuando se suplanta al establecimiento afiliado, mediante la impresión en comprobantes de venta de la placa real o falsificada. Es decir, todo establecimiento de comercio que reciba pagos con tarjeta de crédito, tiene dos modalidades para hacerlo: una, por el datáfono de manera electrónica, el cual lee la banda magnética de la tarjeta y consulta automáticamente si la tarjeta tiene cupo disponible y no está bloqueada por algún motivo. Dos, es manual y consiste en pasar la tarjeta por una máquina *Printer,* que tiene una plaqueta que identifica el establecimiento con la red a la que está afiliado, y se debe llamar por teléfono para solicitar la autorización. Y es, regularmente, en este caso donde solicitan la apertura de una nueva cuenta con documentación falsa y consignando en ésta comprobantes fraudulentos. Esta clase de fraude está de moda. Hay delincuentes que crean comercios con el nombre de otros muy conocidos, pero para que esta suplantación tenga éxito se necesita la participación de un funcionario bancario.

- *Autoría del tarjetahabiente.* Ocurre cuando el tarjetahabiente, personalmente o a través de terceros, utiliza o facilita su tarjeta en transacciones que luego rechazará. El dueño de la tarjeta se la presta a otra persona con su identificación, ésta se traslada a otra ciudad y realiza compras, luego el dueño de la cuenta hace el reclamo al banco y dice que nunca ha salido de la ciudad y lo puede comprobar.

- *Tarjeta expedida con datos falsos.* Se utilizan tarjetas elaboradas por el banco, pero las entidades reciben documentación falsa. El delincuente abre una cuenta con datos y nombres falsos y el banco, por fallas de análisis de crédito y de verificación de la documentación, le expide la tarjeta. El cliente utiliza todo el cupo y nunca cancela. Este fraude es asumido por el banco que aprobó la tarjeta.

- *Carteles de fiadores prefabricados.* Esta modalidad de fraude tiene en alerta a los bancos, sobre todo en aquellos que se confían en confirmaciones telefónicas y no verifican mediante inspección física a los deudores y codeudores. En este caso los estafadores consiguen personas que les prometen un porcentaje de dinero y se prestan para hacer solicitudes de tarjetas con documentos falsos, existe todo un montaje para cuando el banco llama a confirmar los datos, estas tarjetas aprobadas y que luego no son canceladas, son asumidas por cada banco.

- *Cédula falsa.* Este es un problema que se presenta en el sector bancario, tanto por fallas en la revisión de información y falta de entrenamiento adecuado por parte de los empleados que cumplen estas tareas, como por la vulnerabilidad que ofrecen los organismos del Estado.

- *Retiros fraudulentos por cajero automático.* Sucede, en algunos casos, cuando empleados de la institución pueden conocer la clave del cliente y tienen acceso al plástico de manera simultánea. Para esto, las entidades financieras han establecido controles para que sea el cliente quien asigne su clave una vez entregada la tarjeta; sin embargo, aún hay entidades que manejan de manera manual este procedimiento, permitiendo que algún empleado bancario pueda conocer la clave antes de entregarla al cliente. Para estos casos se recomienda al cliente que una vez se le entregue la tarjeta y la clave ésta última, sea cambiada.

- *Cambio de tarjeta, por una robada o bloqueada.* La confianza del usuario al permitir un fácil acceso a su tarjeta, facilita a los delincuentes que ésta sea reemplazada por un plástico robado sin que se percate del hecho, posteriormente, y por lo general después de un fraude, se observa que la tarjeta que porta el usuario no corresponde a su identidad.

- *Doble facturación.* Fraude muy común en Brasil, Colombia y en Centroamérica. La persona paga la cuenta de un restaurante o un bar con tarjeta de crédito, pero el mesero pasa la tarjeta dos o tres veces, y luego trata de imitar la firma del cliente en los otros dos recibos. La doble facturación es un tipo de fraude que va a crear bastantes problemas porque en él se manipulan y se modifican datos; si no hay estrategias de manejo de la informática, el sector va a tener enormes pérdidas no sólo con tarjetas de crédito sino en la operación bancaria y en la parte relacionada con el manejo de la información en las instituciones financieras.

- *Tarjeta gemela.* Es aquella tarjeta igual a otra que ha sido emitida legítimamente por una entidad, teniendo, en consecuencia, las mismas características en materia de seguridad, calidad e información, incluidos los datos procesados en la banda magnética. Esta modalidad es difícil de detectar, excepto cuando se recupera el plástico utilizado para el fraude y puede corresponder a procesos de doble emisión en la misma entidad, por actividad dolosa de funcionarios que tienen que ver con esta etapa del proceso.

- *Fraude en la devolución de tarjetas entregadas por el cliente.* La devolución de la tarjeta de crédito por parte de un usuario requiere de controles eficientes para minimizar fraudes, se dan casos en los que no se anulan los plásticos ni se presenta la evidencia de devolución y posteriormente aparecen cargos fraudulentos ejecutados, generalmente, por funcionarios internos.

- *Fuga de información general.* Este es otro delito que va unido al fraude electrónico, al fraude de banda magnética y a la fuga de información. Como primera medida se contacta a un empleado que tenga facilidad de entregar 50 ó 55 números de tarjeta cada viernes a un delincuente. Naturalmente, la entidad financiera va a sufrir pérdidas. Con la información que suministra el empleado, los delincuentes emiten tarjetas con esta información y realizan compras en todas partes.

- *Empresas de fachada.* Funcionan como entidades legales que adulteran su contabilidad para justificar el incremento de operaciones, especialmente ventas ficticias con tarjetas de crédito, para luego "lavar" el dinero por dicha compra.

- *Empresas ficticias.* Consideradas como compañías de papel que, aunque están registradas en la Cámara de Comercio, no poseen instalaciones físicas y nunca desarrollan su objeto social. Sin embargo, en ellas se generan operaciones con tarjetas de crédito robadas o para la obtención de efectivo cuyo costo se convierte en usura. Consiste en que esta empresa realiza una venta ficticia con el objeto de darle en dinero el cupo al cliente, cobrando por esto un porcentaje muy alto. En este caso no hay fraude, pues el cliente continúa pagando su tarjeta, pero en la mayoría de los casos, estas empresas ficticias son utilizadas, para realizar transacciones con tarjetas robadas que, en la mayoría de los casos, no han sido bloqueadas.

- *Colusión y funcionarios infieles.* Se identifican diferentes ilícitos por parte de los empleados, quienes vulneran los controles para activar tarjetas y usarlas antes de entregarlas al verdadero usuario.

- *Lavado de dinero mediante el uso de tarjeta de crédito.* Hace poco un cliente, con visa de residente en Estados Unidos, llegó a pedir US$30, US$40 y US$50 con tres tarjetas de crédito americanas. La primera se la negaron, pero las otras dos se las aprobaron. Al preguntar con quién vivía y dónde trabajaba, contestó que él no pretendía llevarse el dinero sino constituir unos CDT con esos avances. Poco después, resultó preso por narcotráfico. Ese es un típico caso de lavado de activos que cierra su ciclo cuando se normaliza el cupo, con pagos hechos por el usuario, producto de operaciones ilícitas.

1.3.14.
Fraudes electrónicos

El año anterior el 67% de las transacciones financieras se realizaron mediante canales electrónicos y el 65% requirió de una tarjeta para su realización. En el mundo, los pagos por intermedio de teléfonos celulares, han crecido en

más de 10 veces en los últimos cuatro años. Según la Asociación Bancaria, (Asobancaria), si bien en un futuro no muy lejano las transacciones se harán principalmente por intermedio de teléfonos celulares, las tarjetas de crédito y débito seguirán teniendo una significativa importancia dentro de los medios de pago electrónicos. Además, las tarjetas de crédito ofrecen múltiples beneficios tales como: avances en efectivo en el país y en el exterior, seguros de viajes, acceso a servicios de reservas de pasajes aéreos y hoteles, seguros de vida gratuitos en caso de accidente o enfermedad, servicios gratuitos de asistencia médica, seguros contra fraude, acumulación de millas o puntos para ser redimidos por pasajes aéreos, electrodomésticos, comidas y otras opciones. Para los comercios, señala Asobancaria, las ventajas que brinda el uso del dinero plástico van más allá de incrementar ventas, pues gracias a este sistema se facilita el acceso a nuevos clientes, nacionales e internacionales, se disminuyen los costos por manejo de cheques y efectivo y se eliminan procesos como la gestión de cobro, mantenimiento de cajas de seguridad y permanente de efectivo.

El aumento en el número de fraudes bancarios y comerciales desde Internet se debe, en parte, al explosivo crecimiento de transacciones en línea que ofrecen los bancos del país. A continuación hay una descripción de las modalidades usadas para el fraude electrónico y cómo funcionan.

- *Phishing (pesca).* Es una de las más 'novedosas' formas de engaño. Aquí las víctimas reciben un correo electrónico a nombre de una entidad financiera —normalmente el banco donde tiene su dinero— para invitarlo a hacer clic en un enlace que lo llevará a una supuesta página segura para que actualice sus datos. (Como el número de cuentas, números de las tarjetas de crédito, sus claves, nombre y contraseña de cuentas, número de cédula, entre otros). La página a donde lleva el enlace es una falsificación de la página original del banco. El usuario, engañado, entrega sus datos (con la promesa de recibir premios o incluso bajo amenazas de cancelación de su cuenta si no lo hace) y así cae en el ilícito.

- *Spoofing (engaño).* Es una técnica que permite al delincuente 'llevar' al usuario hacia sus páginas Web falsas, cuando se digita en el navegador de Internet la dirección del banco o la entidad financiera. "Con 'ayuda' de software espía, el delincuente sabe a qué banco se conecta la víctima. Toma control del navegador y lo redirecciona a sus páginas ficticias, allí el cliente digita sus datos creyendo que está en el sitio Web de su banco". Otra modalidad de *spoofing* es una denominada de 'salto', en donde la víctima, cuando trata de entrar a la página del banco, es redireccionada a otra página para que 'por seguridad' digite sus datos y luego es enviada al sitio original del banco.

- *Software espía.* Son un conjunto de programas que se instalan en el PC de la víctima y permiten que los delincuentes monitoreen sus actividades (páginas que visita, tipo de información que busca, entre otros.).

- *Key logger (captura de teclado).* Son herramientas de software o hardware que permiten grabar el texto que escribe una persona en su teclado. En el caso del software, el *key logger* captura todo lo que escribe la víctima y lo envía a una dirección de correo electrónico configurado por el delincuente. Estos programas se instalan y funcionan de manera 'invisible' (no se da cuenta el usuario). Existen también unos dispositivos USB y PS2 que se conectan entre el PC y el teclado, los cuales graban en una memoria interna el texto tecleado en el computador.

- *Copiado de banda.* La finalidad es obtener la clave y la información de la banda magnética para tener acceso a los recursos del cliente. Se utilizan copiadores o *skimer*, elementos que son instalados dentro de la lectora de los cajeros automáticos, o manipulando los datáfonos en restaurantes y comercios. También se usan lectores falsos, que son dispositivos instalados encima o debajo de las lectoras, de tal forma que el cliente, al pasar la tarjeta, la pasa tanto por el lector del cajero automático como por el falso lector, de manera que captura la información y la envía a algún tipo de almacenamiento (diskette, CD, memoria, entre otros.).

- *Opción abierta.* El cliente comienza la operación en un cajero automático, cuando personas de la fila le sugieren pasar al otro cajero contiguo. El cliente no cancela la transacción, pasa a otro módulo y abre otra transacción. Las personas continúan con la transacción abierta en el primer cajero.

- *Bloqueo de teclado*. Consiste en usar elementos como pedazos de papel o láminas pequeñas, extraños al teclado, que simulan el bloqueo del teclado y el usuario no identifica esta situación hasta después de haber digitado la clave. En este momento el usuario se retira del cajero creyendo no haber realizado la transacción y en ese momento, el delincuente realiza transacciones o toma el dato de PIN.

- *Cambiazo*. Una persona se apodera de la tarjeta del cliente y el delincuente observa la clave secreta sin que el cliente lo note. Por lo general, este evento ocurre por exceso de confianza, y desatención a las recomendaciones.

1.3.15. Fraude en cajeros automáticos

Cada cajero es, prácticamente, una pequeña oficina bancaria. Los cajeros multiplican las posibilidades de atender a los clientes, en forma cercana, permanente, rápida, eficiente, y con el mínimo de molestias. Pero como en toda innovación, los cajeros amplían el campo de las responsabilidades en materia de seguridad y lo dispersan tanto en el espacio como en el tiempo. Los clientes usuarios, el personal que los sirve, el personal que les da seguridad y las máquinas

mismas, crean necesidades de protección, muy asociadas a la eficiencia del sistema. Y la eficiencia del sistema justifica el esfuerzo.

En la actualidad se vienen desarrollando estrategias para minimizar el riesgo, inclusive insistiendo en que todos los cajeros tengan video para registrar a quienes realizan las transacciones, ya que el mayor índice de fraudes y delitos se registra cuando no hay video de seguridad, Algunos ejemplos son: retiros por personas no autorizadas, retiro de efectivo por usuarios coaccionados y retiro de la máquina por métodos violentos, entre otros.

- *Obstrucción del movimiento de la ventanilla.* La primera de las formas adoptadas por la delincuencia fue la de impregnar de algún tipo de pegamento (goma) la ventanilla móvil, para impedir su movimiento. El cliente se quedaba esperando que aquella se abriera, y terminaba retirándose, atribuyéndole mal funcionamiento o falla. El delincuente esperaba que el cliente se alejara y con variados instrumentos forzaba la ventanilla y retiraba el dinero del frustrado cliente.

  La misma finalidad se lograba cuando se ponen elementos extraños, como piedras, pedazos de suela de zapato (de goma), paletas de helados; todos impedían el levantamiento de la ventanilla.

  Para engañar al cliente, se cubría la ventanilla real con una falsa que, aunque la real se levantara, la falsa se mantenía impidiendo al cliente retirar su dinero. Al retirarse el cliente, los delincuentes quitaban la falsa y se apoderaban del efectivo dispensado. Esta modalidad tuvo variantes en el tipo de impedimentos que ponían, y las medidas que se tomaban no tardaban en ser burladas mediante algún otro truco.

  La falsa ventanilla tenía un aspecto muy similar a la real. Era construida de lata o de fórmica y forrada en papel contac de color negro mate. De material similar eran los cartones que se usaban para recibir el dinero que debería caer en el receptáculo que existe detrás de la ventanilla. Posteriormente, se las ingeniaron para hacer una metálica con la que lograban obstruir el movimiento ascendente de la ventanilla, una vez que el dinero había caído en el citado receptáculo.

  Emplearon el sistema de obstruir con la mano la salida del efectivo que, usando la tarjeta, habían solicitado. Con lo que provocaban el error de que el cajero actuara como si el dinero no hubiera sido dispensado, y por lo tanto, lo dejara de cargar en la cuenta del delincuente usuario.

  Después provocaban, con el uso normal de su tarjeta, el levantamiento de la ventanilla, y ponían, en la salida del efectivo hacia el lugar de dispensación, una lámina con las dimensiones exactas y necesarias para retener tras ella

el efectivo dispensado a un usuario y hacer creer al cliente que por alguna razón el cajero no había dispensado el dinero. Como siempre, cuando se retiraba el cliente, venía el delincuente y, forzándola o usando su tarjeta, hacía abrir de nuevo la ventanilla, retiraba su dispositivo y lo que había sido dispensado supuestamente al cliente y que se había quedado entre la salida normal y la lámina que le había sido puesta.

- *Retención fraudulenta de la tarjeta.* Otro modo de delincuencia, muy ingenioso y que han estado perfeccionando, es el de introducir por la ranura por la que se debe insertar la tarjeta, una cinta de determinadas dimensiones que entra y su extremo vuelve a salir, pegando ambos extremos, uno hacia arriba de la parte superior interna de la ranura, y el otro hacia abajo en la parte inferior. La cinta es del material que se usa para las radiografías, y tiene un ancho que no obstruye la lectura de la banda magnética de la tarjeta. La cinta lleva, además, cortada una "uña" que sirve de retención, de manera que al introducirse, vaya hasta el fondo, pero luego no logre salir porque con esa uña se le impide la maniobra.

  Cuando termina su transacción, que puede realizarse en forma normal, el cliente espera la devolución de su tarjeta por parte del cajero. Advierte que ésta ha sido retenida, supone que algo raro ha pasado y se retira molesto. Lo aconsejable de inmediato es llamar a los teléfonos del banco que se han suministrado para esos casos y notificar lo ocurrido. Durante el corto lapso de la espera del cliente, aparece un "buen ciudadano" en su auxilio y le pregunta qué le ha ocurrido. Entonces, "muy amablemente" le recomienda marcar su número clave tres veces seguidas, con lo que el cajero le devolvería su tarjeta. Al proceder el ingenuo cliente a marcar tres veces su clave, el delincuente la capta, se la aprende, y como esto no sirve para obtener devuelta su tarjeta, el cliente se retira. El delincuente, con unas pinzas, retira su cinta que arrastrará consigo la tarjeta. Ahora tiene la tarjeta y la clave. Inicia, tan pronto como le sea posible, los retiros, antes de que el cliente solicite que le anulen su tarjeta.

  Es oportuno poner atención en el reclutamiento y selección del personal que sirve a los cajeros y, además, llevar un registro de aquellos que han prestado ese servicio y se han retirado de los bancos del país y si le es posible del extranjero. Pues algunos de estos procedimientos difícilmente son aplicables sin el conocimiento o la asesoría de quienes dominen bien las intimidades técnicas de las máquinas.

  El caso del empleo de un taladro con el que perforan en las vecindades de las ventanillas, justo en un lugar donde penetran con un instrumento fino (tipo alambre) y de una longitud determinada provocan la activación de un pestillo presionado que libera el mecanismo y facilita la apertura de la ventanilla.

- *Usurpacion de identidad.* Citaré ahora un procedimiento que es en realidad una estafa, pero que se inicia a través de los cajeros, aprovechándose de sus características. Los bancos lo califican como "usurpación de identidad". El delincuente abre una cuenta de ahorros con un monto mínimo. Solicita luego su tarjeta para uso del cajero. Ubica, mediante complicidad de algún empleado del banco, cuentas con saldos elevados y con una cédula de identidad con los datos del cliente propietario de esas cuentas pero con su foto (la del delincuente), hace la solicitud de incorporar aquellas cuentas a su tarjeta. Cuando lo logra, empieza a hacer transferencias de éstas a su cuenta de ahorros y los correspondientes retiros. Abandona pronto el "trabajo", por el temor a ser descubierto, mientras se busca a otra víctima. Lo normal es que la documentación usada para abrir su cuenta de ahorros haya sido falsa, y, por ende, se hace difícil su identificación y captura.

Los clientes con cuentas de saldos muy elevados hacen poco uso de la tarjeta, por eso no notan lo que les está ocurriendo. Como para afiliar otras cuentas a una nueva se requiere anular la tarjeta con la que podían mover las anteriores, el delincuente, cuando pide que se afilien las nuevas cuentas a su tarjeta, empieza por solicitar la anulación de la anterior; lo que logra porque se identifica como propietario. Generalmente, da como explicación haber olvidado el número de su clave.

Claro que cada vez que uno de estos procedimientos se empieza a aplicar, se inicia la investigación y la consecuente toma de las medidas que lo dificulten.

1.3.16.
Otras modalidades de fraude

- *Hurto a clientes (fleteo).* Es una modalidad delictiva de hurto calificado en la que el delincuente espera a su víctima, una vez sale del banco o cajero automático, luego de retirar dinero en efectivo. Después, la sigue en motocicleta para detener a la persona con armas de fuego y hurtarle el dinero.

- *Atraco a oficinas.* Pérdida sufrida por sustracción de efectivo o títulos valores, disponible en la caja (de los cajeros humanos) o en las bóvedas.

- *Suplantación*. La suplantación de funcionarios es una modalidad de fraude en la que las personas desconocidas se hacen pasar por funcionarios de la entidad bancaria y reciben documentos o valores para luego desaparecer. También de clientes: una persona desconocida se hace pasar por un tercero en el momento de efectuar una solicitud de crédito, utilizando un documento de identificación robado o una reproducción falsa, de manera que el crédito es desembolsado al delincuente y queda como moroso el cliente suplantado.

- *Fraude interno.* Se puede presentar de diferentes formas: empleados que tienen acceso a cuentas direccionan los recursos por medio de abonos a cuentas propias. O funcionarios con perfiles de acceso amplios que manipulan la información del sistema y la confianza que tienen de sus compañeros de trabajo para apoderarse de depósitos de los clientes. Empleados ajenos a las funciones de recaudo de efectivo, que se ganan la confianza de los clientes de la oficina, recibiendo de éstos dineros que no son abonados a las obligaciones, o cuentas en las que el cliente tiene.

Conclusiones

A pesar de las medidas de seguridad que las tarjetas de crédito y débito llevan integradas en su propio sistema, no hay nada seguro. El fraude en las tarjetas de crédito y débito es un problema costoso que debe ser atacado con un esfuerzo de todos, pero principalmente capacitando y concientizando al usuario de su responsabilidad y de los riesgos que asume.

Por esto, las medidas de seguridad deben procurarse no sólo por las entidades prestatarias de servicios financieros automatizados sino también por parte de la misma clientela (consumidores) y crear responsabilidades ante actitudes negligentes.

Administrar la tarjeta y protegerla del abuso es algo que lleva muy poco tiempo y esfuerzo. Unos pocos minutos ahora pueden ahorrarle horas de frustración más tarde.

Los delincuentes, una vez tienen el número de cuenta de la tarjeta y su fecha de caducidad, pueden comprar lo que sea. Comprar por catálogo o comprar tiquetes de avión por teléfono. Y ellos utilizan todo tipo de tretas, desde un comprobante elaborado (que es un documento falso) hasta una compra fraudulenta por teléfono.

Algunas recomendaciones son:

- Tenga cuidado cuando facilite información sobre su tarjeta de crédito y debito.
- ¡Guarde todos los recibos y compárelos cada mes con su estado de cuentas!
- ¡Si ve una compra que no reconoce o nota inconsistencias, llame o escriba a la entidad emisora de su tarjeta de crédito inmediatamente! (Concilie oportunamente).
- ¡No revele ninguna información personal cuando use su tarjeta de crédito!
- El vendedor sólo puede exigir su tarjeta de crédito vigente, su documento de identidad, el teléfono y su firma.

- Si un miembro cercano de su familia 'toma prestada' su tarjeta de crédito para realizar una compra, usted es el responsable. Trate su tarjeta de crédito como la importante propiedad privada que es.
- Si usted se separa o divorcia y su cónyuge es co-titular de la tarjeta, podría ser responsable por las compras que realice. Asegúrese de modificar el status de su tarjeta de crédito cada vez que su estado civil cambie.
- No olvide que su tarjeta le ofrece grandes ventajas y beneficios, pero también requiere todos los cuidados en su manejo.
- ¡Las tarjetas, como la confianza, también se pueden perder y no volverse a recuperar!
- En caso de que se realice una transacción fraudulenta con su tarjeta, una vez extraviada, usted estará cubierto por un seguro de fraudes, siempre y cuando haya informado el hecho de manera oportuna.
- Cuando realice compras, no permita que retiren su tarjeta para legalizar la compra en otro sitio.
- Exija que el comprobante de pago sea tramitado en su presencia.
- No arroje a la basura la copia del comprobante de pago.
- Nunca porte sus documentos de identificación junto con las tarjetas débito o crédito.
- Cuando reciba su clave personal, memorícela y destruya el documento donde venía. Si decide anotarla, no la registre junto con los documentos que porta habitualmente.
- Si recibe llamadas en las que le solicitan información personal, constate que se trata de la entidad financiera que le otorgó su tarjeta.
- Si perdió sus documentos y le avisan que fueron encontrados, pero que necesitan su clave para realizar el bloqueo, por favor no la suministre. Se trata de una estafa.
- No suministre ningún tipo de información que soliciten por correo electrónico, sólo es seguro ingresar a la página de cada banco.

Bibliografía

Asociación Bancaria y Entidades Financieras de Colombia- Asobancaria. Informe anual 2006. Bogotá: 2006. Capítulo 3. P. 39-43.

Banco de pagos internacionales. Documento consultivo. Nuevo acuerdo de capital de Basilea. Traducción realizada por la Asociación de Supervisores Bancarios de las Américas (ASBA). Enero 2001.

Estupiñán. Rodrigo y Cano Miguel (2003). Control interno y fraude. Bogotá: Ed. Roesga.

Sitios en Internet:

www.asobancaria.com,http://www.asobancaria.com/upload/docs/docPub2971_2.pdf. Fecha de consulta: septiembre 5 de 2007.

www.bancosantander.com, http://www.bancosantander.com.co/servlet/co.com.pragma.documenta.servlet.seccion.MostrarSeccion?seccion=/HOME/BANCOSANTANDER/SEGURIDAD/. Fecha de consulta: septiembre 9 de 2007.

http://www.superfinanciera.gov.co/. Siguiendo la ruta: Comunicados y Publicaciones. Superintendencia Financiera de Colombia 2006. Título: Riesgo de la Actividad Fiduciaria. Congreso Latinoamericano de Fideicomiso – COLAFI. Montevideo, Uruguay. 18 de octubre de 2006. Fecha de consulta: agosto 25 de 2007.

http://www.redebanmulticolor.com.co/portal/page?_pageid=473,762568&_dad=portal&_schema=PORTAL. Fecha de consulta: septiembre 1 de 2007.