Trabajo Monográfico para obtener el título de Contador Público presentado ante la Facultad de Ciencias Económicas y de Administración de la Universidad de la República.

Cátedra: Control Interno y Organización de Sistemas Contables.

PROCEDIMIENTOS PARA MITIGAR EL RIESGO DE FRAUDE EN TARJETAS DE CRÉDITO EN EL SISTEMA FINANCIERO URUGUAYO

Borbonet, Luis

Pereyra, Germán

Tejedor, Alejandro

Orientador: Cr. Fernando Borba

Diciembre 2012

AGRADECIMIENTOS:

Queremos agradecer en primer lugar al Cr. Fernando Borba por su colaboración y guía en este trabajo monográfico y al Cr. Luis Sauleda quien confió en nosotros permitiéndonos presentar esta investigación.

Además, queremos agradecer a todas las personas entrevistadas, que gentilmente nos brindaron su disposición, colaboración e información valiosa para la realización del presente trabajo.

Hacemos una mención especial a las siguientes personas: Sr. Rafael Saldain, Sr. Héctor Cabano, Lic. Juan Tejedor, Sr. Daniel Pereyra, Sr. Daniel Colet; las cuales de diversas maneras fueron sumamente provechosos para nuestra investigación.

Por ultimo no queremos olvidar a nuestras familias, amigos, y entorno laboral por el apoyo incondicional que recibimos por parte de ellos.

PRÓLOGO

El presente trabajo monográfico trata sobre el producto tarjeta de crédito y los riesgos de fraude que el mismo conlleva. Se involucrarán en el mismo los demás agentes que intervienen en el ciclo de vida de la tarjeta como son las instituciones financieras bancarias y no bancarias, las cuales juegan el papel de agente emisor de la misma; la empresa embozadora que es la encargada de realizar el plástico; correo o courier como encargado de trasladar el producto objeto de estudio ya sea a la institución financiera como así también al usuario o cliente; los procesadores de las transacciones; el cliente o usuario (también visto como tarjetahabiente) y como última instancia el comercio en el cual la tarjeta será utilizada, que de alguna manera será el inicio de la transacción.

El objetivo del trabajo realizado es informar al lector acerca de cómo una persona en Uruguay, puede llegar a obtener una tarjeta de crédito, con los riesgos que esto trae aparejado desde la instancia en que solicita la misma, pasando por el momento en que la utiliza hasta llegar al punto que puede deshacerse de ella. Además se analizará cómo puede afectar el fraude a los diferentes sujetos intervinientes, las medidas de control que cada uno desarrollará y aplicará para minimizar el impacto en caso de ocurrencia del mismo. Se muestra el rol del procesador, tanto adquirente como emisor, respecto al papel que juega a la hora del control que realiza sobre el fraude con tarjetas de crédito en Uruguay. La redacción del mismo apunta al público en general, que según una encuesta realizada por nosotros antes de realizar este trabajo, reveló que no existe conciencia por parte del usuario respecto al cuidado y las precauciones que deben ser tenidas en cuenta a la hora de la utilización de cualquier tarjeta de crédito. Se desarrollarán y analizarán varios ejemplos prácticos para una mejor comprensión de cómo los procesadores realizan el control para evitar así el fraude, no solamente dentro de nuestro país, sino con tarjetas emitidas en Uruguay y que son utilizadas fuera de fronteras.

Se utilizaron diferentes métodos de investigación, siendo la entrevista personal, el más utilizado. Otros fueron la entrevista telefónica, la observación directa, además de la lectura de documentos bibliográficos, lectura de instructivos y manuales, como así también de documentos bibliográficos. Fueron entrevistadas cinco **instituciones financieras bancarias**: Banco Santander, Banco de la República Oriental del Uruguay, Citibank, Banco Itaú y Nuevo Banco Comercial. Tres **instituciones financieras no bancarias**: Pronto, Creditel y Oca; **dos procesadores** de los cuales uno es emisor, Sistarbanc, y el otro es emisor y adquirente a la vez, como es el caso First Data; y una **empresa de desarrollo de software para detección y prevención de fraude** como lo es PayTrue.

Los diferentes capítulos del trabajo, mostrarán en primer lugar un análisis del ciclo de vida de una tarjeta de crédito, desde su solicitud hasta que la misma es destruida. En los capítulos siguientes se desarrolla el concepto de fraude junto con los diferentes tipos clasificados por un sello internacional en particular, el concepto de procesador (adquirente y emisor), así como también el sistema neural, utilizado para detectar el fraude a través de las transacciones con tarjeta de crédito. En los capítulos finales, se explicarán los tipos de fraude más comunes en nuestro país y la región, se mostrarán gráficas con datos actuales del mercado tarjetas en nuestro país y la región, para concluir con un cuadro de identificación de riesgos y aplicación de actividades de control realizado básicamente a través del enfoque del procesador emisor, basado en la metodología del Informe Coso. En el mismo se evaluarán los controles por nosotros detectados así como también se realizarán algunas recomendaciones que servirán de utilidad a la hora del análisis. Para terminar el mismo, se exponen las conclusiones finales, en donde se explicita qué sucede en este país respecto al fraude en la región, además de realizar comentarios acerca de lo que se pudo rescatar una vez finalizada la investigación.

CAPÍTULO I

CICLO DE VIDA DE LA TARJETA DE CRÉDITO

1.1. Sujetos intervinientes

En toda transacción comercial existen dos actores principales. Por un lado quien compra el bien o servicio; por otro, quien lo vende o presta. El vínculo entre ambas partes es la entrega o prestación del bien o servicio respectivo, generalmente a cambio de la entrega de dinero. Ésta es una de las tantas formas que existe. Así como en su momento surge la moneda como necesidad de las personas en las operaciones comerciales para sustituir al trueque, diversas características del comercio tales como grandes volúmenes de operaciones o cuantía de las mismas, sencillez para compras internacionales, compras por internet, comodidad, seguridad y otras, hicieron surgir la necesidad de contar con un medio de pago que sustituya la entrega de efectivo en el momento de la transacción. Esta nueva forma de pago, va a tener ventajas para ambas partes; una de ellas es que no va a ser necesario el dinero para realizar dicha transacción, lo cual trae aparejado otras ventajas, como evitar el robo de dinero, la utilización de dinero falso, entre otros. Además, el que vende podrá hacerlo a crédito, teniendo la seguridad de que va a cobrar el mismo, aparte de hacerse del cobro en menos tiempo del crédito que otorgó. Mientras que para el que compra la gran ventaja es la posibilidad de comprar a crédito en todos los comercios que acepten tarjetas y muchas veces sin pagar intereses. Es por estas ventajas y otras, como el caso de no tener la necesidad de realizar transacciones en efectivo en el exterior, que dicha forma de pago ha tenido gran utilización.

Vista esta necesidad es que se crea el producto tarjeta de crédito, el cual va a ser el nuevo vínculo entre el ofertante y el demandante. No sustituye las demás formas de compra venta, sino que es un medio de pago alternativo entre los tantos que existen.

La tarjeta como medio de pago hace que intervengan nuevos sujetos que ahora están intermediando entre quien presta el servicio o vende y quien paga por el mismo. Los mismos son: las entidades financieras bancarias o no bancarias y los sellos.

Dada la complejidad en este tipo de transacciones y los múltiples riesgos existentes, es que aparecen otros actores que estarán vinculados directa o indirectamente a la logística por temas comerciales, por temas de seguridad principalmente y funcionarán como soporte a los intermediarios referidos anteriormente.

Para comprender el rol de cada uno de los sujetos intervinientes es que en el siguiente trabajo de investigación se desarrollará el ciclo de vida de una tarjeta de crédito; desde su nacimiento hasta que se destruye el plástico, contemplando todas las etapas, quiénes intervienen y la interacción entre los mismos.

Luego se visualizará claramente de qué forma intervienen cada uno de los sujetos en las diferentes etapas del ciclo de vida de una tarjeta de crédito así como también los principales riesgos que conlleva cada etapa para cada sujeto.

1.2. Etapas del ciclo de vida de la tarjeta de crédito

La tarjeta como intermediador contempla la participación de dos sujetos fundamentalmente que son: por un lado la **entidad financiera** la cual puede ser una institución bancaria o no, y por otro lado los **sellos** (Visa, MasterCard, Cabal, Diners, American Express entre los principales). En Uruguay, existen casos que estos dos sujetos están comprendidos en la misma entidad, como son los de Oca y Creditel a manera de ejemplo.

Cada uno de estos dos sujetos intermedia con una de las partes. Por un lado, las instituciones bancarias o no bancarias, que se vinculan con el **consumidor final,** quien hace uso de la tarjeta para sus compras; y por otro lado, los sellos que se vinculan con el **comercio**, quien vende el producto o servicio requerido por el consumidor final. Por ejemplo, un comercio que trabaja con Visa, aceptará todas las tarjetas con ese sello sin importar quién es la institución financiera emisora de la misma.

1.2.1. Vinculación del consumidor final de la tarjeta con la entidad financiera

Generalmente el inicio se da con la solicitud de la tarjeta, tanto sea porque el usuario concurre a solicitar el producto o porque le es ofrecido y éste lo acepta. Se da así entonces el primer contacto que se produce entre el usuario y la institución financiera.

Para el caso en el que el cliente concurre a la institución financiera a solicitar la tarjeta, se le exige presentar cierta documentación, ya que con la misma se decidirá por parte de la primera si se le otorga la tarjeta y los límites de crédito de la misma. Para algunas instituciones, la solicitud también la puede hacer vía internet, aunque de todas maneras debe siempre como última instancia presentar la documentación correspondiente. La misma puede variar entre las distintas instituciones en la forma, pero se puede resumir en:

A) Cédula de identidad.

B) Comprobante de domicilio del titular.

C) Comprobante de ingreso.

Es en este último punto donde varían las instituciones, algunas solo aceptan recibo de sueldo, otras aceptan certificado de ingresos firmado por contador y otras, comprobantes de gastos del titular e infieren ingresos con los mismos. Esto último se da básicamente con las instituciones financieras no bancarias, cuyo segmento de mercado más importante se compone de clientes que carecen de comprobantes que prueben sus ingresos, haciendo que la medición del gasto sea la mejor manera de determinar los mismos. También se da el caso, en instituciones bancarias, que no es necesario llevar comprobante de ingreso, siempre que presente declaración de los mismos a través de un estado de cuenta de otra tarjeta de crédito con otra institución. De esta manera queda respaldado el ingreso declarado por el usuario y el banco aplicará su política crediticia para así otorgarle un límite de crédito en base a dicho ingreso. De todas formas, es importante resaltar, que cada institución (bancaria o no) puede estimar los ingresos del tarjetahabiente para otorgarle un límite de crédito, basado en criterios propios de cada institución, pero siempre sin desviarse de aquellos autorizados por la normativa banco centralista vigente que regula el riesgo crediticio y en particular el vinculado a instituciones financieras.

Para el caso de empresas, el Banco Central del Uruguay tiene diferentes exigencias respecto a personas físicas en lo referente a la información a exigir por parte de las instituciones financieras, tanto bancarias como no bancarias[1]. Las mismas están orientadas a controlar el riesgo crediticio que cada institución lleva asociada.

Como se mencionara anteriormente, el producto tarjeta de crédito se le otorga a clientes nuevos o ya con antecedentes en la institución, y esto puede hacer variar la documentación que se solicita, es decir que haya documentación que no sea necesario solicitarla. A modo de ejemplo si el cliente cobra el sueldo por esa institución, hay casos en el que no se le pide ni comprobante de ingreso ni de domicilio, aunque hay instituciones que de todos modos lo hacen. Lo mismo para otros productos de la institución financiera que el cliente haya solicitado, como es el caso de los préstamos.

Cuando la institución financiera ofrece la tarjeta de crédito al cliente se hace de forma masiva, ya sea a través de bases de datos de clientes propios de las instituciones financieras o de potenciales clientes. Lo que busca la financiera en este caso es, mediante el

[1] Las mismas se encuentran principalmente en la Norma Particular 3.8 y la Comunicación 2006/195, ambas del Banco Central del Uruguay (fuente: www.bcu.gub.uy)

ofrecimiento a un grupo grande de clientes, captar la mayor cantidad posible de éstos. En el primer caso, cuando es cliente del banco, ésta ya tiene los datos del mismo y ahí aplicando sus políticas crediticias decidirá a quién le otorga la tarjeta. Posteriormente determinará qué límite de crédito le otorga ya sea porque conoce los ingresos del cliente o tiene que inferir los mismos (sujeto a normativa B.C.U. vigente que regula el límite de crédito a otorgar el cual es un porcentaje respecto a la R.P.B.B.). Los ingresos del cliente se conocen porque, o bien éste adquirió recientemente algún producto con la entidad financiera, o porque son clientes que cobran el sueldo a través del banco (clientes nóminas). En el otro caso, cuando se habla del ofrecimiento a potenciales clientes, se realiza a través de convenios con socios comerciales donde éstos comparten parte de la base de datos propia con la financiera. Esta decidirá a quién le otorga la tarjeta y posteriormente qué límite de crédito otorgará infiriendo ingresos, siempre teniendo en cuenta la normativa B.C.U. ya mencionada. En ambas situaciones la tarjeta generalmente es ofrecida pero hay casos donde la misma ya está formalizada (cuando se imprime el plástico) sin conocimiento previo del cliente, a quien se le da aviso que tiene la tarjeta para retirar o la misma le llega al domicilio y éste solamente decidirá si la acepta o no. Esto dependerá de las políticas comerciales de las instituciones financieras. Es común observar esta situación en socios comerciales donde el usuario integra la base de datos del mismo y al momento de realizar una compra se le da aviso que tiene la tarjeta para retirar. Por lo tanto, a modo de resumen, para el caso en que la tarjeta es ofrecida al usuario, siempre serán requeridos, ya sea en sucursal como en el stand del socio comercial, todos los datos personales junto con la documentación correspondiente. Los casos en que la tarjeta es enviada al cliente directamente, se dan porque ya hay un conocimiento previo de la institución con éste. Por este motivo no requiere realizar la solicitud, ni tampoco presentar la documentación señalada anteriormente, y se espera la aceptación por parte de la institución.

Siempre el vínculo entre el cliente y la institución va a estar documentado mediante la firma de un contrato, en el cual el cliente acepta todas las condiciones del producto. La financiera se queda con un registro de la firma que se verá más adelante la importancia que tiene al mencionar en el capítulo cinco las responsabilidades ante casos de fraude.

Al solicitar u ofrecer la tarjeta, la entidad financiera debe consultar al usuario con qué sello quiere tener la misma. O sea primero se elige al primer intermediario que en este caso es la institución financiera y luego se opta por el segundo que pasa a ser el respectivo sello (se aclara que existen casos en que por determinados acuerdos comerciales algunas tarjetas sólo trabajan con un sello). El sello se encarga de establecer el vínculo con el comercio. Para comprender un poco más acerca de la elección del mismo por parte del usuario, se describe el siguiente ejemplo: una persona solicita una tarjeta de crédito en el banco “equis”, y éste le da a elegir con qué sello quiere la misma. En nuestro país los principales sellos con los cuales más se trabaja son Visa y MasterCard, por lo tanto la persona va a

optar por un sello en particular, en este caso suponemos que elige MasterCard. La mayoría de los comercios trabaja con los dos sellos pero puede pasar que el supermercado Y trabaja con Visa solamente. A su vez el banco "equis" realiza una campaña comercial con este supermercado en el cual otorga beneficios comerciales por la compra con su tarjeta. El usuario no sólo no podrá acceder al beneficio sino que directamente no va a poder comprar con la tarjeta debido a que el comercio no trabaja con el sello elegido por el usuario. Con este ejemplo se ve la diferencia entre los vínculos; por un lado el del comercio con el sello y por otro lado el del usuario con la institución financiera, teniendo en cuenta que el vínculo entre el comercio y la institución financiera va a ser solamente comercial. Hay excepciones, como el caso de Oca, en el cual ambos intermediarios son uno solo, es decir que Oca se contacta con el comercio y con el usuario.

La tarjeta puede ser doméstica (uso solamente en Uruguay), regional (con países cercanos en la región) o internacional. No todas las instituciones financieras ofrecen tarjetas internacionales ya que ésto va a depender del sello con los cuales trabajan. Es el usuario quien elegirá el tipo de tarjeta a solicitar y luego será la institución quién decidirá si se la otorga o no en base al análisis del riesgo implícito.

La misma va a estar a nombre de la persona que la solicita (titular), pudiendo ser persona física o jurídica. En este último caso estamos ante el caso de tarjetas corporativas donde la misma pertenece a la empresa y estará a nombre de la persona física que trabaja para la misma. La solicitud va a requerir la firma del apoderado de la empresa ante el banco.

Caso similar se da para los adicionales (se desarrollará más adelante en este capítulo), en los cuales la solicitud es a través del titular de la tarjeta que solicita un plástico adicional a nombre de un tercero bajo la responsabilidad del titular.

1.2.2. Aceptación de la solicitud de la tarjeta de crédito

Una vez hecha la solicitud, la aceptación de la tarjeta puede o no ser sistematizada. Encontramos que en las instituciones financieras no bancarias la aprobación es mayoritariamente sistematizada. La autorización está sistematizada cuando existe un software que en base a determinados parámetros preestablecidos, y luego de haber sido cargados los datos del usuario, es quien termina de autorizar el producto y las condiciones del mismo, en este caso el límite de crédito. Esto hace que la solicitud sea aceptada o no en el mismo momento que se cargan los datos; es algo automático lo cual hace que no dependa de la decisión de una persona, sino que son parámetros preestablecidos anteriormente por las áreas de riesgo y comercial. Esta sistematización está focalizada en determinar el riesgo crediticio existente para el producto solicitado.

En cambio, en instituciones financieras bancarias si bien el proceso está sistematizado, ya que los datos del usuario son ingresados al sistema y el mismo define el nivel de riesgo para cada cliente, pueden haber casos donde sea una persona la que termina aprobando o no la solicitud y las condiciones de la misma, según el riesgo crediticio definido por éste una vez cargados los datos. Dentro del análisis de riesgo se estudian los antecedentes financieros del solicitante y en especial los que tenga con la propia institución donde se solicita. Ejemplos de esto son: préstamos ya otorgados por la misma a la persona, el cliente tiene una cuenta corriente en la institución, cobra el sueldo a través de la misma por tarjeta de débito, entre otros. En estos casos ya hay antecedentes del cliente con la institución y de solicitarse la documentación es para corroborar los datos ingresados y procesados anteriormente.

Si la tarjeta no es aceptada por parte de la institución financiera, finaliza el vínculo entre ambas partes. Si en cambio es aceptada, se pasa al proceso de embozado de la tarjeta, que significa realizar la confección del plástico identificatorio. El mismo define la identidad de la tarjeta con la persona física, ya que contiene el nombre de la persona, un número de tarjeta, fecha de vencimiento de la misma, el código de verificación correspondiente (los tres números que se encuentra al dorso de la tarjeta), y el CVC2 o CVV que es el número que aparece encriptado en la banda magnética. Éste último no está visible y por lo tanto el usuario desconoce del mismo. Como veremos más adelante, en los capítulos cuatro y cinco, estos datos son indispensables ya que identifican a la persona como titular de la tarjeta lo cual tendrá diferentes implicancias.

1.2.3. Embozado y traslado de la tarjeta de crédito

El embozado puede estar a cargo de la propia institución financiera o puede solicitar a un agente externo que lo realice. Éstos son quienes se encargan de emitir el plástico según la información que se le envía desde la financiera. El embozado puede realizarse tanto dentro del Uruguay, como en el exterior. Un ejemplo de embozado en el exterior es el caso de First Data que emboza desde la República Argentina.

En el proceso de embozado se realiza un control mediante un informe diario de quién realiza cada una de las actividades relacionadas al proceso (embozo, ensobrado, custodia en depósito y traslado). El personal que trabaja en el proceso de embozo, custodia y traslado es contratado teniendo en cuenta los antecedentes laborales anteriores.

Al terminar el proceso de embozado, la tarjeta se puede decir que está pronta para ser trasladada al usuario. Lo único que hay que analizar es si la misma está activa o no, es decir si ya puede ser utilizada por el usuario. En caso de que el servicio de embozado sea tercerizado, la tarjeta puede ser enviada desde la embozadora a la propia institución

financiera o al domicilio del titular. La institución financiera, ya sea porque embozó ella misma o porque la recibió de la empresa embozadora, puede hacérsela llegar al cliente o distribuirla entre sucursales para que el mismo la retire. En el caso de instituciones financieras no bancarias siempre se retira en la propia institución y nunca es enviada al domicilio del titular. El traslado desde la embozadora hacia la institución financiera o entre sucursales se realiza en cartera cerrada precintada de origen en correo privado como custodia de valores. En todos los casos estudiados el envío de la tarjeta al domicilio del cliente se hace mediante correo o courier privado. Por un tema de costos, de logística y de responsabilidades, es que las instituciones deciden tercerizar este servicio en vez de tenerlo incorporado. Cada tarjeta viaja en sobre cerrado y protegido. Dentro del mismo se encuentra una hoja de papel doblada de tal forma que impida que el plástico sea visible, salvo el nombre de la persona impreso en el mencionado papel tal cual aparece en el estado de cuenta. Al hablar de sobre protegido, significa que el mismo es inviolable por estar confeccionado de un nylon especial que de ser abierto queda evidencia de la acción y no hay forma de que vuelva a su estado de origen.

Cuando la tarjeta es enviada al domicilio se dan dos opciones, dependiendo de cada institución financiera:

1) Entrega "puerta adentro", que significa que la misma se entrega a la persona que atiende en el domicilio siempre y cuando ésta sea mayor de edad.

2) Entrega únicamente al titular de la tarjeta contra entrega de documento de identidad, lo que significa que si el mismo no se encuentra en el domicilio la tarjeta no se entrega.

Siempre al entregar la tarjeta se solicita firma a la persona que recibe la misma, tanto se entregue "puerta adentro" como al titular de la tarjeta, ya que es la constancia de entrega que tiene el correo o courier. El mismo tiene un plazo determinado en días para hacer la entrega en donde realizará varios intentos. Además de estos intentos se puede convenir entre el courirer y el titular de la tarjeta, que éste la retire por la sucursal del primero, siempre y cuando esté permitido en el vínculo comercial con la institución financiera. Vencido ese plazo, la tarjeta es devuelta a la institución financiera junto con un informe de las tarjetas entregadas y de las no entregadas. La institución financiera sabe con exactitud dónde se encuentra cada plástico, es decir, si el mismo fue entregado al cliente o si el mismo permanece en custodia del courier (en la empresa), o si por el contrario fue devuelto a la institución financiera. Luego ésta, decidirá según sus políticas, si aguarda un tiempo adicional para que el titular retire la misma en una dependencia de la institución o si por el contrario procederá a la destrucción de la tarjeta de crédito. Si la misma se destruye se da por finalizado el vínculo teniendo que volver a realizar la solicitud de la tarjeta, con la

diferencia que en este caso no tenga que realizar todo el procedimiento de entrega de documentación. Puede que le soliciten firmar un nuevo contrato de solicitud o realizar una reimpresión del plástico.

En algunos casos el tarjetahabiente puede retirar la tarjeta en la sucursal del socio comercial, como es el caso de un supermercado por ejemplo. Esta situación se puede dar porque él mismo así lo solicitó o porque sin solicitarla, la misma fue ofrecida al cliente por parte de la institución financiera a través del socio comercial.

En todo este proceso de entrega, se deja constancia a través de actas, de cada movimiento realizado. Es decir, se elaborará un acta cuando la tarjeta sale del embozo; cuando llega a la custodia; cuando se le entrega al servicio de courier; cuando el courier sale a entregarla, marcando en este caso con qué plásticos vuelve y con cuáles no. Con los que no vuelve, deberá mostrar recibo de entrega con la firma de quien la recibió. En algunas ocasiones, entregada o no la tarjeta, se le exige que deje constancia de algunas características del domicilio de entrega para verificar que efectivamente concurrió a la dirección establecida.

El procedimiento de envío de una tarjeta adicional tiene las mismas características que el envío de la tarjeta al titular.

Para el caso de la entrega de la tarjeta, se debe diferenciar si se da como consecuencia de una reimpresión del plástico ante denuncia por robo o extravío, o si la misma se da como consecuencia de una renovación. Para el caso de reimpresión del plástico ante denuncia por robo o extravío, el usuario debe realizar una llamada telefónica directamente al procesador para realizar la denuncia. La consecuencia de realizar dicha denuncia es que la tarjeta automáticamente es dada de baja y no se pueden realizar más transacciones con ella ya que el número de la misma queda cancelado. La nueva tarjeta va a tener los mismos datos visibles en lo que refiere a nombre y fecha de vencimiento, mientras que va a cambiar el número identificatorio de dieciséis dígitos, el CVC2 o CVV y el código de verificación. En estos casos es la propia procesadora quien se encarga de enviar la tarjeta a la casa del usuario, también vía courier, y en caso de no poder entregar la misma en un determinado número de intentos sigue el mismo proceso que para la solicitud el cual fuera explicado anteriormente. En este caso, además, cabe aclarar que dependiendo del sello de la tarjeta la misma puede llegar activa al domicilio del usuario o no. En caso de no llegar activa, la persona debe realizar una llamada telefónica a un número que aparece en el sobre en el que se encuentra la tarjeta. Dicho número pertenece al procesador, quien tiene el legajo del cliente. Al realizar la llamada, éste deberá responder ciertas preguntas personales que solamente el usuario y el procesador conocen la respuesta. Ejemplos de las mismas son: nombre de la persona, domicilio, si tiene adicionales, dónde realizó la última compra, entre otras. En estos casos no solo se estudia si las respuestas son correctas o no sino también

otros aspectos como la rapidez y la precisión en la respuesta ya que se entiende que las mismas se deben dar en forma espontánea y fluida.

1.2.4. Renovación

La renovación se da en forma automática salvo que el usuario no haya concurrido a la institución para firmar la no renovación o no haya llamado para comunicarlo. También va a depender de otros factores como por ejemplo que el usuario no esté atrasado en los pagos de la misma. En el caso de los adicionales, el cliente no vuelve a firmar otro contrato con la institución, sino que rige el que está vigente desde que solicitara por primera vez el plástico. A su vez, también existe la variante de que el número de dieciséis dígitos de la tarjeta puede mantenerse o puede ser cambiado dependiendo del sello. Lo que cambia inexorablemente es la fecha de vencimiento, el CVC2 o CVV y el código de verificación. En este caso es la institución financiera la encargada de hacerle llegar al usuario el adicional. En la práctica en nuestro país se observa que es costumbre que ante una renovación, la tarjeta viaja activa al domicilio del titular.

Volviendo al tema denuncia por robo o extravío, se debe hacer un paréntesis respecto a ésto. El hecho que exista un lapso de tiempo entre el hurto o extravío y la denuncia, se generará un período en que la tarjeta está activa y por lo tanto puede ser usada por alguien ajeno al titular. Una vez que la misma es denunciada, automáticamente el procesador la bloquea. Cuando la tarjeta ha sido usada por un tercero sin aún ser denunciada por el titular, dependiendo del procesador, pueden existir las siguientes posibilidades: a) que los gastos de la misma sean cubiertos a partir del momento de la denuncia; b) desde la hora cero del día en que se hizo la denuncia; c) veinticuatro horas antes del momento de la misma. El hecho que exista denuncia no es condición necesaria para el reembolso de gastos incurridos con la tarjeta, ya que puede darse cuenta con posterioridad que la tarjeta le fue hurtada y al momento de llegarle el estado de cuenta podrá desconocer los gastos que entienda no le corresponden. Existe un punto de riesgo elevado ya que la tarjeta se encuentra en manos de otra persona y puede suceder que el período de tiempo en el cual la tarjeta estuvo activa en poder de un tercero sea mayor al que cubre la tarjeta según lo mencionado. De ser así, existe la posibilidad de que en el estado de cuenta aparezcan gastos no realizados por el titular, lo cual no implica que éste deba hacerse cargo de los mismos ya que puede desconocerlos ante la financiera y ahí, ésta procederá a ver si el gasto corresponde o no. Es decir que se cuenta con ciertas garantías si no se actúa con negligencia.

Si hablamos de un adicional en la tarjeta de crédito, cabe destacar que la primera vez que se solicita, el usuario debe firmar contrato (firman ambos). En este caso la institución financiera no analiza si califica o no para obtener el respectivo plástico ya que el usuario es

codeudor y la deuda entra en la del titular. Sí puede existir "control de clearing o embargo", o sea que si el adicional está embargado o su nombre aparece en el clearing de informes, la tarjeta puede no ser otorgada por más que no exista ningún inconveniente con el titular. Para dar de baja un adicional es necesario en todos los casos la autorización del titular; por más que el adicional tenga la intención de dar de baja a la tarjeta no puede hasta tanto el titular no lo autorice. Siempre la tarjeta adicional sale activa del procesador y viaja en esa condición hasta la institución bancaria y luego al domicilio del cliente. Es importante destacar en este punto que los adicionales no son tan comunes en instituciones no bancarias.

1.2.5. Utilización de la tarjeta

Una vez que el usuario tiene la tarjeta en su poder y la misma está activa, ya está en condiciones de poder usarla en cualquier comercio que trabaje con el sello de la misma.

Existen dos formas de realizar compras con tarjeta; "compras con tarjeta presente" y "compras a distancia". En el primer caso, el tarjetahabiente concurrirá al comercio en donde hará uso de la tarjeta y éste último pedirá autorización al procesador, vía POS[2] o telefónicamente, quien en definitiva será el que autorice la compra. Una vez realizada ésta, el comercio entrega al titular el voucher para que firme como comprobante de pago. En el comprobante aparece el sello, los datos del comercio como R.U.T. y código de éste ante el procesador, datos de la transacción como importe y número de cuotas, número de autorización, número de voucher y los datos de la tarjeta como número, fecha de vencimiento (ambos encriptados por razones de seguridad) y el nombre del titular. El mismo se imprime en dos vías, las cuales una sola se firma y queda en poder del comercio y la restante queda en poder del cliente.

Para el caso de "compras a distancia", se identifican dos maneras de realizar las mismas, siendo la más frecuente la compra por internet y en menor medida la venta telefónica. En la compra por internet se ingresan los datos de la tarjeta vía web a través de una página segura, la cual puede ser propia del negocio donde se hace la compra o propia del procesador (la página del negocio deriva directamente a la página del procesador)[3]. Primero se ingresa el sello de la tarjeta y posteriormente el número de la misma, su código de verificación y fecha de vencimiento. Al confirmar la compra, la autorización por parte del procesador es instantánea y en la misma página aparece a continuación si la compra fue realizada con éxito o no, y en caso de serlo, el código de autorización de la misma. En

[2] POS: Point of sale (punto de venta).
[3] Se detallará todo lo vinculado a este tema en el capítulo cinco y en el anexo correspondiente.

cambio en la venta telefónica, son solicitados por este medio los datos del cliente para posteriormente realizar la autorización. La misma se solicita llamando al procesador, al cual se le pasan los datos del cliente para que éste autorice o no la compra. Posteriormente a estar autorizada la compra, al cliente se le informa el número de autorización.

La autorización es solicitada por parte del comercio al procesador. La institución financiera puede tener su propio procesador o en su defecto que el mismo se encuentre tercerizado. ¿Qué significa tener su propio procesador? La institución financiera es quien se encarga en todos los casos de aceptar o no al cliente, es decir otorgarle la tarjeta y también de determinar su límite de crédito, por esto es que siempre es responsable del riesgo crediticio del mismo. No sucede lo mismo con el procesador. Una de las principales funciones que realiza el procesador y de particular interés para este trabajo, es la de autorizar o no las transacciones con tarjeta de crédito (es decir aprobar las compras realizadas con las tarjetas). Para ello debe tener un legajo del socio, en el cual además de los datos filiatorios del mismo, antecedentes en plaza y el límite de crédito autorizado, posee un historial de transacciones realizadas con la tarjeta así como también guarda registro de toda comunicación de la persona con el procesador. Esta información sumada a las características del mercado es lo que le permite al procesador contar con la información para poder realizar la tarea de autorizar las transacciones dentro del procesamiento de las mismas.

Por lo tanto, la institución financiera puede tener procesador propio o tercerizarlo. Cuando la mencionada base de datos o legajo de transacciones lo administra la financiera, decimos que tiene procesador propio y es la encargada de autorizar o no las transacciones y por lo tanto es responsable de la administración del riesgo de fraude, además del riesgo crediticio (esto último es siempre responsabilidad de la financiera). Esta tarea también puede ser tercerizada, contratando el servicio de procesador a un tercero el cual administra al cliente, el legajo y las transacciones del mismo. Se hace una breve introducción en este párrafo para ubicar al procesador dentro del ciclo de vida de la tarjeta de crédito. Dada la importancia que tiene en la detección de fraudes, se verá con detalle en el capítulo tres de este trabajo monográfico.

La institución financiera, como administrador del cliente, es quien define el límite de crédito de éste y por lo tanto está vinculado al riesgo crediticio. El administrador se encarga de aceptar o no al cliente como socio y le establece el límite del crédito y sus condiciones, y esto lo hace a través del estudio de riesgo crediticio. Por esta razón es que separamos administrador de procesador. El administrador se encarga solamente de lo mencionado anteriormente. Las tareas del procesador no están vinculadas al riesgo crediticio sino al riesgo de fraude. Si no existiese riesgo de fraude, las funciones del procesador cambiarían sustancialmente.

El procesador le informa periódicamente (diariamente es lo más usual) todas las transacciones procesadas a la institución financiera por cada usuario. Las mismas se acumulan en períodos mensuales según la fecha de cierre de la tarjeta y se le envían al cliente en un resumen que se llama estado de cuenta, en el cual se indica los datos del titular, la fecha de cierre y de vencimiento del pago, el número de tarjeta (el estado de cuenta puede acumular más de una tarjeta del titular en la misma financiera), monto a pagar, recargos aplicables en caso de no pago o de pago mínimo, limite de crédito y crédito disponible; además de diversos datos por otros productos que tenga el usuario con la financiera.

En el cuerpo del estado de cuenta aparece el detalle de transacciones, donde en cada renglón se individualiza cada consumo, detallando la fecha del mismo, tarjeta (se identifica la tarjeta que origina el gasto, para distinguirla si fue la del titular o una adicional, por eso se ingresan los últimos tres números) detalle del comercio donde se realizó la compra (en caso de compras en el exterior, aparece además del nombre un número que la identifica), importe en origen para compras en el exterior, importe en pesos e importe en dólares, y en caso de corresponder, número de cuota que se abona en cada transacción.

El resumen indica el monto a pagar y su vencimiento. El usuario podrá abonar total o parcialmente el mismo, en caso de esta última deberá abonar en su momento los intereses correspondientes.

En caso de no abonar al menos el importe mínimo, las financieras manejan cierto tiempo luego de pasada la fecha de vencimiento para realizar lo que se llama el **bloqueo blando**. Este tiempo varía mucho según cada financiera y la exposición al riesgo del mercado en el que actúan. Se le llama bloqueo blando porque si bien se bloquea la tarjeta y por lo tanto no se pueden realizar transacciones con la misma, se le permite al usuario cancelar su deuda en un lapso de días, desbloqueándosela para que continúe con su uso. En caso de no cancelar la deuda en el mencionado lapso de tiempo durante el bloqueo blando, se procede a lo que se conoce como **bloqueo duro** y en este caso por más que cancele su deuda, la tarjeta no será activada nuevamente y en caso de querer una nueva tarjeta de crédito deberá iniciar el proceso de solicitud, ahora teniendo en cuenta este antecedente crediticio negativo que generó con la financiera.

1.2.6. Baja de la tarjeta

El final de este ciclo de vida, se da con la baja de la tarjeta. El usuario tiene que concurrir personalmente a la dependencia de la institución financiera ya que debe firmar el acta de destrucción y además simbólicamente la tarjeta es cortada con tijera por el funcionario de la

institución financiera. Al firmar dicha acta, el usuario queda cubierto ante cualquier eventualidad que ocurra con la tarjeta ya que hay un documento firmado por la persona que avala la baja de la misma. Cualquier eventualidad puede ser que el banco por error no dé de baja la misma, se le envíe una nueva con su respectivo costo de emisión entre otras.

También ante fallecimiento del titular se da de baja la misma. Diariamente cada institución financiera recibe información por parte del Estado a través del Índice General de Deudores (I.G.D.) en donde se detallan los fallecimientos ocurridos en el país. Si existe una cuenta a nombre de una persona que aparece en el listado enviado por dicho índice la misma se bloquea automáticamente. Al bloquearse la cuenta también quedan sin efecto todos los adicionales que la misma tiene. Cualquier cargo que exista entre el momento del fallecimiento y el momento de la baja, el mismo es responsabilidad del cliente (difunto), por lo que ese cargo pasará a la masa acreedora de éste, salvo que cuente con un seguro de vida sobre saldo deudor.

CAPÍTULO II

INTRODUCCION AL FRAUDE, CONCEPTO Y CLASIFICACION

2.1. Introducción

Todo medio de pago, incluido el de tarjeta de crédito, sufre del flagelo del fraude. El cheque, el efectivo, puede ser falsificado o robado y así sucede también con la tarjeta de crédito. El fraude es una consecuencia del negocio. El equilibrio está en que ese fraude no perjudique mayormente al negocio, que la tarjeta de crédito sea usada por la mayor cantidad de usuarios posible, para así los comercios puedan vender más y como coralario las instituciones financieras hagan su negocio.

Dentro del riesgo de fraude con tarjetas de crédito en nuestro país, se debe enfatizar que existe un conflicto de intereses entre quienes otorgan o venden el producto tarjeta de crédito (generalmente el área comercial de las instituciones financieras) y quienes controlan las mismas para que no exista fraude. Esto se da tanto para aquellas que no se procesan por sí mismas sus transacciones, como para las que sí lo hacen (en este caso el conflicto es interno con el área de riesgos de la institución). Este conflicto de intereses se subsana encontrando un equilibrio entre los controles que pueda aplicar el área de riesgos y las limitaciones que pueda originar al área comercial. El mismo buscará optimizar la relación costo beneficio.

El negocio de emisión y distribución de tarjetas de crédito representa riesgos para la institución financiera y a la vez es una parte significativa de la rentabilidad de la misma.

Existen dos riesgos principales:

1) Riesgo de crédito (no pago)

2) Riesgo de fraude

El objetivo principal es maximizar el beneficio a través de la utilización de herramientas para el análisis y la implementación de medidas que permitan minimizar estos riesgos.

¿Qué es riesgo?[4]

Son todas aquellas circunstancias o eventos que se interponen en el cumplimiento de los objetivos propuestos por la empresa.

Los riesgos afectan la capacidad de la organización de sobrevivir, competir con éxito o mantenerse con una fortaleza financiera adecuada, la imagen pública positiva o la calidad de productos o servicios que brinda. No obstante, es claro que eliminar o reducir los riesgos a cero es imposible, ya que el ambiente de negocios donde se mueven las diferentes organizaciones es riesgoso por naturaleza, ya que es cambiante.

También podemos ver al riesgo como una medida de la incertidumbre. En este sentido, se ha definido al riesgo como "el nivel de exposición a las incertidumbres que una empresa debe entender y efectivamente administrar para lograr alcanzar sus objetivos y crear valor para sus interesados". En todo proceso de negocios, el logro de los objetivos involucra un cierto nivel de incertidumbre. Y en todo proceso de negocios, existen diversos factores que se interponen o pueden interponerse en el logro de dichos objetivos.

Los riesgos pueden involucrar "consecuencias" positivas o negativas. Consecuencias se define como aquellos resultados tangibles derivados de los riesgos en las decisiones, eventos o procesos. Las consecuencias positivas son conocidas como oportunidades, y las consecuencias negativas son llamadas amenazas. No podemos ver con seguridad los riesgos intangibles, pero podemos anticipar y observar las consecuencias del riesgo. El riesgo no es ni bueno ni malo, sólo es riesgo. Los efectos del riesgo y la incertidumbre pueden resultar en consecuencias malas o buenas. No obstante, cuando nosotros pensamos en riesgo, la mayoría pensamos en las consecuencias negativas más que en oportunidades. Las consecuencias pueden variar en su impacto dependiendo de un número de factores, algunos de los cuales se detallan a continuación:

- Los activos de riesgo
- El tipo de amenaza
- La duración de la consecuencia
- La efectividad del control

[4] Conceptos y clasificaciones extraídos del material publicado por la cátedra de Control Interno y Organización de Sistemas Contables de la Facultad de Ciencias Económicas y de Administración en Julio 2003 bajo el título "Apreciación de riesgos" (www.ccee.edu.uy).

Podemos definir el riesgo en tres perspectivas: riesgo como incertidumbre, riesgo como amenaza y riesgo como oportunidad.

Riesgo como incertidumbre: Nivel de exposición a las incertidumbres que una empresa debe entender y efectivamente administrar para lograr alcanzar sus objetivos y crear valor para sus interesados.

Riesgo como amenaza o peligro: Eventos potenciales negativos tales como pérdidas financieras, fraudes, robos, daño en la imagen, injurias o muerte, fallas en los sistemas o problemas legales.

Riesgo como oportunidad: Cuanto mayor es el riego, mayor el retorno potencial y necesariamente mayor la pérdida potencial.

2.2. Concepto de fraude

Según la ***Real Academia Española*** en su vigésima segunda edición, fraude es definido de la siguiente manera:

- Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.
- Acto tendente a eludir una disposición legal en perjuicio del Estado o de terceros.
- Delito que comete el encargado de vigilar la ejecución de contratos públicos, o de algunos privados, confabulándose con la representación de los intereses opuestos.

Fraude también, es toda acción encaminada a eludir cualquier disposición legal, sea fiscal, legal o civil siempre que con ella se produzca un perjuicio contra el estado o contra terceros[5].

Por otra parte, es engaño, inexactitud consciente, abuso de confianza que ocasiona un daño, generalmente material[6].

También es definido como una transacción en la cual el tarjetahabiente no participó ni autorizó[7].

[5] Definición de fraude según diccionario Salvat.
[6] Definición de fraude según diccionario Durvan de la lengua española.

En nuestra opinión, respecto a la definición de Visa Internacional, haremos una salvedad en lo que al tarjetahabiente respecta, ya que la misma establece que para que exista fraude el tarjetahabiente no debe haber participado en la transacción ni autorizado la misma. Si se piensa en el caso del auto fraude, el cual se puede dar tanto porque el mismo tarjetahabiente desconoce una transacción que él mismo realizó, o hasta incluso puede ser partícipe entregando su tarjeta a un tercero para que accione en su lugar, desconociendo posteriormente dicha transacción. Queda claro que en cualquiera de estos dos casos el tarjetahabiente de alguna manera o participó de la transacción o autorizó la misma. Por lo tanto existe una inconsistencia en dicha definición si se considera al auto-fraude como uno de los tipos de fraude.

Respecto a las demás definiciones todas coinciden en que hay un engaño en donde se elude la disposición legal, produciendo un daño contra el Estado o contra un tercero.

Respecto a la incertidumbre puede provenir de dos lados: del lado crediticio a través de la cual el usuario no realice el pago de sus gastos mediante el uso de la tarjeta de crédito; y por otro lado a través del fraude que es el objetivo de este trabajo monográfico. En el fraude, como mencionamos anteriormente, hay una intención negativa hacia un tercero de engañarlo, de mostrarle una realidad distinta a lo que en definitiva sucede o va a suceder. El tercero en este caso puede ser la institución financiera, los sellos, los procesadores y el propio tarjetahabiente.

En definitiva el riesgo de fraude no se puede eliminar pero lo que se trata de hacer en todos los casos es minimizarlo. Profundizaremos sobre el engaño en el uso de la tarjeta de crédito para actividades ilícitas.

Situaciones que no son fraude

Para dejar en claro el concepto de fraude y para tratar de llevar a la práctica el mismo, se debe dejar en claro que tipo de actividades no son consideradas fraude en la utilización de la tarjeta de crédito. Entre las principales podemos encontrar:

- cargos duplicados
- alteraciones de montos
- reclamos por mercancía no entregada

[7] Definición de fraude según Visa Internacional.

- casos de telemercadeo (telemarketing)[8]

2.3. Tipos de fraude

A continuación se enumeran los tipos de fraude según la clasificación del sello internacional Visa[9], con su respectiva definición y sus principales características. No obstante en el capítulo cinco se realizará un análisis más profundo de aquellos fraudes con mayor incidencia en el mercado.

En lo que respecta a los tipos de fraude existentes hoy en día, se encuentran principalmente los siguientes:

(1) Tarjeta perdida

(2) Tarjeta robada

(3) Tarjeta no recibida

(4) Solicitud fraudulenta

(5) Tarjeta falsificada

(6) Tarjeta no presente (uso fraudulento del número de cuenta)

(7) Misceláneo (suplantación de identidad)

A continuación se detallarán cada uno de los tipos mencionados anteriormente.

[8] El telemercadeo o telemarketing es una forma de marketing directo en la que un asesor utiliza el teléfono o cualquier otro medio de comunicación para contactarse con clientes potenciales y comercializar los productos y servicios. Los clientes potenciales se identifican y clasifican por varios medios como ser su historial de compras, encuestas previas, participación en concursos o solicitudes de empleo (por ejemplo a través de Internet). Los nombres también pueden ser comprados de la base de datos de otra compañía u obtenidos de la guía de teléfono u otra lista pública o privada. El proceso de clasificación sirve para encontrar aquellos clientes potenciales con mayores probabilidades de comprar los productos o servicios que la empresa en cuestión ofrece.

[9] Clasificación obtenida del manual de operaciones para Visa Internacional.

1) TARJETA PERDIDA

Definición: Aquellas que el tarjetahabiente extravía y otra persona utiliza después para hacer compras no autorizadas.

Características:

- La firma en el recibo de compra (voucher) no se asemeja a la firma de la tarjeta.
- Altos volúmenes de compra en un período corto de tiempo.
- El delincuente no conoce datos de identificación positiva del tarjetahabiente (si el analista llama al delincuente este no sabrá los datos q identifiquen al titular de la tarjeta, nombre fecha de nacimiento, si tiene adicionales, cuando fue la última compra).

El fraude no es solamente la pérdida de la tarjeta por parte del tarjetahabiente sino que además la posterior utilización de la misma, con desconocimiento del tarjetahabiente. La utilización será por parte de un tercero que se hará pasar por el titular de la misma. El fraude por pérdida será entonces por aquellas transacciones no realizadas o desconocidas por el tarjetahabiente, el cual no cuenta con la tarjeta en su poder al momento de desconocer las transacciones y no hizo la denuncia por la ausencia de la misma.

2) TARJETA ROBADA

Definición: El emisor confirma que la transacción es fraudulenta como resultado de un reclamo del tarjetahabiente de que la tarjeta ha sido robada.

Características:

- La firma en el recibo de compra (voucher) no se asemeja a la firma de la tarjeta.
- Altos volúmenes de compra en un período corto de tiempo.
- El delincuente no conoce datos de identificación positiva del tarjetahabiente.

Este punto es similar al anterior en cuanto a las características mencionadas con la diferencia que en este caso existe una denuncia por parte del usuario al banco emisor de la tarjeta en donde éste confirma que la misma le ha sido hurtada. En el primero el contacto es del analista con el tarjetahabiente y este último le confirma la ausencia del plástico; cuando

es el tarjetahabiente quien se comunica con el emisor para notificar de la ausencia del plástico estamos ante tarjeta robada. La diferencia puede llegar a estar en algunos casos en la responsabilidad ante algunos consumos que el tarjetahabiente desconozca, esto lo veremos con mayor profundidad más adelante en el capítulo cinco.

Al igual que el caso anterior, el tarjetahabiente de no contar con un seguro, será responsable ante la deuda generada con la tarjeta.

3) TARJETA NO RECIBIDA

Definición: Existe una transacción fraudulenta a causa de una reclamación realizada por el tarjetahabiente de que no recibió la tarjeta emitida, aunque el emisor confirma que la misma fue enviada (por medio de cualquier método).

Características:

- La firma en el recibo de compra (voucher) no se asemeja a la firma de la tarjeta.
- Altos volúmenes de compra en un período corto de tiempo.
- El delincuente no conoce datos de seguridad.

Este es el caso en que la tarjeta es embozada y es derivada al courier para que la entregue al usuario. Si el emisor confirma que la misma fue enviada es porque el courier encargado de entregar la tarjeta al usuario confirmó que así fue. Debe existir un estricto control entre la institución emisora y el courier ya que del total de tarjetas emitidas, algunas fueron derivadas a sus respectivos dueños mientras que otras no por diferentes motivos. Las que no pudieron ser entregadas deben estar controladas ya sea por la propia institución emisora o por el propio courier, lo cual queda a criterio de cada emisor, ya que para algunos dejarlas en custodia del courier hace que éste tenga más responsabilidad sobre las mismas. El fraude por tarjeta no recibida entonces será por aquellas tarjetas no entregadas al usuario final, pero fueron sustraídas y utilizadas por alguien en algún momento del proceso de entrega y custodia luego del embozado. Recordamos que la entrega de tarjeta es contra firma del titular de la misma en algunos casos o de alguien del domicilio de entrega (puerta adentro).

4) SOLICITUD FRAUDULENTA

Definición: El emisor confirma que una transacción efectuada en una determinada cuenta es fraudulenta como resultado de una reclamación del tarjetahabiente al efecto de que nunca solicitó la tarjeta, o el emisor confirma que la información dada en la solicitud fue falsificada.

Características:

- Alto volumen de compra tan pronto se emite la tarjeta.
- Uso de efectivo alto.
- El cliente no es conocido por el número de contacto (el cliente al solicitar la tarjeta llenará los formularios respectivos donde informará sus datos personales, como nombre, fecha de nacimiento, cédula de identidad, y además brindará sus referencias de contacto como domicilio y número de teléfono; en los casos de solicitud fraudulenta, estos casos son falsos, por lo que el analista emisor tratará de ubicar al tarjetahabiente por estos datos y no podrá hacerlo).

5) TARJETA FALSIFICADA

Definición: El tarjetahabiente no participó en la transacción y aún conserva todas sus tarjetas de crédito.

El emisor además confirma que la tarjeta estuvo presente durante la transacción.

Características:

- Alto volumen de compras con precios altos (ejemplo joyas, equipos electrónicos, etc.).
- Compras fuera del país.
- Cambios drásticos en el comportamiento de compra del tarjetahabiente.

En esta clasificación, se encuentra el fraude por clonación de banda magnética, una de las dos formas de fraude de mayor magnitud en el mercado.

Es el típico caso de clonación de banda magnética, también conocido como duplicado de tarjeta o "skimming". El duplicado de la tarjeta se realiza y se codifica sin el permiso de la compañía de la misma. La mayoría de los casos implican la copia de la información de la banda magnética de una tarjeta genuina sin el conocimiento del titular. Éste desconocerá la concreción del fraude hasta que el procesador emisor detecta el mismo o bien le aparecen al tarjetahabiente en el estado de cuenta las transacciones que no realizó. No hay pérdida ni hurto de la tarjeta. Esto se analizará con mayor detalle en el capítulo cinco.

De esta manera el tarjetahabiente no participa de la transacción. La tarjeta es conservada por él mismo pero la transacción se realiza con "tarjeta presente" a través de la tarjeta falsificada que es la que contiene la copia de la banda magnética de la tarjeta genuina.

6) TARJETA NO PRESENTE (uso fraudulento de número de cuenta)

Definición: Un delincuente se apodera ilegalmente de una cuenta, incluyendo un cambio de dirección no autorizado.

Características:

- Varios casos reportados en el mismo comercio.
- Re-emiten tarjetas con información del tarjetahabiente alterada (la dirección por ejemplo) y cambian su patrón de compras.

Ocurre cuando le roban la información al titular de la tarjeta por ejemplo durante una transacción o por medio de un recibo, y la misma es utilizada para hacer compras a distancia, por ejemplo por teléfono o a través de Internet.

7) MISCELÁNEO

Esta clasificación abarca todos los demás tipos de fraude que no están incluidos en las mencionadas anteriormente. Los más conocidos son suplantación de identidad y auto fraude.

A) SUPLANTACIÓN DE IDENTIDAD

Definición: Un delincuente se apodera ilegalmente de una cuenta, incluyendo un cambio de dirección no autorizado.

Características:

- Varios casos reportados en el mismo comercio.

- Re-emiten tarjetas con información del tarjetahabiente alterada (la dirección por ejemplo) y cambian su patrón de compras.

La definición de este tipo de fraude es la misma que para tarjeta no presente. La diferencia radica en que en este caso (tarjeta no presente) el defraudador se apodera de la cuenta pero sin sustituirlo, es decir que ambos podrán utilizar la cuenta al mismo tiempo.

A diferencia de la solicitud fraudulenta, en la cual el cliente no existe al momento de la solicitud, en este caso el defraudador haciéndose pasar por el cliente buscará alterar los datos del mismo para suplantar su identidad.

En los casos de suplantación de identidad, a diferencia del hurto o extravío, el defraudador utiliza un plástico que nunca estuvo en manos del tarjetahabiente, ya sea porque éste nunca lo recibió o porque el plástico en poder del tarjetahabiente fue denunciado por el defraudador haciéndose pasar por éste, interceptando luego el nuevo plástico emitido. Esto se verifica fácilmente con la firma de recepción del nuevo plástico.

¿Cómo se lleva a cabo la falsificación de tarjetas de crédito por robo de identidad?

- Recogiendo extractos e información sobre datos personales directamente de la basura.

- Robo de correspondencia de los buzones para obtener tarjetas de crédito.

- Accediendo a informes crediticios de la persona en forma fraudulenta (esto es muy difícil ya que se exigen muchas garantías para acceder a este tipo de información).

- Obtener datos personales de los ficheros del trabajo (en este caso ya estaríamos en la órbita del delito).

- Espiando en los cajeros automáticos para identificar el número PIN tecleado (en el caso que la tarjeta de crédito pueda ser utilizada para retiro de efectivo).

- Enviando mensajes simulando ser comunicados del banco del titular de la tarjeta, solicitando datos de confirmación (Phishing) o inclusive mediante llamadas telefónicas.

B) AUTO FRAUDE

Definición: El tarjetahabiente participa directa o indirectamente del engaño.

Características:

- El tarjetahabiente es quien intenta engañar a un tercero.
- Desconocimiento de las transacciones por parte del tarjetahabiente.

2.4. Intento de fraude

El hecho del extravío de la tarjeta, del hurto de la misma, de que ésta sea clonada o cualquiera de los tipos mencionados recientemente no configura en sí mismo un intento de fraude, sino que son lo que puede dar origen a que se cometa el mismo propiamente dicho.

¿Cuándo se configura el intento de fraude?

Cuando a través del engaño se solicita la aprobación de una tarjeta de crédito como medio de pago en una transacción comercial. El engaño se puede dar ya sea o porque un tercero se hace pasar por el tarjetahabiente, existiendo desconocimiento de la situación por parte de éste; o bien porque el propio titular de la tarjeta quiere cometer el engaño, situación conocida como auto fraude.

¿Por qué se habla de intento de fraude?

Porque al momento de realizar la transacción debe existir una autorización de la misma. En caso de que se apruebe la autorización decimos que se consumó el fraude, mientras que si la misma es rechazada éste no se configura y se lo categoriza como intento de fraude.

Quien se encarga de autorizar las compras, como ya se mencionó anteriormente, es el procesador. Por lo tanto es responsable de controlar y detectar toda transacción fraudulenta. Por este punto entendemos que es el sujeto de mayor importancia en lo que a fraude respecta.

CAPÍTULO III

PROCESADOR

3.1. Introducción al concepto de procesador: rol adquirente y rol emisor

Como se mencionara en el capítulo anterior, es función del procesador autorizar las transacciones y por esta razón es el responsable de controlar y detectar toda transacción fraudulenta.

Para entender y analizar un procesador es necesario aclarar que existen dos partes qué procesar: por un lado la parte adquirente la cual refiere a los comercios y por otro lado la parte emisora correspondiente a las instituciones financieras tanto bancarias como no bancarias encargadas de la emisión de las tarjetas de crédito.

Dentro de la industria de las tarjetas de crédito y vinculado precisamente a la función del procesador dentro de ella, es importante describir la existencia de dos roles fundamentales. Ellos son el rol adquirente y el rol emisor, los cuales se vinculan entre sí a causa del tarjetahabiente, que es el actor principal en esta industria debido a que es quien le da uso al producto tarjeta de crédito. Mediante el uso de la misma y en la aprobación de las respectivas transacciones es que se aparece el concepto de fraude, objeto de estudio en nuestro trabajo monográfico.

Rol Adquirente: Dentro de este rol se encuentran comprendidos el comercio objeto de la transacción comercial, el tarjetahabiente y el procesador adquirente.

El comercio entrega el bien o servicio adquirido al tarjetahabiente.

El tarjetahabiente paga con la mencionada tarjeta de crédito por el respectivo bien o servicio adquirido.

El procesador adquirente se encarga de la adhesión de los establecimientos comerciales facilitando mediante el arrendamiento de las respectivas terminales (POS) para que los mismos puedan operar con tarjetas de crédito. A través del procesador adquirente los comercios no podrán operar con tarjeta de crédito si no están adheridos. El procesador adquirente es quien da al comercio la respectiva autorización en línea de sus sistemas de crédito.

Rol Emisor: Dentro de este rol se encuentran comprendidos la institución financiera emisora de la tarjeta de crédito, el tarjetahabiente y el procesador emisor.

El emisor de la tarjeta de crédito (institución financiera) tiene la función de proveer al tarjetahabiente de la respectiva tarjeta de crédito.

El tarjetahabiente por su parte pagará por el uso de la tarjeta al emisor de la misma.

Por su parte, el procesador emisor se encarga de embozar la tarjeta (él mismo o a través de un tercero) además de administrar todo lo relativo al intercambio entre emisor y tarjetahabiente.

Desde el punto de vista adquirente existe un control que se realiza sobre el comercio, mientras que desde el punto de vista emisor existe otro control que se realiza sobre la tarjeta de crédito. Para la parte adquirente en nuestro país, para las dos tarjetas de crédito internacionales principales que son Visa y MasterCard, cada una tiene su procesador adquirente propio que son VisaNet y First Data respectivamente, lo que hace que exista exclusividad en cuanto al procesador adquirente. En lo que respecta al procesador emisor no sucede lo mismo, ya que cada institución financiera podrá procesar lo concerniente a la parte emisora o tercerizar la misma. Los principales agentes tercerizados que operan procesando el rol emisor en nuestro país son First Data y Sistarbanc, y lo hacen fundamentalmente para MasterCard y Visa respectivamente sin tener exclusividad.

Es decir que una institución financiera determinada puede solicitar a un tercero que le procese la operativa de la tarjeta o hacerlo ella misma. El hecho de que un solo agente opere todas las transacciones tiene como ventaja más clara el concentrar la información, es decir que podrá visualizar totalmente la operativa de todas las tarjetas de crédito de los tarjetahabientes de los distintos comercios.

En el caso de First Data puede darse que sea procesador emisor y adquirente a la vez. Esto solo sucederá con las tarjetas MasterCard de aquellas financieras que decidieron tercerizar con esta empresa la parte emisora. Caso similar ocurre con Oca, ya que dicha institución se procesa sus transacciones y ella misma es quien se contacta con los comercios. Corresponde aclarar que existe la tarjeta Oca con sello Visa la parte adquirente la operará VisaNet.

Obviamente que las instituciones financieras al momento de decidir entre procesar ellas mismas la operativa o tercerizar, además del manejo de fraude, tienen en cuenta otros aspectos, principalmente comerciales. La relación costo-beneficio es un aspecto fundamental que tienen en cuenta las mismas, no solo por el costo que puede significar tercerizar el servicio, sino por el hecho de dominar las autorizaciones. Recordar que parte

del negocio para las tarjetas son las comisiones por efectuar el servicio de medio de pago y el financiamiento relacionado, por lo tanto querrán tener un mayor control sobre las mismas. En cierta forma, a veces prefieren asumir más riesgos con tal de tener el mencionado control de las autorizaciones. Esto lo vemos más claro en el punto de que las principales financieras internacionales de mayor volumen operativo del país asumen ellas mismas el rol emisor, concentrando las autorizaciones en regiones de mercado (por ejemplo Latinoamérica). Dicha situación, como se verá al final del trabajo puede tener ventajas y desventajas.

3.2. Procesador adquirente

Como se mencionara anteriormente, el control adquirente es el que se realiza sobre el comercio, por lo que procesador adquirente es quien administra y centraliza la atención a los comercios. Su misión específica es afiliar comercios en todo el territorio uruguayo para poder operar con determinado sello, brindar a los comercios nuevas formas de pago y otros servicios y productos del respectivo sello, efectuar el procesamiento de las operaciones de los comercios y el pago de las mismas.

First Data tiene la exclusividad en la actualidad del procesamiento de las tarjetas de crédito MasterCard en nuestro país para la parte adquirente. Esto significa que nadie, con excepción de First Data, puede realizar el procesamiento de información (transacciones) para los comercios de nuestro país. Existe entonces una relación de exclusividad entre First Data y los comercios en Uruguay en lo que a procesamiento de información refiere. Será pues quien le paga a cada comercio y la única institución que puede afiliar comercios para MasterCard. Caso similar ocurre con Visanet, quien tiene la exclusividad del procesamiento adquirente de tarjetas de crédito Visa en nuestro país. Es decir que todo contacto de los comercios con Visa se da a través de Visanet. Recordar que otro procesador adquirente importante para nuestra plaza es Oca para las tarjetas con su propio sello.

El procesador adquirente podrá analizar todas las transacciones ocurridas en cada comercio según cada sello que se procese dentro del Uruguay. Se ven todas las transacciones realizadas dentro de nuestro país sin importar el origen de las tarjetas utilizadas (locales o extranjeras) y sin importar la vía de compra (con tarjeta presente o por internet por ejemplo). El procedimiento de autorización indica que la misma viaja desde el procesador adquirente hacia el procesador emisor para que luego vuelva la respuesta. Es por esto que el primer control de fraude lo hace el procesador adquirente, controlando las transacciones realizadas en el comercio de origen. Al procesador adquirente le interesa que no se cometa fraude en los comercios (que no se realicen transacciones fraudulentas) y por lo tanto que sus comercios adheridos no muestren vulnerabilidad al fraude. De llegar a mostrar

vulnerabilidad ante el fraude, va a traer más transacciones fraudulentas, lo cual puede serle perjudicial al momento de asignar responsabilidades por los sellos internacionales. Para evitar que los sellos internacionales tengan consecuencias negativas, es que a los procesadores adquirentes le interesa controlar la operativa de los comercios.

El control más complejo de realizar para el caso de un procesador adquirente es el de e-commerce con tarjetas del exterior. Más del noventa y nueve por ciento de la base de datos de tarjetas de crédito son extranjeras, por lo que en el mundo existe mayor posibilidad de robo de datos de las mismas. Nuestro país tanto a nivel de e-commerce como de venta con tarjeta presente constituye un porcentaje insignificante a nivel mundial. Por lo tanto el procesador adquirente debe tener mucho cuidado cuando recibe una compra en un comercio de nuestro país con una tarjeta emitida en el exterior. Puede suceder que dicha tarjeta tenga un historial de compras en nuestro país, caso que no sería de gravedad justamente porque ese historial da la pauta que tiene costumbre de uso en Uruguay lo que reduce de alguna manera el riesgo de fraude. Un ejemplo claro es una tarjeta emitida en Estados Unidos cuyo titular compra vía e-commerce a través de la página web todas las semanas en algún supermercado de nuestro país para enviarle el surtido a un familiar. El problema se da cuando existe una compra a través de Internet con una tarjeta que no tiene historial atrás. En estos casos, como existe buena relación con el comercio (es la gran ventaja que tiene Uruguay como país pequeño), se le suele pedir al mismo la dirección IP desde donde se solicita la transacción, además de la dirección hacia donde es enviado el producto, e inclusive el banco emisor de la tarjeta de crédito y de acuerdo a ésto se puede llegar a realizar un análisis más profundo. Si por ejemplo, la dirección IP es de Bolivia, el tarjetahabiente tiene nombre “John Stuart” y el banco emisor de la tarjeta está ubicado en Nueva Zelanda, por supuesto que da para sospechar. Lo que se hace en estos casos (recordar que al no ser procesador emisor no se puede bloquear la tarjeta) es dar aviso al banco emisor. Enviando la información tan detallada es más fácil para el banco emisor poder rastrear y hasta bloquear la tarjeta en el acto, además de poder dar tiempo necesario para cancelar la transacción.

Otra de las variables puede ser que atrás de esa compra existieron cinco intentos distintos de la misma persona para comprar el mismo producto (por ejemplo un pasaje aéreo), pero con el agravante que se realizó con cinco tarjetas distintas y a su vez de distintos países, lo que indica que existe certeza de fraude. El adquirente podrá ver si esa persona utilizó cinco tarjetas distintas para una misma compra solamente si las mismas son del mismo sello; si utilizó distintos sellos solo verá la o las que él procesa, por lo que para poder enterarse de los demás intentos, será el propio comercio quien debe comunicárselo. Se observa así la importancia que tiene el buen relacionamiento entre ambos para el control adquirente.

Las acciones en lo que respecta a la prevención de fraude por parte del procesador adquirente pueden tener mayor dificultad a la hora de su visualización y comprensión respecto a las que realiza el procesador emisor. Para simplificar y entender el control a nivel adquirente, es necesario visualizar que existen diversos objetivos a cumplir por parte de éste. Los mismos estarán vinculados a proteger de fraude a todos los comercios adheridos, a los que pertenecen a un rubro específico o a un comercio en particular, buscando encontrar situaciones sospechosas para estos casos mencionados, así como también prevenir un posible fraude, además de encontrar las situaciones que lo pudieron provocar. Se citarán así, algunos casos del por qué el procesador adquirente busca detectar el fraude en los comercios.

Un ejemplo es que puede interesarle al procesador encontrar algún comercio que está siendo atacado para hacer fraude con tarjetas de crédito justamente en dicho negocio. El mismo puede ser un comercio legítimo que opera honestamente pero que fue objeto de un ataque por parte de defraudadores para realizar su cometido. En la mayoría de los casos se dan en comercios de rubros riesgosos como agencias de viaje, supermercados, venta de electrodomésticos o artículos electrónicos y cada vez más frecuente en aquellos comercios que venden artículos virtuales que no impliquen llevarse un objeto, como por ejemplo entradas de cine.

Otro caso ocurre cuando no es un comercio en particular sino la totalidad de la red adquirente. En este caso estará compuesto por un sinnúmero de comercios distintos que pertenecen a dicha red, la cual fue elegida por los delincuentes para realizar fraude. Éstos pueden obtener acceso a una base de datos de un emisor obteniendo datos de muchas tarjetas de crédito las cuales tendrán una misma identificación (B.I.N.)[10] y podrán ser utilizadas en determinados lugares donde detectaron que los controles son débiles. Por lo tanto, en este caso ninguno de los comercios está realizando nada indebido pero terminan siendo víctimas de fraude.

Otro ejemplo se da en aquellos casos en que el comercio es legítimo, su dueño es una persona honesta pero tiene un empleado que está trabajando en el mismo para realizar fraude. Este empleado puede copiar determinada tarjeta de crédito para realizar fraude en el momento o no. Para hacer fraude, por lo general, el delincuente que trabaja en el comercio está asociado a una banda de defraudadores y es éste quien les permite a los integrantes de la banda que puedan realizar transacciones a través del POS de la empresa con tarjetas clonadas que ni siquiera fueron falsificadas, sino que son tarjetas blancas que lo único que le hicieron fue cargarle los datos de la banda magnética y nada más. Son tarjetas que es imposible utilizarlas en cualquier otro lugar porque salta a la vista claramente que son

[10] B.I.N.: Business Identification Number, se verá en el capítulo cuatro.

tarjetas falsas ya que no tienen número, no tiene vencimiento, no tienen logo ni de la institución emisora ni tampoco del sello. Las tarjetas son absolutamente blancas con los datos de la banda magnética cargados. Pero lo que sí hay es complicidad con alguna persona que trabaja en el comercio para así poder realizar fraude a través del POS de éste. Estas actividades pueden ser realizadas en un horario donde hay pocos clientes o fuera del horario normal de atención del negocio, por lo que en estos casos al comercio le puede servir analizar la hora en que dichas transacciones fueron realizadas. Lo mismo para el caso de compararlas con los datos históricos del comercio, ya que pueden aparecer ventas a un horario determinado en el cual históricamente las mismas no se daban.

Por otro lado se puede dar el caso que el comercio esté realizando actividades indebidas, y ahí pueden existir infinidad de casos. Uno de los propósitos de estos comercios puede ser el de realizar fraude a las tarjetas. Son los llamados "comercios golondrinas" que además de hacer fraude al procesador adquirente seguramente estará evadiendo impuestos ante la Dirección General Impositiva también. Dentro del total de transacciones que realizará, se encontrarán ficticias, duplicadas, entre tantas otras, y para esto basta nada más con pasar dobles todas las transacciones por mencionar algo básico. Una vez que sospeche que lo están por descubrir, cerrará y desaparecerá, trasladándose hacia otro lugar para seguir con su actividad fraudulenta.

Lo mismo para cuando la tarjeta se está clonando en determinado negocio, existen sistemas de detección de puntos de compromiso que sirven para identificar estos casos. La utilidad en este caso se da para determinar por ejemplo que el fraude se realizó con cierta cantidad de tarjetas las cuales están identificadas. La detección de puntos de compromiso servirá entonces como mecanismo de control identificando en este caso que el fraude lo pudo haber realizado determinado empleado del comercio, identificando así la posible vulnerabilidad en el mismo.

Para entender este concepto, se define **punto de compromiso** como todo aquel vínculo que existe entre dos o más transacciones fraudulentas. Para que exista punto de compromiso primero que nada deben existir un mínimo de dos transacciones fraudulentas y que las mismas estén vinculadas en algún punto. A este punto en común se lo denomina compromiso ya que refleja que probablemente fue vulnerable de que se originara el fraude, es decir, es el momento donde se sacan los datos necesarios para cometer el mismo. A manera de ejemplo, puede suceder que distintas tarjetas con casos de fraude fueron utilizadas en un mismo comercio (lo más usual) o que las mismas fueron repartidas por determinada empresa de correo o courier, entre otros.

Como lo más común es encontrar un punto de compromiso a través de un vínculo según comercio utilizado, es el procesador adquirente quien cuenta con mayor información para

vincular los mismos. Es el adquirente quien tiene mejor y más fidedigna información sobre los datos de los comercios en general, por lo que es quien más elementos tiene para detectar un posible punto compromiso. Esto no implica que el emisor o los propios sellos puedan detectar puntos de compromiso. Existen softwares realizados para detectar puntos de compromiso.

El emisor por lo general tiene una información básica de los comercios para que pueda aparecer en el estado de cuenta del tarjetahabiente. No tiene una identificación exacta del comercio sino que tiene información genérica. No tiene un código que diga claramente dónde el usuario realizó la compra. Muchas veces los datos que aparecen en el estado de cuenta del emisor se originan directamente del POS del comercio a través del cual se realizó la transacción según como esté configurado el mismo. Puede llegar a darse el caso que el comercio tenga varios POS por ejemplo y uno esté configurado con el nombre real del mismo y el o los otros estén configurados con los nombres fantasías del mismo. Inclusive hay comercios que tienen los POS configurados con otros datos debido a que los mismos pueden ser comprometedores para el usuario al momento de aparecer en los respectivos estados de cuenta.

El procesador adquirente debe tener identificado claramente el comercio porque es a quien le paga, por lo tanto debe existir un contrato comercial que medie entre el adquirente y cada uno de los comercios que procesa. El procesador emisor, por tanto, a diferencia del adquirente no tiene ningún tipo de relación directa con el comercio y por lo tanto tiene menos información acerca de éste. La única excepción se da para los casos en que tanto procesador adquirente y emisor son la misma entidad, entonces la parte emisora necesariamente tendrá estos datos porque los necesita para su función de adquirente.

Todos estos casos son de fraude que suceden en el comercio. Como se analizó, es el adquirente quien oficia de contacto con el comercio y por lo tanto es a quien le debe importar en mayor medida estos fraudes. Veremos más adelante, en el tema responsabilidades al final del capítulo cinco, cómo le puede afectar el mismo.

3.3. Procesador emisor

La función en esta parte radica en controlar las transacciones del tarjetahabiente y no del comercio. Acá se controlarán todas las transacciones de cada producto que tenga el socio (titular o adicionales) en todo el mundo, a diferencia del control adquirente que solo tiene acceso a las transacciones locales. Esta es una de las funciones a cargo del procesador emisor. La otra diferencia radica en que el emisor solamente analizará las transacciones de

sus socios, mientras que el adquirente analiza transacciones que realizan diferentes tarjetahabientes con tarjetas del sello que procesan en los respectivos comercios adheridos.

Como se mencionara anteriormente, dicha función puede ser realizada por las instituciones financieras bancarias emisoras o puede estar tercerizada en agentes encargados de dicha función.

En lo que a compras locales respecta, este control no adquiere una importancia relativa pero sí adquiere relevancia y mayor complejidad para compras internacionales. Esta se da con las compras que un tarjetahabiente realiza en el exterior por el hecho que no tiene la historia de la totalidad de los comercios del exterior. Sí seguramente tenga la historia de todos los comercios de nuestro país. Lo anteriormente señalado es importante porque el hecho de conocer la historia de cada comercio hace que exista la posibilidad de tener conocimiento de cuáles pueden llegar a ser más vulnerables respecto al fraude. Al no tener la historia de los comercios extranjeros hace que exista la necesidad de confiar en los procesadores adquirentes del país de origen, con los cuales en algunas oportunidades no se cuenta con el mismo "feedback" que con los procesadores de este país. Esto por diferentes motivos como ser el idioma, uso horario, frecuencia en la comunicación, entre otros. Si bien ésto no garantizará nada, ya que el fraude en Uruguay existe, el hecho de tener un conocimiento previo de los involucrados siempre genera a priori una ventaja por la información que se posee (o sea en las compras realizadas en Uruguay, se conoce al comercio, se tiene un historial y se conoce al procesador adquirente con el cual se tiene contacto frecuente).

Puede suceder, como ya se mencionó, que el procesador emisor y adquirente sea el mismo sujeto; esto sucede para las tarjetas MasterCard que el procesamiento emisor es realizado por First Data. La principal ventaja de ser emisor y adquirente al mismo tiempo es que se pueden observar más cantidad de transacciones, lo que alimenta el historial del software, una herramienta de gran utilidad como veremos más adelante.

El aspecto más interesante dentro del control emisor es la forma cómo se controla. Desde el punto de vista emisor se utiliza un sistema informático, el cual puede ser neural o no, donde se carga toda la información del socio, incluyendo un historial de operaciones del mismo. En el mismo se cargan lo que se llaman reglas, las cuales son creadas para generar alertas de fraude. Si lo comparamos con los procesadores adquirentes, éstos también utilizan sistemas informáticos a los cuales también se les cargan reglas, con la diferencia que la configuración de ambos es diferente. Por lo tanto a nivel técnico no existen grandes diferencias entre los programas de detección de fraudes a nivel de emisores y adquirentes, sino que la diferencia se basa en la manera en cómo se configuran ambos, que en definitiva es la forma como se configuran las reglas que generan las alertas de fraude.

Todos los procesadores estudiados en este trabajo monográfico tienen sus propios sistemas informáticos para procesamiento de transacciones y detección de fraudes. Estos pueden ser diseñados por ellos mismos (en este caso se elaboran para la región, ya que obviamente Uruguay es un mercado muy pequeño para esta inversión) o por un tercero. Este último caso es el ejemplo de Sistarbanc el cual tiene como principal herramienta un sistema neural integrado de varias funciones dentro de las cuales se encuentra la de reglas de alerta para la detección de fraude. El proveedor del mismo es Paytrue, una empresa uruguaya que desarrolló el sistema como piloto para Uruguay y dado el buen resultado obtenido se adaptó y aplicó para otros procesadores Visa de otras regiones como es el caso de Brasil. Otro caso es el de First Data cuyo sistema (Falcon) fue desarrollado también por un tercero. En los casos que las financieras no tercerizan el procesamiento emisor, encontramos que el análisis de fraude es realizado a nivel regional (son los casos de Citibank y Santander por citar algunos).

El hecho de que existan más de dos sistemas procesadores funcionando a la vez, también es una garantía, no solo para la detección de fraudes que pueda hacer uno u otro, sino porque en caso de que alguno sufra un inconveniente, los demás siguen funcionando. De todas formas se aclara que hay planes de contingencia para cuando esto sucede, y tanto el personal de fraude como el de sistemas del mismo, tienen guardias que están las veinticuatro horas, los trescientos sesenta y cinco días del año trabajando.

La detección de los fraudes se da generalmente en las solicitudes de autorización de las transacciones.

CAPÍTULO IV

SISTEMA NEURAL

4.1. Concepto y características

El capítulo anterior finalizaba haciendo referencia a los sistemas informáticos utilizados para detectar y controlar el fraude, tanto a nivel adquirente como a nivel emisor. Cabe destacar que son diversos los sistemas utilizados para la detección de fraude.

Todos los tipos de sistemas diseñados para la detección de fraude, tienen como principal componente el historial de las transacciones del tarjetahabiente y del mercado. La diferencia radica en la información obtenida y la forma como ésta se obtiene, sin embargo todos tienen un mismo objetivo que es la detección de transacciones fraudulentas de manera eficiente, y una misma fuente principal que es el historial de transacciones.

En este capítulo se focalizará sobre los tipos de sistemas que utilizan los dos principales procesadores emisores en plaza (Sistarbanc y First Data), conocido como sistema neural. Si bien ambos son sistemas desarrollados por proveedores diferentes, tienen un funcionamiento similar que es lo que analizaremos a continuación.

Sistema neural, o también llamado ***sistema predictivo***, es aquel que tiene la capacidad de generar un "score" o "scoring" de forma automática y no en base a una ponderación manual realizada por quien configuró el sistema. Como se mencionara al cierre del capítulo anterior, las reglas son creadas y por tanto cargadas a los sistemas para generar alertas de detección de posibles casos de fraude. Para dar una breve definición, "score" o "scoring" es una forma de ponderar las diversas alertas de fraude generadas por el sistema, para que sean analizadas por parte de los analistas, en base a determinados parámetros preestablecidos.

Este tipo de modelo se realiza aplicando ciertas técnicas llamadas de "inteligencia artificial" a nivel informático, a partir del histórico de transacciones de la institución o del tarjetahabiente. Dependerá de si el mismo ha sido realizado para un procesador adquirente, que analizará transacciones de una institución por ejemplo, o si ha sido desarrollado para un procesador emisor, quien realizará lo mismo con las transacciones de determinado tarjetahabiente. Lo que hace en realidad es aplicar algún algoritmo matemático que analiza históricamente si determinada transacción fue objeto de fraude o si por el contrario no lo fue. Es así que a partir de este histórico de transacciones, para cada una de ellas, va a

inducir un modelo matemático en el que aplica esa experiencia previa para seguir definiendo y clasificando transacciones nuevas. Este tipo de sistemas deberían ser entrenados y actualizados periódicamente por la misma razón que se deben ajustar las reglas.

Como también se mencionara en el capítulo anterior, las diferencias a nivel técnico entre los sistemas utilizados por procesadores adquirentes y emisores son mínimas, ya que fundamentalmente las mismas se dan a nivel de cómo se configura cada uno.

Una de las diferencias a nivel técnico entre ambos es la forma en que está implementada la parte de cálculo del sistema, pero por ser algo interno al mismo no es visualizado por parte del usuario. Esta diferencia radica en la cantidad esperada de transacciones que va a necesitar analizar cada uno de los sistemas. Para un emisor por ejemplo, sus clientes serán en la mayoría de los casos, personas que realizarán alrededor de veinte transacciones por mes. Así como son veinte pueden llegar a ser cinco transacciones, treinta, etc., pero es difícil que exista un individuo que realice tres mil transacciones mensuales con su tarjeta de crédito. Esto lo puede calcular y mostrar el sistema con su "memoria" en el momento en que se le solicita ya que al ser pocas transacciones las que procesa no necesita mucho tiempo de espera para el cálculo. En cambio, desde el punto de vista del adquirente a la hora de analizar un comercio, éste tendrá muchas más transacciones que cualquier individuo en particular. Tendrá miles, cientos de miles, dependiendo de la magnitud del comercio, por lo que la memoria de momento ya no es efectiva como en el caso del emisor. En este caso, sí se van pre calculando en una base de datos todas las sumarizaciones y agregaciones de datos.

La segunda diferencia es más visual aunque tiene el mismo origen que la anterior. Los programas de detección de fraude tienen una consola de análisis donde los analistas de riesgo ingresan al mismo con su clave de usuario y analizan las alertas que va generando el sistema. A la consola de cada analista de fraude le llegarán determinada cantidad de alertas las cuales son distintas entre uno y otro justamente para que dos analistas diferentes no estén analizando la misma alerta. Esa es una de las funcionalidades de estos sistemas, o sea distribuir todo el trabajo entre las diferentes personas que integran el equipo de trabajo. Para un emisor, esta consola de análisis mostrará los datos de la persona que se necesite analizar y las últimas transacciones realizadas por ésta. Las últimas transacciones, como se mencionara anteriormente, no serán demasiadas y podrán ser fácilmente visibles a través de una pantalla de computadora. Un analista con un mínimo de experiencia, al observar solamente la lista de las últimas transacciones se dará cuenta inmediatamente por qué se disparó la alerta, lo mismo que si el comportamiento es fraudulento o no, o si debe ponerse en contacto con el tarjetahabiente, situación que se da cuando se sospecha que dicho comportamiento es fraudulento. Por el contrario, para el caso de un adquirente, si se dispara

una alerta y se generan todas las últimas transacciones del comercio objeto de análisis, no hay pantalla que pueda mostrar las mismas porque las transacciones van a ser miles. Por lo tanto más que una lista con transacciones, lo que aparecerá serán gráficas para darle al usuario la mayor información necesaria y de la manera más resumida y detallada. Estas gráficas resumirán el histórico de transacciones del comercio sin tener que recurrir a los listados que sí aparecen en la parte emisora.

El término "score" o "scoring" refiere no solo a tratar de generar una alerta sino asociar esa alerta a un indicador numérico que refleje cuál es la probabilidad de que esa alerta realmente sea fraude. Por ende la mayor utilidad de éste es ayudar al analista de riesgo a que priorice las alertas con las que tiene que trabajar. Si dicho analista está recibiendo cien alertas por hora, por ejemplo, va a estar sobrecargado de trabajo y va a tener que priorizar las mismas porque no va a poder analizarlas todas. A través de este score, entonces, decidirá qué alerta analizará primero, qué alertas tendrá que dedicarle más tiempo de análisis, cuáles tendrá que contactar a la persona para consultarle, cuáles no habrá problemas en caso de no analizar y demás. La decisión acerca de qué realizar con la alerta la tomará el analista en base a su criterio profesional., basándose en ciertos datos, como por ejemplo los que se mencionarán a continuación:

1) ***Monto de la transacción:*** Una transacción cuyo monto es importante y tiene sospecha de fraude, tiene más importancia que una transacción con sospecha de fraude pero de menor importe.

2) ***Saldo disponible de la tarjeta al momento de la transacción:*** Por el mismo criterio anteriormente señalado, no es lo mismo una transacción por determinado importe que parece fraudulenta en una tarjeta con un saldo importante en la misma que una transacción con una tarjeta con un saldo mucho menor o insignificante. Por ejemplo, una transacción por pesos uruguayos doscientos con sospecha de ser fraudulenta con un saldo disponible en la tarjeta de dólares americanos dos mil, va a ser más importante de analizar que una transacción por el mismo importe o hasta incluso un importe mayor pero con un saldo disponible en la tarjeta de dólares americanos doscientos.

3) ***"Scoring" propiamente dicho:*** Significa cuál es la probabilidad de que la respectiva alerta sea realmente un caso de fraude. Si la probabilidad es muy baja, las chances de que el analista pierda tiempo de trabajo analizándola son mínimas por lo que la descartará; mientras que por el contrario, si la probabilidad de que la alerta sea fraudulenta es alta, entonces el analista sí se tomará su tiempo en analizarla.

Los tres datos arriba mencionados son algunos de los tantos en los que un analista puede basarse para tomar decisiones a la hora del análisis. Según lo indagado en las diferentes

entrevistas realizadas a procesadores, cada analista tiene su propia metodología de trabajo y puede considerar como importantes ciertos datos que por el contrario otro puede no hacerlo. El "scoring" es un dato que a nuestro criterio será sumamente útil a la hora de analizar una alerta, pero será más utilizado en aquellos casos en que el analista recibe una gran cantidad de éstas en un lapso determinado de tiempo (por ejemplo por hora o por día), por lo que su aplicación puede ser de mayor utilidad en mercados de mayor tamaño y no tanto en nuestro país. Otros datos principales que el analista podrá tener en cuenta a la hora de analizar las alertas pueden ser, por ejemplo, el país de la transacción, si es por lectura de banda o no, el historial de transacciones, el tipo de producto, el M.C.C.[11], entre otros.

De todas maneras siempre se analizará en combinaciones, o sea una combinación con probabilidad baja de ser fraude y con un monto también bajo, se descartará o se analizará después; mientras que por el contrario, una con probabilidad alta de fraude y de monto relativamente grande o inclusive con un saldo en la tarjeta importante, se le dará mayor prioridad.

El "scoring" por lo tanto, es un dato muy difícil de determinar. Si el analista configuró reglas, a las mismas les puede asignar un determinado "scoring" de forma manual, lo cual hará que ciertas reglas, de llegar a ocurrir, tengan un "scoring" muy alto y otras, por el mismo hecho, tengan uno bajo. Este determinará un orden de importancia al momento de analizar las alertas. Las mismas son estudiadas por analistas preparados que contarán con la alerta, la probabilidad de fraude de la misma (dada por el score) y el historial del socio con lo cual estudiarán la transacción sospechosa.

Dicha alerta podrá ser descartada siempre que el analista considere que no hay riesgo de fraude, o si por el contrario corresponderá llamar al usuario o en su defecto al banco emisor de la tarjeta de crédito. Para el caso en que la llamada sea realizada y el fraude sea descubierto, se procederá automáticamente a bloquear la tarjeta y como consecuencia a la confección de un plástico nuevo con un número nuevo también respetando por supuesto el vencimiento de la misma para el titular de la misma. Hay alertas que dada la alta probabilidad de fraude pueden generar automáticamente el bloqueo de la tarjeta sin necesidad previa de analizarla ni comunicarse con el titular.

[11] M.C.C.: Merchant Commerce Code

4.2. Reglas de alerta

4.2.1. Concepto

Una **regla de alerta** es un dato o parámetro través del cual se definen una serie de condiciones para las transacciones que solicitan autorización; condiciones que pueden ser genéricas o específicas y que tienen en cuenta características de cada cliente, como por ejemplo la velocidad en las transacciones, lugares donde opera habitualmente, rango de importes de las transacciones, entre otras. De acuerdo a estas reglas cargadas en el sistema, el mismo va alertando de las transacciones de cada cliente a través de las respectivas **alertas** y en base a éstas se analizan las distintas operaciones sospechosas de fraude. A cada alerta, como se mencionara anteriormente, se le asigna un score de acuerdo a la probabilidad de que la misma sea fraudulenta o no. Las alertas tienen como objetivo buscar la atención del analista para que el mismo estudie determinada transacción por diversos motivos, uno de ellos es que la misma pueda ser fraudulenta.

4.2.2. Proceso de elaboración de las reglas de alerta

Las reglas, como se mencionara recientemente, son un conjunto de datos y parámetros que se cargan al sistema. Éstas, sean genéricas o no, se adaptarán a cada usuario para emitir las alertas respectivas, de acuerdo al historial de transacciones del mismo. Esto es realizado automáticamente por el sistema, sea neural o no. Es decir que el sistema toma por un lado las reglas cargadas en él, y por otro lado toma el historial de transacciones del tarjetahabiente, y en un análisis combinado de ambos, procederá a autorizar o no una transacción, además de emitir un aviso de alerta en caso que corresponda.

Por lo tanto, el primer punto es definir las reglas a cargar en el sistema. Las reglas funcionan como condiciones que le son exigidas a éste para aprobar, o en todo caso dar aviso de una transacción (se debe tener en cuenta que la transacción puede ser aprobada y además generar una alerta).

Las reglas son establecidas por el propio procesador (ya sea emisor o adquirente). El origen de las mismas es diverso; pueden ser en base a la experiencia del procesador, pueden ser sugeridas por los sellos, o pueden ser acordadas con la institución financiera en caso de que el servicio del procesamiento esté tercerizado. Esto último se da porque en estos casos el responsable ante el sello es el procesador emisor, pero luego en los acuerdos entre procesador emisor e institución financiera, será esta última responsable ante los fraudes, por lo tanto al ser ésta quien asuma los riesgos, tendrá interés en determinar tanto las reglas de alerta como las restricciones de transacciones. Recordar además que es la institución

financiera quien tiene contacto fluido con el cliente y que toda la información de éste que la misma maneja, será de gran utilidad cargarla en el sistema para que, tanto éste como el analista la tengan en cuenta a la hora de llevar a cabo una autorización. Un ejemplo de esto se da cuando el tarjetahabiente se va de viaje a determinado país y comunica oportunamente a la institución financiera que aparecerán transacciones a partir de determinada fecha en el país al cual viaja.

Cuando el procesador se encuentra tercerizado existe cierta oposición de intereses entre la institución financiera, a la que le interesará que sean aprobadas la mayor cantidad de transacciones posibles por motivos comerciales lógicos, y el procesador al cual le interesará estudiar toda transacción con sospecha de fraude y limitar así las autorizaciones respectivas. Es por esto entonces, que en varias oportunidades se "negociarán" tanto las reglas de alerta como las restricciones a cargar al sistema. También sucederá cuando es la propia financiera quien se procesa las autorizaciones, pero en este caso existirá un conflicto interno de la misma entre el área de riesgos y el área comercial.

De todas formas, la principal fuente de datos para determinar las reglas de alerta es la experiencia del propio procesador. Esta experiencia puede generarse de diversas maneras. Puede originarse por antecedentes de fraudes anteriores, y que ante la aparición de alguno de ellos, aplicando determinada regla logra solucionar el problema. A esto se le puede agregar que generalmente ante la aplicación de determinadas reglas impuestas para detectar fraude, los delincuentes suelen emplear técnicas para evadir la detección de los mismos y así seguir actuando. Por lo tanto servirá la experiencia en lo relativo a lo sucedido ante la aparición de determinado fraude, como así también cuáles fueron las consecuencias por la aplicación de las nuevas reglas. En este caso el procesador se basa en la experiencia obtenida en el pasado. Para estos casos se podrá crear una regla para evitar el fraude y otra regla para prevenir los posibles movimientos de evasión que realicen los defraudadores ante la aplicación de la regla, ya que es conocido que ante la regla impuesta, el o los defraudadores operarán de determinada manera. Estos casos detallados anteriormente son para referirnos en todos los casos al procesador emisor.

También tendrá la experiencia del mercado; de lo que sucede a nivel internacional. Hoy en día con el avance en las comunicaciones, se sabe al instante cuáles son los tipos de fraude que están ocurriendo a nivel mundial, por lo que dicha información podrá ser tenida en cuenta para desarrollar reglas para evitarlos. También pero en menor escala, servirá la experiencia a nivel local, que no siempre se condice con lo que sucede a nivel internacional, sumado a que al ser un mercado chico hay un fluido contacto con los demás procesadores de plaza y las instituciones financieras, lo que permite el intercambio de información ante los fraudes que suceden y las posibles estrategias para evitarlos.

Una vez definidas las reglas que son cargadas a cada sistema, conviene describir brevemente cómo se realiza este proceso. Cargar las reglas no es una tarea sencilla, ya que las mismas pueden tener diversas soluciones y deben contemplar innumerables alternativas, además de la información a tener en cuenta. Como se expresara anteriormente, una regla es la conjunción de una serie de parámetros preestablecidos. Para cargar estos parámetros se utiliza un sistema de codificación, es decir códigos que identifican diferentes ítems relacionados a cada transacción. Estos códigos pueden ser, a modo de ejemplo, el tipo de comercio, país de origen de la transacción, por citar algunos como los más importantes.

El **B.I.N.** podrá ser considerado como un código también a tener en cuenta. Se compone por los primeros seis dígitos de la tarjeta de crédito. Identifican el origen de la misma (institución financiera emisora) y brinda ciertos datos de utilidad al procesador que muchas veces desconoce, especialmente el adquirente. Al emisor también le interesará el mismo porque es una forma que tiene para cargar reglas teniendo en cuenta grupos de tarjeta por B.I.N.[12]

El B.I.N., como ya se indicara, permite agrupar también las tarjetas por el procesador emisor, incluso por producto del mismo (tarjeta de débito, de crédito, platino, oro, entre otras).

Teniendo en cuenta el B.I.N., y la posible codificación a ingresar en el sistema, el analista podrá cargar las diferentes reglas; de alerta o de restricción. De esta forma mediante la paramétrica establecida se podrá cargar al sistema una regla genérica o específica para un grupo de usuarios (ya sea por tipo de tarjeta, por banco emisor, por grupo de afinidad como puede ser el caso del Grupo de Viaje Ciencias Económicas). También podrá ser específica para determinadas compras en determinados comercios o en determinados países, por web o lectura de banda, por determinado importe y muchas más características comerciales e incluso combinaciones de varias de ellas. Toda esta codificación es anexada a la instrucción determinada como regla y de esta combinación es que queda cargada la regla de alerta. A manera de ejemplo, al B.I.N. que especifica las tarjetas “gold” del sello “Y” del banco “X” de Uruguay, se le indica que en caso de realizar una compra mediante lectura de banda en determinado país, a toda compra posterior por misma vía exija disparar una alerta. Esto es un ejemplo de miles de combinaciones que se pueden hacer; podemos incluso no definirla para un B.I.N. especifico, o puede ser para todos los B.I.N. de determinado banco de plaza, o para todas las tarjetas que procesa ese emisor. La combinación tiende a infinito, lo importante es tener en cuenta que ésta se da por la diversidad de códigos y datos que se cargan para la elaboración de la misma. Esta es la principal herramienta para el estudio de

[12] Dado que se entiende como un tema importante el de los B.I.N., es que se amplía el mismo en el Anexo I al final de este trabajo.

posibles transacciones fraudulentas y para evitar que las mismas se concreten. Con diferentes perspectivas, todos los sistemas de detección de fraude funcionan en base a un conjunto de reglas de alerta.

Los sellos proveen a los procesadores de sistemas de detección de fraude (el sistema de Visa por ejemplo se llama "*Advance Control")*, igual muchas veces este no alcanza por lo cual los procesadores tienen sus propios sistemas y trabajan a la par con el de los sellos. En el caso de Uruguay, y en base a lo analizado, los principales procesadores trabajan con sistemas propios (ya sea hechos a medida o adaptados a las necesidades), lo que no significa que no utilicen los sistemas de los sellos sino que toman como sistema de preferencia el propio; todos los sistemas trabajan con reglas de alerta y riesgos de fraude.

4.2.3. ¿Cómo funcionan las reglas de alerta?

Cada vez que el tarjetahabiente utiliza la tarjeta en un comercio, éste solicitará autorización para que la transacción sea aprobada. Esta solicitud de autorización llega al procesador emisor (responsable final de autorizar la transacción), el cual decidirá si autoriza o no la misma. Esta decisión la toma el propio sistema, visto en el capítulo anterior, teniendo en cuenta los datos de la propia transacción y los parámetros que tienen establecidos las reglas de alerta. Esto lo hace en un lapso de tiempo muy breve y siempre debe devolver una respuesta de manera automática (la respuesta debe llegar al comercio en menos de ocho segundos, sino el sello responde por el procesador). El sistema estudiará la transacción y la comparará, tanto con los parámetros preestablecidos en las reglas de alerta, como también con el propio historial del tarjetahabiente. Una vez realizado esto, el sistema está preparado para realizar las siguientes funciones:

1) *simplemente autorizar la transacción;*
2) *denegar o rechazar la transacción porque no cumple ciertas condiciones;*
3) *autorizar la transacción pero disparando una alerta de fraude o;*
4) *rechazar la transacción por considerar que la transacción es fraudulenta.*

Lo más habitual es que se dé el primer caso, que la transacción siga los parámetros normales del tarjetahabiente y no cumpla ninguna de las condiciones para disparar una alerta o ser restringida, por lo que la transacción será aprobada sin dar ningún aviso. La transacción se generó y el tarjetahabiente pudo realizar la compra, pagando la misma después a través del estado de cuenta. Esto es lo que sucede con mayor frecuencia.

Cuando se solicita una autorización de cualquier transacción comercial, el sistema estudiará las condiciones de la misma, como ser fecha, lugar, modo, comercio, historial del socio, historial del comercio, entre otras. De acuerdo a esto, el sistema podrá aprobar la transacción pero puede suceder que por alguna causa la transacción sea rechazada, no por ser fraudulenta sino porque se dio alguna condición de incompatibilidad en la misma como por ejemplo que se digitó mal alguno de los datos de la tarjeta, exceso en el límite autorizado de la misma, o que existe un bloqueo blando en ésta (generalmente se da por falta de pago).

El segundo caso implica que también puede ser rechazada por reglas específicas que tampoco indiquen que la transacción sea fraudulenta. Un claro ejemplo de este caso podría ser que para determinados países que cuentan con un importante nivel de fraude, se imponga una regla que solo permita una transacción diaria en el mismo.

Todos estos casos pueden disparar también alertas, ya que a manera de ejemplo un tarjetahabiente puede digitar mal sus datos en una compra por e-commerce, pero también puede darse que exista un sistema fraudulento que esté probando miles de numeraciones al azar buscando concretar transacciones. Es por esto que no se descartan simplemente, sino que está en la experiencia del analista descubrir rápidamente que se trata de un error y no un engaño (también es probable que el propio software con su estudio paramétrico ya le asigne un score bajo a la mayoría ayudando al analista en su análisis).

En otro caso, el tercero mencionado, lado la transacción podrá ser aprobada, pero por determinadas características de la misma disparará también una alerta para que el analista la estudie. La transacción fue aprobada, es decir se concretó, pero como es sospechosa será analizada posteriormente por el especialista quien anteriormente tuvo en cuenta la probabilidad de fraude de la misma (“scoring”). Esta alerta, por más que la transacción fuera aprobada, tiene el objetivo de que sea estudiada por el analista, ya que al considerarla como sospechosa, se buscará que el especialista la examine con la información que posee (historial del tarjetahabiente) para poder corroborar la transacción buscando así evitar futuras transacciones fraudulentas, siempre y cuando que aquella que disparó la alerta lo haya sido. Corresponde aclarar que en este caso la transacción sospechosa fue aprobada por lo que si la misma no fue realizada por parte del tarjetahabiente, el fraude se concretó de todas maneras.

La operativa se da de esta manera ya que si cada transacción sospechosa fuera rechazada o puesta en suspenso, esto haría que cientos o miles de éstas no se realizarían. Hay que tener en cuenta que una de las características que persigue cualquier tarjeta es un uso simple y rápido de la misma como medio de pago. Lo que sí debe quedar claro es que si existe absoluta certeza de que cierta transacción es fraudulenta, la misma será rechazada y

automáticamente la tarjeta será bloqueada. Este es el último caso, el cuarto, en donde el analista no estudiará el fraude sino que contactará al socio para darle el aviso respectivo del caso. Un ejemplo claro para esta situación, es una tarjeta con la cual se le aprueba una compra en Montevideo y cuatro horas después vuelve a solicitar autorización para realizar una nueva compra, pero esta vez en la ciudad de Londres, lo cual hará que se rechace dicha transacción por ser considerada fraudulenta y tendrá como consecuencia el bloqueo automático de la tarjeta. Existe una regla para compras fuera del Mercosur, por lectura de banda, que para compras realizadas fuera de esta región cuatro horas posteriores a una compra dentro de nuestro país se considera fraude inminente si ambas fueron por lectura de banda En este caso no se disparará alerta alguna para ser analizada, pero sí se aparecerá una alerta que funciona para informar al tarjetahabiente sobre la situación, además de que será impreso un nuevo plástico debido a que ha sido víctima de un fraude con lectura de banda. Esta alerta, será de interés para el analista para que pueda estudiar qué transacciones del tarjetahabiente pudieron ser fraudulentas, además de la detectada claro está, aparte de que es de utilidad para estudiar también dónde se originó el fraude.

Lo más importante a resaltar es que en el proceso de autorización nunca se espera un tiempo considerable por la respuesta ya que la misma demora segundos, pero ésta debe llegar indefectiblemente. O se autoriza o se deniega, por lo tanto la regla de alerta se puede disparar aprobando o no la compra, según la certeza o probabilidad de fraude que posea la misma, pero nunca quedará en suspenso. Si el procesador emisor demora en responder será el propio sello internacional quien responde por el primero. A manera de ejemplo el recorrido funciona de la siguiente manera: se realiza una compra a un comercio de China, suponiendo en este caso que es por lectura de banda. El comercio pasará la banda por la lectora (o llamará al procesador para pasar los datos, en caso de autorización por teléfono), pero de todas formas el comercio le indica la transacción al procesador adquirente de China solicitando la autorización del medio de pago. El procesador adquirente repetirá la solicitud ante el sello internacional el cual lo envía al destino del procesador emisor, quien estudia la transacción y los datos del tarjetahabiente para dar una respuesta al sello el cual repite hacia el procesador adquirente, llegando por último al comercio. Todo este proceso no puede durar más de ocho segundos y como vimos funciona como un camino de ida con la solicitud de autorización y de vuelta con la respuesta positiva o negativa de la misma. El software lo que hace es ver pasar la solicitud y en caso de considerarla sospechosa, emitirá una alerta de fraude (esto si encuadra con los parámetros establecidos para la misma), pero también debe darle una respuesta a esa solicitud de autorización aceptando o negando la misma, ya que como se mencionó anteriormente, siempre debe existir una respuesta.

4.2.4. Características

Las reglas pueden ser genéricas o no. Una **regla genérica** significa que puede existir para todas las tarjetas de crédito. A su vez, las reglas pueden ser creadas para que informen o para que rechacen una transacción. Una regla impuesta para que rechace una transacción se da únicamente porque hay gran seguridad de que exista fraude en la misma. Muchas de las reglas de rechazo no son genéricas, ya que se adaptan al perfil del tarjetahabiente. La regla genérica de rechazo por excelencia es la regla de distancia o regla geográfica, asociada a lectura de banda. Esta regla refiere, por ejemplo, a la imposibilidad física de realizar una compra en Montevideo y dos horas después realizar otra en Dubái. La misma regirá para todas las tarjetas sin importar el perfil de consumo del tarjetahabiente; lo sustancial en este caso es que ambas transacciones son físicamente imposibles de realizar para cualquier tarjetahabiente. Este tipo de transacción se rechaza automáticamente y no se consulta. El analista no perderá tiempo en analizar el caso ya que el sistema se encarga de rechazar la transacción de forma automática. No es un detalle menor destacar el hecho de que la transacción sea rechazada directamente, no solo por el ahorro en el tiempo de análisis por parte del analista, sino porque evita que se consuma el fraude ya que si la transacción fuera aceptada a pesar de generarse la alerta, dejaría de ser un intento de fraude para pasar a ser un caso de fraude consumado.

Una **regla no genérica**, por el contrario, existirá para cierto rubro, para cierta clase de usuario, para cierta clase de tarjetas. El ejemplo más claro en nuestro país y con el que más cuidado trabajan los procesadores emisores es el rubro agencias de viaje por ser éste muy riesgoso. El por qué de ser un rubro riesgoso no es por otra razón que por los importes que se manejan en este ámbito. Por lo general, los dueños de estas agencias compran los llamados “paquetes” compuestos por pasajes aéreos y estadías en hoteles con su propia tarjeta, lo cual hace que la misma deba tener un tratamiento especial ya que debe estar excluida de estas reglas. Por lo tanto, existirán reglas no genéricas que serán específicas para los casos de tarjetas de crédito asociadas a agencias de viaje ya que como se expresaba anteriormente manejan importes altos en las transacciones. Si las mismas fueran analizadas por reglas genéricas, se activarían permanentemente las alertas comunes para cualquier tarjeta habitual.

Se busca que las reglas sean eficientes y dinámicas. Una regla es eficiente cuando por ejemplo de cien casos que alerta, cinco son fraude, teniendo por ende un cinco por ciento de eficiencia. Si en cambio alerta mil casos y solamente cinco son fraude, no solo lleva más tiempo el analizar mil fraudes en lugar de cien sino que además conlleva un costo más elevado porque quiere decir que se necesitará más personal (analistas de fraude) trabajando

en dichas alertas, existiendo siempre la posibilidad de no contar con los recursos humanos suficientes. Además existe la necesidad que cada analista que está analizando cada situación que se le presenta, esté concentrado de tal manera en su trabajo para que pueda estudiarla de manera adecuada, y cuántos más casos analice por día jugará en contra de ello. Por lo tanto, al crear las reglas, las mismas deben alertar la menor cantidad de casos y éstos deben asemejarse lo más posible a un comportamiento fraudulento. Por ejemplo si una persona no acostumbra a comprar por Internet y lo hace, esa alerta probablemente se va a disparar, o si por el contrario no acostumbra realizar compras por importes mayores a mil dólares y en cambio sí realiza una compra por un importe mayor, también se deberá disparar la respectiva alerta.

Existen infinidad de indicadores a tener en cuenta para considerar si las reglas son eficientes o no. Los dos más analizados son:

1) Cobertura

2) Falso positivo

Cobertura o efectividad indica qué porcentaje de transacciones fraudulentas fueron identificadas por intermedio de los analistas, del total de casos de fraude que tuvo la empresa. Existen diferentes maneras de medirlo, las cuales van desde la cantidad de transacciones hasta la suma de los importes de las mismas, pero generalmente se miden a través de la cantidad de las mismas. Por ejemplo, si el procesador tuvo ciento cincuenta transacciones de fraude y logró encontrar quince, significa que la misma tiene una cobertura del diez por ciento y ese mismo porcentaje será el propio indicador. Esto se mide tanto a nivel general de fraudes concretados, como también puede analizarse por tipo de comercio o por comercio especifico. Sirve especialmente para el procesador emisor, pero es de utilidad para la parte adquirente también. Un ejemplo que sirve para ambos casos es que el procesador emisor en este caso, está detectando pocos fraudes en aerolíneas a pesar que se están concretando muchos; es decir, el índice de efectividad o cobertura es bajo, por lo que al procesador le interesará tener en cuenta esto para incluir nuevas reglas de alerta o ponderar con mayor importancia las transacciones en este rubro de comercio. De esta forma podrá detectar los fraudes mediante las respectivas alertas. Se puede aplicar el mismo razonamiento para un comercio específico, con la salvedad, claro está, que debe ser un comercio que por su magnitud pueda ser identificado específicamente. El historial del tarjetahabiente incorporará la totalidad de las transacciones quedando registro de aquellas que fueron alertadas como así también de la resolución de las mismas (hayan sido fraudulentas o no).

Todos los casos de fraude son cargados al sistema. Puede ser instantáneamente, o sea en el momento que el analista descubre cierta transacción fraudulenta, o incluso con

posterioridad, o sea una vez que se produjo el desconocimiento de la transacción por parte del tarjetahabiente concluyéndose que se trata de un caso de fraude. Es de vital interés que se carguen todos los casos de fraude al sistema, para así poder alimentar el historial del sistema de manera de extraer información de utilidad, como puede ser un índice de cobertura o incluso un historial de fraude. También será de particular interés, informar a los sellos acerca de la cantidad de fraude y el volumen de transacciones respectivo.

Falso positivo expresa cuántas alertas deberá generar el sistema para que el mismo pueda identificar el fraude. Por ejemplo, el sistema debió generar veinte alertas para encontrar un caso de fraude o si por el contrario tuvo que generar cincuenta alertas para encontrarlo. Visto de otra manera, cada veinte o cincuenta alertas que realizó el sistema, dependiendo del caso planteado anteriormente, una es fraude.

De todas maneras, lo que las procesadoras tienen en cuenta a la hora del análisis es qué tanto fraude son capaces de identificar en relación a la cantidad de empleados que se encuentran trabajando para tratar de detectarlo; que tan grande es el equipo de gente trabajando que se necesita para analizar las alertas que dispara el sistema. Como mencionáramos anteriormente, si cada analista debe analizar un gran número de alertas por día, tendrá que dedicar menos tiempo a cada una si es que su intención es analizar la totalidad de las mismas. Esto por una cuestión lógica de tiempo además que existirá una sobrecarga de trabajo y por ende un cansancio lógico en el analista que difícilmente pueda analizar de la misma manera una alerta respecto a otra.

Las reglas se van modificando, quitando o agregando de acuerdo a la evolución que tiene el fraude que se va detectando; es un trabajo día a día. Así por lo tanto, cuando una regla va quedando obsoleta, se puede quitar o se puede modificar según sea el caso, y en la medida que van surgiendo nuevos riesgos se van agregando otras que cubran estas nuevas alternativas. Son los indicadores de eficiencia que fueran definidos párrafos atrás, los que justamente miden si las mismas se volvieron obsoletas o no y de acuerdo a ese resultado es que las mismas serán modificadas o directamente eliminadas del sistema.

Es muy importante tener en cuenta tanto la dinámica del mercado como el seguimiento que se hará de la regla de alerta diseñada. La misma se crea en un mundo dinámico y probablemente al poco tiempo deba ser anulada, modificada o sustituida. Esto lo marca el propio mercado al que hay que estar monitoreando de manera constante. Es importante también, además de este monitoreo, la experiencia que se obtenga como consecuencia del uso de las mismas, además de analizar la eficiencia de las reglas en cuanto a la cantidad de fraudes detectados y qué tan obsoletas son. Igual nivel de importancia debe tener analizar el comportamiento del mercado ante determinado fraude, es decir cómo reaccionó éste ante la aplicación de determinada regla, y ésta experiencia obtenida será fundamental también ya

que la propia dinámica puede hacer que aparezca un fraude similar y que una regla obsoleta vuelva a ser aplicada. La experiencia entonces, será de gran utilidad.

En lo que a la experiencia respecta, también es de utilidad para detectar que determinado fraude ya existió con anterioridad y que al aplicar determinada regla sucedió otra cosa. Para estos casos se podrá crear una regla para evitar el fraude y otra regla preventiva porque se conoce que ante la regla impuesta, el o los defraudadores operarán de otra manera. De esta forma se puede prevenir dicha situación en base a la experiencia, y siempre en lo que al procesador emisor respecta.

Si bien fueron mencionadas varias características de las reglas de alerta, (dinámicas, eficientes, precisas), otra característica que es importante destacar es que deben ser, en lo posible, preventivas (detectar el fraude antes que suceda), o de lo contrario de rápida acción, es decir que si sucedió un caso de fraude la misma debe tratar de evitar que siga ocurriendo. En caso de detectarse tarde el efecto puede ser muy perjudicial, tal cual sucede como fuera analizado anteriormente con los puntos de compromiso, en donde su detección se debe dar con la mayor celeridad posible.

Tanto las reglas de alerta como su análisis, son la principal herramienta para contrarrestar el fraude, por lo que la correcta definición y utilización de las mismas es imprescindible si se busca minimizar el fraude con tarjetas de crédito.

4.2.5. Clasificación de las reglas de alerta

Si bien no fue encontrada una clasificación específica de reglas de alerta, en la investigación realizada se comprobó que es gran utilidad agrupar a las mismas de acuerdo a determinada característica que identifican o diferencian a las reglas entre sí, para poder comprender mejor su funcionamiento. Las reglas servirán tanto para el control emisor como para el control adquirente, y se adaptaran según cada caso.

A continuación describiremos más ejemplos de reglas de alerta y su respectiva clasificación:

- **Reglas de velocidad:** Es una regla que mide la cantidad de autorizaciones solicitadas en determinado período de tiempo. Una persona que realiza un número determinado de transacciones en un lapso de tiempo básicamente breve, hará que se dispare una alerta. Cuando existe un hurto de tarjeta de crédito, el delincuente tratará de utilizar la mayor cantidad de veces la tarjeta en un período corto de tiempo ya que la misma puede ser denunciada por parte del titular y ante este caso,

como ya se reiterara anteriormente, la misma será automáticamente bloqueada. Incluso sucederá lo mismo ante los casos de robo de datos o de lectura de banda magnética. Una vez disparada la alerta, el analista estudiará el comportamiento habitual del tarjetahabiente de acuerdo al historial de éste. Una tarjeta de crédito con pocas transacciones diarias, ante un caso de que en menos de dos horas se intenten realizar cinco o más transacciones, el sistema disparará una alerta justamente por existir una regla creada al respecto. El analista entonces, analizará el historial del tarjetahabiente y tomando en cuenta el score de probabilidad que el sistema previamente asignó definirá el tratamiento a seguir con la misma. Una tarjeta con muy poco uso, que se le disparen a manera de ejemplo siete autorizaciones en menos de dos horas, probablemente dispare la alerta justamente por el historial que tiene atrás, además que tendrá una elevada probabilidad de fraude. Si el analista visualiza además que las transacciones se dan en ramas de comercios no habituales para el tarjetahabiente, elevará aún más la sospecha de fraude.

- **Reglas exclusivas al tipo de transacción:** Puede ser una regla específica para lectura de banda o una regla específica para transacción por e-commerce (estas últimas son las reglas más frecuentes a utilizar)**.** Un ejemplo de esto se da en individuos que no acostumbran a realizar transacciones a través de Interne. Es probable entonces que al intentar realizar una, surja una alerta. Nuevamente aparece la importancia del sistema neural ya que la alerta se generará como consecuencia del análisis que realizará el sistema sobre el historial de la persona conjuntamente con el respectivo score asignado. Si el historial marca que el individuo acostumbra a realizar compras por Internet, seguramente no existirá alerta. Esta regla según el tipo de transacción (tanto por venta a distancia como por e-commerce) puede ser combinada con otro tipo de reglas, como por ejemplo la de cantidad de transacciones en determinado lapso. En este caso, puede ocurrir que la persona realiza compras por Internet con normalidad pero de carácter esporádico, y al realizar varias en un lapso relativamente corto de tiempo, probablemente se disparará una alerta al respecto. Es importante destacar que una regla es una combinación de varias condiciones, que en este caso serán el tipo de transacción (e-commerce) y la cantidad realizada en un lapso de tiempo determinado. Incluso la combinación puede contemplar muchas más características a la hora de definir la regla de alerta.

- **Reglas por origen de la transacción:** Es un tipo de regla muy utilizada para efectuar el control emisor e implica establecer como condicionante a la misma el lugar de origen desde donde fuera efectuada la transacción. Puede ser un país o incluso una ciudad, y es muy frecuente su uso dado que hay zonas que aparecen como muy vulnerables al fraude. Si un procesador sabe que determinado país o

ciudad está siendo atacada por defraudadores podrá poner reglas especiales para las transacciones que provengan de ese lugar, ya sea para rechazar las mismas o para realizar un seguimiento especial a las tarjetas que operaron en la región. Este tipo de reglas se caracterizan también por su dinamismo ya que las zonas vulnerables cambian con rapidez. Por ejemplo, debido a los Juegos Olímpicos Londres 2012, dicha ciudad fue una zona vulnerable al fraude, razón por la cual los procesadores crearon reglas especiales de seguimiento para tarjetas que fueron utilizadas allí durante los mismos.

- **Reglas por tipo de comercio:** Los comercios se codifican según un rubro o código específico, como fuera analizado. Así entonces, hoteles, agencias de viaje, supermercados, aerolíneas, joyerías, por nombrar algunos de los rubros más comunes, tendrán cada uno, su propio código. Dado el tipo de transacciones que se realizan en los mismos y la tendencia de que ocurran transacciones fraudulentas en mayor medida en alguno de ellos, es que existen reglas por tipo de comercio. Muchas veces están asociadas además, a la cantidad de transacciones e incluso al historial. A modo de ejemplo puede existir una regla que indique que más de tres compras en joyerías el mismo día dispare una alerta. A priori parece difícil pensar que un tarjetahabiente realice tres compras en joyerías el mismo día considerando los elevados importes que seguramente traigan aparejadas dichas transacciones por el rubro en cuestión. Si por el contrario estas compras se dan en casas de venta de ropa, dicha alerta no va a existir. Esto estará vinculado al historial del mismo, ya que parece difícil pero existen usuarios que pueden llegar a utilizar la tarjeta más de una vez al día en joyerías, y para estudiar y analizar justamente eso se encuentra el analista. Incluso hay tipos de comercio que a la segunda transacción en determinado período dispara la alerta. Esto es usual para el caso de agencias de viaje o aerolíneas, rubro no usual para el tarjetahabiente en líneas generales pero sí en cambio muy utilizado por defraudadores. Para este caso existirán excepciones a estas reglas genéricas ya que, como se mencionara anteriormente, si se consideran las agencias de viaje, las mismas compran muchos “paquetes” en lo que respecta a vuelos y estadías con tarjetas de crédito. De no existir estas excepciones, sería imposible que las mismas pudieran realizar las mencionadas compras ya que implicarían transacciones de miles de dólares. Las reglas de alerta por tipo de comercio son muy utilizadas para efectuar el control adquirente. Para que sea visualizado de forma más clara, se mencionará el siguiente ejemplo. Una tarjeta internacional realiza cinco compras en diferentes supermercados de nuestro país. No es habitual que una persona extranjera compre en diferentes supermercados el mismo día, y esta situación será visualizada por el adquirente en primera instancia, quien dará aviso al emisor; emisor que se encuentra en el exterior. Es el procesador adquirente quien puede visualizar en qué supermercados se realizaron dichas

compras, analizando si las zonas son muy distantes respecto al transcurso del tiempo entre compra y compra. El emisor no tiene acceso a esta información, pero puede ser alertado por el adquirente al respecto de esta situación la cual tiene las características de ser sospechosa. El estudio y aviso de este tipo de transacciones tendrá especial interés también para el tema de las responsabilidades, el cual será desarrollado en el capítulo cinco. Con este tipo de reglas también podemos ver un ejemplo de que cada alerta no implica que haya fraude y las mismas podrán ser descartadas rápidamente por el analista. El propio supermercado solicitó tres autorizaciones respecto de la misma tarjeta en escasos segundos. Esto como consecuencia de que la cajera, luego de pasar la tarjeta por el POS para solicitar la respectiva autorización, ante la demora en la respuesta del sistema del propio comercio, vuelve a solicitarla pasando una y dos veces más nuevamente el plástico por dicho dispositivo. Dicha situación hará disparar una alerta la cual será descartada rápidamente. En este caso debería existir una sola autorización para dicha transacción, y ante el caso que al momento de llegar el estado de cuenta, apareciera más de una, el tarjetahabiente tomará conocimiento de la existencia de la compra duplicada y podrá hacer el descargo respectivo.

- **Reglas por importe:** La regla en este caso será monetaria y se disparará cuando una o varias transacciones estén por encima o por debajo de determinado importe. Como los fraudes son muy dinámicos, en un período pueden aparecer cantidad de transacciones fraudulentas por lectura de banda, por ejemplo. Para este caso se puede imponer una regla que dispare alertas para todas las transacciones por lectura de banda por importes mayores a dos mil quinientos dólares americanos. Puede existir para e-commerce también. La cantidad de alertas que disparará el sistema dependerá entonces del importe que se le cargue como tope a la regla. Si el tope es de cien dólares americanos, la regla será totalmente ineficiente como vimos anteriormente ya que se dispararán varias alertas. Si bien el ejemplo analizado es de regla genérica, puede darse también como regla específica para determinadas tarjetas que así lo indiquen sus titulares. Por ejemplo, un titular puede solicitar al procesador que se le modifique el tope mencionado, tanto hacia arriba como hacia abajo del mismo, entonces la alerta se disparará para su posterior estudio pero la transacción, en caso de efectuarse, resultó rechazada.

- **Reglas condicionadas:** Este es un tipo de regla especial, la cual condiciona una transacción debido a otra que ocurrió con anterioridad. Este tipo de reglas nacen de la experiencia del analista en fraudes de hechos que sucedieron en el pasado. Un ejemplo de este tipo de reglas es que informe toda transacción realizada en Europa con determinada tarjeta de crédito con previa prueba de un dólar americano en Estados Unidos a través de Internet. Quien va a realizar el fraude no tiene

conocimiento del estado de la tarjeta por lo que verifica si la misma está habilitada mediante una transacción a través de Internet de un dólar americano en Estados Unidos. Si la misma es aceptada, el defraudador concluye que la misma está habilitada para así poder operar en cualquier país de Europa. Se disparará la alerta entonces la cual será analizada por el analista quien se encargará de determinar si bloquea la tarjeta o no dependiendo del historial del titular, ya que quizás es recurrente que el mismo realice compras a través de Internet en Estados Unidos y posteriormente viaje a Europa. En el caso que el tarjetahabiente no acostumbre realizar este tipo de transacciones se tratará de contactar al mismo para realizar la consulta y en caso que éste la confirme, se dejará constancia en el sistema mediante una nota para que la misma sea tenida en cuenta en el futuro. De no ser confirmada por el titular la tarjeta, la misma será bloqueada automáticamente y se procederá a la confección de un nuevo plástico.

- **Reglas de exclusión:** Son reglas que sirven para excluir a determinados tarjetahabientes de determinadas reglas genéricas. Habitual en el rubro ya mencionado de agencias de viaje, que por su habitualidad de compras de altos importes, disparará constantemente reglas de alerta y de rechazo.

- **Reglas de rechazo:** En base a la experiencia, puede crearse una regla que rechace toda compra en determinado tipo de comercio, fundamentalmente porque existe desconfianza por parte del procesador emisor respecto al procesador adquirente en cuanto a los controles que éste realiza. Este tipo de reglas se aplica para transacciones internacionales en donde los riesgos de que ocurran transacciones fraudulentas son mayores (esto para el procesador emisor). Si en base a la experiencia se detecta que están sucediendo fraudes de tarjetas con transacciones en boutiques de Holanda, por ejemplo, se rechazará toda compra realizada en estos comercios además de instalarse otra regla más específica para las tarjetas que realizaron compras en ese lugar ya que por más que la transacción sea rechazada, los datos pudieron haber sido robados y por esa razón se le hace un especial seguimiento en el futuro. La regla de rechazo también es utilizada cuando existe cien por ciento de seguridad que la transacción es fraudulenta, entonces en estos casos también se bloquea la tarjeta. Dentro de las reglas de rechazo podemos ubicar a las **restricciones**, que son reglas de alerta que funcionan como **preautorizadores**, es decir que aparecen antes de las autorizaciones y funcionan como filtros para aquellas transacciones que cumplen alguno de los parámetros que se quieren restringir. Las preautorizaciones pertenecen al sistema de autorizaciones, y dada su importancia se analizarán con detalle más adelante en este capítulo.

La necesidad de precisión y dinamismo al momento de cargar las reglas de alerta es fundamental para que la herramienta sea eficaz. Un ejemplo de regla que muestra la dinámica de las mismas se da para el caso que exista una cantidad elevada de fraudes en boutiques de Holanda. Cada rubro de comercio tiene un código por lo que se le solicita al sistema que informe de transacciones superiores a doscientos dólares americanos, por ejemplo, en Holanda en determinado período con previa transacción en Alaska, porque se conoce que en Alaska existió robo de datos con anterioridad (en este punto es fundamental la experiencia). Esto es muy general y dinámico, porque es algo característico al fraude, por lo que el procesador tendrá que crear las condiciones así como también las reglas para que el sistema informe en base a la experiencia obtenida de fraude. No solamente en base a esta experiencia sino además en base a los fraudes que siguen sucediendo. Puede ocurrir que algo no esté considerado en las reglas y como consecuencia puedan aparecer algunos desconocimientos de compra por parte de algunos tarjetahabientes en particular. Dicha situación será analizada y se concluye que la causa es la aparición de una cantidad elevada de fraudes en otro país, por ejemplo Finlandia, razón por la cual se decide poner una regla nueva, cambiar otra existente o inclusive hasta mejorarla.

Ante la posibilidad de que se tenga certeza que en determinado país se robaron datos de tarjetas de crédito, se puede crear una regla que dispare alertas para todas las transacciones con tarjetas realizadas por e-commerce, que previamente hayan operado en el país en el cual se robaron los datos. Como el procesador emisor no tiene cien por ciento de seguridad de que al socio le hayan robado los datos y dado el elevado costo que implicaría remplazar la totalidad de las tarjetas, se crea esta regla. Se realizará entonces un seguimiento de todas las transacciones realizadas mediante e-commerce teniendo en cuenta que con anterioridad a la misma, hayan comprado en el país donde se dio el hurto de datos. En este caso el procesador emisor tiene absoluta seguridad que existió hurto de datos y no copia de banda magnética, razón por la cual aplicará la regla solamente a las transacciones realizadas por venta a distancia.

4.3. Preautorizaciones – Restricciones

Anteriormente se desarrolló el concepto y las características de las reglas de alerta, así como también una posible clasificación de las mismas. Uno de los tipos analizados son las reglas de rechazo cuya función es la de negar una transacción. Dentro de las reglas de rechazo se encuentran las restricciones, las cuales funcionan dentro del sistema como preautorizaciones, es decir, antes de que el sistema analice la autorización de la transacción. En caso de que la misma sea rechazada por parte del preautorizador, es decir que éste la deniegue, llegará al sistema autorizador ya rechazada.

El sistema de restricciones, sería entonces como un filtro de transacciones y es el primer paso a través del cual dejará pasar o referirá la misma. Se dice transacción referida cuando la misma fue denegada por el preautorizador. El hecho de que no sea restringida la transacción no implica que luego no pueda disparar una alerta. Para esto viene el segundo paso del sistema, que es el disparador de alertas. En el caso del sistema de la empresa Paytrue[13], éste se llama "Advance Control".

Las restricciones, al ser una forma de reglas de alerta, son también la combinación de determinados parámetros que se establecen en el sistema informático, que en caso de que la transacción cumpla algunos de ellos, la misma no será autorizada. Pueden estar relacionados a diversas características de la transacción como por ejemplo el importe, país, tipo de comercio, por nombrar algunas de las características a las que más restricciones se le indican.

Las restricciones aparecen antes que el procesador estudie la autorización, y esto se da porque previamente el sistema fue configurado de tal manera que de cumplirse determinada condición, la transacción no será autorizada. Si por ejemplo el procesador está en conocimiento de que existe un elevado riesgo de fraude en peluquerías de México, ingresará al sistema una restricción que indique que toda solicitud de autorización del comercio peluquerías, país de origen México, sea denegada. Esto no implica que no se dispare el aviso de alerta, sino que por el contrario sí se disparará la misma y el analista la estudiará y probablemente se contacte con el tarjetahabiente para verificar que éste tuvo intención de realizar la transacción. De ser así entonces, pondrá algunas reglas para hacerle un seguimiento especial ya que dicha tarjeta puede ser riesgosa de haber sufrido robo de datos. En este ejemplo el analista tendrá dos opciones, o colocar una regla de alerta para las peluquerías de México, implicando un algoritmo especial para su estudio de probabilidad de transacciones fraudulentas; o directamente poner una regla de rechazo. Seguramente entendió que existe un alto riesgo además que la cantidad de transacciones en este comercio no afectará la operativa comercial y por esto es que tomó esta última opción. Cada caso es particular, por lo que nunca hay una respuesta única sino que varía por la dinámica mencionada.

Transacción referida se le dice a aquella transacción denegada por el preautorizador. En algunas ocasiones cuando se da una transacción referida, al comercio le llega el mensaje

[13] PayTrue Solutions es una empresa uruguaya de software dedicada al diseño de soluciones integrales para el negocio de medios de pago, tanto a nivel nacional, como de Latinoamérica y el mundo. Desarrolla productos y soluciones que contemplan todas las etapas o componentes del ciclo del negocio de medios de pago. Desde la emisión y adquirencia de tarjetas (crédito, débito y prepago); cubriendo la administración, autorización de transacciones, manejo de marcas internacionales, análisis de riesgo y detección de fraude.

que el tarjetahabiente debe localizar al banco emisor para solucionar el problema. Este llamará y según el caso le exigirá responder las preguntas de verificación de identidad para que le deje realizar la operación; esto siempre y cuando la restricción sea posible de levantar. Algunas no son posibles de ser levantadas por parte del procesador como por ejemplo el límite de crédito el cual es un tema pura y exclusivamente de riesgo crediticio que escapa a la responsabilidad del procesador.

En el caso de que una transacción sea referida, la misma no se concreta, a diferencia de lo que ocurre con las alertas que no tienen restricción, en las cuales la transacción puede ser aprobada o no según el riesgo de fraude.

Al ser una forma de reglas de alerta, también existen restricciones genéricas y específicas.

Las restricciones se cargan al sistema de la misma forma mencionada al inicio de este capítulo para las reglas de alerta, es decir, teniendo en cuenta los diversos B.I.N. y códigos posibles. Esto es lo que permite cargar reglas genéricas o específicas. Este método permite que las restricciones sean para un único tarjetahabiente, para un grupo de usuarios y a su vez establecer restricciones por códigos de comercio, importe, cantidad de compras y demás variables y combinaciones de ellas.

Las restricciones genéricas son aquellas que por defecto se establecieron para todas las tarjetas. Estas pueden ser por monto (dos mil quinientos dólares americanos por ejemplo), por cantidad de transacciones diarias, semanales, mensuales, entre otras. Es decir, si un individuo intenta realizar una compra por dos mil quinientos un dólares americanos, la misma será referida por haber sido restringida y por esta razón la transacción no podrá realizarse. El sistema de restricciones permite a su vez establecer ciertas reglas específicas que no restringen sino que por el contrario permiten, pero también serán reglas específicas. Siguiendo con el ejemplo, una regla especifica puede ser establecer como ilimitado el tope de compras según importe, lo que será específico para determinado B.I.N. que se ingrese en el sistema, o para determinado código que agrupe un rubro específico, como pueden ser las agencias de viaje (si no existiera esta restricción específica prácticamente estas empresas no podrían hacer compras). También puede hacerse para determinado cliente que así lo solicite, incluso existen los tarjetahabientes VIP, los cuales no tienen restricciones específicas de ningún tipo, salvo que el tarjetahabiente así lo indique.

Las reglas específicas se imponen a las genéricas porque como se detallara anteriormente las restricciones pueden contradecirse; en este caso primará la restricción más específica. La regla más específica de todas es la que rige solo para una tarjeta. El ejemplo más claro es la regla VIP, que permite prácticamente todo tipo de transacción a la tarjeta, por lo que se contradice con la gran mayoría de las restricciones restantes, sean especificas o genéricas. En este caso, la regla positiva que se incluyó en el sistema de restricciones

permite que el tarjetahabiente VIP pueda realizar compras por importes superiores a los que están restringidas las demás tarjetas (esto se usa para aquellas tarjetas sin límite de crédito). Usar este sistema para las restricciones es lo que permite darle la dinámica necesaria al sistema, para ingresar nuevas restricciones o reglas específicas para determinadas tarjetas.

El hecho de que una transacción no sea referida no implica que no se dispare una regla de alerta; son cosas distintas. Puede suceder que no esté restringida la transacción pero que sea sospechosa de fraude y genere la alerta respectiva. A modo de ejemplo, una tarjeta VIP sin restricciones, genera una alerta debido a que con ella fueron realizadas transacciones con lectura de banda en Brasil y en Estados Unidos con pocas horas de diferencia el mismo día. El analista al estudiarlas determina que es una clara transacción fraudulenta por lo cual puede bloquear la tarjeta. Lo que se pretende demostrar con este caso es que por más que se trate de una tarjeta denominada VIP, de todas maneras se dispararán las alertas y se podrán bloquear las tarjetas.

Para el caso de que la transacción sea referida, al comercio le aparecerá el mensaje de que el usuario debe llamar al banco emisor o al procesador, y uno de estos eliminará la restricción (obviamente luego de realizada la identificación positiva del mismo y de quien la realice tenga autorización para eliminar la misma). Conviene aclarar que el encargado de suprimir las restricciones siempre es el procesador emisor, en todo caso si el servicio se encuentra tercerizado, el banco se comunicará con el mismo para realizarlo.

No todos los avisos de alerta, ni las restricciones son casos de fraude. Un ejemplo claro de restricción son las tarjetas regionales. En los hechos, no existen tarjetas regionales ya que todas las tarjetas son internacionales por defecto (en el caso de los sellos internacionales), pero al aplicarles la restricción de la región les restringen su utilización fuera de la misma. Esto es algo que no es común fuera de fronteras y que es una práctica más bien utilizada en nuestro país.

Según se informó durante la investigación, este sistema de restricción por B.I.N. y códigos redujo el fraude en más de un cuarenta por ciento.

4.4. Otros ejemplos de restricciones

Volviendo al sistema de parámetros y reglas, se mencionó que estas últimas pueden ser generales o particulares. Otro ejemplo es el caso que para un determinado B.I.N. que pertenece a determinada institución financiera, se impuso una restricción que indica un máximo de diez compras por día y dos mil dólares americanos de gasto total; para siete días un máximo de veinte compras y siete mil dólares americanos de gasto total. Esto es lo que

determinó la financiera para toda su cartera, solicitándole al procesador que ingrese estas restricciones. Se deber tener en cuenta que podrán existir restricciones específicas para determinadas tarjetas de esta institución financiera que tengan límites mayores o menores a los determinados en el ejemplo y las mismas restricciones se impondrán a las genéricas (sino no tendrían efecto las restricciones específicas). Incluso otro caso dentro de este mismo ejemplo es que un determinado usuario puede solicitar a la financiera que le aumenten el límite de crédito de su tarjeta con motivo de un viaje que hará o que simplemente va a realizar determinada transacción puntual que excede los parámetros restringidos para así ser habilitado por medio de las restricciones de los B.I.N. y códigos. Le aumentarán el límite de crédito a su tarjeta o lo pondrán dentro de categoría VIP provisoriamente mientras dure el viaje o la transacción mencionada. Con este ejemplo queda claro como la restricción genérica no afecta la operativa ya que se cuenta con las restricciones específicas y también con las restricciones positivas. Las alertas seguirán funcionando por más que se levanten todas las restricciones con la restricción VIP en particular.

Siguiendo con el ejemplo anterior, al momento de la recopilación de datos esa financiera tendrá por restricción genérica el poder realizar diez compras por día, pero a su vez el procesador tendrá como restricción específica que para el código que indica lugar de transacción “484”, solo se podrán realizar cinco compras diarias. Esta es una restricción específica que no fue solicitada por la financiera sino que fue impuesta por el propio procesador para el lugar de la transacción y eso se debe a que el lugar no ofrece las mayores garantías en cuanto a fraude (son lugares un tanto vulnerables con muchos casos de fraude a esa fecha). Incluso hay países que directamente refieren toda transacción además de que realizan un seguimiento especial a aquellas tarjetas que lo intentan, porque pudieron haberle robado los datos al tarjetahabiente a pesar de no haber podido realizar la transacción. De todas maneras, generalmente los defraudadores no prueban hacer transacciones con tarjetas que fueron rechazadas durante la transacción original porque desconocen la razón por la cual la misma fue rechazada, entonces prefieren realizar el fraude con las que sí tienen certeza que están habilitadas. En caso de que cualquier usuario viaje a estos países, siempre y cuando el mismo no haya dado aviso del mismo, no podrá utilizar la tarjeta. Al momento de realizar esta investigación uno de los países que se vislumbraba como más vulnerables al fraude era Gran Bretaña (el hecho de las Juegos Olímpicos genera un caudal muy importante de tarjetas de todas partes del mundo y lo hace más vulnerable al riesgo). Otros países con riesgo elevado de fraude al momento de la investigación eran Líbano y Australia (este último caso tenía en ese momento una restricción de cien dólares americanos semanales, pero para el caso particular del código de afinidad que identifica al Grupo de Viaje de Ciencias Económicas, se los ubica como VIP por tiempo limitado teniendo en cuenta además el plan de viaje tentativo). Una tarjeta a la

que se le copia la banda magnética o se le roban los datos, puede ser utilizada por distintos lugares del mundo, ya sea mediante falsificación de plástico o por compra vía e-commerce.

El límite funciona como restricción no solo para el fraude, sino también para el consumo. Se utiliza mucho con las tarjetas de crédito adicionales a las cuales se les aplican límites por compra, por cantidad e importe, tanto diarios como semanales. Incluso a una tarjeta con restricción VIP, se le puede indicar que es VIP con límite de crédito de diez mil dólares americanos. Este límite funciona como otra restricción específica para esta tarjeta.

Como se indicara anteriormente, en caso de transacción referida, el tarjetahabiente deberá llamar para levantar la misma, con previa identificación positiva. Es una molestia tanto para el caso del usuario como para la institución financiera, pero es una excelente herramienta y por este motivo se recomienda dar aviso cuando se realiza un viaje. En general esta herramienta no entorpece en gran medida la operativa; por ejemplo, en uno de los días en que realizáramos la investigación, se llevaban cuatro transacciones referidas a media tarde, de las cuales algunas eran tarjetas adicionales que tienen la restricción impuesta por el propio tarjetahabiente. El sistema permite ver todo el historial del tarjetahabiente, incluso los adicionales que tenga adheridos, claro que cada tarjeta titular o adicional se puede identificar, y tendrá sus restricciones como ya fuera analizado (titular y adicional comparten algunas restricciones y otras no, ya que éstas no tienen por qué ser las mismas).

Para tarjetas de débito, también hay parámetros de restricciones, como por ejemplo en Uruguay y para tarjetas del B.R.O.U. que solo se permite una extracción diaria fuera del país.

4.5. ¿Cómo funciona el estudio de las alertas generadas por parte del analista?

El analista es parte del equipo de trabajo del procesador, y es el encargado de estudiar las alertas que dispara el sistema de autorizaciones y el de restricciones. Es decir que el analista estudiará alertas por transacciones referidas como por transacciones concretadas. Según lo indicado al principio de este capítulo, el mismo revisará las alertas según una “cola” de éstas que generará el sistema teniendo en cuenta el scoring de cada una de ellas. El analista podrá estudiar las restricciones siguiendo su propio criterio de prioridades en base a su experiencia, o podrá estudiar las mismas en base al criterio de prioridades ponderado que se cargó en el sistema si la cola de alertas es extensa. Este, además de contar con esta herramienta para el análisis (el scoring), también realizará su estudio teniendo en cuenta el historial del tarjetahabiente y toda la información referente al mismo, la cual, como ya se

indicó, se encuentra en el propio sistema y el analista podrá observarla al instante. Para el análisis, aparte de su propia experiencia, también se basará en la información del mercado local e internacional (en el caso de un analista para un procesador adquirente el historial que tendrá será el del comercio).

En todos los casos de análisis es fundamental el estudio del historial del tarjetahabiente. El conocimiento del cliente es un aspecto importante para el análisis pero no siempre se cuenta con esta información (en lo que refiere más precisamente a la información personal del tarjetahabiente). Uruguay cuenta con una ventaja en este aspecto por ser un país pequeño, pero en países grandes como Brasil por ejemplo, esto se dificulta mucho más. Recordar también que en nuestro país se procesan tarjetas de instituciones financieras del exterior cuyos clientes residen en el extranjero y no se cuenta con la información personal de éstos. Menos aún, alguna forma de poder contactarlos y es en este punto donde el analista deberá basarse exclusivamente en el sistema y en el historial de transacciones.

Para tarjetas locales, además del historial, generalmente se cuenta con datos de la persona y diversas formas de poder ubicarlo, además de que para clientes importantes el propio ejecutivo de cuenta de la institución financiera es el contacto y conoce al tarjetahabiente personalmente lo cual sirve de mucha ayuda para el análisis. Volviendo al ejemplo de las tarjetas del Grupo Viaje de Ciencias Económicas, para este caso de conocimiento del cliente, las mismas tienen un grupo de afinidad creado por el emisor y al momento de revisar una alerta el analista puede identificar el código sabiendo que el cliente se encuentra realizando dicho viaje. Esto no implica que la alerta sea descartada, pero es información útil a tener en cuenta.

Cuando la alerta se dispara, la misma llega al analista. Si el mismo cree que la probabilidad de fraude es muy elevada, puede bloquear preventivamente la tarjeta hasta tanto confirme o no el fraude (por ejemplo puede intentar comunicarse con el cliente). Es un **bloqueo preventivo**, que luego puede desbloquear o bloquear definitivamente con la consecuente reimpresión del plástico. Esto se hace para evitar que sigan cometiéndose fraudes. El analista puede no bloquearla sin antes tratar de ubicar al cliente, pero lo decide en base a la percepción de fraude que vea en la transferencia alertada (recordar que otra opción es descartar la alerta o directamente bloquear la tarjeta cuando hay elevada seguridad de fraude).

Como se mencionara anteriormente, existen alertas que pueden referir transacciones que el analista estudiará, pero en estos casos las mismas no fueron aprobadas por lo que el fraude no llegó a concretarse pero sí existió un intento (si es que la transacción era fraudulenta). De esta manera el analista estudiará la transacción sin que se haya concretado el fraude y podrá bloquear la tarjeta si considera que realmente hubo un intento. El analista entonces

estudiará los parámetros que hicieron que la transacción fuera referida y los comparará con el historial del tarjetahabiente.

El analista puede ver toda la información, de donde compró, tipo de comercio, fecha y moneda, transacciones anteriores por fechas, rubro, país, e incluso saldo del límite de crédito.

El análisis se dificulta cuando el posible fraude se está cometiendo en el mismo país donde se encuentra el tarjetahabiente. Esto se debe a que es más difícil detectar el perfil del usuario para compras locales que para compras internacionales.

Detectar el fraude a través de una sola alerta es difícil. Generalmente con el estudio de las alertas se genera una sospecha; si la misma es grande el analista bloqueará preventivamente la tarjeta lo cual ya es una medida dura porque el tarjetahabiente no podrá utilizarla. Además de bloquearla, siempre que la sospecha de fraude sea grande, podrá pedirle al comercio que retenga la tarjeta lo cual es la medida más dura de todas. Si llegara a haber una equivocación en la presunción de fraude en este último caso, sería una muy mala imagen para con el cliente ya que de suponer que éste estuviera de viaje sería una complicación para él no poder contar con la tarjeta. La denegación de la compra obviamente es la menos dura de todas, mientras que el bloqueo, si bien es una medida más fuerte que la denegación, se puede levantar mediante una simple comunicación con el procesador.

El bloqueo se realiza ingresando un código al sistema (por ejemplo para el caso del sistema utilizado por Sistarbanc es el 0895), por lo que toda compra posterior será referida y se indicará con ese código, además en notas se le agregará “posible ataque fraudulento”. Todas las compras sospechosas de fraude se pueden enviar por listado al banco quien se comunicará de manera más fácil con el tarjetahabiente y éste responderá por las mismas. En caso de haber respuesta negativa (o sea que el titular de la tarjeta confirme que la compra no fue realizada por él), se cambiará el **bloqueo** preventivo a **permanente**. En este caso, el bloqueo provisorio evitó que se sucedieran fraudes entre el lapso que se consultara al banco y llegara la respuesta por parte de éste. La comunicación con el cliente la puede realizar el propio emisor según con qué información cuente el mismo. La misma se realizará por mail al igual que la respuesta, quedando ambas guardadas en el sistema del procesador. La comunicación vía mail entre procesador e institución financiera generalmente demora unos días.

En ocasiones hay varias transacciones referidas, tanto las enviadas como las que llegan después de la consulta de determinada tarjeta ya que los defraudadores la siguen probando algunas veces más. En este caso, estas transacciones referidas, son intentos de fraude porque el mismo no fue concretado. En todo caso habría que comparar con transacciones

anteriores para analizar si alguna no es reconocida por el tarjetahabiente y en ese caso si existiría fraude consumado.

Todo movimiento, ya sea generado por el procesador, por una restricción o por una alerta, genera un código lo cual facilita y agiliza su comprensión al momento de su análisis. Por ejemplo, en el caso anterior se bloquea la tarjeta con código 0895, "posible ataque fraudulento", y toda compra posterior que se intente realizar con ese plástico será referida, ya que no pasará el pre-autorizador, y generará una alerta con dicho código. Cuando el analista observa la misma, inmediatamente sabe que se debe a que se intentó usar un plástico bloqueado por posible ataque fraudulento. Esto no implica que se siga intentando usar la tarjeta clonada por parte del delincuente sino que puede ser el propio tarjetahabiente que quizás, por equivocación, intentó usar el plástico ya bloqueado.

Hay casos en que se bloquea preventivamente y es el propio usuario el que exige que se desbloquee la tarjeta, pero resulta que efectivamente el bloqueo había sido correctamente realizado ya que habían existido transacciones fraudulentas. En este caso se puede poner como ejemplo un cliente al cual se le bloquea preventivamente la tarjeta por haber sufrido intentos de uso de la misma en Brasil. Este llama para informar que efectivamente se encuentra de viaje en Brasil por lo que solicita la activación de la misma nuevamente. Sin embargo, los intentos de fraude para con este cliente eran verdaderos y continuaron, por lo que al haberse quitado el bloqueo a pedido de él, no tuvo otra opción que asumir la responsabilidad por las transacciones fraudulentas ocurridas como consecuencia del pedido de activación de la tarjeta por parte de él.

El analista, como se analizara anteriormente, en caso de transacción sospechosa tratará de ubicar telefónicamente al tarjetahabiente. Si no puede encontrarlo o carece de información para hacerlo, dará aviso al responsable de la institución financiera emisora de la tarjeta de crédito, ya que al tener más contacto con el cliente podrá ubicarlo más fácilmente. Uno de los softwares de procesamiento analizados en este trabajo, tiene la funcionalidad que en caso de generarse una alerta, podrá enviar, en caso de ser necesario, una serie de mails a los responsables de su análisis con el aviso de la misma y con el subject: *"ver alerta 1234"*, por ejemplo. De esta manera el responsable dentro de la institución financiera podrá recibir la alerta y contactarse con el cliente (la institución financiera es quien más contacto con el cliente tiene) para que este último confirme o no la compra, para luego ingresar a la página del procesador y escribir notas acerca de lo actuado. Al actualizar estas notas, el responsable en la financiera disparará un mail de respuesta para el analista respectivo. Este tipo de soluciones le permite al banco interactuar con el procesador emisor, pudiendo analizar "en línea" todo lo realizado en materia de seguridad con cada uno de sus clientes (ver los bloqueos, las denuncias referidas, las alertas y demás). Para esto se debe tener en

cuenta siempre el perfil del empleado quien delimitará las autorizaciones o accesos propios, siempre a través del uso de contraseñas.

Una vez generada la alerta, la misma llegará al analista para que éste la estudie. En el análisis, lo primero que tratará de identificar es por qué se generó la misma (muchas veces puede identificarla por el código de restricción como fuera visto anteriormente en el caso de uso de tarjeta bloqueada). Para este caso se puede suponer que un tarjetahabiente realizó una compra en Miami por un importe considerable o que el mismo venía realizando transacciones en cantidades suficientes que dispararon la alerta. El analista entonces, estudiará el historial de las últimas transacciones y deberá ser preciso en la información a analizar ya que tendrá que saber exactamente qué es lo que busca encontrar en su análisis. Como el historial es muy completo, de no ser preciso con la información a solicitarle al sistema, su análisis podrá volverse complejo y hará que el mismo le consuma demasiado tiempo, volviéndose ineficiente en su función. En este caso y continuando con el ejemplo, el analista filtrará las transacciones por tiempo y lugar (compras realizadas en los últimos seis meses en Miami). Observará así que el tarjetahabiente realizó compras similares a las de la alerta que está analizando, además que recientemente tiene una compra en un hotel en Miami, lo que también da cierta tranquilidad porque ubica al tarjetahabiente en esa ciudad (de todas maneras tener presente que no quiere decir que no le hayan clonado la tarjeta y la estén usando en ese lugar). Este tipo de fraude es difícil de detectar para el analista porque el tarjetahabiente y el defraudador utilizan la tarjeta en el mismo lugar. Las compras en hoteles son difíciles de observar en defraudadores porque implican que el mismo se quedará en ese lugar lo cual lo expone de cierta manera y por ello tratará de evitar. Siguiendo con el ejemplo pero para otro caso, la alerta la dispara una compra en una concesionaria de autos (como el caso de BMW) y el historial reciente muestra transacciones en la misma ciudad de la concesionaria; dos con tarjeta presente, una en el comercio Best Buy y otra en un hotel. El analista determina que estas compras están acordes al patrón de conducta del tarjetahabiente pero lo que determina que aparezca la alerta es el importe elevado en la transacción. Como las mismas son comunes en este tarjetahabiente, el analista para este caso no considera que exista fraude, razón por la cual descartará la alerta y el sistema dejará constancia de ello para que sea tenido en cuenta en el historial (quién y cuándo, y de corresponder las notas debidas, cómo puede ser que se llamó a la persona quien confirmó la compra o en todo caso que el contacto comercial del banco la confirmó). El analista, además de todas las transacciones, podrá observar también la totalidad de alertas generadas para ese tarjetahabiente.

En este caso el cliente tiene un perfil de consumo masivo, con compras elevadas y ésto es observado por parte del analista, mientras que el defraudador difícilmente lo sepa. Por esta razón, al analista le llamará la atención, por ejemplo, compras en casas de comida rápida cuando no son el perfil del usuario. Por ello, el analista podrá desconfiar de la compra, pero

como no sabe qué está sucediendo realmente, puede en vez de descartar la alerta, bloquear preventivamente la tarjeta. La misma es una medida un en cierta manera dura, ya que el tarjetahabiente no puede usar la tarjeta mientras el bloqueo continúe. El mismo deberá durar poco tiempo, además de que para realizarlo el analista deberá tener cierta presunción de fraude y deberá evacuar la duda de manera rápida.

El analista, al momento de estudiar la alerta, cuenta con toda la información al instante, es decir que la alerta no solo indica por qué se generó, sino que a su vez trae consigo toda la información referente necesaria (datos de la tarjeta y de la financiera emisora, información del comercio, categoría, detalles de la autorización como puede ser importe, hora, lugar y datos del tarjetahabiente). También tiene ligado el histórico de transacciones, donde se pueden observar las mismas según los filtros que aplique el analista (por fecha, por importe, por lugar de compra, por transacciones con alertas, puede también ver el "block de notas"). Esto será de especial interés para el analista para así conocer el perfil del tarjetahabiente y poder hacerse una idea acerca de la transacción bajo sospecha para determinar si la misma es fraudulenta o no; esto último es muy subjetivo y tendrá un margen de error, el cual se busca minimizar con la utilización de todas estas herramientas.

Otro ejemplo de análisis de éstas se da cuando al analista le llega una alerta con determinado código, por ejemplo el "41" para el caso del sistema utilizado por Sistarbanc, el cual significa tarjeta perdida. Es decir que surgió una alerta porque hubo un intento de realizar una transacción con una tarjeta que fue denunciada como perdida. La transacción no fue aprobada, ya que la denuncia realizada en su momento bloqueó la tarjeta además de que obviamente se dispara la alerta para que sea estudiada. El analista observa que la transacción se da vía e-commerce y cuando estudia al comercio a través del historial observa que anteriormente se había realizado una transacción. Analizando el tipo de comercio deduce que el gasto probablemente es por una licencia de algún software que se está actualizando. Esto no es un fraude, ya que cuando se firmó el contrato original entre el comercio y el tarjetahabiente, este último permitió la renovación automática y el comercio conservó los datos del tarjetahabiente y automáticamente solicitó la autorización en la renovación, con los datos cargados anteriormente, solo que en ese lapso de tiempo la tarjeta se venció (suponemos que el comercio cumple con las condiciones para guardar datos de la tarjeta, la implicancia de ésto se verá en el próximo capítulo).

Esta es una alerta muy común que se descarta, y sucede con las renovaciones automáticas (ya sea por compra de licencias, o de suscripciones por ejemplo) en el cual el comercio renueva el contrato con los datos de la última carga, por lo que si la tarjeta se venció, se canceló o por determinada razón fue bloqueada, la transacción será referida ya que los datos de la tarjeta son incorrectos y además se genera la alerta. Esto no implica fraude porque no hubo intención de engaño, sino que fue una transacción normal. En todo caso el

comercio después contactará al cliente para una nueva autorización, lo que escapa a las funciones de los procesadores (el comercio se quedó con todos los datos de la tarjeta porque el contrato que firmó con el tarjetahabiente así se lo permitió y porque el cliente a su vez se encontraba autorizado para hacerlo, para esto debe cumplir con los estándares de calidad que así lo exigen).

Otro ejemplo de alerta referida, se da cuando la misma llega al analista con determinado código; en este caso de estudio y para el sistema utilizado por Sistarbanc, el código 14 implica tarjeta inexistente. El analista al observar dicho código sabe que es referida (o sea que no se realizó la transacción, no se autorizó), por lo que supone que no hubo intento de fraude sino que ve que es por Internet y concluye que fue un error del tarjetahabiente al introducir algún número en la transacción por Internet. Si el analista observa que siguen ingresando transacciones erróneas de ese comercio, ahí sí sospechará. De todas maneras no se descarta, porque siguiendo con este ejemplo, se puede dar el caso que una institución financiera alerta la existencia de fraudes con instituciones de calidad vía e-commerce. El analista, como conoce este tipo de fraude, tendrá especial recaudo con el código 14, ya que en muchas oportunidades estos fraudes se prueban con números tratando de llegar a datos de tarjetas verdaderas, y de ahí a que en los intentos salen tarjetas inexistentes (estos fraudes son generalmente por montos menores en dólares americanos).

Otra restricción existente es el código “07”, el cual es una restricción para tarjetas que anteriormente fueron víctimas de fraude, es decir se consumó el fraude con ellas, y por lo tanto las mismas resultaron bloqueadas. Luego de este bloqueo, existe un intento de utilización de las mismas, por lo que el analista tendrá que definir cuál de estas dos situaciones es la verdadera: pudo ser el propio tarjetahabiente que sin darse cuenta utilizó el plástico bloqueado (por eso debió haber roto el mismo en su momento), o pudo ser el defraudador, entonces habrá que dar aviso del intento de fraude para que sea tenido en cuenta para las estadísticas. Vuelve a ser un intento ya que el fraude no se cometió.

El código “0057 transacción no permitida”, se da para tarjetas que se encuentran inhabilitadas o suspendidas (siempre para el sistema utilizado por Sistarbanc). El analista deberá analizar la causa de las mismas, las cuales pueden ser que está vencido el plazo de pago y el mismo no fue realizado, por ejemplo.

Para finalizar este capítulo es importante recordar que el responsable de cargar las reglas de alerta es el procesador, quien podrá tener en cuenta indicaciones dadas por la institución financiera, pero en definitiva es éste quien decide cuáles cargar y cómo hacerlo. También se vuelve a recordar que quien bloquea y desbloquea plásticos es el procesador, mientras que la institución financiera solamente podrá dar instrucciones para que se habiliten o

deshabiliten determinadas tarjetas, pero nunca bloquear o desbloquear (siempre y cuando el servicio esté tercerizado).

Cuando el procesador realiza consultas al banco por determinadas alertas, le interesa respuestas concisas de éste. Por ejemplo si tenemos una compra dudosa hecha por el tarjetahabiente en Francia, al procesador le interesa que le de el "ok" o no a esa compra, y no que solo se mencione que el cliente había avisado que viajaba a Francia. Puede ser que esté en Francia y le hayan clonado o robado la tarjeta y se la estén usando, por lo que esa información de donde está sirve pero en este caso es incompleta. Para los casos de transacción con sospecha, se precisa que se confirme o no la compra.

CAPÍTULO V

FRAUDE EN URUGUAY Y LA REGIÓN

5.1. Introducción

En el capítulo uno se hizo mención a los diferentes tipos de fraude, los cuales fueron clasificados según las características que los identifican. Si bien existen diversos tipos de fraude con tarjetas de crédito que se están realizando hoy en día en la región, son dos los que más preocupan y más atención prestan los procesadores. Los mismos son:

1. **Fraude por lectura de banda**
2. **Fraude por venta a distancia, el cual se subdivide en dos categorías:**
    - **E-commerce**
    - **Venta telefónica**

5.2. Fraude por lectura de banda

Esta forma de fraude es la que fuera clasificada previamente en el capítulo uno como fraude por tarjeta falsificada, que implica que el tarjetahabiente no participa en la transacción y aún conserva su tarjeta de crédito. Para que exista fraude por lectura de banda, necesariamente debe existir contacto entre quien realiza el fraude (delincuente o defraudador) y la tarjeta de crédito del tarjetahabiente que lo sufre, ya que en algún momento el primero debe haber realizado la copia de la banda magnética de la tarjeta mencionada. Se lo conoce con el nombre de “fraude con tarjeta presente” y el ejemplo más común se da cuando un individuo concurre a un restaurante y al momento de pagar entrega la tarjeta de crédito junto con la cuenta al mozo del lugar. Éste se traslada con la misma hacia la caja del local debido que allí es el lugar donde generalmente se encuentra el POS que autorizará o no la respectiva transacción. El tarjetahabiente entonces, pierde de vista su tarjeta de crédito y es en este momento que el mozo o el cajero, o cualquiera de las personas involucradas, pasan la tarjeta por el lector el cual copia la banda magnética de la misma (“skimmer”). Recordar que en la banda magnética se encuentra información secreta que incluso no sale a luz con la impresión de cualquier “voucher” o recibo. Un lector de

banda magnética es un instrumento que se puede adquirir en cualquier comercio de venta de equipos electrónicos, con la diferencia que quienes realizan este tipo de fraude, realizan la conversión de este simple lector en lector grabador y con este último es que graban la información que se encuentra en la respectiva banda. Deben tener la tarjeta de crédito original para poder copiar los datos de la misma; de no contar con ésta, es imposible acceder a los datos que ésta contiene.

Como detalláramos anteriormente la información que es necesaria grabar es:

- el número de la tarjeta
- la fecha de vencimiento de la misma
- CVC 2 o CVV (código de seguridad)

En la imagen a continuación se observa un **"skimmer"**. Podemos observar el tamaño del mismo en comparación a la palma de una mano. El mismo es utilizado para robar los datos de una tarjeta de crédito. Se puede llevar en el bolsillo de cualquier pantalón o incluso hasta en el cinturón, pasando totalmente desapercibido. Una vez que la tarjeta toma contacto con el dispositivo, en cuestión de segundos lee y graba los datos de la misma sin que el cliente tome conocimiento de ello.

5.2.1. Definición de "skimming"

"Skimming": Codificación de una banda magnética con información válida de otra banda magnética, incluyendo el CVC2 o el CVV.

El sistema llamado "skimming" es un método por el cual se copia la información que contiene la banda magnética de una tarjeta de crédito. "Skimmer" es básicamente un

copiador de tarjetas portátil muy pequeño. Por ejemplo en Estados Unidos de América, han sido detenidos camareros que lo llevan debajo de la camisa, y antes de pasar la tarjeta por la caja hacen una copia rápida. De esta manera logran obtener la información que posee la banda. Luego con la misma procederán al falsificado del plástico de la tarjeta de crédito al cual le adjuntarán la información de la banda copiada.

Un sistema más ingenioso todavía, para las tarjetas de crédito con las cuales se puede retirar efectivo**,** es instalar un skimmer en la puerta de un banco o en un cajero. Los delincuentes lo instalan encima del lector de "abrir la puerta" en un horario poco habitual de concurrencia por parte del público, por ejemplo la madrugada. Al pasar la tarjeta por el lector, la misma queda copiada. También se han visto skimmers como "apéndices" de la ranura normal donde se introducen las tarjetas, de modo que primero se copia y luego entra en la ranura de verdad. Además, los delincuentes se hacen con el PIN solamente mirando a la gente por encima del hombro mientras teclean en un cajero, con una cámara desde cierta distancia, y de otras formas. Luego si tienen un skimming de la tarjeta (o el número para así generar una nueva tarjeta) pueden extraer dinero del cajero sin problemas.

Siguiendo con los cajeros automáticos, existe otro tipo de fraude que se realiza colocando en los mismos, entradas de tarjetas falsas que puedan leer la banda magnética y almacenarla para ser copiadas más tarde. La tarjeta es introducida por parte del usuario en el cajero automático para realizar la extracción de dinero, pero la entrada del mismo (la ranura en la cual se introduce el plástico) fue adulterada por parte de los delincuentes introduciendo un dispositivo que lee la banda magnética. Este método normalmente se combina con un teclado que también almacena el código secreto (PIN) o una cámara en la parte superior para poder grabar el número. De esta manera podrá hacerse una copia de la tarjeta y extraer dinero de los cajeros sin ningún problema gracias a la obtención del PIN.

5.2.2. Proceso de identificación de skimming

Se puede desarrollar el proceso de identificación de si se está realizando skimming a través de dos pasos.

Como primer paso, se encuentra la confirmación de si realmente existió fraude por falsificación. Esto se puede dar por dos motivos. Por un lado porque el tarjetahabiente realiza una reclamación ante la institución emisora o ante el procesador emisor como consecuencia que visualiza en su estado de cuenta cargos por transacciones que desconoce. Por otro lado también, puede ser la misma institución financiera quien identifica una transacción sospechosa y se comunica con el cliente para confirmar si la misma transacción fue realizada por él mismo y descartar así la presunción de que la misma sea sospechosa.

Ante esta situación, se debe determinar si el tarjetahabiente tiene en su poder la tarjeta de crédito lo cual abre dos posibilidades, que la tenga en su poder o que no la tenga. En caso de no tenerla, se puede confirmar entonces que la persona perdió o le robaron la tarjeta lo que demuestra claramente que la transacción puede haber sido verdadera pero no realizada por su titular, claro está. Ante la posibilidad que el tarjetahabiente tenga en su poder la tarjeta, es que se da el segundo paso de este proceso. Como la tarjeta no ha sido robada ni la misma fue perdida por parte del titular, se debe evaluar dicha transacción como sospechosa. Es en este momento que la institución financiera debe analizar dos situaciones: en primer lugar si la transacción recibida se realizó con lectura de banda magnética y en segundo lugar si el CVV o el CVC2, el cual fue validado en la transacción, fue transmitido en el proceso de autorización. Si para ambos casos la respuesta es **SÍ**, entonces la institución concluye que la tarjeta de crédito ha sido falsificada por skimming. Si en cambio la respuesta es **NO**, entonces quiere decir que existieron otros tipos de fraude, por ejemplo e-commerce, pero no skimming. Todo esto teniendo en cuenta siempre que ante la consulta por la transacción sospechosa el tarjetahabiente no reconoce la misma. También se supone para este caso que no hay autofraude, lo cual se investigará cuando se analicen las transacciones.

5.2.3. Tipos de falsificaciones

A nivel internacional, cuando se habla de fraude por lectura de banda o skimming, los sellos identifican diferentes tipos de falsificaciones. Los mismos dependen de cómo se realizó la falsificación, tanto sea por cómo se fabricó el plástico, por la apariencia del mismo, o hasta incluso por la tecnología empleada, entre otras.

- **Plásticos blancos:** Cualquier plástico embozado que cuenta con información válida.
- **Tarjetas adulteradas:** Plásticos genuinos con información embozada que ha sido alterado o dañado.
- **Tarjeta falsificada:** Tarjeta fabricada sobre materia prima para crear tarjetas/plásticos con características de seguridad falsas.
- **Banda magnética adulterada:** Banda magnética codificada con información del tarjetahabiente que puede o no puede coincidir con la información de la tarjeta.

Así entonces, un plástico blanco, podrá ser utilizado siempre y cuando exista complicidad de parte del comercio donde se realiza la transacción, ya que se debe entender que este tipo de tarjetas no cuentan con ningún logo, ni tampoco nombre ni fecha de vencimiento; es el

plástico de color blanco con su respectiva banda magnética. El empleado del comercio no debería aceptar este tipo de tarjetas porque es notoria su falsedad, salvo en los casos de autoservicio (como son los casos de estaciones de servicio o incluso supermercados) donde es el mismo usuario (en este caso el propio delincuente) quien realiza el pago con la tarjeta ante la máquina correspondiente sin que exista atención por parte de un empleado del comercio en cuestión. Este tipo de plásticos podrá ser utilizado también para otros tipos de transacciones como por ejemplo e-commerce o venta telefónica en las cuales no es necesario exhibir el plástico, pero resulta contradictorio que el defraudador utilice el mismo en transacciones en las cuales, en primer lugar no necesita de éste, y en segundo lugar también debe contar con otra información que no es posible obtener a través de la copia de la banda como es el caso de código de seguridad (código de tres números que se encuentra al dorso de la tarjeta de crédito).

Una tarjeta adulterada se diferencia de una tarjeta falsificada por el simple hecho de que la primera es un plástico genuino de determinado sello embozado por un ente emisor legítimo que como bien marca la palabra ha sufrido algún tipo de adulteración, mientras que en el segundo caso el plástico no es embozado por ningún agente emisor sino que es realizado por los defraudadores por lo que todas las características de seguridad que posee son falsas.

Que una banda magnética adulterada con información del tarjetahabiente puede coincidir o no con la información de la tarjeta de crédito, significa que en todos los casos de adulteración de banda magnética, los datos del titular de ésta no coinciden con los del plástico. O sea que el plástico utilizado, genuino siempre, es de un tarjetahabiente en particular al cual se le cargan los datos de la banda magnética de otro tarjetahabiente que nada tiene que ver con el primero.

5.3. Fraude por venta a distancia

Esta forma de fraude fue categorizada en el capítulo uno como fraude sin tarjeta presente, que implica que el defraudador se apodera ilegalmente de un número de cuenta para realizar transacciones a nombre del tarjetahabiente.

A diferencia del fraude por lectura de banda, el fraude por venta a distancia es el que se da sin presencia física de una tarjeta de crédito. Erróneamente se le suele llamar fraude por Internet o “e-commerce” debido a que éste es el tipo de fraude por venta a distancia más común, existiendo también por otra parte el de venta telefónica. Fraude por venta telefónica es aquel en el que el defraudador realizará una compra por teléfono, y por esta misma vía le pasará al comercio los datos de su tarjeta de crédito, como ser el número y la fecha de vencimiento. Puede ser con o sin complicidad del comercio, e incluso la venta telefónica

puede ser una forma para el hurto de datos. El fraude por venta telefónica es casi inmaterial, como así lo demuestra el nivel de fraude por tipo en la región el cual se desarrolla en el capítulo seis de este trabajo, lo cual se debe a la tendencia a reducir al mínimo la solicitud de autorizaciones mediante esta vía. A la fecha, no se ha eliminado esta forma de solicitar autorizaciones ya que funciona como contingencia o soporte en casos de que el comercio se queda sin el funcionamiento del respectivo POS por ejemplo.

Es importante diferenciar los dos tipos de fraude ya que por ejemplo el fraude por venta a distancia existe porque el tarjetahabiente, tanto sea por comprar por Internet (e-commerce) o mediante venta telefónica, revela sus datos a algún individuo quien será el encargado de realizar el fraude a posteriori. En este caso no hay lectura de banda, no hay falsificación de tarjeta por el hecho de que no se cuenta con los datos suficientes como para falsificarla. Quien obtiene los datos solamente podrá utilizar los mismos para cometer fraude por ésta vía, o sea solamente por e-commerce o venta telefónica. Dado que la mayoría de las transacciones de venta a distancia y la concreción de los fraudes son por e-commerce (Internet), es que nos referiremos a e-commerce cuando hablemos de fraudes.

De la manera inversa, o sea una vez clonada la banda magnética que se realice fraude tanto por e-commerce como por venta telefónica es difícil que suceda, aunque puede existir. Para que esto ocurra, además de copiar la banda magnética, se deberá tomar nota de todos los datos de la tarjeta de crédito que son solicitados por e-commerce, o sea número de tarjeta, fecha de vencimiento y código de seguridad (los tres números ubicados en la parte trasera del plástico). La razón de tomar nota de estos datos se da porque toda la información que contiene la banda magnética se encuentra encriptada de tal forma que ante la impresión del respectivo “voucher” de compra, solamente aparecen visibles los últimos cuatro números de la tarjeta, siendo imposible visualizar el resto. En definitiva, la información está dentro de la banda magnética pero la misma no es visible. El tema de la encriptación es un mecanismo más de control de fraudes empleado para evitar el fraude cruzado. Para el caso contrario, quien realiza fraude por e-commerce o venta telefónica, los datos son obtenidos únicamente para realizar fraude por esa vía, ya que para realizarlo por lectura de banda se necesitarán los números del CVC2 o CVV, según sea el sello de la tarjeta, que únicamente se encuentran dentro de la banda y en ningún otro lugar.

El fraude de mayor crecimiento es el de e-commerce pero el más perjudicial para cada procesador es el de lectura de banda. Esto se da porque el fraude de lectura de banda se da con tarjeta presente. Para el caso de la compra de un bien quien la realiza se hace acreedor de la mercadería en el mismo instante (distinto podría ser la contratación de un servicio), y esto hace que sea muy difícil poder detener la transacción y evitar que quien realizó el fraude no se retire del comercio con la mercadería que compró. Por el contrario, en el caso de e-commerce, generalmente existe un servicio de delivery que entrega el bien adquirido a

quien lo compra y ante la eventualidad de detectarse el fraude, tanto los sistemas de alerta como la velocidad de los analistas, hacen que puedan contactarse rápidamente con el comercio para que éste cancele la entrega de la mercadería. Además, por más que la transacción haya sido aprobada, existe la posibilidad de que la misma sea anulada, tanto si la transacción fuera realizada dentro de Uruguay como si la misma fuera realizada fuera de nuestro país, claro que para aquellas realizadas en el exterior es más complejo pero no implica que no puedan realizarse. Por esta razón es que puede concluirse que para los procesadores es preferible el fraude de e-commerce al de lectura de banda. De todas maneras, dentro de e-commerce, el fraude se puede desarrollar de dos maneras; por un lado en la que a pesar de que le roban los datos al usuario para realizar el fraude, el comercio hace entrega de la mercadería comprada; y por otro lado en la que la entrega de la misma nunca se efectiviza. El primer caso es el que menos se sospecha porque la compra fue normal y el objeto comprado fue recibido por el usuario pero con el correr del tiempo empiezan a aparecer en el estado de cuenta de su tarjeta de crédito cargos que no le corresponden. De todas formas, ambos casos son considerados fraude, aunque no se considera como tal cualquier problema de entrega de la mercadería comprada (esto sería un tema de fraude comercial); el fraude de tarjeta es el generado por el hurto de datos.

Como se observara en el capitulo anterior, tanto sea fraude por lectura de banda como por e-commerce, el mismo es contrarrestado de la misma manera, o sea creando reglas efectivas que en algunas ocasiones son las mismas para ambos casos y en otras oportunidades son exclusivas tanto para e-commerce como para lectura de banda. Un ejemplo es darle la función al sistema que informe sobre venta a distancia de cualquier tarjeta que haya operado en determinado rubro de cierto país. Según sea el caso, puede dar alerta solamente para luego monitorear los cargos de la misma, o inclusive hasta cancelar la transacción con el bloqueo de la tarjeta.

En todos los casos, para que exista fraude por e-commerce, tiene que existir previamente robo de datos (número de tarjeta, fecha de vencimiento, código de seguridad). El robo de datos puede darse de varias maneras. Las más conocidas son:

- **“Phishing”:** robo de datos mediante la suplantación de identidad vía correos electrónicos fraudulentos (el defraudador se hace pasar por algún agente con el cual el tarjetahabiente opera para hurtarle los datos).

- **“Ingeniería Social”:** robo de datos mediante llamadas telefónicas fraudulentas o mensajes de texto para hurtar datos.

- **Robo de datos a comercios:** se da porque los mismos no guardan de manera segura toda la información respecto a la base de datos de las tarjetas de crédito que operaron con ellos.

- **Robo de datos al tarjetahabiente:** ya sea con o sin tarjeta presente, en algún momento un defraudador pudo hacerse de los datos necesarios de la tarjeta del usuario.

Suele encontrarse en las páginas web de las instituciones financieras, información y recomendaciones referidas al hurto de datos. Como se entiende que la misma es de gran utilidad para el tarjetahabiente, se agrega el Anexo II al final de este trabajo.

La recomendación que se le da al usuario para evitar casos de fraude por e-commerce es ingresar a páginas seguras o en el caso de comprar por Internet en un comercio no conocido, googlear el nombre del mismo. Ingresar a los "blogs" puede dar indicios del historial y de las prácticas del comercio en cuestión, a través de los comentarios que los clientes que han interactuado con éstos, puedan haber plasmado en los mismos. A su vez, debe existir un nivel de seguridad en el sitio que se conoce por las siglas "SSL" (Secure Socket Layer). El SSL es un sistema de seguridad que encripta la información enviada por el usuario, de tal manera que ésta sólo puede ser descifrada por el ordenador que recibe la información y posee la clave secreta para hacerlo. ¿Qué es lo que protege el sistema SSL? Principalmente el número de tarjeta de crédito, para evitar que caiga en manos de personas indebidas y también los datos confidenciales del comprador, para que no se almacenen en ninguna base de datos comercial. Una de las formas de saber si el sitio tiene o no este sistema de seguridad implementado, es por la certificación que usualmente está visible en la página, aún así ésta puede ser falsificada, por ello el método más confiable es revisar la "URL" (Uniform Resource Locator) en la barra de direcciones del navegador donde se apreciará lo siguiente **"https://"**, lo cual indica que es una página segura. En el Anexo III, se muestra una imagen de un sitio de compra segura.

Dentro de este punto se podrán diferenciar dos tipos de comercio. Por un lado aquellos que brindan máxima seguridad a los clientes a la hora de manejar toda la información y datos personales de cada uno, que son aquellos que cumplen con normas PCI (Payment Card Industry); y por otro lado aquellos comercios que no guardan la información de forma segura y que por lo tanto no cumplen con normas PCI. Cumplir con normas PCI significa cumplir con normas "standard". La información a la que se refiere es la relativa a los datos de aquellos clientes que operan con estos comercios. La complejidad está dada porque internacionalmente no se conoce qué comercios guardan toda la información de sus clientes de manera segura y cuáles no lo hacen. De todas maneras, firmas importantes como Best Buy, Apple, Amazon, entre otros, sí lo hacen, por lo que podemos estimar si cumplen con normas PCI o no dependiendo de la magnitud y de la importancia que los mismos tienen. No cumplir con normas PCI, además de hacer al comercio vulnerable al robo de datos, tendrá implicancia para el mismo a la hora de asignar responsabilidades ante transacciones desconocidas por el tarjetahabiente.

Dado que el tema de normas PCI es de particular interés para este trabajo monográfico, se desarrollará sobre las mismas en el Anexo IV.

En la actualidad no hay comercios en el Uruguay que cumplan con normas PCI, básicamente por temas económicos ya que no resulta redituable. Cumplir con las normas requiere de auditorías anuales las cuales pueden representar erogaciones importantes de dinero y hasta hoy a ningún comercio en nuestro país la ecuación económica respecto a cumplir normas PCI le ha sido rentable.

Es aquí que aparece nuevamente el rol del procesador adquirente quien sí debe cumplir estas normas (como es el caso de First Data por ejemplo) para poder guardar de forma segura los datos de todos los tarjetahabientes que compran en comercios adheridos. Al comprar por e-commerce, a la hora de cargar los datos de la tarjeta de crédito, al usuario se le despliega una pantalla en su computadora a través de la cual éste cargará sus datos. El usuario no se da cuenta, pero dicha página no es la del comercio en cuestión sino que es la del procesador adquirente, quien interviene en el momento en que los datos del titular de la tarjeta de crédito son requeridos. La página del procesador adquirente mantiene las mismas características que la página del comercio (mantiene el logo del mismo, el mismo formato, colores, etc.) pero la información que el cliente carga en ella no quede registrada en la página del comercio sino que quede registrada en la página del respectivo procesador. Tanto First Data como Visanet, al cumplir ambos con las normas PCI, brindan el servicio a comercios para que operen por internet utilizando las páginas de estos que guardarán la información de manera segura. En el Anexo V se podrán visualizar ejemplos de compra en dos comercios distintos de plaza que utilizan los servicios de Visanet y de First Data respectivamente. En ambos se podrá apreciar el logo del comercio y a su vez el logo del procesador.

Por otra parte existen los comercios que aparentemente sí venden por Internet pero en realidad lo que hacen es solicitar a través de su página web los datos personales al cliente. Éste los carga y el comercio a través de la misma le comunica que a la brevedad se comunicarán con él para autorizar la transacción. Lo que sucede en estos casos es que el comercio en ese momento se comunica con el procesador adquirente para solicitar autorización telefónica de la transacción utilizando los datos de la tarjeta que el cliente cargó en la página web. Por lo tanto estos casos no son de compra por Internet sino que se asemejan a los de venta telefónica porque las autorizaciones en todos estos casos son manuales. Considerando que los datos son cargados en la página web del comercio de forma no segura (no cumple normas PCI), puede ser riesgoso para el tarjetahabiente que está realizando la transacción. Este tipo de transacciones no están permitidas para los comercios por lo que quienes las realicen están realizando actividades indebidas, ya que para realizar ventas por internet, como fuera visto anteriormente, deben ser sitios que

guarden de manera segura los datos, y evidentemente estos sitios no lo son. El problema para el procesador adquirente es que no identifica que estos comercios están simulando una operación por Internet debido a que para ellos, al momento de dar la autorización, les aparece como una venta telefónica. El tarjetahabiente puede darse cuenta que no está realizando una compra por Internet sino que en realidad lo está haciendo vía venta telefónica (el comercio realiza una transacción manual), porque la autorización de la transacción no será automática sino que vendrá después a través de un llamado telefónico o a través de un mail, pero nunca vendrá "on line" a través de la página por la cual se está realizando la compra. Esto conlleva los riesgos mencionados anteriormente de que el comercio se hace de los datos del usuario para luego digitar manualmente la autorización de la transacción. Después estará en el comercio la forma en que utiliza los datos, o sea si los utiliza con buenas o malas intenciones.

Otro mecanismo que existe para realizar transacciones por Internet es mediante la participación de un tercero que oficia de intermediador entre quien compra y quien vende. Una de las funciones que cumplen es la de recibir el pago del cliente con tarjeta de crédito el cual acreditará la cuenta del vendedor. Por ejemplo, éste es un servicio que se utiliza mediante compras a través de la página web de la empresa eBay. El vendedor utiliza la página para ofrecer su producto y para habilitar el pago con tarjeta de crédito al comprador, quien utiliza a "PayPal". Esta es una empresa que ofrece el servicio de intermediación en el pago, en el cual el cliente le pagará a ésta (PayPal) con tarjeta de crédito y a su vez PayPal le depositará en la cuenta del vendedor el dinero correspondiente. Como dicha empresa cumple con normas de compra segura, habilita este sistema de compra – venta por Internet.

Para cualquier tipo de transacción vía Internet, siempre habrá que fijarse en el Certificado Digital, el cual se encarga de verificar que el sitio que se visita es el original y no una copia de éste.

El Certificado de Seguridad identifica al titular de la página como un sitio seguro lo cual no quiere decir que cumpla con normas PCI; son dos conceptos distintos. El usuario puede estar seguro que está ingresando a la página web del comercio y no a una página fraudulenta de características similares. Por ejemplo, una persona recibe un mail con una oferta para comprar vía Internet determinado producto con un veinte por ciento de descuento en determinado comercio. Como el usuario se encuentra suscripto al mismo, no sospecha de que el mail es fraudulento y accede al comercio a través del link que aparece en el mencionado mail. Este link lo lleva a una página fraudulenta de similares características a la del comercio pero que no es tal. El usuario no se preocupa si cumple con normas PCI o no, ya que siempre realizó compras a través de la misma sin problema alguno, además de que el mismo es conocido en plaza. El problema está en no haberse dado cuenta de que el sitio al cual accedió no era el real sino que se trataba de uno fraudulento a

través del cual le estaban robando los datos (Phishing). Más allá de que no debió acceder a la página a través del link, el usuario podría haber detectado que no era la página original del comercio de haber examinado el Certificado de Seguridad. Se detalla en el Anexo VI, al final de este trabajo monográfico, un ejemplo de certificado de seguridad para que pueda ser visualizado por el lector.

Los datos que verifica este certificado son los nombres y apellidos del titular de la empresa, correo electrónico, entre otras cosas. Estos certificados poseen período de vigencia y la autoridad que los certifica. El certificado chequea que el titular del dominio de un sitio web corresponda a los datos del titular y nombre de la empresa.

CES (Comercio Electrónico Seguro) es un sistema para asegurar las transacciones en Internet promovido por Visa Internacional, MasterCard, Microsoft y Netscape, entre otros. El fin principal es dar mayor seguridad tanto al usuario de Internet como a los comercios que venden a través de la Red, al autentificar al comprador como legítimo titular de la tarjeta que está utilizando.

En la práctica, al pagar con una tarjeta Visa o MasterCard "securizada", se le solicitará, además del número, fecha de caducidad y el código de seguridad, una clave personal de uso exclusivo para compras por Internet que le identifica, de manera inequívoca, como su propietario. De esta forma, nadie podrá hacer una compra en Internet si desconoce dicha clave. Podrá distinguir si está activado el protocolo de Comercio Electrónico Seguro por los logos de Visa ***"Verified by Visa"*** y de MasterCard ***"MasterCard Secure Code"***.

Este es un servicio que prestan los sellos que sirve para proporcionar mayor seguridad en las compras ya que obliga a la autorización de una contraseña al momento de realizar la transacción. El es opcional, tanto para el tarjetahabiente como para el comercio, es decir que para que funcione este mecanismo de seguridad ambos deberían tener el servicio contratado. Pierde eficacia si la mayor parte del sistema (comercios y tarjetahabientes) no se encuentran adheridos al servicio[14].

[14] A través de este sitio: http://www.visanet.com.uy/verified_faq.aspx#01, se podrá encontrar más información respecto a uno de estos servicios.

5.4. Otros Tipos de Fraude

Los dos tipos de fraude mencionados anteriormente son los que tienen mayor consideración por parte de las procesadoras por temas de magnitud, no solamente en términos de cantidad sino también en lo que respecta a la cuantía, además de las posibles consecuencias que puede traer aparejado.

Además de ésto, existen otros tipos de fraude que trataremos a continuación, alguno de los cuales adquieren una importancia relativa en la región. En lo que respecta a Uruguay, si bien nuestro país no está alejado de lo que ocurre en ésta, el fraude con tarjeta de crédito no es material. No obstante, igual se mantiene un monitoreo constante de la situación, ya que por lo pequeño que es el mercado uruguayo, de concretarse algún fraude de magnitud cambiaría de manera significativa los guarismos de éste. Esto se verá con más detalle al analizar las estadísticas de fraude en Uruguay y la región en el capítulo seis de este trabajo.

Así como el fraude por lectura de banda y venta a distancia se pueden identificar otros tipos como: solicitud fraudulenta, suplantación de identidad, auto fraude, robo o hurto de tarjeta de crédito.

Los tipos de fraude están relacionados al contexto socio económico del país en el cual se desarrollan; ante situaciones de crecimiento económico, las instituciones financieras realizan campañas masivas de tarjetas de crédito y esto trae un crecimiento de los mismos.

5.4.1. Solicitud fraudulenta

Hoy en día viene tomando fuerza tanto en nuestro país como también en la región, el fraude categorizado como solicitud fraudulenta, el cual se manifiesta como ya se comentara en el primer capítulo de este trabajo, cuando la entidad emisora confirma que una transacción efectuada en una determinada cuenta es fraudulenta como resultado de una reclamación del tarjetahabiente a los efectos de que nunca solicitó la tarjeta, o cuando el emisor confirma que la información dada en la solicitud fue falsificada.

El mismo se puede manifestar de varias formas, siendo las más comunes las que se detallan a continuación:

i) El cliente falsifica documentación, por ejemplo presentando ante la institución financiera recibos de ingresos que no son verdaderos o de empresas que no existen; los datos brindados distan de ser reales.

ii) Otras veces el cliente se hace pasar por otra persona (muchas veces toma la personalidad de una persona fallecida), presentando por lo tanto documentación falsificada a la entidad financiera.

iii) Existen otros casos, donde hay organizaciones que se dedican a este tipo de fraude, las cuales mediante una suma de dinero, logran convencer a un indigente de presentarse con su cédula de identidad ante la institución financiera. Junto con la cédula, presentará otra documentación como ser comprobantes de ingresos o de domicilio, entre otros, los cuales también serán falsos. Se entiende que la identidad de una persona no está compuesta solamente por el nombre sino también por aquellos datos que la identifican; en este caso se está falsificando el domicilio, los ingresos, el lugar de trabajo, entre otros. Como probablemente nunca solicitó una tarjeta de crédito, esta persona, estará completamente limpia respecto a los "bureau de crédito negativos" y accederá sin inconvenientes al crédito solicitado.

Incluso en este tipo de fraude, los delincuentes a veces hasta le generan un perfil al usuario fraudulento. Es decir que utilizan la tarjeta y realizan pagos por la misma (pueden ser los pagos mínimos o incluso pagos totales) de manera de crear un perfil de usuario y al tiempo dejan de pagar los estados de cuenta, cuando el fraude ya lo concretaron por importes mayores. De esta forma, al generar un perfil de usuario, buscan evadir las reglas de alerta. Es muy importante en este punto el estudio del historial del tarjetahabiente para otorgar la tarjeta, fijar límites de crédito, así como asignar algunas reglas de alerta específicas. El punto crítico en este caso será la solicitud y el posterior estudio de toda la documentación que identifica al tarjetahabiente.

5.4.2. Suplantación de identidad

El fraude por falsificación o suplantación de identidad implica obtener información acerca de la identidad de otra persona sin su consentimiento, con el propósito de hacerse pasar por ella y así cometer fraude.

El defraudador utiliza diversas técnicas para obtener los datos necesarios como para suplantar la identidad del tarjetahabiente, como puede ser hurgar la basura, robar correspondencia, acceder de manera ilícita a base de datos del mismo.

El Phishing o estafa electrónica (vía Internet) también puede ser utilizado por el defraudador para recabar información financiera delicada que puede utilizar en su beneficio para robarle la identidad al tarjetahabiente. Si bien Phishing a nuestro entender está más

vinculado a la concreción de fraude por e-commerce, también puede ser considerado para la obtención de datos para suplantar identidad.

Con esta información, el defraudador se hace pasar por el tarjetahabiente. No le roba la identidad, ya que el tarjetahabiente era usuario de la tarjeta con anterioridad, siendo ésta la principal diferencia con el tipo de fraude anterior. Una de las formas a través de las cuales se lleva a cabo este fraude es mediante la denuncia de la tarjeta como robada o perdida, la cual es realizada por el defraudador quien ya conocía de antemano los datos del tarjetahabiente. La institución financiera reimprime el plástico ante la denuncia y lo envía al domicilio del tarjetahabiente. El defraudador estará atento a interceptar al courier cuando hace la entrega para hacerse pasar por el tarjetahabiente y así obtener la tarjeta de crédito. En ciertas ocasiones incluso, el defraudador previamente a la denuncia, cambia el domicilio de entrega de la misma.

A veces este tipo de fraude se da sin la denuncia, apoderándose de una tarjeta que se entrega por renovación o por ser una nueva tarjeta promocional que le llega al tarjetahabiente o incluso también ante el caso de un adicional. Sin importar la forma, al apoderarse de la misma el defraudador, consumirá como si fuera el tarjetahabiente, quien se dará cuenta de la concreción del fraude de diversas maneras. Para el caso de remplazo de identidad mediante denuncia de pérdida o hurto, el tarjetahabiente tomará conocimiento de tal situación al momento de tratar de utilizar la tarjeta para realizar alguna transacción ya que no podrá hacerlo debido a que la tarjeta de crédito estará bloqueada, o incluso cuando le llegué el estado de cuenta y verifique que se le cargaron transacciones que no realizó. Para el caso de solicitud de un adicional, se dará cuenta también por la aparición de gastos en el estado de cuenta que no realizó, o simplemente porque demora la entrega de la misma y al consultar a la institución financiera, ésta le confirme que la misma ya fue entregada.

Un ejemplo de este tipo de fraude fue el que se realizara en nuestro país hace unos años atrás en el cual se denunciaron tarjetas de origen brasileño como robadas o perdidas. Como existía conocimiento de parte de los defraudadores que los titulares de las mismas se encontraban veraneando en nuestro territorio, los mismos solicitaban al procesador emisor en Brasil que las enviara a Uruguay para así hacerse de la tarjeta. Además, los defraudadores contaban con comercios “golondrina” o ficticios, a través de los cuales utilizaban las tarjetas de crédito para así realizar los gastos y recibir el efectivo. Una vez finalizada la temporada, se fugaban del país.

En este tipo de fraude se encuentra como punto crítico la identificación positiva por parte del tarjetahabiente al hacer la denuncia telefónica al procesador. Una buena identificación positiva debería detectar, por más que el defraudador conozca los datos del tarjetahabiente, que no es el titular de la tarjeta quien se está comunicando.

Otro punto crítico es la capacitación del empleado que realiza el courier. El hecho de que no cumpla con el protocolo de entrega de la tarjeta puede provocar que el defraudador se apodere del plástico haciéndose pasar por el tarjetahabiente.

Para el último ejemplo citado podemos considerar como punto crítico también el estudio por parte del procesador adquirente del comercio adherido, buscando evitar los comercios "golondrina", con fines ajenos a los comerciales.

5.4.3. Auto fraude

La característica principal de este tipo de fraude es la participación del propio tarjetahabiente, concretándose cuando el mismo desconoce compras que aparecieron en su estado de cuenta, las cuales fueron realizadas por él o contaron con su aval.

La participación del tarjetahabiente como defraudador se puede dar de manera directa o indirecta, pero siempre con conocimiento y consentimiento para la concreción del fraude.

La participación directa se da cuando es el propio tarjetahabiente quien utiliza la tarjeta para una transacción y luego desconoce el cargo, aduciendo que él no la realizó. Por ejemplo, puede realizar una compra por e-commerce, y luego denunciar que él no la hizo. Otro ejemplo puede ser denunciar la tarjeta como robada, y desconocer compras realizadas anteriormente aprovechándose de la cobertura previa a la denuncia que otorgan algunos sellos.

La participación indirecta puede ser prestar su tarjeta para que sea clonada o para que sea usada por un tercero, y así luego desconocer las compras realizadas. No es el propio tarjetahabiente quien realiza la transacción, pero sí participa dando el consentimiento.

Siguiendo un criterio de materialidad, el procesador solicitará toda la información respectiva para investigar estos fraudes, como puede ser obtener la dirección IP desde donde la compra fuera realizada, dirección de envío, o hasta incluso videos de seguridad en caso de ser una compra con tarjeta presente.

Como se mencionara anteriormente, se realizará siguiendo un criterio de materialidad ya que no existirán investigaciones por compras de importes menores. Pero otra herramienta de investigación que utilizará el investigador será el historial del propio tarjetahabiente, ya que si es recurrente que le suceda ésto, generará antecedentes que provocarán que no se le otorguen más tarjetas o se considere que no toma las debidas precauciones para el uso de la misma y por ello no se le devolverán los importes reclamados.

5.4.4. Fraude por hurto o extravío

Este fraude se da cuando el tarjetahabiente deja de tener el plástico en su poder, y éste pasa a manos del defraudador quien lo utiliza para realizar transacciones. La diferencia entre hurto y extravío consiste en que el primero implica una denuncia de inexistencia del plástico, y el segundo no; en el segundo el tarjetahabiente no se da cuenta del faltante de la tarjeta hasta que aparecen los cargos en su estado de cuenta.

El mismo se diferencia del de suplantación de identidad, en el hecho de que ante la denuncia por hurto por parte del defraudador, la institución financiera emitirá un nuevo plástico con una numeración diferente. Con este nuevo plástico el defraudador podrá de alguna manera "tomar la identidad del titular" ya que éste último no tendrá conocimiento de la existencia del mencionado plástico hasta tanto no intente utilizar la tarjeta "vieja" que tiene en su poder y le sea rechazada, o hasta tanto aparezcan cargos que desconozca en el estado de cuenta justamente porque le están utilizando una tarjeta nueva, hasta el momento desconocida por parte del titular. En el hurto entonces, quien realiza el fraude se apodera de un plástico que es propiedad de un tercero (titular).

Todos estos tipos de fraude tienen características similares, como la de que crecen en momentos de campañas masivas; tienen menor grado de elaboración y preparación que los de lectura de banda y venta a distancia; generalmente son de consumo masivo, es decir que el defraudador tratará de utilizar lo más rápido posible la tarjeta de crédito; la mayoría de las veces son de rápida detección; y habitualmente si se analiza individualmente cada fraude, no son de importes significativos. Generalmente se realizan dentro del país con tarjetas locales y los defraudadores son residentes, lo que agiliza aún más la detección y la prevención, ya que al ser el nuestro un país pequeño se cuenta con una mayor colaboración policial y se identifica rápidamente a los delincuentes. Esto último no sería aplicable para el fraude por hurto, en especial para el que se realiza fuera del país, el cual es un fraude de difícil detección a través de reglas de alerta ya que el tarjetahabiente se encuentra en el mismo lugar donde se realiza el consumo y habrá que esperar a que, o bien se denuncie la tarjeta, o se detecte por las mencionadas reglas. Además, generalmente son de muy corto plazo, salvo ciertas ocasiones el de falsificación de identidad como ya fuera analizado anteriormente.

Todas estas características son similares si son comparadas con los fraudes por lectura de banda o e-commerce. Si se comparan entre sí, encontraremos diferencias ya que algunas serán más elaboradas que otras, de menor o mayor alcance y duración. A modo de ejemplo y como fuera analizado, tanto el fraude por suplantación de identidad como el de falsificación de identidad tienen cierta preparación y elaboración, muchas veces hay una

organización delictiva detrás de ellos, a diferencia del auto fraude con mínima elaboración o el fraude por hurto. Pero todos son de escasa elaboración si los comparamos con los fraudes de e-commerce y lectura de banda, los cuales generalmente tienen atrás organizaciones delictivas internacionales, con toda una estructura armada y una planificación elaborada y que en muchas ocasiones se dedican a varias actividades delictivas además del fraude con tarjeta de crédito. Son estos fraudes los que más daño monetario hacen, y así lo demuestran las estadísticas, razón por la cual los procesadores ponen especial atención a los mismos para su detección. Para evitar no ser detectados, estos tipos de fraude poseen una mayor planificación evasiva, con una dinámica constante como fuera visto en el tema del diseño de las reglas de alerta.

Una vez detectado el fraude y bloqueada la tarjeta, el sistema y los analistas tratarán de identificar si encuentran algún punto en común con otra tarjeta que haya sido fraudulenta, para de esta forma detectar el punto de compromiso. Esto le será de utilidad para identificar que otras tarjetas actualmente activas pasaron por ese punto de compromiso siendo entonces calificadas como tarjetas “con riesgo”. Una vez identificada, el procesador según el riesgo de esa tarjeta, determinará si corresponde un bloqueo y posterior reimpresión o simplemente un monitoreo más preciso de la misma a través de reglas de alerta. Como también fuera aclarado, quien cuenta con mayores posibilidades para detectar puntos de compromiso es el procesador adquirente, porque es el que visualiza a los comercios. El emisor también puede detectarlos, pero cuenta con menos información en lo que a comercios respecta.

Para el caso de hurto de datos en el proceso de entrega, quien contará con mayor posibilidad para detectar ese punto de compromiso será el procesador emisor, porque estará vinculado a la entrega de la tarjeta emitida por éste y no al comercio objeto de la transacción.

El punto de compromiso más difícil de detectar existe cuando no hay utilización de la tarjeta en el lugar donde se clona la banda o se roban los datos y tampoco existe Phishing. Esto sucede en comercios tales como centros de buceo o spa, donde el tarjetahabiente suele pagar contado y dejar la tarjeta fuera de su alcance por un tiempo prolongado mientras recibe el servicio. Es en ese momento donde el defraudador se aprovecha del descuido de las pertenencias por parte del tarjetahabiente clonando la tarjeta o robando los datos, sin dejar rastro alguno como para que el usuario tome conocimiento de tal situación. No se deja rastro para que el sistema no pueda identificar el punto de compromiso según los desconocimientos por fraude recibidos; las tarjetas no fueron utilizadas en los mismos comercios, quizás tampoco en la misma ciudad, por lo que no existe un patrón para poder unir el vínculo entre ellas y es ahí donde se hace difícil al procesador poder identificar el punto de compromiso. La forma de identificarlos será mediante consultas por parte de los

analistas a cada uno de los usuarios involucrados, de algunos usos y costumbres, de actividades realizadas y lugares visitados por el tarjetahabiente.

Así como el tarjetahabiente con el uso de la tarjeta se genera un perfil de usuario, lo mismo sucede con el defraudador y la secuencia de fraudes cometidos por éste por lo que también se genera un perfil de delito, y esto puede servir también para identificarlo y ubicarlo.

Uno de los fraudes más temidos es el hurto de datos a un procesador, ya que los defraudadores contarían con los datos de miles de tarjetas de crédito. Las opciones en este caso son, o reimprimir los miles de plásticos (con el costo que implicaría por la reimpresión y por el no uso del mismo durante el periodo en que se vuelve a imprimir), o como otra opción, establecer reglas de alerta especiales para estas tarjetas riesgosas por el hecho que pueden haber recibido hurto de datos. Esto le sucedió a uno de los procesadores más importantes de Estados Unidos, el cual decidió por no reimprimir los plásticos sino aplicar reglas de alerta especialmente diseñadas. En este punto el efecto fue positivo, ya que el hurto de datos implicó fraudes por un importe inmaterial. El problema fue que el hecho generó una desconfianza tal en el mercado, que provocó una baja muy fuerte del valor de sus acciones por lo que la empresa terminó quebrando (le robaron datos de más de doce millones de tarjetas mientras que sufrió fraude por poco más de ocho mil quinientos dólares).

5.5. Contracargo

Es el desconocimiento por parte del usuario de una transacción en particular, sin implicar que la misma tenga que ser fraudulenta ya que se puede dar el caso de que el mismo cargo aparezca duplicado en el estado de cuenta como consecuencia de un simple error del comercio. El desconocimiento no solamente implica no reconocer determinado cargo imputado en el estado de cuenta, sino que como bien detallaremos a continuación puede ser una diferencia en el importe o bien que la mercadería o servicio contratado no fuera entregado al usuario. Como consecuencia del desconocimiento de dicha transacción, la misma tratará de ser recuperada.

El contracargo lo realiza el usuario y el mismo debe ser dirigido hacia la institución financiera con la cual el tarjetahabiente solicitó la tarjeta de crédito. Existen dos formularios de reclamo, los cuales se detallan en el Anexo VII de este trabajo, los cuales el usuario deberá completar con sus datos. Los mismos son: número de tarjeta de crédito, institución financiera emisora de la tarjeta, nombre del tarjetahabiente, nombre del comercio con el cual existe la diferencia, fecha e importe de la transacción desconocida y el motivo por el cual se realiza el reclamo. Justamente el tema del motivo es fundamental ya

que se pueden presentar dos situaciones bien diferenciadas que es necesario precisar. Por un lado la tarjeta de crédito puede haber sido robada o extraviada por parte del usuario, por lo que el mismo debe declarar la fecha en la cual extravió la tarjeta o la misma le fue sustraída ya que la transacción reclamada deberá ser posterior, sino el reclamo no tendrá efecto. Por otro lado, puede existir el caso que el tarjetahabiente nunca perdió su tarjeta ni le fue robada la misma, entonces entramos dentro del concepto que definimos en más de una oportunidad como "tarjeta presente" ya que la misma siempre estuve en poder de su titular. Ante esta circunstancia el tarjetahabiente deberá declarar que la transacción no fue realizada por él; que la tarjeta de crédito siempre estuvo en su poder; y que no autorizó ni participó de la transacción en disputa. De no declarar las tres opciones mencionadas anteriormente, además que la tarjeta del mismo debe haber sido bloqueada por parte del procesador emisor con motivo "fraude", el reclamo no será procesado.

Dentro del motivo, se debe declarar también si el desconocimiento se da como consecuencia de una diferencia en el procesamiento de la transacción o si por el contrario se da por incumplimiento del servicio y acá detallamos posibles ejemplos de casos ante los cuales se realiza un contracargo. Algunos de ellos son:

- El tarjetahabiente no recuerda la transacción y solicita información adicional para identificarla, como por ejemplo un "voucher" con su firma o algún otro elemento que le permita recordar la misma.

- Cargos que aparecen duplicados en el estado de cuenta.

- Importe incorrecto o alterado; en estos casos el tarjetahabiente debe conservar el "voucher" de la compra firmado por el donde detalla que el importe de la transacción no es el mismo que aparece debitado en el estado de cuenta.

- Mercadería o servicio no recibido por parte del tarjetahabiente pero si debitado en el estado de cuenta de la tarjeta de crédito.

- Transacción realizada en un número determinado de cuotas, sin embargo el débito en el estado de cuenta aparece contado; en este caso también es importante que el usuario tenga en su poder el "voucher" de compra para que pueda demostrar que en el mismo se detalla claramente que la compra no fue contado sino en la cantidad de cuotas reclamada.

Los formularios son dos completamente diferentes. Ambos serán completados por el tarjetahabiente, solo que uno será para la institución financiera y el otro es el que irá para el sello ante el reclamo realizado.

Una vez que el mencionado formulario es completado y firmado por el usuario, la institución financiera lo trasladará al procesador emisor, que como bien explicamos en capítulos anteriores, puede ser la misma institución quien procese sus transacciones. Una vez cumplidos estos pasos, comenzará entonces una disputa entre el procesador emisor y el procesador adquirente, disputa en relación a que el adquirente intentará cobrar la transacción en discordia y el emisor se opondrá al pago de la misma por considerar que no fue realizada por el tarjetahabiente que está representando. El procesador emisor entonces, oficiará de interlocutor de la institución financiera y por ende del tarjetahabiente, mientras que el procesador adquirente hará lo mismo para con el comercio responsable de haber realizado el cargo que está desconociendo el cliente. La disputa se puede dar tanto a nivel nacional como a nivel internacional, y es a nivel internacional donde adquiere mayores inconvenientes para el procesador emisor ya que debe enfrentarse con un procesador adquirente generalmente desconocido por el primero. Generalmente el contacto se da de parte del procesador emisor con el procesador adquirente, ya sea local o internacional, y rara vez hay contacto directo entre el procesador emisor y el comercio. Al comercio lo contactará el procesador adquirente.

A nivel de nuestro país, y para el caso de Visa puntualmente, siempre la disputa, sea el caso que sea, será con Visanet Uruguay por lo que es más fácil para ambas partes ya que sea el caso que sea, la relación comercial existe y es frecuente. Siguiendo con el ejemplo de este sello pero a nivel internacional, el procesador emisor se contactará con Visa Internacional para que traslade la disputa con el procesador adquirente del país en cuestión (sería una Visanet de ese país para ejemplificar) quien tendrá que comunicarse con el comercio a través del cual se realizó la transacción. A nivel nacional, es un negocio donde las partes que interactúan en él están en contacto permanentemente, por lo que de una manera u otra, por más que se esté ante una disputa, que exista vínculo entre las mismas facilita este tipo de controversias.

Como se ve, el tema de la documentación exigible es muy importante dentro del contracargo, supuesto que deja de serlo para los casos de compras por Internet en donde no existe documentación que respalde las transacciones. En estos casos existirán otras herramientas que el procesador emisor deberá tener en cuenta a la hora de formular el contracargo. Una de ellas es la confirmación de que el usuario es cliente habitual del comercio referido y que realiza compras con frecuencia en la página web de éste. Otra herramienta es la confirmación que la mercadería fue entregada y para ello el comercio puede adjuntar, en caso de tenerlo, el comprobante que una persona en la dirección detallada firmó la aceptación de la mercadería entregada. En todos los casos en que se espera que la mercadería sea entregada, el usuario debe ingresar los datos de su domicilio para que el pedido le sea entregado. El caso de la **“dirección IP”** es otra herramienta que se puede emplear, claro que es un tema más complejo y requerirá de otros mecanismos de

análisis. Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (del inglés Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP (del inglés Transmission Control Protocol). Para clarificar esto, se trata de un protocolo que proporciona transmisión fiable de paquetes de datos sobre redes, y que proviene de los dos protocolos anteriormente definidos, el "IP" y el "TCP". El TCP/IP es la base de Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PCs, minicomputadoras y computadoras centrales sobre redes. Por lo tanto, al identificar la dirección IP se puede probar que la compra por Internet realmente se realizó de un computador localizado en la dirección en que está domiciliado o no el tarjetahabiente en cuestión, lo cual no es un detalle menor.

En estos casos de disputas, cuando no se logra un entendimiento o un acuerdo entre los, procesadores quien termina resolviendo es el sello internacional. Esto no es necesario muchas veces para contracargos donde adquirente y emisor son de plaza, pero sí es el sello internacional quien termina resolviendo estas controversias a nivel internacional. Según estadísticas brindadas precisamente por la empresa Sistarbanc, gracias al contracargo se puede recuperar aproximadamente el veinte por ciento de los fraudes. Esto significa que en el veinte por ciento de los casos de fraude los bancos recuperan el importe que es motivo de controversia.

5.6. Responsabilidades

Como se mencionara anteriormente, el contracargo surge de un desconocimiento por parte del tarjetahabiente de una transacción. El resultado de dicho proceso, puede terminar en que efectivamente él mismo haya realizado la misma, y en este caso no el proceso iniciado no generará ningún efecto. Por ejemplo se le muestra la compra realizada a través del respectivo voucher y el tarjetahabiente termina reconociendo la misma ya que anteriormente no la recordaba; ésto es algo que sucede habitualmente según fuera informado. Distinto es el caso cuando efectivamente el tarjetahabiente, luego de recopilar la información, sigue desconociendo la misma, por lo cual una vez finalizado el proceso de contracargo, habrá que determinar a quién corresponde responsabilizar por el importe de la transacción desconocida, porque en definitiva alguien se tendrá que hacer cargo del pago.

El tema de la responsabilidad no es un caso menor ya que, como en todo el proceso de la vida útil de una tarjeta de crédito, involucrará tanto al tarjetahabiente, como a la institución financiera emisora, así como también al procesador y comercio respectivo. Esto quiere

decir que nadie queda librado del tema de la responsabilidad ante una transacción en particular.

Ante un contracargo, el sello decidirá quién es responsable por la transacción; si la parte emisora o la parte adquirente. En principio es siempre la parte emisora, por eso se habla de recupero, porque el emisor tratará por medio del contracargo de que la parte adquirente reintegre el importe por esa transacción desconocida, y quien decide si corresponde el mismo o no será el sello.

En líneas generales, se podrá decir que aquellas transacciones desconocidas por fraude con tarjeta presente (por ejemplo lectura de banda) son responsabilidad del banco emisor, mientras que de ser por compras a través de e-commerce, en el caso de que el comercio involucrado no cumpla con normas PCI, son responsabilidad del procesador adquirente. Si el banco emisor terceriza el servicio de procesamiento, no implica que traslade la responsabilidad, y la misma ante el sello seguirá siendo del banco emisor, lo cual no implica que entre el banco y el prestador del servicio de procesamiento emisor acuerden la transferencia de responsabilidad (será un acuerdo entre partes en este caso).

Todo esto que se menciona es en líneas generales, ya que la responsabilidad cambiará radicalmente si el procesador adquirente no cumple su función de controlar a sus comercios adheridos. Esto se medirá por la cantidad de transacciones fraudulentas recibidas; si las mismas están por encima de la media del mercado, una de las consecuencias que puede recibir el procesador es la pérdida ante algunos casos de contracargo.

Al visualizar este análisis desde el punto de vista de las tarjetas de crédito internacionales más importantes (Visa y MasterCard), se distinguen algunas diferencias las cuales es importante remarcar.

MasterCard

Internacionalmente mide el nivel de fraude de un país a través de lo que se conoce como **puntos base**. Un punto base es la diez mil parte de un entero, esto es un dólar de transacción fraudulenta por cada diez mil dólares de transacciones totales, o sea que si existe un fraude de un dólar cada diez mil dólares de transacciones totales, se tiene un punto básico. Se utiliza esta forma de medición porcentual para poder comparar el nivel monetario de transacciones fraudulentas en países con distinto nivel de facturación (como lo pueden ser Uruguay y Brasil por ejemplo).

En el caso de Uruguay, First Data que es el procesador adquirente exclusivo para MasterCard, no puede tener más del promedio de la región en dos trimestres consecutivos. Por ejemplo, si la región está en 14 puntos básicos en dos trimestres cualquiera, First Data no puede tener dos períodos de 15, ya que de ser así todo fraude por lectura de banda será responsabilidad de ésta. En cambio, si el índice es menor a los 14 puntos base, no será responsable ante cualquier desconocimiento de transacciones, los cuales corresponderán al emisor. Todo los agentes del exterior están informados que determinado país está por encima del promedio de la región de puntos base, entonces todo fraude en Uruguay se puede contracargar y ganar porque no hacen un buen control sobre su comercio. Por esto también la necesidad del procesador adquirente por detectar las compras fraudulentas, porque por más que en principio no sea responsable, las mismas se van sumando y esto hará crecer el índice de puntos base, lo que puede hacerlo responsable si la suma de todas las transacciones sobrepasan el mencionado índice.

Según datos históricos proporcionados, First Data siempre se ha mantenido por debajo de la región (hoy en día el índice es de 5.8 puntos mientras que el de la región es de 13.7), pero de todas maneras existe la consigna permanente de no descuidarse, ya que al ser Uruguay un país chico con facturación menor, puede ocurrir que algunas tarjetas realicen ciertos fraudes de consideración en el país y hagan disparar el índice. Por lo tanto, por más reducido que sea el mercado, se tendrá que estar monitoreando siempre las transacciones, de manera de tener un control estricto para que no se dispare el índice del país. Esto para lectura de banda, en donde por lo general como ya se comentara anteriormente, el responsable es el procesador emisor; nunca se le descontará al adquirente salvo que se pase del índice.

Visa

Existe un estándar de puntos base que proporciona el sello en el cual se debe estar por debajo de lo que el mismo marca. Hoy en día el estándar se encuentra en 7 puntos base y en caso de situarse por encima no cambia la responsabilidad por fraude, a diferencia de lo que mencionábamos para el caso de MasterCard. Todos los emisores están obligados a reportarle a Visa los fraudes, quien con dicha información realiza un estudio de fraudes en cada país, y en los comercios.

Si un comercio en particular tiene un porcentaje elevado de fraude sobre ventas, Visa enviará un aviso al procesador adquirente del país del comercio (en el caso de Uruguay será a Visanet), para que tome medidas respecto al mismo. Si después de ésto, el nivel de fraude continúa, se abrirá una ventana de contracargos y todo lo reclamado contra ese comercio será de responsabilidad de este último (por un período de noventa días). Visa no

hará mención a que dicho comercio se encuentra con "ventana abierta" porque de hacerlo se le reclamaría por todo.

O sea que nunca se dará aviso al emisor que existe un comercio con ventana de contracargos, y por noventa días el comercio será responsable ante todo reclamo. Esto es el concepto de "TC40", que es la transacción mediante la cual se de aviso de fraude a Visa Internacional. Dicho concepto es clave para Visa porque lo hace de manera de estar al tanto del fraude en el mundo. Por este motivo es obligatorio reportar los fraudes en los que se incurre, razón por la cual se realizan auditorías para controlar que se reporten los fraudes a Visa Internacional. Se puede encontrar que se informó mal un fraude o que existieron ciertos errores, pero nunca omisiones de fraude, porque tienen multas muy grandes. Se puede dar el caso que se detecte que no hubo fraude, cuando por el contrario se pensó que sí; en este caso es posible revertir el TC40.

Una vez definida la responsabilidad, de si la misma corresponde al adquirente o al emisor, habrá que analizar qué hacen los procesadores, es decir si se la trasladan a sus clientes o no, o si pueden trasladarlo a otro agente porque previamente trasladaron la responsabilidad.

Procesador adquirente

Para el caso del procesador adquirente, éste deberá decidir si le traslada el fraude al comercio o no. Para esto deberá analizar qué tan implicado estuvo en la acción fraudulenta, así como también si actuó con los debidos recaudos o no. Obviamente si el comercio en cuestión participó en la misma, es muy probable que le traslade el importe del contracargo. El procesador analizará varios puntos respecto a ésto, como por ejemplo si fue el propio comercio quien participó en la acción fraudulenta o en realidad fue alguno de los empleados del mismo. También tendrá en cuenta la relación comercial que mantiene con el mismo.

Para los contracargos por compra duplicada, el importe desconocido (justamente por estar duplicado) será trasladado al comercio porque claramente es un error de éste.

En caso de que sea un comercio que tiene reiterados casos de transacciones fraudulentas, probablemente se le de aviso en primera instancia de que opere con mayores recaudos, para luego, de seguir sucediendo reiteradas veces más, trasladarle la responsabilidad al comercio y cobrarle así los importes por desconocimiento. Siempre será decisión del procesador si traslada o no el importe. Puede suceder, por ejemplo, un comercio que tiene una ventana abierta para Visa, y el propio procesador decide hacerse cargo de los contracargos por la importancia que tiene el mismo para su negocio. Por otro lado, si el procesador observa que

el comercio sigue siendo vulnerable al fraude y continúa sin tomar los recaudos necesarios, podrá desvincularlo del sello.

Para compras por e-commerce, si el comercio no cumple con normas PCI, probablemente se le traslade a éste el importe desconocido, además de darle el aviso de que no puede seguir operando de esa forma.

En los demás casos, generalmente el procesador adquirente asume los cargos del desconocimiento que le impuso el sello. Los comercios responden al procesador, son clientes de éste, y la mayoría de las veces la responsabilidad de los fraudes le pertenece a los comercios. Esto se puede dar porque el mismo, o no verificó que la firma fuera la correcta o porque directamente no la solicitó, por mencionar algunos recaudos que le son exigidos a los comercios. Pero como todo negocio, el procesador prefiere no trasladarle estos desconocimientos al comercio y asumir los costos, ya que de trasladarlo probablemente haya muchos comercios que no estén de acuerdo y no se adhieran al sello.

Siempre que el sello haya responsabilizado al procesador adquirente, se podrá decir que la responsabilidad es trasladada al comercio en la mayoría de los casos, pero por un tema de relación comercial y de costo beneficio es que el procesador decide asumir el costo. Un claro ejemplo son los supermercados que no exigen cédula de identidad al momento de realizar la firma del voucher, debido al tiempo que se pierde al chequear el documento. En caso de existir un desconocimiento, éste podrá ser trasladado al supermercado, pero dado el elevado importe de facturación que éstos manejan, es que el procesador decide asumir el costo.

Para terminar con el procesador emisor, es importante destacar el tema de la securitización en las compras a través de Internet. Para los casos en que existe clave personal de uso exclusivo para comprar por esta vía que identifica al usuario de manera inequívoca como su propietario (“Verified by Visa” y “MasterCard Secure Code”), y el comercio no posee la misma, en caso de que la existiera una transacción fraudulenta, la responsabilidad será del comercio.

Procesador emisor

En estos casos, para el sello, la responsabilidad ante transacciones fraudulentas es del banco emisor, y luego habrá que ver si éste se la traslada al cliente (tarjetahabiente) o no. Corresponde aclarar que es el banco o institución financiera emisora la responsable para con el sello y no el procesador, en caso de que este servicio se encuentre tercerizado. No obstante, en el vínculo comercial que se establezca con éste, puede trasladarle la

responsabilidad ante determinados fraudes. También puede contratarse o establecerse un seguro que cubra los desconocimientos recibidos. Este es el caso de First Data, que como procesador emisor cuenta con un seguro que los bancos, por tarjeta emitida, aportan un peso con tres décimas a un fondo administrado por First Data. Cuando ocurre un fraude, lo afectan a ese fondo, y en caso de no haber aportado ese peso con tres décimas, lo tendrán que sacar de sus propios fondos. No es un seguro externo sino que es un seguro del propio sistema y se aporta por tarjeta emitida como se mencionó.

Al igual que para el caso de procesador adquirente, la responsabilidad muchas veces es trasladada al cliente en el contrato que se firma, pero no siempre se traslada el costo del fraude, ya que esto está relacionado también al negocio y la relación costo-beneficio. Si se le trasladan todos los contracargos al cliente, probablemente éste no tendrá la suficiente confianza para el uso de la tarjeta y ésto repercutirá negativamente al negocio, por lo tanto en la balanza de la relación costo beneficio, la institución financiera adoptará la medida de hacerse cargo de la mayoría de los fraudes que pudieran corresponder al cliente (tarjetahabiente).

En líneas generales, usualmente las transacciones fraudulentas que le son imputables al cliente, son las relacionadas al auto fraude, y a las de hurto o extravío. La primera lógicamente le será trasladada porque el tarjetahabiente avala el fraude ya que se da con su consentimiento explícito o tácito. En el segundo caso, porque se entiende que el tarjetahabiente no tuvo los recaudos para cuidar el plástico y denunciar a la brevedad la desaparición del mismo. Algunas tarjetas tienen un seguro que cubren cierto lapso de tiempo desde la denuncia hacia atrás, precisamente por este tema, o sea por el período estimado que demora el tarjetahabiente en darse cuenta de la desaparición. Pero volviendo al concepto inicial, ésto estará ligado a un vínculo comercial con el cliente, puede pasar que el mismo no tuvo los recaudos necesarios de cuidado de la tarjeta, pero por ser un cliente importante no se le trasladen los cargos desconocidos.

Los fraudes por falsificación de identidad son de cargo de la financiera, ya que el cliente en realidad no existe, y fue la financiera la que no tomo los recaudos de controlar la información presentada.

Para el caso de suplantación de identidad, el responsable también es la financiera ya que la tarjeta no está en poder del tarjetahabiente pero por causas ajenas al mismo, y esta es la gran diferencia con el hurto, porque si bien en la suplantación de identidad puede considerarse que hay un hurto de la tarjeta de crédito, no es al tarjetahabiente que se lo realizan. Incluso se puede considerar que no se tuvieron los controles adecuados por parte del procesador al no haber detectado la participación del defraudador en algunos casos, como cuando es éste quien llama al procesador para realizar la reimpresión del plástico.

Cuando el fraude se sucede en alguna parte del ciclo de vida en que el servicio está tercerizado, como puede ser el reparto de las tarjetas por el courier como en el caso anterior, se podrá delegar, por acuerdo entre partes, al servicio tercerizado la responsabilidad ante el caso y el costo por el fraude. Igualmente para el sello el responsable será el procesador.

Los casos de fraude por venta a distancia (e-commerce) y de lectura de banda generalmente los asume la institución financiera. Puede pasar que se sucedan casos de fraudes de un tarjetahabiente, por lo cual se le bloquea provisoriamente la tarjeta y al comunicarse con el mismo éste solicita que se le active nuevamente y le continúen ingresando transacciones fraudulentas. En este caso la responsabilidad y los cargos se le trasladarán al cliente ya que fue el mismo quien no dejó que se le aplicaran las medidas contra el fraude y por lo tanto asumió las responsabilidades. También puede ocurrir que sea un cliente que recurrentemente le aparezcan transacciones fraudulentas, por lo cual la financiera probablemente le traslade la responsabilidad y los costos por dichas transacciones o incluso desista de tenerlo como cliente.

Podemos resumir entonces, que el traslado de la responsabilidad hacia el cliente estará ligado a la actitud que tome el mismo respecto al uso y cuidado de la tarjeta. Si el tarjetahabiente no toma los recaudos necesarios respecto al uso, si no la cuida debidamente como puede ser el caso de perderla o sufrir un hurto y no denunciarlo a la brevedad, probablemente sea pasible de que se le traslade la responsabilidad por las transacciones fraudulentas y con ello el costo monetario que implica. Se puede observar en el Anexo IX, al final de este trabajo, lo que informa Visa a sus usuarios a través de su página web oficial en Estados Unidos de América respecto a las responsabilidades de éstos ante el uso de una tarjeta de crédito de su sello.

5.7. Ejemplos de fraude

Se detallarán una serie de casos de fraude, ocurridos fundamentalmente en nuestro país, en el Anexo VIII del presente trabajo. Los mismos fueron extraídos de la prensa tal cual fueron publicados.

CAPÍTULO VI

INFORMES GRAFICOS

6.1. Mercado de tarjetas de crédito en Uruguay

En el primer semestre del año 2012 se dio un crecimiento del siete por ciento (7%) en la cantidad de operaciones con tarjetas de crédito, las que llegaron a 36 millones. En tanto, el monto operado fue de dos mil ciento ocho millones de dólares americanos (US$ 2.108 millones), lo que representó un incremento del diez por ciento (10%) frente al segundo semestre del año pasado.

El aumento en el número de tarjetas fue del dos por ciento (2%) llegando a un total de 2,49 millones de plásticos.

En la primera mitad del año, el monto operado a través de tarjetas de crédito aumentó un diez por ciento (10%), mientras que en las de débito el aumento porcentual fue mayor, aunque todavía con una lenta penetración en el mercado. Así surge del reporte sobre el sistema de pagos minorista publicado esta tarde por el Banco Central.

El monto promedio por operación fue de cincuenta y ocho dólares americanos (US$ 58). En las tarjetas emitidas por instituciones bancarias, el valor promedio de las operaciones fue de ochenta y tres dólares americanos (US$ 83), mientras que en las emitidas por entidades no bancarias la media fue de cuarenta y dos dólares americanos (US$ 42).

En cuanto a **tarjetas de débito** se dio una suba del cuarenta y siete por ciento (47%) en el número de operaciones de pago. En el primer semestre del año las operaciones llegaron a 1,65 millones. El monto total fue de ciento dieciocho millones de dólares americanos (US$ 118 millones), un treinta y siete por ciento (37%) más que en el segundo semestre del año. El mayor porcentaje de incremento fue en el exterior del país tanto en cantidad como en monto de pagos.

A pesar del fuerte avance en la cantidad de operaciones y en el número de plásticos, la operativa con este tipo de tarjeta sigue claramente por debajo del uso de tarjetas de crédito. El Banco Central del Uruguay señala que este tipo de instrumento "aún no ha logrado un posicionamiento destacado" debido a la "pasividad" de los emisores y a la "reticencia" de

los comercios. Es así que las tarjetas emitidas "se siguen utilizando fundamentalmente como instrumentos de retiro de efectivo"[15].

A continuación se expresa el siguiente cuadro, donde se muestra la cantidad de transacciones y el monto, identificándolas según el lugar de compra y el origen de la tarjeta. Este dato es para el primer semestre de 2012.

Compras Realizadas con Tarjetas Emitidas en	Lugar de la Compra	Operaciones (miles)	Monto (millones USD)
Uruguay	Uruguay	31.644	1.586
Uruguay	Extranjero	1.270	146
Extranjero	Uruguay	3.206	377
Total		36.120	2.108

El siguiente gráfico muestra la tendencia evolutiva de la cantidad de operaciones, del monto total en dólares estadounidenses y la cantidad de tarjetas en circulación por semestre, para los últimos cinco períodos.

Fuente: Reporte Informativo 1er Semestre 2012 – Sistema de Pagos Minorista – BCU

[15] Fuente: BCU, extraído del diario El País del 05/10/2012

http://www.elpais.com.uy/121005/ultmo-667916/ultimomomento/fuerte-aumento-de-las-compras-con-tarjeta-de -credito/

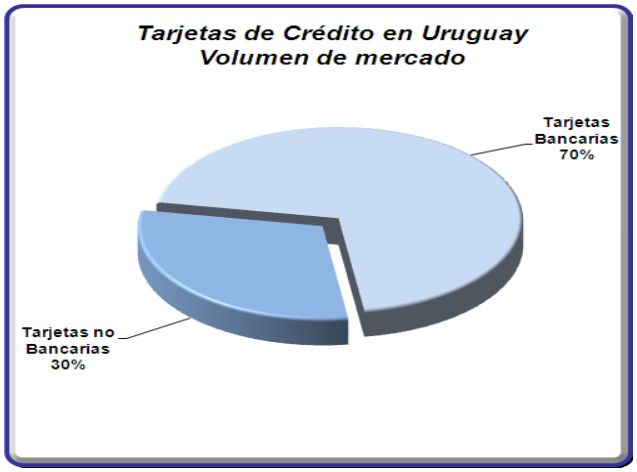
6.1.1. Evolución del mercado – estimado 2014

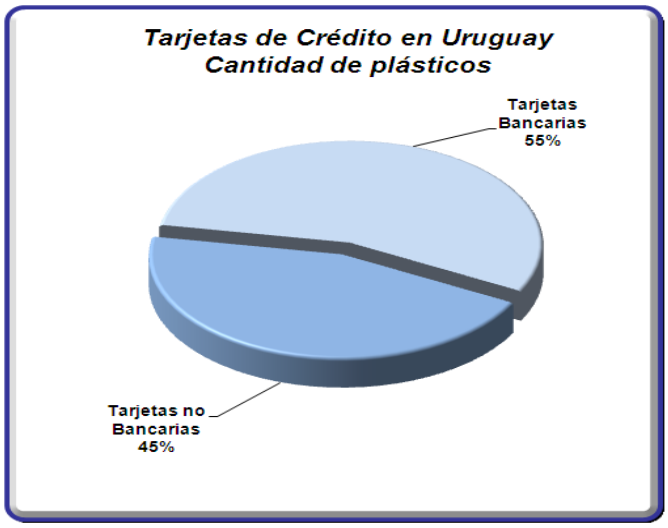
El siguiente gráfico muestra la tendencia evolutiva de plásticos de los últimos 10 años y la evolución esperada para los próximos 2 años.

Fuente: Reporte Informativo 1er Semestre 2012 – Sistema de Pagos Minorista – BCU

6.1.2. Tarjetas bancarias vs. tarjetas no bancarias

Los siguientes dos gráficos muestran un comparativo en volumen y en cantidad de plásticos entre tarjetas bancarias y no bancarias, donde se observa un predominio de las primeras sobre las segundas.

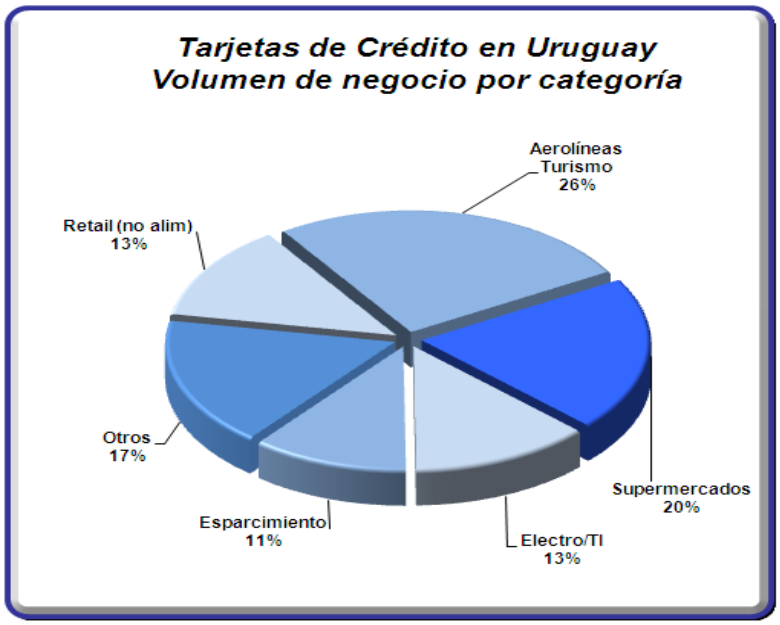


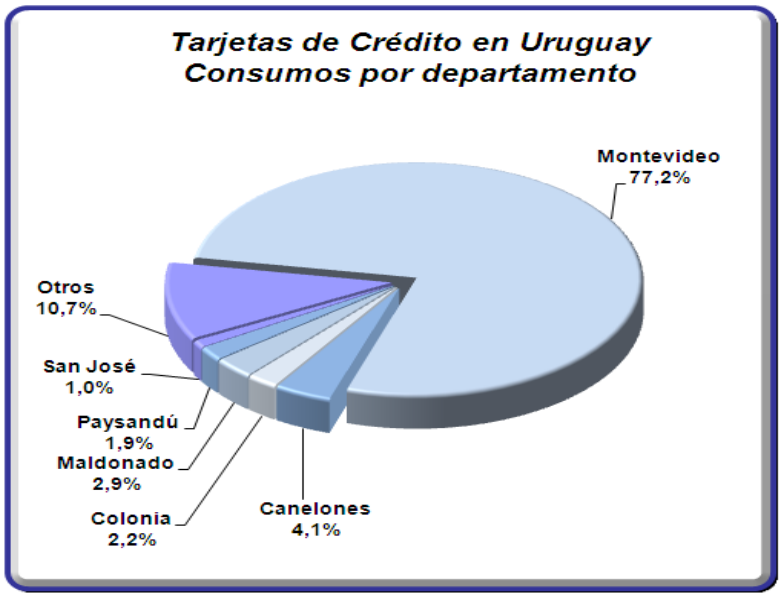


Fuente: Reporte Informativo 1er Semestre 2012 – Sistema de Pagos Minorista – BCU

6.1.3. Uso por categoría de negocio

Los siguientes gráficos muestran como se distribuye porcentualmente el volumen de transacciones según el tipo de comercio y por distribución geográfica (departamentos del Uruguay).





Fuente: Reporte Informativo 1er Semestre 2012 – Sistema de Pagos Minorista – BCU

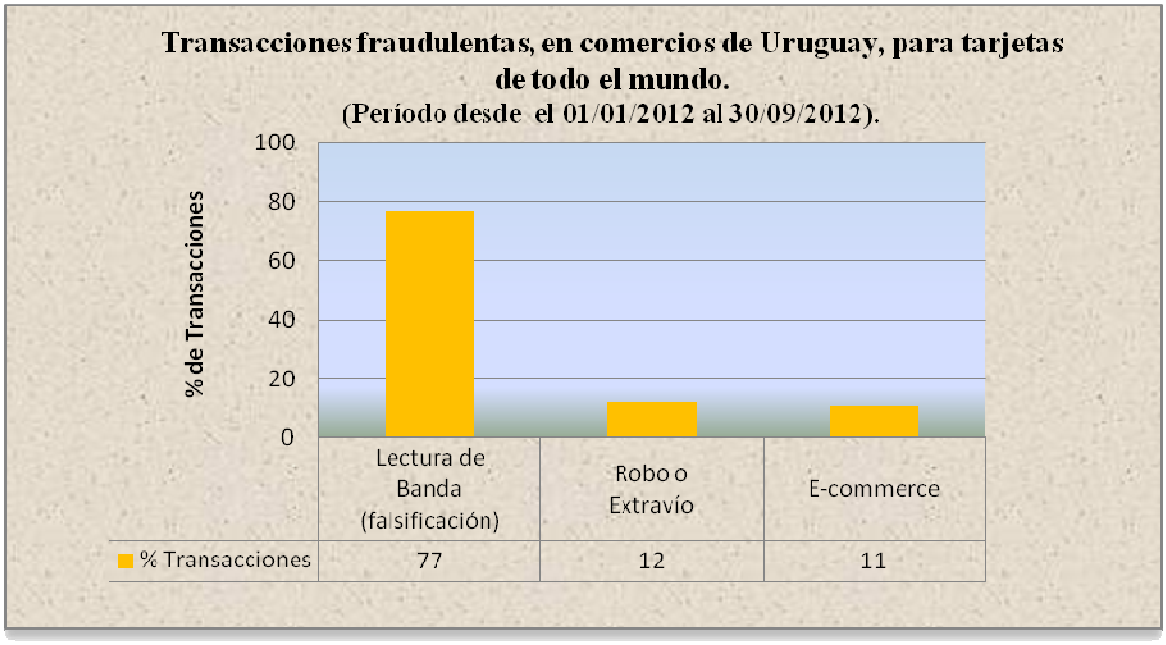
6.1.4. Comentarios

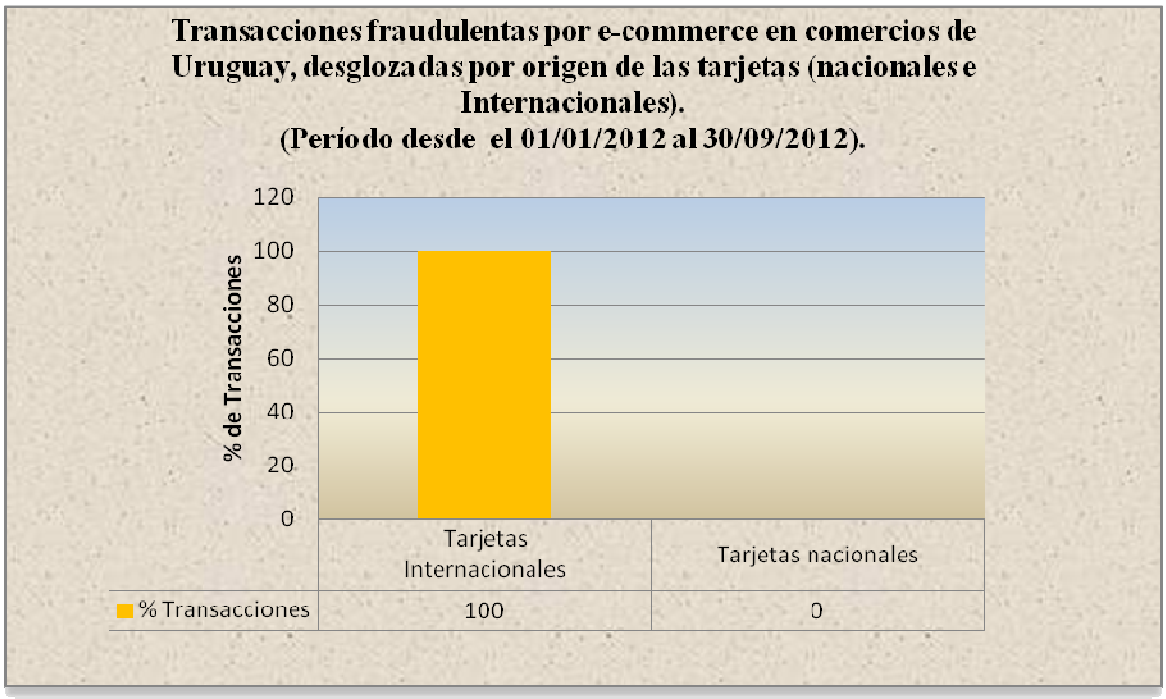
El análisis de las gráficas muestra un crecimiento sostenido tanto en la emisión como en el uso de las tarjetas de crédito. En la economía uruguaya, además de tener un crecimiento en el gasto/consumo por parte de la población, puede verse un cambio en las costumbres de los habitantes que tienden a sustituir el medio de pago efectivo por el de la tarjeta de crédito. Como es un mercado no del todo explotado, se espera un crecimiento sostenido para los próximos ejercicios tanto en tarjetas emitidas como en el uso de las mismas. Los rubros más utilizados para el consumo con tarjeta son aerolíneas y supermercados, los cuales ocupan casi el cincuenta por ciento (50%) del consumo total con tarjeta de crédito.

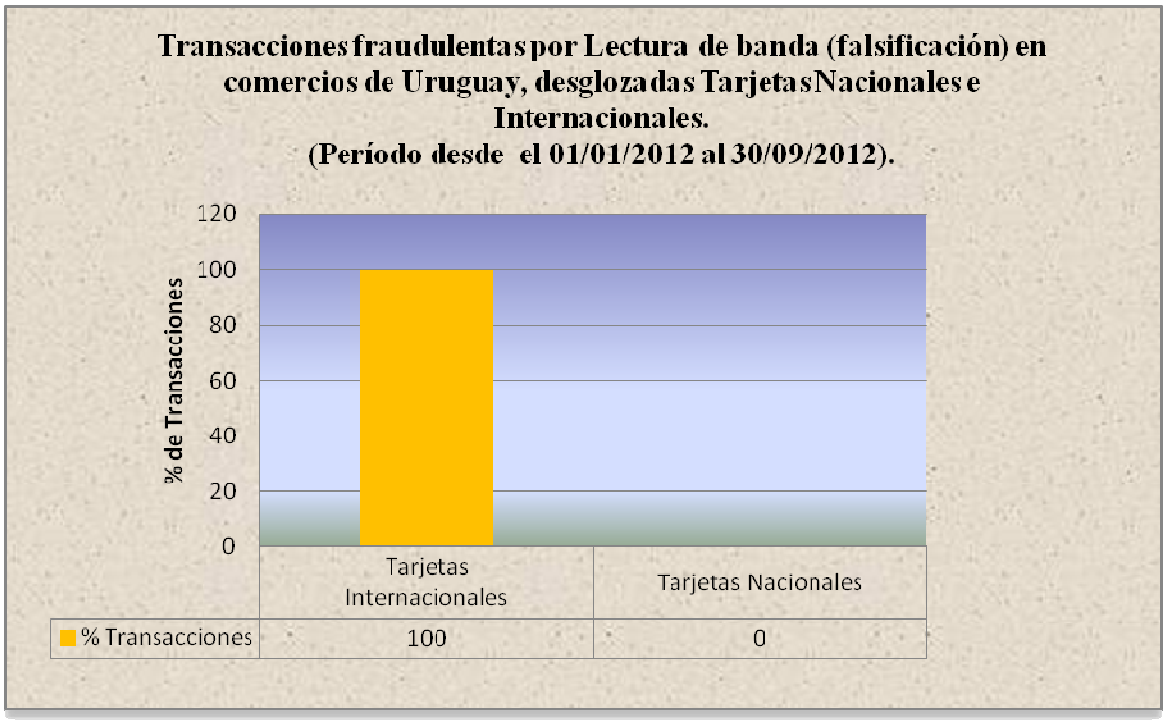
6.2. Fraude en todos los comercios de Uruguay para tarjetas de todo el mundo (datos medidos en cantidad de transacciones).

Los siguientes cuatro gráficos están vinculados al control adquirente, estudiando el fraude sucedido en los comercios del Uruguay para todas las tarjetas, desglosando por tipo de fraude y luego para cada uno de estos por país emisor de la tarjeta.

Aclaración: Para las gráficas relacionadas al control adquirente (comercios del Uruguay), cuando se utiliza el término de tarjetas internacionales el mismo se refiere al origen de la tarjeta y no al producto.






Transacciones fraudulentas por Lectura de banda (falsificación) en comercios de Uruguay, desglozadas Tarjetas Nacionales e Internacionales.
(Período desde el 01/01/2012 al 30/09/2012).
% de Transacciones
120
100
80
60
40
20
0
Tarjetas Internacionales
Tarjetas Nacionales
% Transacciones
100
0


Transacciones fraudulentas por Robo o Extravío en comercios de Uruguay, desglozadas Tarjetas Nacionales e Internacionales.
(Período desde el 01/01/2012 al 30/09/2012).
% de Transacciones
100
90
80
70
60
50
40
30
20
10
0
Tarjetas Internacionales
Tarjetas Nacionales
% Transacciones
5
95

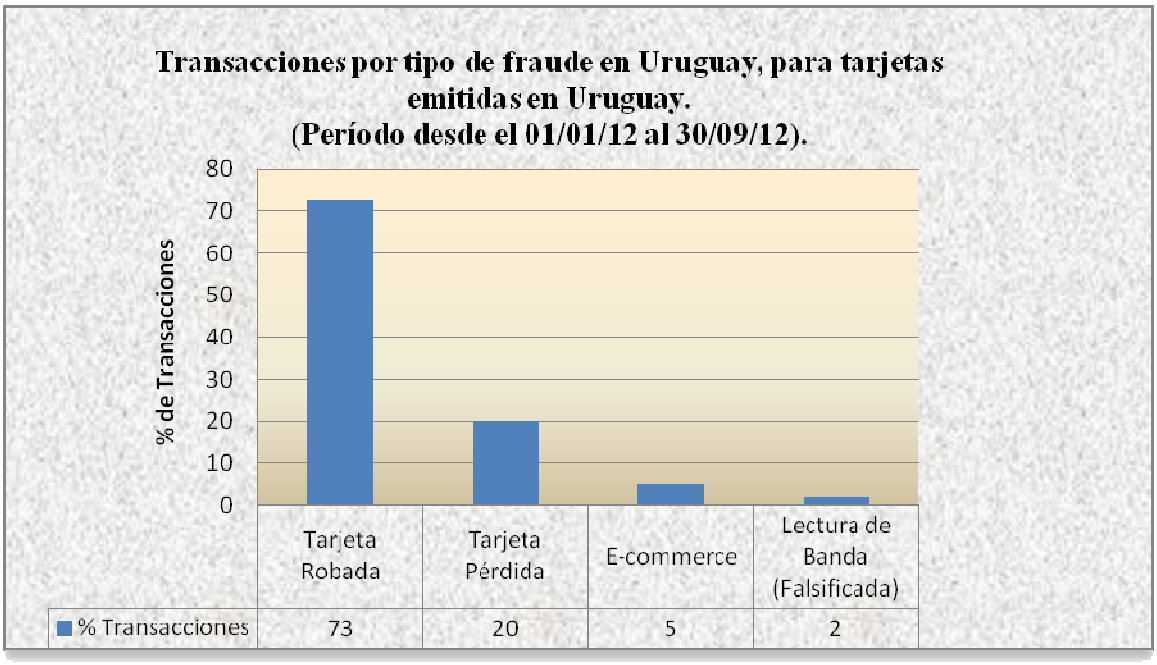
6.2.1. Comentarios

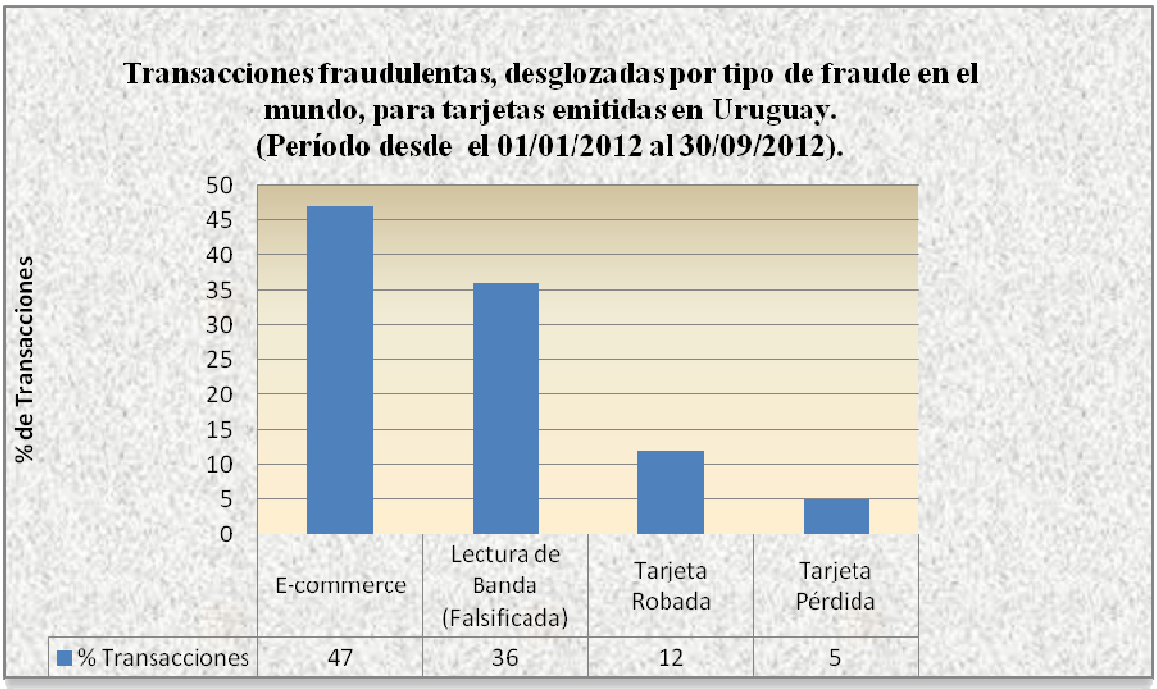
Estos cuatro gráficos, muestran primero que nada que el fraude por falsificación conjunto al fraude por e-commerce suman el ochenta y ocho por ciento (88%) del fraude total a comercios del Uruguay, con una preponderancia del primero acumulando el setenta y siete por ciento (77%) del fraude total. Ambos fraudes son totalmente realizados con tarjetas de origen internacional. Todo esto permite decir que casi el noventa por ciento (90%) de las transacciones fraudulentas sucedidas en comercios de Uruguay son con tarjetas extranjeras. Si se tiene en cuenta el cuadro de volumen de transacciones con tarjetas de crédito que aparece en el capítulo 6.1, vemos el hecho de que el uso de tarjetas extranjeras en el Uruguay representa menos del diez por ciento (10%) del total de transacciones ocurridas en el país, lo cual representa un quince por ciento (15%) aproximadamente en términos monetarios. Todo esto permite concluir que existe una fuerte concentración del fraude, es decir que las transacciones con tarjetas del exterior son las que con menos frecuencia ocurren en Uruguay pero las que más fraude concentran. También se puede concluir que es difícil observar grupos delictivos que clonen bandas o roben datos de tarjetas de crédito uruguayas para utilizarlas en Uruguay.

Continuando con el análisis de fraude a nivel de comercios en Uruguay, las tarjetas extranjeras acumulan el cien por ciento (100%) del fraude por e-commerce y lectura de banda, y por el contrario, las tarjetas nacionales acumulan cerca del noventa y cinco por ciento (95%) del fraude por hurto.

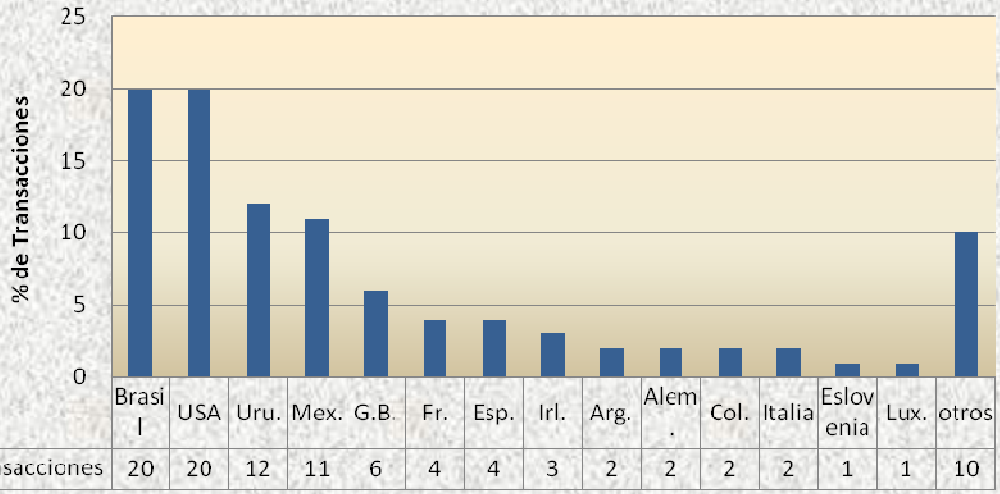
6.3. Fraude para tarjetas emitidas en Uruguay

Los siguientes cuatro gráficos están vinculados al control emisor, estudiando el fraude sucedido para tarjetas emitidas en el Uruguay en los comercios de todo el mundo, desglosando por tipo de fraude dentro de Uruguay y fuera del país, fraude por país con tarjetas uruguayas y fraude por producto de tarjeta de crédito.


Transacciones por tipo de fraude en Uruguay, para tarjetas emitidas en Uruguay.
(Período desde el 01/01/12 al 30/09/12).
% de Transacciones
80
70
60
50
40
30
20
10
0
Tarjeta Robada
Tarjeta Pérdida
E-commerce
Lectura de Banda (Falsificada)
% Transacciones
73
20
5
2

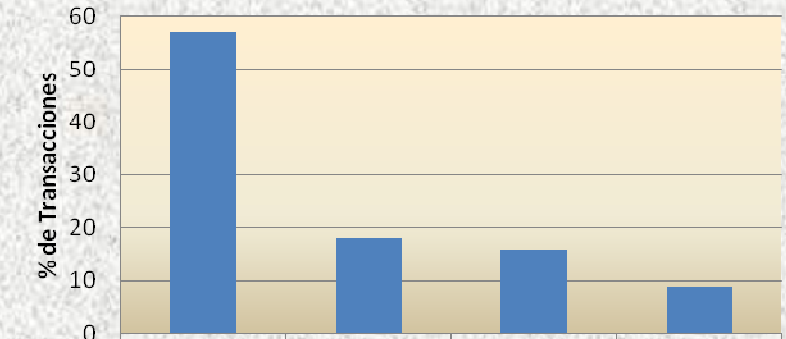

Transacciones fraudulentas, desglozadas por tipo de fraude en el mundo, para tarjetas emitidas en Uruguay.
(Período desde el 01/01/2012 al 30/09/2012).
% de Transacciones
50
45
40
35
30
25
20
15
10
5
0
E-commerce
Lectura de Banda (Falsificada)
Tarjeta Robada
Tarjeta Pérdida
% Transacciones
47
36
12
5

Transacciones fraudulentas realizadas en cada país para tarjetas emitidas en Uruguay.
(Período desde el 01/01/12 al 30/09/12).



	Brasil	USA	Uru.	Mex.	G.B.	Fr.	Esp.	Irl.	Arg.	Alem.	Col.	Italia	Eslovenia	Lux.	otros
% Transacciones	20	20	12	11	6	4	4	3	2	2	2	2	1	1	10

Transacciones fraudulentas, desglozadas por tipo de producto, para tarjetas emitidas en Uruguay.
(Período desde el 01/01/2012 al 30/09/2012).



	Intern.	Oro	Regional	Débito
% Transacciones	57	18	16	9

6.3.1. Comentarios

Los primeros dos gráficos muestran la distribución distinta que tiene el fraude de tarjetas emitidas en Uruguay según el origen de la transacción. Para transacciones fraudulentas realizadas dentro del país, predomina el fraude por hurto o extravió con el noventa y tres por ciento (93%) del total del fraude en Uruguay para tarjetas emitidas en Uruguay, algo similar de lo que se comentó en el punto anterior y también vinculado al hecho de que las bandas defraudadoras que clonan bandas o roban datos no los utilizan en la plaza; por lo general, si se roban datos o clonan bandas magnéticas en Uruguay, se utilizan en el exterior. A su vez en el exterior predomina el fraude por e-commerce con el cuarenta y siete por ciento (47%) del total, seguido por falsificación con el treinta y seis por ciento (36%); hurto y extravío ocupa el tercer lugar de fraudes según el tipo, con el diecisiete (17%) por ciento del total.

El tercer gráfico de este subcapítulo nos muestra que del total de fraudes con tarjetas emitidas en Uruguay, el ochenta y ocho por ciento (88%) ocurre en el exterior, por lo tanto solo el doce por ciento (12%) es ocurrido en Uruguay. Este es un dato de gran relevancia, ya que si se tiene en cuenta el cuadro de consumo que aparece al inicio de este capítulo, en el mismo se hace referencia a que menos del diez por ciento (10%) del total de transacciones con tarjetas emitidas en Uruguay son realizadas en el exterior. Esto permite concluir que existe una alta concentración del fraude, ubicándose en el segmento de transacciones en el exterior con tarjetas emitidas en nuestro país, esto por lo que se mencionó recientemente, desde el punto de vista emisor, se observa que menos del diez por ciento (10%) de las transacciones totales realizadas con tarjetas emitidas en Uruguay, acumulan el ochenta y ocho por ciento (88%) del total de transacciones fraudulentas. No quiere decir que el robo de datos o la clonación se hayan realizado en el exterior, pero sí que la transacción se realizó en el exterior.

Por lo tanto, se puede afirmar que para el control emisor, el principal cuidado lo debe tener con las solicitudes de autorización de origen en el exterior.

A su vez, el procesador adquirente deberá tomar los mayores recaudos durante el uso de tarjetas del exterior en comercios de plaza.

Ambos deberán tener recaudos en lo referente a tarjetas robadas; el emisor deberá apuntar las medidas de control a la realización de denuncias y detección rápida, mientras que por su parte el adquirente deberá tener los controles necesarios para detectar transacciones con una tarjeta que no pertenece al quien la utiliza.

Estos ítems mencionados son de especial interés para el análisis de los riesgos y actividades de control que se realizará en el siguiente capítulo. Este análisis, sumado a lo ya analizado en capítulos anteriores, serán las principales herramientas para realizar las conclusiones pertinentes.

La información obtenida para los gráficos pertenece a dos procesadores distintos, además de la obtenida a través de la página web del BCU. Si bien se utilizaron fuentes distintas en los gráficos, la tendencia es la misma. Por un tema de reserva de información no se citan las fuentes, salvo la que puede ser obtenida a través del Banco Central del Uruguay.

También se concluye que fraudes por sustitución o falsificación de identidad no son fraudes de consideración en el mercado. No es que no sucedan, pero sus guarismos son ínfimos lo cual puede deberse a varios factores como por ejemplo la efectividad por parte de las actividades de control, no ser un mercado atractivo para bandas delictivas, o por ser un delito de fácil detección (ambas pueden suceder por las actividades de control).

CAPÍTULO VII

EVALUACION DE RIESGO DE FRAUDE Y ACTIVIDADES DE CONTROL

7.1. Introducción

En este capítulo se buscará identificar y explicitar los diferentes riesgos de fraude encontrados en este trabajo, así como también las actividades de control existentes para minimizar los mismos. El riesgo es analizado básicamente desde el perfil del procesador emisor, el cual es a nuestro criterio el principal agente a la hora de detectar, prevenir y contrarrestar el fraude con tarjeta de crédito, y así fue como ha sido desarrollado a lo largo de los capítulos anteriores.

Si bien el objetivo de este capítulo no busca desarrollar conceptos teóricos de la materia Control Interno y Organización de Sistemas Contables[16], se entendió necesario ubicar al lector dentro contexto del fraude con tarjeta de crédito en nuestro país, a través de un cuadro en el cual se detallan los riesgos detectados, así como también las actividades de control que los mismos realizan para minimizar o detectar los riesgos encontrados.

El análisis de riesgos de una entidad, así como también la identificación de las actividades de control de la misma, son dos componentes básicos del Control Interno según la definición dada por el Informe COSO[17]. Según este, el control interno es un proceso efectuado por el directorio, la gerencia y el resto del personal, diseñado para proveer una seguridad razonable respecto al logro de los objetivos de las organizaciones, a los que subdivide en las categorías de efectividad y eficiencia de las operaciones; vinculados con la confiabilidad de la información contable a publicar; y relacionados con el cumplimiento de leyes y normas aplicables a la entidad. Además, establece que el control interno consta de cinco componentes que son: a) Ambiente de Control; b) **Identificación y evaluación de riesgos**; c) **Actividades de Control**; d) Información y Comunicación; e) Monitoreo.
El cuadro desarrollado a continuación, no busca realizar un análisis de todos los componentes del control interno. El objetivo es ubicar al lector en el contexto del fraude con tarjeta de crédito en nuestro país. Quien lea este trabajo, deberá entender los riesgos a los cuales, directa o indirectamente, estará expuesto ante una simple solicitud o ante el uso

[16] Control Interno y Organización de Sistemas Contables es la Cátedra a través de la cual se nos permitió realizar el presente trabajo.

[17] Committe of Sponsoring Organisations of the Teadway Commission

propiamente dicho de una tarjeta de crédito. Se trata de llevar a la práctica los componentes mencionados que se conectan con el alcance de este trabajo.

Identificar riesgos implica analizar todas las interacciones significativas de la entidad con tercero relevantes, como por ejemplo empleados, accionistas, proveedores, clientes, Estado, competidores, etc. Se deben identificar los peligros más significativos que puedan afectar el cumplimiento de los objetivos fijados por la organización, con el fin de diseñar un plan que permita decidir cómo tratarlos. El proceso de análisis de riesgos incluye determinar la probabilidad de ocurrencia de los mismos (con qué frecuencia ocurren los mismos), estimar la importancia del perjuicio (ver qué impacto tienen), así como también considerar las acciones que deben ser tomadas.

Como existen riesgos que pueden afectar la consecución de los objetivos propuestos por cualquier entidad, es que existe el concepto de **"control"**. Actividades de control son por lo tanto, las políticas y los procedimientos que se aplican para asegurar que se cumplen las directivas establecidas para acotar los riesgos. Las políticas determinan lo que debería hacerse mientras que los procedimientos son las acciones necesarias para llevar a cabo las políticas. Sólo tendrán sentido si están integradas tanto con la identificación y evaluación de riesgos, como así también con su gestión. Muchas veces la relación entre el costo y el beneficio no hacen viable las actividades de control. Este aspecto deberá ser evaluado por cada organización en función de sus objetivos.

En resumen, el cuadro a continuación intentará describir (una vez desarrollados los principales objetivos que persiguen los procesadores respecto a minimizar el riesgo, sin dejar de considerar también otros objetivos, ya sea de los tarjetahabientes como de las instituciones financieras y comercios) los riesgos identificados así como también las actividades de control que éstos aplican para lograr así reducir los mismos, ya que se debe tener presente que eliminar el riesgo es imposible. La única medida posible para eliminarlo, es hacer desaparecer la actividad de negocio respectiva; mientras exista negocio, siempre habrá riesgo asociado.

PLANILLA DE ADMINISTRACION DEL RIESGO Y ACTIVIDADES DE CONTROL PARA EL PROCESADOR EMISOR

OBJETIVO PROCESADOR EMISOR: Incrementar el nivel de detección del fraude sin afectar la operativa comercial.

***Objetivo Solicitud**: Otorgar tarjetas de crédito a personas que no tienen intenciones ilícitas.*

Ciclo	Tipo de Fraude	Riesgo	Evaluación del Riesgo		Actividades de control existentes	Evaluación de las actividades realizadas	Recomendaciones
			Probabilidad	*Impacto*			
Proceso de solicitud	Solicitud fraudulenta	El tarjetahabiente presenta información adulterada/falsificada.	Baja	Bajo	• Solicitud de comprobantes de domicilio, ingreso y cédula de identidad. • Para el caso de profesionales independientes, se verifica Certificado DGI, y declaraciones de pago IVA e IRPF. • Se verifica la veracidad de los datos presentados. • Se revisa el Índice General de Defunciones.	Insuficiente	• Revisar con mayor detalle la información brindada por el futuro tarjetahabiente, sobretodo para el caso de nuevos clientes y campañas masivas. • Compartir información con otras entidades financieras. • En caso de duda verificar de manera más detallada la fuente de ingresos declarada por el tarjetahabiente (verificación telefónica laboral y de domicilio).
					• Se revisa historial del tarjetahabiente en el mercado financiero.	Insuficiente	• Creación de un "bureau positivo", de manera de identificar si el cliente tiene historial con otras financieras. • Manejar límites de crédito bajos para los clientes que no es posible identificar un historial crediticio en el mercado financiero.

Objetivo Emisión: *Considerar todos los recaudos necesarios para evitar cualquier tipo de actividad fraudulenta en el proceso de emisión.*

Ciclo	Tipo de Fraude	Riesgo	Evaluación del Riesgo		Actividades de control existentes	Evaluación de las actividades realizadas	Recomendaciones
			Probabilidad	*Impacto*			
Proceso de emisión y custodia	Lectura de banda / Venta a distancia	Robo de datos o copia de banda en el proceso de embozo y custodia de la tarjeta, tanto del personal que participa en el mismo como ajeno a él.	Baja	Medio	• Informe diario de actividades de embozo, ensobrado, custodia en depósito y traslado de cada plástico y por quien fue realizado.	Eficiente	• N/C
					• Acceso restringido al área de embozo.	Eficiente	• N/C
					• Acceso restringido a la bóveda de seguridad.	Eficiente	• N/C
					• Movimiento de plásticos blancos y embozados desde bóvedas hacia Courier en bolsas pre-cintadas, con actas detalladas de movimientos y cantidades.	Eficiente	• N/C
					• Control de los antecedentes del personal contratado.	Eficiente	• N/C
					• Informe diario de actividades de embozo, ensobrado, custodia en depósito y traslado de cada plástico y por quien fue realizado.	Eficiente	• N/C

Objetivo Entrega: *Entrega de la tarjeta en forma íntegra, exacta y oportuna.*

Ciclo	Tipo de Fraude	Riesgo	Evaluación del Riesgo		Actividades de control existentes	Evaluación de las actividades realizadas	Recomendaciones
			Probabilidad	*Impacto*			
Proceso de entrega	Lectura de banda / Venta distancia / Suplantación de identidad	Robo de datos de la tarjeta o clonación de banda magnética por parte del personal que participa en el proceso de entrega o ajeno a él, mientras se traslada la misma al tarjetahabiente.	Baja	Bajo	• Traslado de la tarjeta en sobre cerrado y protegido hasta que llega al cliente.	Eficiente	• N/C
		Personal no cumple con los estándares de entrega estipulados.	Baja	Bajo	• Comprobante de entrega firmado por quien recibe la tarjeta o el mismo sobre en caso de no poder realizar la entrega adjunto al acta de recepción y entrega.	Poco eficiente	• Mayor control del personal que participa en la entrega de la tarjeta.
		Mecanismo de entrega de la tarjeta de crédito inadecuado (no le llega al tarjetahabiente).	Baja	Bajo	• Entrega de la tarjeta puerta adentro del domicilio estipulado en el contrato, contra firma y entrega del documento de la persona que atiende dentro del mismo, siempre mayor de edad.	Eficiente	• N/C
					• Entrega en mano solo al titular de la tarjeta contra documento de identidad y firma.	Eficiente	• N/C

					• Retiro en sucursal del Courier, contra entrega de documento de identidad y firma.	Eficiente	• N/C
					• Entrega en sucursal de la financiera contra documento de identidad y firma.	Eficiente	• N/C
					• Entrega en sucursal del socio comercial contra documento de identidad y firma	Eficiente	• N/C
		Hurto o extravío del plástico en el proceso de entrega	Baja	Bajo	• Acta de recepción y entrega de tarjetas.	Eficiente	• N/C
					• Mecanismo de traslado de la tarjeta (activa o inactiva).	Poco eficiente	• La tarjeta debe viajar inactiva y ser activada por el titular al recibirla.
					• Identificación positiva de los datos personales del titular a la institución financiera para activar la tarjeta.	Eficiente	• N/C

Objetivo Utilización: *Reducir el hurto y posterior utilización de datos robados.*

Ciclo	Tipo de Fraude	Riesgo	Evaluación del Riesgo		Actividades de control existentes	Evaluación de las actividades realizadas	Recomendaciones
			Probabilidad	*Impacto*			
Utilización	Venta distancia	Hurto de datos en un comercio.	Baja/Media	Medio	• Seguimiento por parte del sello, a través de puntos base o ventana de contracargo, al control adquirente realizado a comercios (página 83).	Eficiente	• N/C
					• Detección del punto de compromiso (página 30).	Eficiente	• N/C
					• Las instituciones financieras comunican a sus tarjetahabientes aspectos a considerar para realizar una compra segura por venta a distancia.	Ineficiente	• Mecanismo alternativo de comunicación: folleto informativo con estado de cuenta, mail recurrente, publicidad.
		Hurto de información en el proceso de solicitud de la autorización.	Baja	Medio	• Traslado de información siempre encriptada.	Eficiente	• N/C
		Robo de datos a procesadores.	Baja	Alto	• Aplicación de normas PCI (ver Anexo IV)	Eficiente	• N/C
		Hurto de datos mediante engaño (phishing e ingeniería social).	Baja	Medio	• Las instituciones financieras comunican a sus tarjetahabientes la forma en que se le pueden robar los datos.	Ineficiente	• Mecanismo alternativo de comunicación: folleto informativo con estado de cuenta, mail recurrente, publicidad.

		Utilización de los datos hurtados para realizar transacciones	Baja/Media	Media	• Reglas de alerta diseñadas teniendo en cuenta el historial de consumo del tarjetahabiente.	Eficiente	• N/C
	Clonación de banda	Facilidad para copiar y regrabar las bandas magnéticas	Media	Medio	• La información de la banda magnética está encriptada.	Ineficiente	• Utilizar tarjeta con chip con PIN, cuya copia y regrababilidad es más compleja, además de estar encriptada la información.
		Accesibilidad en el mercado a los materiales para copiar bandas	Media	Medio	• Destrucción de tarjetas cuando se cancela una cuenta.	Ineficiente	• Destrucción total de tarjetas, incluyendo las inactivas por vencimiento.
		Utilización de la banda clonada en transacciones fraudulentas	Baja/Media	Medio	• Presentar documento de identidad y firma (para el caso de tarjeta presente).	Poco eficiente	• Utilizar PIN que identifique al titular, el cual no aparecerá en la tarjeta.
					• Reglas de alerta diseñadas teniendo en cuenta el historial de consumo del tarjetahabiente.	Eficiente	• N/C
	Misceláneo	Solicitud duplicada o adulterada de una transacción.	Baja	Bajo	• Sistema de contracargo (solicitud de la información respaldatoria al tarjetahabiente y al comercio).	Eficiente	• N/C
	Lectura de Banda / Venta a distancia	Utilización de la banda magnética clonada para cometer fraude por venta a distancia para falsificar una tarjeta.	Baja	Bajo	• EL CVV o CVC2 esta encriptado en la banda.	Eficiente	• N/C

		Utilización de los datos de una banda clonada para cometer fraude por e-commerce	Baja	Bajo	• Los datos de la banda están encriptados.	Eficiente	• N/C
					• En la banda no aparece el código de seguridad, dato necesario para cometer fraude por e-commerce.	Eficiente	• N/C
	Suplantación de identidad	Que el defraudador pueda hacerse pasar por el tarjetahabiente para suplantarle la identidad.	Baja	Bajo	• Identificación positiva.	Eficiente	• N/C
		Utilización de la cuenta (tarjeta) sustraída.	Baja	Bajo	• Reglas de alerta diseñadas teniendo en cuenta el historial de consumo del tarjetahabiente.	Eficiente	• N/C
	Hurto / Extravió	Utilización del plástico en el período transcurrido entre que el tarjetahabiente pierde o le roban el plástico y el mismo es denunciado (bloqueado)	Media	Bajo	• Presentación de documento de identidad y firma (para el caso de tarjeta presente).	Poco eficiente	• Utilizar PIN que identifique al titular, el cual no aparecerá en la tarjeta.
					• Reglas de alerta diseñadas teniendo en cuenta el historial de consumo del tarjetahabiente.	Eficiente	• N/C

Objetivo tarjetahabiente: *Buscar colaboración del tarjetahabiente para minimizar el fraude.*

Ciclo	Tipo de Fraude	Riesgo	Evaluación del Riesgo		Actividades de control existentes	Evaluación de las actividades realizadas	Recomendaciones
			Probabilidad	*Impacto*			
Utilización	Lectura de banda/Venta a distancia/ Hurto o extravío	El tarjetahabiente no toma los recaudos necesarios para el cuidado del plástico	Media	Bajo	• Informar a los tarjetahabientes de las formas y recaudos que deben tener en cuenta para un uso correcto de la tarjeta de crédito (recomendaciones a través de sitios web de las instituciones financieras).	Ineficiente	• Establecer mecanismos alternativos de comunicación que logren mayor eficacia en cuanto a la recepción de la información por parte del tarjetahabiente (folleto informativo con estado de cuenta, mail recurrente, publicidad, charlas informativas al solicitar la tarjeta especialmente si es por primera vez o es una internacional).
	Hurto o extravío	Denuncia tardía de la pérdida o hurto del plástico.	Media	Bajo			
	Lectura de banda/Venta a distancia/ Hurto o extravío/ Suplantación de identidad	El tarjetahabiente no denuncia o no descubre a tiempo aquellas transacciones no realizadas por el mismo, o aquellas que fueron alteradas.	Baja	Bajo			
	Venta a distancia	El tarjetahabiente otorgue a un tercero los datos de seguridad de su tarjeta.	Baja	Bajo			
	Venta a distancia	Compra en comercios no seguros o por venta telefónica.	Media	Bajo			
	Suplantación de Identidad	El tarjetahabiente informa datos personales y de su cuenta a un tercero.	Baja	Bajo			

Objetivo Solicitud de Autorización: *Detectar de manera oportuna la mayor cantidad posible de transacciones fraudulentas en el proceso de solicitud y análisis para autorizar una transacción, sin afectar la operativa normal de transacciones.*

Ciclo	Tipo de Fraude	Riesgo	Evaluación del Riesgo		Actividades de control existentes	Evaluación de las actividades realizadas	Recomendaciones
			Probabilidad	*Impacto*			
Solicitud de Autorización	Lectura de Banda Venta a distancia/ Hurto o extravío/ Suplantación de identidad	Mal diseño del mecanismo de detección de fraude (sistema neural - reglas de alerta).	Baja	Alto	• Mecanismos puestos a prueba antes de su implementación. Los mismos deben contar con certificaciones de calidad, tanto del sello como del L.A.T.U.	Eficiente	• N/C
		Sistema vulnerable por el personal involucrado o por personas externas al mismo.	Baja	Alto	• Sistema de contraseñas y accesos restringidos según perfil de usuario y con registro de accesos y movimientos generados.	Eficiente	• N/C
		Sistema deje de operar	Baja	Alto	• Soporte y Respaldo de toda la información que se utiliza.	Eficiente	• N/C
					• Utilización de dos o más sistemas de autorizaciones que actúan al mismo tiempo.	Eficiente	• N/C
					• Instalación de generadores UPS para los casos de corte de energía eléctrica.	Eficiente	• N/C
		Regla de alerta obsoleta, inexistente o inadecuada que no detecte transacciones fraudulentas	Baja	Alto	• Estudio de índices de eficacia y eficiencia de las reglas de alerta (índice de cobertura, falso/positivo).	Eficiente	• N/C

					• Reglas de alerta establecidas por el historial de transacciones, por situaciones de mercado.	Eficiente	• N/C
					• Monitoreo de la situación del fraude en la región.	Eficiente	• N/C
		Rechazo de transacción legítima.	Baja	Alto	• Estudio de índices de eficacia y eficiencia de las reglas de alerta (índice de cobertura, falso/positivo).	Eficiente	• N/C
					• Reglas de alerta establecidas por el historial de transacciones, por situaciones de mercado.	Eficiente	• N/C
		Transacciones fraudulentas que puedan sucederse a un mismo plástico o una misma cuenta entre que se analiza una alerta y se confirma la misma	Baja	Medio	• Sistema de bloqueo preventivo y definitivo.	Eficiente	• N/C
		Análisis tardío de la alerta generada por transacción fraudulenta	Baja	Medio	• Guardia durante las veinticuatro horas todos los días del año que se encarga del análisis de las alertas generadas.	Eficiente	• N/C
					• Sistema scoring que marca la probabilidad de fraude en las transacciones.	Eficiente	• N/C
					• Experiencia del analista en determinar prioridades para el análisis de la cola de alertas.	Eficiente	• N/C
		Sobre carga de trabajo del analista (exceso de alertas para analizar)	Baja	Medio	• Distribución equitativa de reglas de alerta por parte del sistema a cada integrante del equipo de trabajo.	Eficiente	• N/C

		Personal encargado del estudio de las alertas no es idóneo.	Baja	Medio	• Política de selección de Recursos Humanos que tienen en cuenta entre otros aspectos, como capacidad adecuada al cargo y análisis del perfil psicológico.	Eficiente	• N/C
					• Capacitación constante del personal	Eficiente	• N/C
		Complicidad fraudulenta del personal encargado del estudio de las alertas.	Baja	Medio	• Segregación de funciones. (El personal que estudia las alertas no es el mismo que el que monitorea).	Eficiente	• N/C
					• Estudio del historial de fraudes detectados sobre alertas generadas.	Eficiente	• N/C
					• Estudio de índices de eficiencia de alertas (falso/positivo – Índice de Cobertura).	Eficiente	• N/C
		Complejidad para contar con información oportuna confiable y exacta al momento del análisis	Baja	Medio	• Historial de todas las transacciones con informes estadísticos y filtros, los cuales se puede acceder desde la alerta generada.	Eficiente	• N/C
					• Comunicación fluida con ejecutivo de cuenta y con el tarjetahabiente.	Poco eficiente	• Buscar acuerdo con área comercial de forma de establecer tiempos de respuesta más cortos ante consultas por transacciones sospechosas de fraude. • Fomentar mayor comunicación del tarjetahabiente acerca de posibles viajes a realizar o transacciones poco habituales, y formas de contacto para cuando se encuentre de viaje.

							• SMS que informan al tarjetahabiente acerca de la realización de transacciones específicas (por importe u origen de la misma).
					• Block de notas y audio donde se deja constancia de información importante.	Eficiente	• N/C
		Respuesta lenta ante dinámica de bandas delictivas para evadir los mecanismos de control existentes.	Baja	Alto	• Reuniones entre procesadores de plaza y de la región con asiduidad, comunicación constante con los mismos y con el sello.	Eficiente	• N/C
					• Sistema de detección de puntos de compromiso.	Eficiente	• N/C
					• Colaboración permanente con los organismos estatales de seguridad correspondientes.	Eficiente	• N/C
					• Historial de la aplicación reglas de alerta ante casos de fraude y el resultado obtenido.	Eficiente	• N/C
					• Determinación de perfil delictivo de bandas o defraudadores para tener una idea de que puede pasar ante la aplicación de determinadas medidas de seguridad.	Eficiente	• N/C

Objetivo Desconocimiento: *Maximizar los recuperos a través de los contracargos por aquellas transacciones fraudulentas que fueron desconocidas por parte del tarjetahabiente.*

Ciclo	Tipo de Fraude	Riesgo	Evaluación del Riesgo		Actividades de control existentes	Evaluación de las actividades realizadas	Recomendaciones
			Probabilidad	*Impacto*			
Contracargo	Auto fraude	Desconocimiento de transacciones por parte del tarjetahabiente en la que tuvo participación directa o indirecta.	Bajo	Bajo	• Estudio de documentación vinculada a la compra (voucher, objeto de la transacción, domicilio de entrega, dirección IP en caso de e-commerce).	Eficiente	• N/C
					• Estudio de antecedentes de transacciones y desconocimientos anteriores por parte del tarjetahabiente.	Eficiente	• N/C

Comentarios:

En la planilla se identificaron los riesgos asociados al procesador emisor para la concreción del objetivo de incrementar el nivel de fraude sin afectar la operativa comercial. A su vez, se estudió la eficiencia de las actividades de control que el mismo aplica y las posibles recomendaciones.

Estos riesgos pueden verse afectados por factores internos o externos que pueden incrementar o reducir los riesgos mencionados. Algunos de estos factores son riesgos en sí mismo y fueron mencionados en el cuadro, en cambio otros no los interpretamos como riesgos, sino como aspectos a tener en cuenta ya que el riesgo seguirá siendo el mismo y por lo tanto la actividad de control también. A continuación mencionaremos algunos factores internos y externos y como pueden afectar los riesgos.

Factores internos:

Cambios en las políticas de los sellos, como puede ser la aplicación obligatoria del chip, lo que generaría la aplicación de un nuevo sistema de control.

Centralización del procesamiento de datos. Algunas instituciones financieras realizan el procesamiento de manera regional, mientras que otras lo realizan de manera internacional. En el segundo caso se procesarán muchos más plásticos que en el primero, pero en éste, si bien son menos plásticos en total, tendrán un patrón de consumo que se asemejará en mayor medida entre los mismos y como éste es un factor que integra el armado de las reglas de alerta puede incidir en el diseño de las mismas.

Factores externos:

El cambio de tecnología por ejemplo, puede ser observado en el traslado a tecnología con chip de las distintas tarjetas de crédito del mundo. Este factor externo puede incrementar los riesgos de clonación de banda magnética, ya que al ser de más difícil copiado, provocará que los defraudadores prefieran las tarjetas con banda magnética para clonación. Las actividades de control, que en este caso son ineficientes, serán las mismas y potenciarán por lo tanto aún más la recomendación de pasar a tarjeta con chip. Hay que tener en cuenta que el hecho de que el plástico sea fácilmente copiable incrementa el riesgo de clonación de banda, pero no tiene por qué incrementar directamente el riesgo de fraude, ya que luego de clonar la banda deberán utilizarla y para ello hay otras medidas de control que ya fueron analizadas en la planilla.

Los cambios en las normativas es un factor externo que también influye. Para el caso se puede mencionar a la normativa BCU que obliga a las instituciones financieras a la aplicación de determinados recaudos para otorgar una tarjeta de crédito, lo que obliga a la aplicación de un mecanismo más de control para conceder el crédito.

Otro factor externo que influye es la situación económica que provoca la existencia de más plásticos. Al expandirse el mercado hace aumentar los plásticos con riesgos potenciales. A su vez, la situación social, hace que riesgos como el de hurto de tarjeta de crédito se incremente. Todos estos factores fueron tenidos en cuenta en el cuadro influyendo en la potencialidad del riesgo. La actividad de control será la misma pero se tienen en cuenta para el análisis de estas actividades.

RIESGO DE FRAUDE PARA EL TARJETAHABIENTE: RECOMENDACIONES.

Anteriormente se analizaron los diferentes riesgos que tiene el procesador emisor respecto a la concreción del objetivo y las actividades de control que realiza para atenuar los mismos. Algunas de las recomendaciones indicadas anteriormente están asociadas a capacitar o concientizar al tarjetahabiente acerca de los recaudos que debe tener con respecto al cuidado y a la utilización del plástico. En una encuesta realizada (ver Anexo X) se puede observar el desconocimiento por parte del tarjetahabiente respecto a lo que implica tener una tarjeta de crédito y las precauciones a tomar en cuenta para evitar cualquier tipo de fraude asociado. Es por esta razón que se considera de interés analizar los riesgos de fraude que están vinculados al tarjetahabiente. El riesgo en sí implica que un defraudador realice transacciones fraudulentas utilizando su plástico, su cuenta o su identidad. Si bien este riesgo muchas veces es asumido por la institución financiera o el procesador al asumir las responsabilidades por el mismo, como no siempre es así, entendemos oportuno analizarlo desde el punto de vista del tarjetahabiente. Si se analizara desde el punto de vista de éste, el riesgo entonces estará asociado a aquellos momentos donde el defraudador se hace de los instrumentos necesarios para hacerse pasar por el tarjetahabiente y así concretar el fraude. A continuación se enumeran los riesgos asociados al tarjetahabiente y las recomendaciones a tener en cuenta para evitarlos.

Riesgos:

- Hurto de datos mediante Phishinf o Ingeniería Social.

- Hurto o extravío del plástico.
- Clonación de la banda magnética.
- Hurto de datos por compra en un lugar no seguro (e-commerce) o por venta telefónica.
- Perder de vista el plástico y que se roben datos del mismo.
- Hurto de cuenta, o que el defraudador se haga pasar por el tarjetahabiente y le robe la cuenta existente (suplantación de Identidad).

Recomendaciones:

- Al realizar compras con tarjeta presente (lectura de banda), no perder de vista la misma. No usarla en aquellos autoservicios o cajeros que veamos alguna alteración en el mismo o no brinde confianza.
- Anunciar a la institución financiera, o al procesador, cuando se realice un viaje, las fechas del mismo y los posibles destinos a visitar. Brindar un número de contacto para verificar transacciones dudosas.
- Guardar el plástico en lugares seguros, no dejarlo en lugares donde quede fuera de la vista y expuesto a que un desconocido pueda sutraerlo con facilidad. El plástico es un medio de pago, como el dinero y los cheques, por lo que se deben tomar los recaudos de cuidado necesarios.
- Controlar diariamente la presencia del plástico.
- Denuncia en forma oportuna de la tarjeta perdida o robada.
- Ante un viaje, llevar siempre anotado el número telefónico para realizar la denuncia ante pérdida o extravío de la tarjeta de crédito.
- Destruir todo plástico que no se utilice más.
- Controlar el voucher de compra antes de firmarlo.
- Guardar documentación que verifique la compra (voucher o factura comercial).
- Para compras por venta a distancia, realizarlas en lugares seguros y de confianza.
- Para el caso de transacciones por e-commerce comprar en páginas seguras, verificando certificado de seguridad y URL (que aparezca la “s” que implica sitio seguro).
- No acceder a links de páginas de Internet por mail (páginas de comercios o de instituciones financieras).
- Googlear página del comercio en que se compra.

- Revisar estado de cuenta periódicamente (on-line) o mensualmente antes de pagar (procurar la primera opción).
- Denunciar todo hecho inusual o sospechoso en alguna transacción.
- No revelar a terceros información de la tarjeta.
- Destruir toda documentación relacionada a la tarjeta (estado de cuenta) antes de tirarla.

RIESGOS DE FRAUDE PARA EL COMERCIO

Al igual que para el tarjetahabiente, el comercio puede tener contacto directo o indirecto con los defraudadores, por lo cual también estará expuesto al fraude. Como ya se analizó en capítulos anteriores, en algunos casos tendrá responsabilidad y en otros no, pero es de interés enumerar los riesgos a los que está expuesto el comercio, mas allá de si tiene responsabilidad o no, y las actividades de control asociadas a éstos . En la práctica, algunas de las actividades de control son realizadas por los comercios y otras no, según el ramo. El procesador adquirente es el responsable de controlar que los mismos se apliquen. Muchas veces se impone la relación comercial a esta situación por lo que para casos de importes inmateriales o incluso grandes volúmenes de transacciones, algunos controles son omitidos. A manera de ejemplo, la firma del voucher no es solicitada en compras de importe menor. También sucede que para algunos comercios al ingresar la compra en el POS se exige que ingresen no solo el código de seguridad, sino también el número de cédula de identidad. Se observa entonces que, a algunos comercios, se les exige mayores controles que a otros. Quien determina esto es el procesador adquirente. A continuación se adjunta el cuadro de administración de riesgo para la detección de fraude por parte de los comercios. Como se ve en el mismo, todas las actividades se valuaron como eficientes, ya que se entiende que las mismas lo son para la concreción del objetivo. En todo caso, el problema no estaría en la actividad, sino en que el comercio no la aplique, lo cual va más allá de la eficiencia de la misma. Como se mencionara renglones arriba, la aplicación o no de estos controles corresponde al procesador adquirente, que a su vez es controlado por el sello internacional mediante los puntos base.

PLANILLA DE ADMINISTRACION DEL RIESGO Y ACTIVIDADES DE CONTROL PARA EL COMERCIO.

<u>Objetivo Comercio:</u> Evitar ventas con pagos fraudulento por tarjeta de crédito.

Tipo de fraude afectado	Riesgo	Evaluación del Riesgo		Actividades de control existentes	Evaluación de las actividades realizadas	Recomendaciones
		Probabilidad	*Impacto*			
Venta a distancia	Hurto de datos al comercio.	Baja	Bajo	• Guardar la información de manera segura, cumpliendo los estándares de calidad para ello (normas PCI).	Eficiente	• N/C
				• Tercerización del servicio de ventas por e-commerce para el caso de que no se puedan cumplir los estándares de calidad para ventas por Internet.	Eficiente	• N/C
Venta distancia/Hurto o extravío/Lectura de banda/suplantación de identidad	Personal no capacitado o cómplice en transacciones fraudulentas.	Media	Bajo	• Punto compromiso	Eficiente	• N/C
Venta distancia / Hurto o Extravió / Lectura de banda / Suplantación	Recibir transacciones fraudulentas con tarjeta presente (tarjeta falsificada, robada, extraviada, suplantación de identidad).	Media	Bajo	• Solicitar documento de identidad y firma, verificar contra tarjeta de crédito.	Eficiente	• N/C
				• Control de medidas de seguridad del plástico.	Eficiente	• N/C

Venta a distancia	Recibir transacciones fraudulentas por venta distancia.	Media	Bajo	• Entrega de producto o servicio vendido en domicilio del tarjetahabiente.	Eficiente	• N/C
				• Feedback oportuno con procesador adquirente en caso de transacciones sospechosas.	Eficiente	• N/C
				• Sistemas de ventas de los grandes comercios que cumplen con certificados de compras seguras y detectan compras fraudulentas.	Eficiente	• N/C

CAPÍTULO VIII

CONCLUSIONES

Como se expresara a comienzos de este trabajo, la tarjeta de crédito como medio de pago es un negocio. Este negocio se compone básicamente por las comisiones que cobran las instituciones financieras y por el interés cobrado sobre el capital financiado. El objetivo principal que persiguen éstas es maximizar las utilidades, donde su principal foco está en los ingresos sin descuidar los egresos.

La búsqueda de estos objetivos traerá aparejado riesgos asociados a la consecución de de los mismos, los cuales se buscarán minimizar sin modificar el margen de utilidad teniendo en cuenta la relación costo beneficio.

No se aprecia que el riesgo de fraude sea considerado como un negocio para los sujetos intervinientes, ya que no se observa que exista competencia entre ellos. No existe confidencialidad en la información que manejan, sino por el contrario se da una comunicación fluida y continua entre los mismos.

Según lo analizado se concluye que el fraude es un riesgo que está monitoreado. Esto se debe a la existencia de sistemas de detección y análisis de transacciones fraudulentas que funcionan de manera eficiente de acuerdo a las características del mercado, así como también al perfil de los consumidores de nuestro país. La eficacia de estos sistemas se ve reflejada en que Uruguay tenga uno de los menores índices de fraude de la región medidos en puntos base. Las características del sistema de autorizaciones hace que se adapte de manera eficaz a los requerimientos del mercado y se realiza un monitoreo constante de la situación del mismo a través del estudio de los índices de eficiencia. Esta herramienta, como todas las destinadas a la detección y prevención del fraude, sigue el objetivo de reducirlo al mínimo sin alterar el margen de utilidad. En resumen, toda herramienta que se haga para detectar fraude debe tener en cuenta la relación costo beneficio.

El análisis y detección del fraude es realizado por dos sujetos principalmente, que son el procesador emisor y el adquirente. Se entiende que es conveniente separar el análisis y las conclusiones de ambos, teniendo en cuenta las diferentes perspectivas que tendrán éstos en lo referente a las transacciones procesadas.

Desde el punto de vista emisor se concluye que la materialidad del fraude se da con transacciones realizadas en el exterior. Como se observara, estas representan menos del diez por ciento (10%) del total de transacciones para tarjetas emitidas en Uruguay. Además

las mismas, acumulan el ochenta y ocho por ciento (88%) de las transacciones fraudulentas. Esta alta concentración implica que los sistemas de alerta de los procesadores pongan énfasis en el origen de las transacciones que son las menos habituales, pero las más riesgosas. A su vez, en esta investigación se encontró que los principales fraudes son por e-commerce y lectura de banda, siendo el primero el porcentaje más elevado, además de tener una expectativa de que, en los próximos años, crezca la cantidad de intentos de fraude por e-commerce, acompañando así la tendencia al crecimiento del mercado por esta vía.

Para el mismo caso, o sea transacciones a nivel internacional con tarjetas uruguayas, no es despreciable el margen que ocupa el riesgo por hurto o extravío. El mismo, es el principal fraude cuando se habla de transacciones locales con tarjetas emitidas en nuestro país. Para este, el procesador no tiene demasiado margen de acción porque dependerá de la rapidez en la denuncia por parte del tarjetahabiente. Sin embargo, dado que la incidencia del margen no es despreciable y tiene un alto componente de factor externo, es que los procesadores también pondrán énfasis en detectar aquellas transacciones que puedan ser sospechosas de este tipo de fraude, por lo que serán de especial interés las alertas vinculadas a la velocidad de transacciones, al tipo de transacciones y ambas vinculadas al patrón de consumo del tarjetahabiente.

Para los principales tipos de fraude mencionados anteriormente (e-commerce, lectura de banda, hurto o extravío) con tarjetas del Uruguay, el sistema de detección y análisis funciona eficientemente. Por este motivo, los procesadores deberán apuntar al origen de estos fraudes, que está vinculado al momento del hurto de datos, de copia de banda magnética o de hurto o extravío del plástico. En este punto es donde hay un contacto directo o indirecto, personal o virtual, entre el tarjetahabiente y el defraudador.

Para entender la perspectiva del tarjetahabiente relacionado con la tarjeta de crédito, el uso y cuidado de la misma, fue realizada una encuesta como soporte a nuestra investigación. El resultado de la misma, que se puede apreciar en el Anexo X de este trabajo, muestra que existe desconfianza a la hora de realizar compras a través de Internet y esto lleva a que el tarjetahabiente sea reticente a este tipo de transacciones. Es por esto que el e-commerce es un mercado no explotado aún pero se vislumbra un cambio en la tendencia. Este factor puede potenciar los riesgos de fraude por e-commerce. Además se debe agregar el desconocimiento por parte del tarjetahabiente para realizar compras seguras a través de e-commerce. Asimismo se encontró un concepto erróneo en lo que refiere a tener precaución con el uso del plástico, sobretodo en transacciones con tarjeta presente. Este punto se aprecia claramente al ver que la mayoría de los encuestados consideran que toman los recaudos necesarios para el cuidado del plástico (sesenta por ciento), pero al mencionarles algunos hechos puntuales referidos al momento de pago con tarjeta y no perder de vista la misma se advierte que no es así, cambiando el resultado considerablemente de manera negativa.

Se aprecia también que el tarjetahabiente detecta de forma tardía la pérdida o el hurto de la tarjeta, lo que genera una demora considerable para realizar la denuncia al procesador. Justamente, una de las características principales de este tipo de fraude es la rapidez de acción por parte de los delincuentes para el uso de la tarjeta de crédito. Las recomendaciones apuntan a capacitar al tarjetahabiente en lo que respecta al uso seguro de la tarjeta, y al cuidado del plástico y de la documentación.

Estas recomendaciones fueron mencionadas en el capítulo VII, luego de analizar el riesgo de fraude al tarjetahabiente. Las mismas no son una sugerencia de los autores de esta investigación, sino que responden a aquellas efectuadas por las instituciones financieras. El problema de la desinformación del tarjetahabiente radica entonces en la equivocación por parte de las instituciones financieras en la elección de los canales de comunicación y en la intensidad con que se comunican.

Por lo tanto, como **conclusión final** para el riesgo de fraude desde el **punto de vista emisor** es que el mismo se encuentra eficientemente controlado. Sus índices muestran poca materialidad teniendo en cuenta el volumen de transacciones y el costo que implican, por lo que las principales herramientas para la detección del fraude son eficientes y cumplen con el objetivo. Bajar el fraude aún más, es posible. Ajustando las reglas de alerta puede lograrse, pero se corre el riesgo de afectar no solo los ingresos, sino también el objetivo principal de maximizar utilidades, por lo que sí es eficiente la herramienta y no habría que modificarla. La inquietud que merece esta situación, que no generará mayores costos, y puede ser de utilidad, es buscar vías alternativas de información y capacitación a los tarjetahabientes de forma que los mismos tomen mayores recaudos y así colaborar con la detección de fraude en el origen de las mismas. Otra recomendación que hay que subrayar, es fomentar una mayor comunicación entre el tarjetahabiente, el ejecutivo de cuentas y el procesador, de manera de contar con la información de forma más rápida, sobre todo para los casos en que el tarjetahabiente se encuentra de viaje.

Desde el punto de vista adquirente, implica analizar el fraude en los comercios del Uruguay del cual casi el noventa por ciento (90%) se realiza con tarjetas del extranjero, las cuales representan menos del diez por ciento (10%) del total de transacciones. Dentro de este rubro se aprecia que mayoritariamente se da por lectura de banda. El porcentaje por e-commerce es menor fundamentalmente por las características de nuestro mercado. Para este tipo de fraude, los comercios más riesgosos son las agencias de viaje y venta de artículos electrónicos. Se concluye, que los procesadores deben apuntar a la aplicación en mayor medida, de las actividades de control en los rubros riesgosos para estos tipos de fraude con tarjetas del exterior, que es donde se concentra fundamentalmente el fraude y a donde debe apuntar el control adquirente.

Para tarjetas uruguayas en comercios locales, el fraude es casi exclusivamente por hurto. Esto es así porque no es atractivo para el delincuente realizar el fraude en el mismo lugar

donde la banda fue clonada o fueron hurtados los datos, principalmente porque al ser un mercado chico se detecta rápidamente. Con respecto al hurto, la recomendación hacia los comercios es la misma que para las tarjetas internacionales, ya que el margen de acción es limitado.

En el cuadro de análisis de riesgos para comercios, se evaluó como eficiente a todas las actividades de control existentes. El problema se origina en algunos casos por la aplicación de manera incorrecta de las mismas. Es decir, no habría que introducir nuevas actividades de control, sino aplicarlas especialmente en los rubros de comercios que son más riesgosos al fraude con tarjeta.

Como **conclusión final** desde el **punto de vista adquirente**, los procesadores involucrados deberán buscar, a través de los canales adecuados, que los comercios cumplan de manera eficiente las actividades de control existentes haciendo hincapié en aquellos rubros considerados en esta investigación como más riesgosos. Como se mencionara anteriormente, el control de fraude no es competencia entre los procesadores adquirentes, por lo tanto puede ser una buena costumbre la colaboración entre los sellos para exigir en mayor grado la aplicación de las medidas de control. Puede ser de utilidad también, realizar seminarios o charlas hacia el personal involucrado del comercio con el objetivo de capacitarlo, lo cual no representa un costo elevado y por lo tanto contribuirá al logro del objetivo.

Este trabajo de investigación hizo foco principalmente en el procesador emisor en lugar del adquirente, ya que a partir de las observaciones anteriormente realizadas se concluye que es este el principal agente involucrado en lo que refiere al análisis y detección del fraude, y quien cuenta con las mayores posibilidades para el logro de esto.

El análisis y las conclusiones realizadas durante todo este trabajo, se dan sobre una situación actual; estamos en un mercado globalizado y muy dinámico por lo que es fundamental el monitoreo ya que el análisis y recomendaciones realizadas pueden variar. Lo más importante es anticiparse a los cambios.

ANEXO I

B.I.N.

Como se sabe, cada tarjeta de crédito tiene un número único que la identifica como tal y que vincula esa cifra con un único titular. Ese número, que como se expresara anteriormente consta de dieciséis dígitos (son los que aparecen al frente de la tarjeta), no es una cifra que se elige al azar sino que tiene cierta implicancia importante, tanto para las instituciones financieras emisoras como también para los procesadores emisores y adquirentes.

Los seis primeros dígitos de este número es lo que se denomina “B.I.N.” (del inglés Business Identification Number), número de identificación del negocio. Es así que las instituciones financieras emisoras se manejan por el llamado “B.I.N.”, a través del cual se identificará cada una de ellas, el tipo de producto (tarjeta de débito, crédito, gold, platinum, entre otros), el país donde se realiza el procesamiento de datos y donde se lleva la contabilidad. El procesamiento y la contabilidad no tienen por qué llevarse en el mismo país donde se encuentra la financiera. Hay muchas tarjetas de otros países que lo referente al procesador emisor y la contabilidad se llevan en Uruguay (en zonas francas principalmente), existiendo un registro mundial que identifica lo anteriormente señalado. Por esta razón, este elemento es una herramienta fundamental a través de la cual cada analista cuenta con información de suma utilidad, ya que no solo detalla el origen de la tarjeta, sino que brinda datos del procesador emisor.

Como mecanismo de seguridad se exige que el B.I.N., o parte del mismo, deba estar impreso en determinado lugar de la cara delantera de la respectiva tarjeta de crédito. A su vez, existen otros mecanismos de seguridad como el de la “v volada” (en el caso de tarjetas Visa) la cual también debe aparecer en la misma, el holograma y el impreso en relieve del número de tarjeta, fecha de emisión, fecha de vencimiento y nombre de la persona. El mecanismo de la “v volada”, se puede apreciar en la cara delantera de la tarjeta en la cual existe una letra “uve” con cierta parábola en uno de sus lados. El holograma puede aparecer tanto en la cara delantera como en la cara posterior de la tarjeta y representa el logo del sello respectivo; una paloma para Visa y un planisferio para MasterCard. Otro mecanismo de seguridad existente es que el código de seguridad no aparece impreso en relieve para evitar el hurto de datos mediante el “raspado o calco” de la tarjeta. Estos son mecanismos que se agregan día a día como consecuencia del flagelo del fraude, para poder evitarlo de alguna manera. Por esta razón, no todas las tarjetas Visa cuentan con la “v volada”.

Existe una página web donde el analista o cualquier usuario puede visualizar la información que contiene cada B.I.N y así poder identificarlo[18].

Si bien cualquier individuo puede acceder a la información que la misma contiene, y por lo tanto a la que identifica a cada B.I.N., hay parte de la misma que está restringida a determinados usuarios a través del uso de contraseñas.

A continuación, y a modo de ejemplo para facilitar la comprensión, se detallarán algunos ejemplos de "BIN" y la información obtenida de la página mencionada:

Bin:	471811
Card Brand:	VISA
Issuing Bank:	SUNRISE BANK OF ATLANTA
Card Type:	DEBIT
Card Level:	BUSINESS
Iso Country Name:	UNITED STATES
Iso Country A2:	US
Iso Country A3:	USA
Iso Country Number:	840
Bank's website:	
Customer Care Line:	
Bank Address:	******** [?]Available on Ultimate Database
Formal Bank:	******** [?]Available on Ultimate Database
Aditional Info:	

Bin:	472811
Card Brand:	VISA
Issuing Bank:	BANCO SANTANDER S.A.
Card Type:	CREDIT
Card Level:	CLASSIC
Iso Country Name:	Uruguay
Iso Country A2:	UY
Iso Country A3:	URY
Iso Country Number:	858
Bank's website:	
Customer Care Line:	
Bank Address:	******** [?]Available on Ultimate Database
Formal Bank:	******** [?]Available on Ultimate Database
Aditional Info:	

[18] www.bindb.com

Bin:	472801
Card Brand:	VISA
Issuing Bank:	ERSTE & STEIERMARKISCHE BANK D.D.
Card Type:	CREDIT
Card Level:	BUSINESS
Iso Country Name:	CROATIA
Iso Country A2:	HR
Iso Country A3:	HRV
Iso Country Number:	191
Bank's website:	www.erstebank.hr
Customer Care Line:	385-62-37-5000
Bank Address:	******** [?]Available on Ultimate Database
Formal Bank:	******** [?]Available on Ultimate Database
Aditional Info:	

Bin:	520394
Card Brand:	MASTERCARD
Issuing Bank:	FIRST DATA CONO SUR S.R.L.
Card Type:	CREDIT
Card Level:	STANDARD
Iso Country Name:	Uruguay
Iso Country A2:	UY
Iso Country A3:	URY
Iso Country Number:	858
Bank's website:	
Customer Care Line:	
Bank Address:	******** [?]Available on Ultimate Database
Formal Bank:	******** [?]Available on Ultimate Database

Bin:	411819
Card Brand:	VISA
Issuing Bank:	EXPRINTER INTERNATIONAL BANK N.V.
Card Type:	CREDIT
Card Level:	GOLD/PREM
Iso Country Name:	NETHERLANDS ANTILLES
Iso Country A2:	AN
Iso Country A3:	ANT
Iso Country Number:	530
Bank's website:	
Customer Care Line:	
Bank Address:	******** [?]Available on Ultimate Database
Formal Bank:	******** [?]Available on Ultimate Database
Aditional Info:	

(*) Los datos encriptados con el * es porque son visibles únicamente para usuarios con contraseña. Este código (B.I.N.), como veremos más adelante, es una buena medida de seguridad ya que permite visualizar quién es el titular de la tarjeta, además de que el mismo debe estar escrito o impreso en la tarjeta.

Este último ejemplo es un caso de tarjeta del exterior que la contabilidad y el procesamiento de la misma se realiza en Uruguay (lo procesa Sistarbanc).

Como vimos, el caso de B.I.N. es una codificación específica para la identificación del producto tarjeta, pero integra un mundo de códigos de identificación, de suma utilidad para los procesadores en su estudio de transacciones.

Otra codificación útil que maneja es el de los comercios, conocido como M.C.C. (Merchant Category Code, que traducido al español significa Código de Categoría de Mercado). Este tipo de codificación universal nos permite identificar el tipo de comercio. Algunos comercios por su gran tamaño tienen su propio código M.C.C.

Ejemplos:

4511 – Aerolíneas en general.

5411 – Supermercados.

5551 – Alquiler de botes.

Algunos comercios como Best Buy, Amazon, American Airlines, entre otros, tienen su código específico.

Ejemplos de códigos por ubicaciones geográficas:

434 – Libia.

752 – Suecia.

784 – Dubái.

824 – Gran Bretaña.

858 – Uruguay

ANEXO II

RECOMENDACIONES REALIZADAS POR LAS INSTITUCIONES FINANCIERAS BANCARIAS RESPECTO AL HURTO DE DATOS

A continuación se brindará información recopilada de algunas páginas de instituciones financieras, las cuales informan a los tarjetahabientes las formas en que sus datos pueden ser robados y brindan recomendaciones para evitarlo. La misma se pone al servicio del lector tal aparece en las respectivas páginas web de las abajo mencionadas instituciones financieras.

Información obtenida de la página oficial del Nuevo Banco Comercial[19]*:*

Recomendaciones de Banco Comercial para el uso seguro de tu tarjeta de crédito o débito evitando el robo de identidad

- Firma tu tarjeta en el momento que la recibes de Nuevo Banco Comercial, de esta manera los comercios donde la utilices podrán comparar tu firma con la de tu documento de identidad, evitando que otras personas puedan hacer uso de la misma.

- No proporciones tu número de tarjeta, la fecha de vencimiento de la misma y/o el código de seguridad a ninguna persona que te lo solicite en forma telefónica, aunque tu interlocutor mencione que la información se solicita por razones de seguridad o verificación, a menos que estés totalmente seguro de la identidad de la persona que te está llamando y de la entidad a la que representa.

- Protege tus tarjetas como si fuese efectivo, nunca las dejes fuera de tu vista o bien a buen recaudo.

- Memoriza tu PIN, no lo lleves impreso junto a tu tarjeta, evita usar claves obvias.

- Verifica siempre que en los comprobantes de venta esté impreso el monto correcto de la compra antes de firmarlos, guarda las copias de tus comprobantes y compara con los estados de cuenta mensuales para asegurarte que no existan cargos no autorizados.

[19] Fuente: www.bancocomercial.com.uy

- No permitas que los cajeros o vendedores anoten tu dirección en los recibos de la transacción (salvo que el mismo sea impreso por el mismo sistema de facturación del comercio), ni el número completo de tu tarjeta, éste deberá aparecer enmascarado en los recibos electrónicos generados por terminales de tipo POS o bien sistemas del propio comercio, no así en los manuales donde se imprime el relieve del plástico, tampoco deberás permitir que tu código de seguridad sea impreso bajo ningún concepto, esta información no es necesaria para el comercio, únicamente se utiliza para gestionar la autorización de la compra por parte del emisor de la tarjeta.

- Limita el número de tarjetas y otra información personal que llevas en la cartera, bolso o billetera, en caso de pérdida o robo, reporte el incidente inmediatamente a nuestro Centro de Autorizaciones Teléfono 2140 - 1800 para evitar que se realicen consumos posteriores al reporte.

- Recuerda que tu tarjeta es para exclusivo uso personal, si deseas extender las ventajas y beneficios de la misma solicita adicionales sin costo.

- Mantén a buen recaudo tus estados de cuenta, en los mismos existe información de interés para alguien que quiera robar tu identidad.

- Mantén tus datos actualizados para que podamos ofrecerte un mejor servicio.

Información obtenida de la página oficial del Citibank[20]:

Prevención y tipos de fraudes a través de Internet

La intención de los correos electrónicos fraudulentos (Phishing) es suplantar la identidad de instituciones financieras y son enviados como spam (correo no solicitado). Estos correos solicitan a sus destinatarios que visiten una página (sitio web) que simula ser, en nuestro caso, de Citi, invitándolos a ingresar sus datos personales y claves, con falsas advertencias y los enruta a una página que parece ser de Citi (website spoofing). En este sitio se solicita ingresar información confidencial o sensitiva del cliente.

A primera vista, el correo electrónico parece proceder de Citi ya que utiliza extensiones que hacen referencia a Citi. Asimismo, la página simula el diseño y la gráfica de las páginas de Citi. Este tipo de correos siempre son investigados a fondo para determinar su procedencia y aplicar la ley según corresponda.

[20] www.citi.com.uy

Es importante anotar que en ningún caso los sistemas del banco o bases de datos están de alguna forma comprometidas.

Cómo prevenir Phishing y Website Spoofing

• Tenga presente que Citi nunca le enviará correos electrónicos solicitando su nombre de usuario, claves de acceso, números de tarjeta, o cualquier otra información confidencial.

• Antes de ingresar cualquier información confidencial, busque el símbolo del candado en la barra inferior del navegador para asegurarse que el sitio está certificado como seguro. Un sitio seguro utiliza un método de transmisión de datos privados que los convierte a un código secreto.

• Evite hacer clicks en links o vínculos contenidos en correos electrónicos, estos links pueden llevarlo a un sitio web falso, con aspecto similar a uno verdadero.

• Siempre acceda a Citi Online, tecleando directamente en su navegador la dirección de nuestra página institucional.

• Opere siempre en computadores conocidos, evitando la utilización de Citi Online en aquellos que sean de uso público.

• Esté alerta de correos electrónicos que parecieran proceder de un negocio o un amigo, pero que verdaderamente están diseñados para motivarle a revelar información confidencial o destinados para descargar un virus.

• No conteste ningún correo electrónico que solicite su información personal incluyendo alguna contraseña, número de cédula de ciudadanía u otra información confidencial. Haga transacciones online solamente en sitios que usted confía. No envíe información personal o financiera a través de correos electrónicos.

• Abra solamente los correos electrónicos de procedencia conocida y sea especialmente cuidadoso al abrir un correo electrónico con archivos adjuntos. Incluso, sin saberlo, personas conocidas le podrían enviar accidentalmente un correo con virus.

• Cerciórese que su computador tenga un software anti-virus actualizado. Los software anti-virus requieren actualizaciones frecuentes para proteger su PC contra virus nuevos. Asegúrese de descargar las últimas versiones de los anti-virus tan pronto éstas estén disponibles.

¿Qué hacer frente a un e-mail fraudulento?

Si usted recibe un e-mail o correo electrónico fraudulento, salga inmediatamente de la página que usted cree que no son lo que pretenden ser. No siga ninguna de las instrucciones que aparecen en el e-mail, pop-up o página web. Informe a la brevedad al banco a través de CitiPhone. Si usted ingresó información confidencial en el sitio que usted considera inseguro por favor comuníqueselo al representante telefónico con el objeto que realice todas las medidas preventivas para evitar un posible fraude.

¿Cómo prevenir los casos de Ingeniería Social (llamadas telefónicas fraudulentas)?

Tenga presente que Citi nunca le enviará correos electrónicos solicitando su nombre de usuario, claves de acceso, números de tarjeta, ni le hará llamadas telefónicas solicitándole información confidencial. ¿Qué hacer frente a un llamado telefónico fraudulento? Si usted recibe un llamado telefónico que le despierte sospechas, corte la llamada. No siga ninguna de las instrucciones que le den quienes pretenden ser funcionarios de Citi. Informe a la brevedad al banco a través de CitiPhone, teléfono 9150000. Si usted les proporcionó información confidencial por favor comuníqueselo al representante telefónico con el objeto que realice todas las medidas preventivas para evitar un posible fraude.

Información obtenida de la página oficial del Banco de la República Oriental del Uruguay[21]*:*

Seguridad en Internet

Recomendaciones a tener en cuenta

Atento a correos electrónicos ilegítimos que han circulado en los últimos días, hacemos saber a nuestros clientes y al público en general, que el Banco de la República Oriental del Uruguay, bajo ninguna circunstancia solicita por medios tales como: mensajería electrónica, comunicación telefónica, correo tradicional, etc., información confidencial a sus clientes.

Asimismo recordamos que la información privada como la contraseña de acceso a los sistemas informáticos publicados en internet o el pin de las tarjetas de los cajeros automáticos, nunca será requerida por el Banco por ningún medio, ni siquiera el personalizado.

Ante cualquier inconveniente o duda, comuníquese con el Centro de Atención al Cliente por el 2900.2900

[21] www.brou.com.uy/web/guest/institutional/seguridad-internet

Información obtenida de la página oficial del banco Itau[22]:

¿¿QUE ES EL PHISHING??

Es una forma de fraude, que utiliza e-mails o mensajes tipo pop ups los cuales dicen ser de alguna empresa con la que usted trabaja, por ejemplo su proveedor de Internet, un banco, o incluso el gobierno.

Estos mensajes generalmente solicitan que "actualice" información o la "valide", piden que usted ingrese su número de tarjeta de crédito, número de cuenta, claves de acceso o cualquier tipo de información similar. Incluso, algunos de estos mensajes lo intimidan a que realice la operación so pena de generar consecuencias negativas en su operativa, si usted se niega a ingresar los datos solicitados.

Generalmente estos mensajes tienen un enlace a otra página, la cual es parecida o igual a la página de la empresa de la cual dicen ser. Sin embargo todo esto es un montaje para obtener datos y luego cometer fraudes, utilizando la información que recogen de quienes caen en este tipo de engaños.

TIPS PARA EVITAR EL PHISHING

- Si recibe un e-mail o un pop up solicitando que ingrese información personal o financiera no responda ni cliquee en el enlace/link en el mensaje. Las empresas legítimas no solicitan esta información vía mail.

- Nunca envíe información personal o financiera vía mail. Si va a ingresar información en algún sitio siempre verifique que aparezca un "candado" o la dirección comience por "https:" (la "s" significa "seguro").

- Verifique siempre sus estados de cuenta o resúmenes de tarjeta ni bien los reciba de forma de detectar si hay operaciones indebidas.

- Utilice software antivirus y manténgalo actualizado. Algunos mensajes tipo "Phishing" contienen software que puede dañar su computadora o rastrear sus actividades en Internet sin usted saberlo.

- Sea cauteloso al abrir cualquier documento adjunto en e-mails que recibe independientemente de quién los envía.

[22] www.itau.com.uy

¿Qué son los e-mails fraudulentos?

Cuando hablamos de mail fraudulento (o Phishing) nos referimos a un tipo de delito informático que, a través de ingeniería social, intenta adquirir información confidencial del cliente (contraseñas, números de tarjeta, número de cuenta bancaria, documento de identidad).

El delincuente se hace pasar por una empresa de confianza a través del envío de un correo electrónico, mensaje de texto o incluso realizando una llamada telefónica.

Los mails fraudulentos se utilizan generalmente para guiar al cliente a un sitio web falso pero estéticamente igual al verdadero de la institución. A través de éstos, se le solicita al cliente (por diferentes motivos) que ingrese información confidencial para posteriormente planificar una estafa.

Información obtenida de la página oficial del BBVA[23]:

¿Cómo se realiza Phishing a través de un mail fraudulento?

- Se envía un correo electrónico masivo, no dirigido exclusivamente a Clientes, falsificando la dirección origen simulando provenir del Banco.

- En el correo se insta a conectarse a una página web e introducir los datos sensibles.

- El nombre de la página simula pertenecer al Banco y se trata de un diseño copiado de la web real del banco.

- Los Clientes engañados que confíen en la autenticidad introducen sus datos personales (usuario y clave).

- Los datos recogidos son enviados a la dirección de correo del autor del intento de fraude, habitualmente cuentas gratuitas tipo yahoo.com, hotmail.com.

- Con dichos datos el autor intentará obtener dinero de las cuentas de los clientes, o acceder a su cuenta para ver los saldos de las mismas directamente en la web del banco.

- Este tipo de intento de fraude es conocido como SCAM.

¿Cómo nos protegemos?

[23] www.bbva.com.uy

Para proteger la seguridad de sus cuentas y sus datos personales recuerde siempre que: BBVA Uruguay nunca le solicitará por correo electrónico que informe de sus claves de BBVA net. Estas Claves son secretas y únicamente Ud. debe conocerlas para su utilización exclusiva en la propia BBVA net.

A su vez, BBVA Uruguay no le remitirá enlaces (links) o le solicitará que acceda a través de los mismos. Si en cualquier momento Ud. desea acceder a BBVA net recuerde hacerlo siempre introduciendo Ud. mismo la dirección www.bbva.com.uy en el navegador y accediendo al link de BBVA net. Por su seguridad BBVA Uruguay ha omitido o enmascarado sus datos personales o económicos.

Ante cualquier sospecha de recepción de correos ilegítimos que intenten suplantar a BBVA Uruguay, y específicamente si estos no están adecuadamente personalizados o no corresponden con una alerta programada por Ud., por favor no facilite dato alguno.

¿Qué pasos debe seguir ante un email fraudulento?

Si usted recibe un correo electrónico fraudulento haciéndose pasar por BBVA Uruguay, siga los siguientes pasos:

- No siga ninguna de las instrucciones que especifica el mail o sitio web.

- No ingrese ningún dato personal y/o confidencial.

- Reenvíe el mail recibido a bbvaresponde@grupobbva.com.uy. BBVA Uruguay se encargará de denunciar la página falsa para prevenir posibles fraudes.

- Borre el mail recibido de su bandeja de entrada.

- Si usted ya ingresó algún dato personal en un mail con las características antes mencionadas, contacte inmediatamente con BBVA Uruguay en el 2916 14 44 o enviando un correo electrónico a la casilla bbvaresponde@grupobbva.com.uy.

Buenas prácticas de seguridad

Se recomienda:

- No elegir claves fáciles de descifrar para terceros. Trate de incluir números, letras y símbolos en sus contraseñas.

- Intente que el largo de sus claves sea mayor o igual a 8 caracteres.

- Cambiar la clave periódicamente.
- Intente no anotar en ningún lado la clave elegida.
- Verificar que al ingresar una clave (cualquiera sea) usted sea el único que la visualice.
- No ingrese a links contenidos en correos electrónicos de origen desconocido.
- Intente no abrir correos donde no conozca al remitente.
- Trate de navegar por sitios seguros.
- Intente utilizar ordenadores de confianza para acceder a sitios donde necesita ingresar claves.

Para saber más sobre la seguridad de BBVA introduzca www.bbva.com.uy en el navegadores ingrese al link Medidas de Seguridad.

¿Cómo se ven los mails fraudulentos?

A continuación se muestran dos ejemplos de mails fraudulentos.

- Ejemplo 1: *BBVA net Office*

BBVAnet OFFICE. Su cuenta ha sido temporalmente suspendida por razones de seguridad. Nuestro Centro de Seguridad ha detectado algunos datos incorrectos de su cuenta. Para reactivar su cuenta haga clic en el enlace de abajo:

http://bbvanetoffice.com/cuenta_activar/userno/21726

Gracias por su tiempo

- Ejemplo 2:

From: oficina@bbvasseguridad.es

Subject: Cuenta temporalmente bloqueada

Date: Sun, 25 Apr 2010 00:15:51 +0300

Estimado poseedor de la cuenta de BBVA, Hemos determinado recientemente que las computadoras diferentes han apuntado en su cuenta de BBVA, y múltiples fracasos de la contraseña fueron presentes antes de las entradas a sistemas. Nosotros ahora le

necesitamos confirmar su información de cuenta. Si esto no es completado en las siguientes 24 horas, seremos forzados a suspender su cuenta indefinidamente, como puede haber sido utilizado para propósitos fraudulentos. Gracias para su cooperación en esta manera y nosotros nos disculpamos para cualquier inconveniente.

Para confirmar sus registros de cuenta de BBVA, por favor clic en la conexión siguiente o lo entra en su examinador de Internet:

hhttp://75.127.66.159:8010/www.bbva.es/TLBS/tlbs/esp/segmento/particulares/index.htm

La NOTA: Si usted recibió este mensaje en usted carpeta de ENVIA SPAM/BULTO, eso es a causa de las restricciones aplicadas por su proveedor de servicios de Internet. Gracias para su paciencia en este asunto. Servicio de atención al cliente de BBVA. Por favor no conteste a este correo electrónico como esto es solo una notificación. El correo mandado a esta dirección no puede ser contestado.

ANEXO III

COMERCIO QUE CUMPLE CON NORMAS DE COMPRA SEGURA

A través de este anexo, se observa un ejemplo de un comercio que cumple con normas de seguridad para compras por e-commerce. A través de su página web informa de qué manera se protege la información de los usuarios, como así también que el comercio no almacena los datos de las tarjeta de crédito empleadas en las transacciones, debiendo el tarjetahabiente volver a ingresar la información de la misma en caso de una nueva compra.

Además aclara que cuenta con certificación PCI, que se verá con detalle en anexo siguiente.

- English
- Español
- Português
- Otros Países

Compras Seguras

En copaair.com nos regimos bajo los más altos estándares de seguridad. Todas sus transacciones en línea son protegidas con tecnología SSL certificada por VeriSign. Esta tecnología permite el cifrado de toda la información confidencial durante las transacciones en línea. El sitio también cuenta con una certificación de McAfee SECURE contra ataques externos y se actualiza diariamente.

En copaair.com no se almacenan los datos de su tarjeta de crédito una vez efectuada la compra. Por esta razón, cada vez que realiza una transacción, deberá ingresar los datos de seguridad de su tarjeta de crédito nuevamente.

Contamos con certificación PCI que involucra toda la tecnología y procedimientos que aseguran la integridad de la información de las tarjetas de crédito, siendo así manejadas íntegramente.

Código de seguridad de mi tarjeta de Crédito (CVV)

Para verificar el código de seguridad de su tarjeta de crédito usted debe revisar el respaldo de ésta. Dependiendo de la franquicia a la que pertenezca el lugar en donde se encuentra puede variar:

Visa y MasterCard:

*El código de seguridad de las tarjetas Visa y MasterCard son los **3 últimos dígitos** que aparecen en el panel de firma en el reverso de su tarjeta.*

American Express:

*El código de seguridad de las tarjetas American Express es un código de **4 dígitos** impreso en el frente de su tarjeta, arriba de su número de cuenta.*

Sistema de verificación de dirección (AVS)
AVS - Address Verification System - Es una de las medidas de prevención de fraude electrónico que consiste en comparar la dirección que aparece en el estado de cuenta de la tarjeta de crédito proporcionada por el cliente con la dirección registrada con la compañía de la tarjeta de crédito. Sólo aplica para Estados Unidos y Canadá.

ANEXO IV

BREVE HISTORIA Y CONCEPTUALIZACION SOBRE NORMAS PCI DSS

En Enero de 2005, las cinco principales marcas de tarjetas de pago de todo el mundo, es decir American Express, Discover Financial Services, JCB, MasterCard y Visa, colaboraron en la elaboración de un estándar internacional para proteger la información de los titulares de tarjetas.

El resultado obtenido fue el Estándar de Seguridad de Datos, del inglés Data Security Standard (DSS) de la Industria de Tarjetas de Pago, del inglés Payment Card Industry (PCI), el cual es una recopilación de las mejores prácticas para asegurar los datos durante todo el ciclo de vida de la información.

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en los procesos de las tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirentes, entidades emisoras y proveedores de servicios, así como también todas las demás entidades que almacenan, procesan o transmiten datos de titulares de tarjetas. Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos. A continuación, se realizará una descripción general de los **doce requisitos** de las PCI DSS, los cuales están comprendidos en **seis áreas lógicas de operación** u “objetivos de control”. Los mismos son:

Desarrollar y Mantener una Red Segura

1. Instalar y mantener una configuración de cortafuegos para proteger la información confidencial de los usuarios

2. No usar contraseñas del sistema y otros parámetros de seguridad provistos por los proveedores.

Proteger los Datos de los usuarios de tarjetas de crédito

3. Proteger los datos de usuarios de tarjetas almacenados por la compañía.

4. Cifrar los datos de usuarios de tarjetas y la información confidencial transmitida a través de redes públicas abiertas o desprotegidas.

Mantener un Programa de Gestión de Vulnerabilidades

5. Usar y tener actualizado el software antivirus.

6. Desarrollar y mantener sistemas y aplicaciones seguras.

Implementar sólidas Medidas de Control de Accesos

7. Restringir y controlar el acceso a la información confidencial teniendo en cuenta las necesidades de acceso por parte de empleados a la información.

8. Asignar una identificación única a cada persona que tenga acceso a un ordenador de la compañía.

9. Restringir el acceso físico a los datos de los usuarios de tarjetas almacenados.

Monitorización y pruebas continúas de las Redes

10. Rastrear y monitorear todo el acceso a los recursos de la red y a los datos de los usuarios de tarjeta.

11. Probar regularmente los sistemas y los procesos de seguridad.

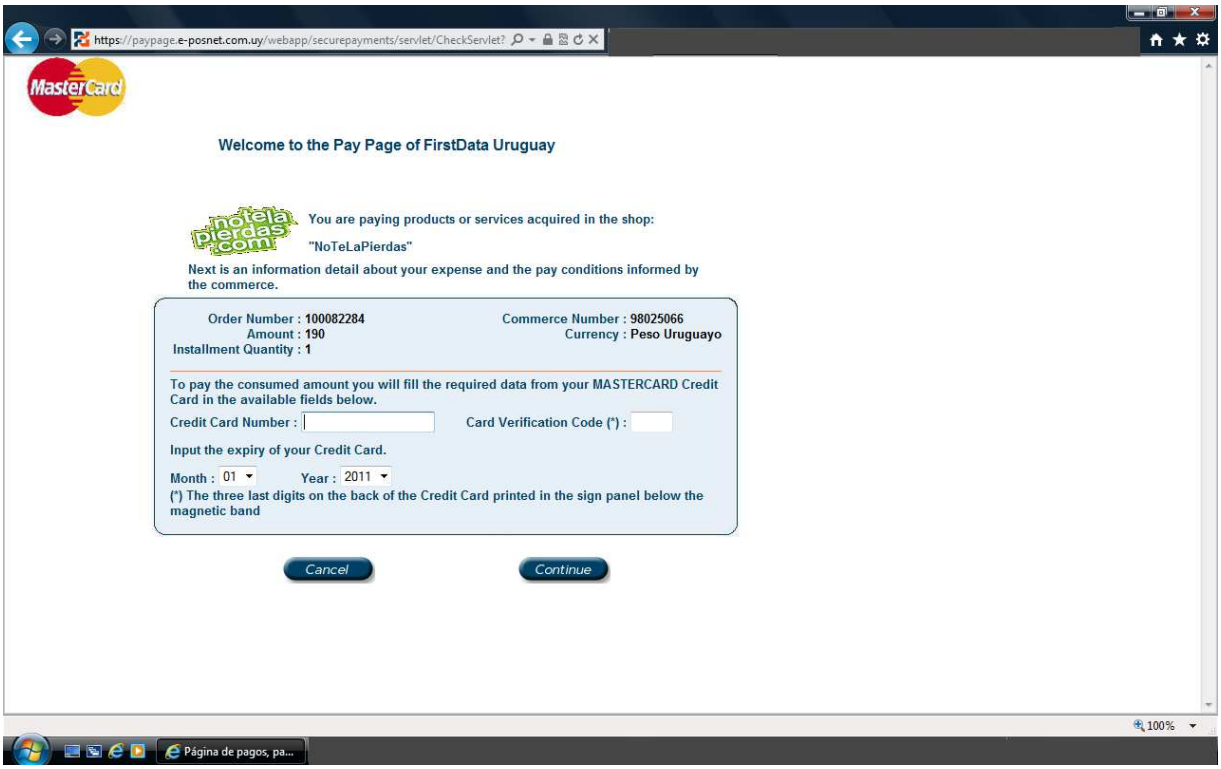
Implementar y Mantener una Política de Seguridad de la Información

12. Mantener una política que contemple la Seguridad de la Información.

ANEXO V

COMERCIOS QUE NO CUMPLEN CON NORMAS DE COMPRA SEGURA Y QUE UTILIZAN LOS SERVICIOS DE FIRST DATA Y VISANET RESPECTIVAMENTE

A continuación se muestran dos ejemplos de comercios que no cumplen con normas seguras para que el tarjetahabiente pueda realizar compras a través de e-commerce. Los mismos deben utilizar los servicios de los procesadores adquirentes más importantes de plaza como lo son First Data y Visanet respectivamente, para poder realizar sus ventas vía Internet.



Datos de Compra

Comercio:	WOOW
Nro. de orden:	200258548
Nombre :	Danilo Baltierra
Monto:	$ 270.00

Datos de Tarjeta

Número de Tarjeta:

4128xxxxxxx9300 VISA

Código de Seguridad:

010

(3 últimos dígitos del reverso de su tarjeta)

Fecha de expiración:

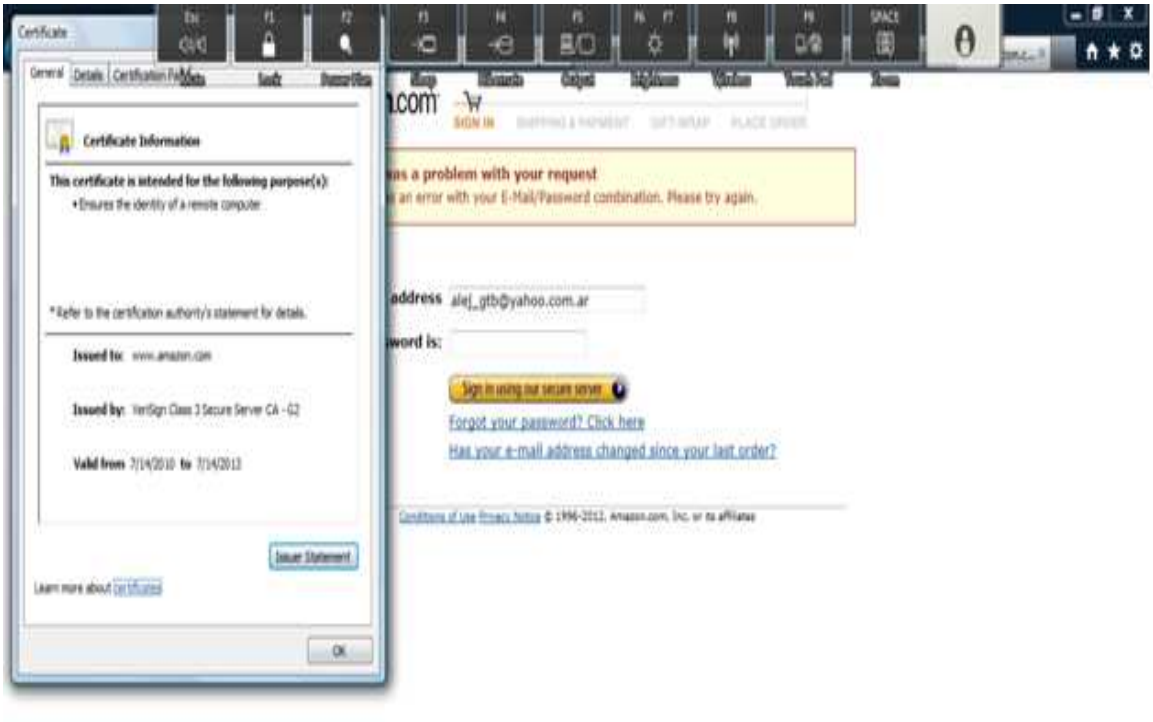
Mayo Mes

2011 Año

Cancelar Continuar

ANEXO VI

CERTIFICADO DE SEGURIDAD



ANEXO VII

FECHA (Date):
dd/mm/aaa

RECLAMO TARJETAHABIENTE VISA
(VISA CARDHOLDER DISPUTE)

Caso:

NRO. TARJETA (Card Number) : ____ - ____ - ____ - ____

NOMBRE DEL BANCO EMISOR (Issuer Name) :

NOMBRE DE T/H (C/H Name) :

DETALLE DE TRANSACCIÓN(ES) RECLAMADA(S). (Claimed Transaction(s) Details)

COMERCIO (Merchant)	FECHA (Date)	MONEDA	IMPORTE (Amount)
		$	
		$	
		$	
		$	
		$	

* (En caso de tener más transacciones, se deberá completar un nuevo formulario)

MOTIVO DE RECLAMO (Claim Reason)

-Desconocimiento de Transacción(es) originada(s) por robo/extravío de tarjeta:

☐ **Mi tarjeta de crédito fue** (My credit card has been): ☐ **perdida** (lost) **el día** (date): ____
Lugar (Place): ____ ☐ **robada** (stolen)

-Desconocimiento de Transacciones sin existir robo/extravío de tarjeta:

☐ **Declaro que la transacción no fue realizada por mi** (I hereby declare that the transaction(s) was not performed by me)
☐ **Declaro que mi tarjeta de crédito estuvo siempre en mi poder** (I hereby declare that my credit card has always been in my possession)
☐ **No autoricé ni participé en la transacción** (I have neither authorized nor participated in the transaction)

(Para poder gestionar este motivo de reclamo se deberán marcar las tres opciones y bloquear la tarjeta con código 95 (fraude), de lo contrario el mismo no será procesado).

-Diferencias originadas en su procesamiento o por incumplimiento de servicio:

☐ **T/H no recuerda la transacción , solicita información adicional para identificarla.** (C/H does not recognize the transaction, additional information is needed to assist the C/H in identifying it)
☐ **Cargo duplicado** (Duplicate Transaction)
☐ **Pago por otros medios, adjunto comprobante** (Paid by other means, see attached receipt)
☐ **Cupón de crédito adjunto no procesado.** (The enclosed credit voucher has not been processed)
☐ **No recibí los servicios/mercadería que me debitaron** (I have not received the services/merchandises charged)
☐ **Debito automático cancelado** (Cancelled recurring transaction)
☐ **Transacción en** ☐ **cuotas procesada contado , adjunto comprobante**
☐ **Reserva de Hotel cancelada el día:** ____ **con el Código de Cancelación Nro.:** ____
(Hotel Reservation cancelled on) (Cancellation Code)
☐ **Importe incorrecto o alterado, adjunto comprobante** (Incorrect or altered amount, see attached receipt)
Importe correcto (original amount): $ ____ Importe facturado (billing amount): $ ____

- Otros (Others): ____

Firma del T/H (C/H Signature) : _____ Se adjunta documentación? S / N Nro.hojas: ☐

Montevideo, ... de ..... de .....

Señores
Banco
Presente.

Ref. Nro: .....

Socio: .....

De mi consideración:

Por la presente solicito a Uds. me sean reintegrados los gastos que he reclamado por el cupón de referencia, en el formulario de ..... de fecha ..... correspondiente a la tarjeta ..... a nombre de ....., número de Socio ....., resumen de cuenta con cierre ..... y vencimiento de pago .....

En caso que ..... no reconozca la devolución de estos gastos, autorizo irrevocablemente a su Banco a:

1) debitar nuevamente en mi resumen de cuenta el importe correspondiente a los gastos reclamados más los intereses más IVA que se hubieran devengado, calculados a la tasa de interés de financiación que figura en el Estado de Cuenta respectivo;

2) debitar en mi resumen de cuenta en concepto de gastos de administración por el trámite de reclamación efectuado,U$S 25. más IVA- por cupón sea en caso de Cupones Locales como de Cupones Internacionales.

Sin otro particular, saludo a Uds. atentamente.

Firma: .....

Nombre: .....

C.I.: .....

ANEXO VIII

CASOS DE FRAUDE QUE TRASCENDIERON EN LA PRENSA

A continuación, se transcribe un ejemplo real publicado en el diario "La República" el 2 de julio de 2001, ocurrido a un uruguayo en el exterior con una tarjeta de crédito emitida en nuestro país:

*"**Un profesional uruguayo fue víctima de un fraude en República Dominicana: copiaron la banda magnética de su tarjeta de crédito y utilizaron U$S 10 mil de su cuenta. Las corporaciones crediticias y los bancos devuelven el dinero a los usuarios**.*

Cuando revisaba su correo atrasado y fijó la vista en el sobre del estado de cuenta mensual de su tarjeta de crédito, el doctor Jorge Irisity no percibió que, como música de fondo de esa escena de su vida, sonaban los acordes de la serie "En la Dimensión Desconocida". Al abrir la correspondencia, la factura de su Oca-Visa del mes de marzo incluía gastos por más de U$S 10 mil.

Abogado y consultor internacional en economía de empresas públicas, Irisity recién había llegado del exterior, al finalizar un contrato que lo mantuvo durante varios meses al frente de un equipo de asesoramiento requerido por el gobierno de República Dominicana. Durante ese tiempo no había controlado el movimiento que se registraba en su cuenta.

Hombre de leyes y dotado de singular paciencia (supo resistir largas sesiones parlamentarias en las ocasiones en que le tocó ingresar al Senado como suplente de Reinaldo Gargano o José Korzeniak), Irisity realizó los trámites de reclamo como cualquier otro mortal sin influencias.

Pese a su inicial escepticismo, confirmó que el servicio de atención al cliente de Oca Casa Financiera lo trató "maravillosamente" y que el propio gerente, Alvaro de Ferrari, le dijo que se despreocupara del tema, que la cuenta no le sería cobrada mientras se confirmaba la validez o falsedad de los bouchers respectivos en los lugares donde se concretaron las transacciones.

Una pizza demasiado cara

Irisity pasó de la sorpresa al asombro cuando a Oca fue llegando el origen de sus supuestos gastos: "Aparecieron cuentas en España, donde no viajo desde hace cinco años y, lo que se me adjudica en República Dominicana corresponde a períodos en los que, o no estaba en ese país, o pertenece a sitios donde nunca estuve, comercios que no existen, o compras que nunca hice".

A través de una colega dominicana, Irisity logró obtener copias de algunos gastos insólitos entre los que se incluye una compra por mil dólares en una ferretería, otra cuenta por una cifra similar por una consulta médica, la adquisición de gasolina equivalente a unos sesenta tanques llenos, o fastuosas cenas en restaurantes de lujo.

Lo curioso es que Irisity no perdió nunca su tarjeta de crédito y sólo recuerda haberse separado una vez del documento: "Cuando pagué unas pizzas para el equipo de la consultora y el vendedor desapareció unos segundos de mi vista con la tarjeta… Serían las pizzas más caras de la historia", se resigna.

La tarjeta de crédito de Irisity fue "clonada": se copió el contenido de la banda magnética, se mantuvo el número 4916 6910 4844 5002, se modificó una letra al apellido otorgando la titularidad a un supuesto ARISITY/JORGE y se inventó una nueva firma que, incluso, es diferente en sendos recibos de compra recuperados en Dominicana."

Fuente: http://www.lr21.com.uy/sociedad/48154-clonaron-una-tarjeta-de-credito-y-le-cargaron-us-10-mil-a-su-cuenta

Se transcribe ahora un ejemplo real, publicado en el diario "El Pais" el 15 de marzo de 2011, por robo de datos a tarjetas de crédito a través de Internet, cometiendo fraude con las mismas en Uruguay:

"Son 15 los detenidos por estafa con tarjetas de crédito

El juez penal Gabriel Ohanian continuará mañana con la indagatoria de los quince acusados de pertenecer a una organización que estafó a una empresa emisora de una tarjeta de crédito internacional por más de cien mil dólares.

No se descarta que la maniobra también haya perjudicado a otros emisores.

La denuncia fue radicada por la empresa emisora de la tarjeta de crédito luego que cientos de tarjetahabientes residentes en el exterior del país comenzaron a denunciar la aparición de cargos por recarga de celulares que no habían ordenado.

La Policía de Maldonado detuvo el pasado lunes a quince personas por su presunta responsabilidad en la maniobra con tarjetas de crédito, lideradas por dos jóvenes, uno de 21 y otro de 25 años.

Entre los detenidos se encuentra la madre de los dos jóvenes, otros hermanos e integrantes de la misma familia y otros sujetos que actuaron como revendedores de los "servicios prestados" por estas personas.

También fue detenida una funcionaria de un juzgado de la ciudad de Florida, quien había advertido a varios integrantes de la banda que sus casas serían allanadas por la Policía.

LA OPERACIÓN. Los ahora detenidos habían montado un servicio de recargo de celulares que era descontado de tarjetas de crédito emitidas a favor de personas residentes en el exterior del país, los cuales jamás pisaron el territorio nacional.

Los dos sujetos organizaron una red de revendedores que eran encargados de brindar el servicio de recarga de teléfonos con precios por debajo de su valor de mercado.

Un interesado se contactaba con los revendedores y podía cargar su celular con mil pesos apenas pagando la cuarta parte de ese valor. Los revendedores cargaban luego esos mil pesos a la cuenta de alguna de las tarjetas de crédito que tenían acceso por su relación con otros delincuentes extranjeros. La recarga se hacía en los sitios web de las empresas que prestan el servicio de telefonía celular del país. Tras ello, se repartían los doscientos pesos cobrados en efectivo.

La maniobra comenzó a gestarse casi dos años atrás y a medida que fueron pasando los meses la misma fue extendiéndose a otros puntos del territorio nacional.

Los responsables de la banda habían logrado acceder a los números y códigos de tarjetas de crédito manejados por delincuentes internacionales en diversos sitios web de Argentina y de Colombia. Por el servicio los responsables locales giraron miles de dólares al exterior.

Los ahora detenidos habían sido indagados y detenidos dos años atrás cuando la Policía investigó una maniobra mediante el mismo sistema para adquirir en ese caso electrodomésticos en casas del ramo. Los sujetos no pudieron ser procesados entonces por la falta de pruebas.

Sin embargo, los policías de Maldonado continuaron investigando a esta banda durante los últimos dos años. El lunes todos los involucrados fueron detenidos y puestos a disposición del juez penal Gabriel Ohanian."

Fuente: http://www.elpais.com.uy/110315/ultmo-553557/ultimomomento/Son-15-los-detenidos-por-estafa-con-tarjetas-de-credito/

El siguiente ejemplo, fue publicado por el diario La República con fecha 15 de Noviembre del presente año (dada la fecha de entrega de este trabajo se puede considerar como de actualidad):

Detienen a tres ciudadanos colombianos por compras con tarjetas truchas

Tienen antecedentes por estafa en el exterior. Gastaron unos US$ 30.000 en Punta del Este y Maldonado

Tres ciudadanos colombianos deberán comparecer este jueves por la tarde ante la jueza de turno de Maldonado Marcela Vargas por estar implicados en decenas de compras con tarjetas de crédito clonadas. Se trata de personas con antecedentes por estafa fuera del país.

Los colombianos habían realizado compras por valor superior a los US$ 30.000 en una decena de comercios de Punta del Este y Maldonado, tras arribar desde Argentina.

Entre los productos que compraron con las tarjetas truchas se encuentran una decena de teléfonos celulares, cuatro tablets, relojes y ropa, dijeron a El Observador fuentes policiales.

Los sospechosos fueron detenidos ayer de tarde por funcionarios de la seccional de Punta del Este luego de que los trabajadores de una estación de servicio del balneario dieran cuenta de que los tres ciudadanos extranjeros, ahora detenidos, habían mostrado una actitud sospechosa al cancelar una compra con una tarjeta de crédito de una financiera internacional.

La Policía del Maldonado ya había sido alertada por la Jefatura de Montevideo de que los colombianos –con profusos antecedentes por estafa- podían estar en el balneario.

Tras mirar las imágenes de las cámaras de seguridad de la estación de servicio los efectivos de la 10ª iniciaron la búsqueda. Los efectivos montaron un operativo en el hotel donde se hospedaban los colombianos, y cuando a media tarde los delincuentes pretendieron retirarse del establecimiento fueron detenidos con los productos que habían adquirido y las tarjetas.

Fuente: http://www.elobservador.com.uy/noticia/237081/detienen-a-tres-ciudadanos-colombianos-por-compras-con-tarjetas-truchas/

ANEXO IX

RESPONSABILIDAD VISA

Lo desarrollado en este anexo, fue extraído de la página oficial de Visa para los Estados Unidos de América. En la misma se puede observar cómo se informa al usuario acerca de su responsabilidad en caso de utilizar una tarjeta de crédito con su sello.

Es fácil. Compra cualquier cosa dentro o fuera de Internet, sin ningún riesgo en absoluto.
Usa tu tarjeta Visa para hacer compras por Internet o en una tienda, y estarás protegido contra el uso no autorizado de tu tarjeta o de tu información de la cuenta. Con la política de protección contra fraude Cero Responsabilidad* de Visa, tu responsabilidad por transacciones no autorizadas es de US$0. ¡No pagas nada!

En esta página

Cero Responsabilidad te tiene cubierto:

- Compras sin preocupaciones
- Lo último en seguridad
- Protección completa contra fraude

No debas nada en transacciones fraudulentas
La política de protección contra fraude Cero Responsabilidad de Visa significa 100% de protección para ti. La política ampliada de Visa te garantiza máxima protección contra fraude. Ahora tienes protección completa de responsabilidad para todas las transacciones de tu tarjeta que se realicen en el sistema de Visa. Si alguien te roba tu número de tarjeta mientras estás de compras, dentro o fuera de Internet, no pagarás nada por dicha actividad fraudulenta. Si te das cuenta de alguna actividad fraudulenta en tu tarjeta, comunícate de

inmediato con tu institución financiera para reportarlo. Es importante que revises tu estado de cuenta continuamente para identificar cualquier transacción no autorizada.**

La política de protección contra fraude Cero Responsabilidad de Visa entró en vigencia el 4 de abril de 2000, y constituye una gran mejora en comparación con la política previa. La política previa requería que reportaras la actividad fraudulenta dentro de dos días hábiles del descubrimiento. Luego de este período de dos días, podrías ser responsable de hasta US$50 de los cargos no autorizados. Con la nueva política de protección contra fraude Cero Responsabilidad, ya no se te requiere reportar actividad fraudulenta dentro de dos días y no eres responsable por ninguna transacción fraudulenta realizada a través de la red Visa.

La política de protección contra fraude Cero Responsabilidad cubre todas las transacciones no autorizadas de tarjeta de crédito y débito Visa procesadas a través de la red Visa, dentro o fuera de Internet. Las únicas transacciones que no están cubiertas bajo la política de protección contra fraude Cero Responsabilidad son transacciones de tarjetas comerciales, cajeros automáticos y números de identificación personal que no sean de la marca Visa.

Para transacciones en otras redes, la decisión de responsabilidad debe ser hecha por la institución financiera que emitió tu tarjeta. El emisor tiene la opción de extender las mismas protecciones provistas por la política de la garantía de protección contra fraude Cero Responsabilidad de Visa.

Obtén crédito provisional rápido para reponer las pérdidas por fraude

La política de protección del titular de la tarjeta Visa establece que todas las instituciones financieras que emitan productos Visa otorguen crédito provisional por pérdidas debido al uso no autorizado de la tarjeta dentro de los cinco días hábiles a partir de la notificación de la pérdida. Sin embargo, muchas de las principales instituciones financieras afiliadas con Visa pueden emitir crédito provisional más temprano: de 24 a 48 horas después de que la pérdida sea reportada.

Compra con seguridad gracias a Visa

Visa toma la seguridad por Internet muy en serio para que puedas hacer tus compras por Internet con seguridad. Con el apoyo de bancos asociados, Visa ha invertido millones de dólares en la construcción de un sistema de pago seguro. Visa trabaja con los organismos policiales y compañías de tecnología para mantenerse siempre un paso más adelante que los criminales.

Como resultado de estos esfuerzos, el fraude, como porcentaje de nuestro volumen total, se ha ido reduciendo con el tiempo. A principios de 1990, el fraude daba cuenta de aproximadamente 0.15 por ciento del total del volumen de transacciones de Visa; hoy es apenas 0.06 por ciento: eso es menos que 1/13 del uno por ciento.

Con la garantía de protección contra fraude Cero Responsabilidad, Visa sigue siendo líder en la industria de pago de tarjetas en protección del consumidor. Aunque el fraude con tarjetas es extremadamente raro, la política de Visa elimina cualquier riesgo al que te enfrentarías haciendo compras dentro o fuera de Internet.

Estás protegido con Visa

Visa tiene instaladas soluciones de detección de fraude altamente sofisticadas, y trabaja con compañías de tecnología todos los días para aumentarlas. Los comerciantes también reciben capacitación de Visa sobre protección contra fraude.

Visa también asigna códigos de verificación del titular de la tarjeta en el dorso de las tarjetas para ayudar a los comerciantes a comparar las tarjetas usadas para hacer compras con sus titulares de la tarjeta autorizados. Los emisores de tarjetas Visa deben tener estos códigos en todas las tarjetas nuevas emitidas a partir de 2001. El servicio de verificación de dirección de Visa también ayuda a los comerciantes a detectar transacciones de tipo "tarjeta-no-presente".

Sin importar dónde hagas tus compras, disfruta de la comodidad de saber que estás protegido con Visa.

* Cubre solamente las tarjetas emitidas en los EE.UU. La política de Cero Responsabilidad de Visa no se aplica a tarjetas de crédito comerciales, transacciones en cajeros automáticos (ATM) o a transacciones con número de identificación personal (PIN) no procesadas por Visa. El titular debe notificar al emisor de la tarjeta de cualquier uso no autorizado. Consulta al emisor para obtener detalles adicionales.

Fuente: http://usa.visa.com/espanol/seguro/cero_responabilidad.html

ANEXO X

ENCUESTA

A continuación se entrega una encuesta realizada sobre una muestra de 70 personas. La finalidad de la misma es visualizar una tendencia en cuanto a patrones de conducta del tarjetahabiente vinculado al conocimiento del mismo sobre el uso y cuidado de la tarjeta.

	RESPUESTAS		
Preguntas	**SI**	**NO**	**A VECES**
1. ¿Posee tarjeta de crédito?	90%	10%	0%
2. ¿Lleva siempre consigo el plástico?	55%	29%	16%
3. ¿Cuando no lo tiene con usted, lo guarda en un lugar seguro?	60%	40%	0%
4. ¿Revisa periódicamente el plástico?	13%	71%	16%
5. Si descubre que perdió el plástico, o se lo roban. ¿Sabe lo que tiene q hacer?	80%	20%	0%
6. ¿Toma usted los recaudos necesarios para el uso de la misma?	60%	27%	13%
7. Cuando entrega el plástico para realizar un pago. ¿Sigue atentamente los movimientos que hacen con el mismo?	10%	74%	16%
8. ¿Conoce lo que es el Phishing o Ingeniería Social?	19%	81%	0%
9. ¿Si le llega un mail o un llamado telefónico, pidiéndole datos personales como el número de tarjeta, usted los dice?	0%	100%	0%
10. ¿Conoce las precauciones a tener en cuenta para comprar seguro en Internet?	20%	80%	0%

11. ¿Compra habitualmente por Internet?	13%	55%	32%
12. ¿Compra habitualmente por venta telefónica?	10%	80%	10%
13. ¿Usted compartiría con un tercero datos personales de su cuenta?	0	90%	10%
14. ¿Lee usted los folletos que aparecen en los estados de cuenta?	48%	32%	20%
15. ¿Le llega a usted información acerca de formas para prevenir el fraude o engaño con tarjetas de crédito?	10%	74%	16%
16. ¿Revisa su estado de cuenta?	80%	10%	10%
17. ¿Guarda la documentación de las compras, revisa al momento de hacer la transacción los datos ingresados en el voucher?	61%	19%	20%
18. ¿Tiene los números de tarjeta anotados en algún lugar?	13%	87%	0%
19. ¿Tiene débito automático para pagar la tarjeta?	14%	86%	0%

ANEXO XI

TARJETA CON CHIP

Este tipo de tarjetas se diferencia de las tarjetas de crédito convencionales porque en lugar de tener la respectiva banda magnética en la cara trasera de la misma, tendrán un chip en la parte delantera de la misma como se aprecia en la siguiente imagen:

Una banda magnética en el reverso de una tarjeta de crédito transmite información numérica sencilla a la terminal del POS cuando se desliza. Posteriormente, la terminal envía la información a una institución financiera para su autorización y el tarjetahabiente firma un recibo emitido por la respectiva terminal después de la aprobación.

Ventajas

En lugar de deslizar la tarjeta para comunicar su información del pago, la tarjeta con chip se inserta en una terminal y permanece allí mientras dura la transacción. El chip almacena las reglas de autorización del emisor electrónicamente; puede aprobar una compra fuera de línea o pedir la autorización en línea, dependiendo de las circunstancias. Según sea el caso, la tarjeta con chip también puede verificar el PIN o NIP (Número de Identificación Personal) del tarjetahabiente como un medio alternativo de autentificación. El resultado es que se tiene más seguridad, una transacción de pago más ágil y mejor servicio al cliente.

Cuando un tarjetahabiente hace una compra, se inserta la tarjeta con chip en una terminal en el punto de venta (POS) y permanece allí durante la transacción. El chip se comunica con la terminal para validar la identidad del tarjetahabiente y registrar información importante de la transacción. Por lo general, los tarjetahabientes con chip se autentifican con el ya mencionado número de identificación personal, que es un medio más seguro de autentificación que una simple firma.

Las transacciones con chip que usan un PIN proporcionan seguridad adicional para las tarjetas robadas o perdidas. Los negocios que usan chip y PIN en sus terminales reducen significativamente el riesgo generado por el costo de fraudes con tarjetas, sea que los tarjetahabientes ingresen su PIN o su firma, siempre y cuando los cajeros de los comercios sigan las instrucciones indicadas en los mensajes de la terminal y usen las prácticas rutinarias de seguridad indicadas por el procesador adquirente.

Las tarjetas con chip también son más difíciles de falsificar que las tarjetas con banda magnética, convirtiéndolas en un medio muy poderoso para desalentar el fraude.

La tecnología de chip también ofrece más seguridad para los negocios afiliados en línea. En un mayor número de mercados en todo el mundo, los compradores pueden insertar su tarjeta con chip en un lector de tarjetas manual y sencillo e ingresar su PIN para generar una contraseña que los identifica en el sitio web del negocio afiliado. Estas soluciones están ayudando a reducir el fraude y a que las compras en línea sean más redituables para los negocios afiliados.

Por lo tanto, todo lo mencionado anteriormente reafirma que la tarjeta con chip es una posible solución al fraude no solamente para el tarjetahabiente, sino también para los comercios.

A continuación se transcribirá un fragmento de un artículo publicado en la página de MasterCard Internacional para México, la cual menciona algunas de las ventajas de esta tecnología:

Beneficios adicionales de aceptar tarjetas con chip

Mayor seguridad

Cuando acepta tarjetas con chips, obtiene varias ventajas de seguridad.

- *Las tarjetas con chip son más difíciles de falsificar y así se reduce el número de fraudes.*

- *El uso de un NIP proporciona una característica adicional de seguridad para las tarjetas perdidas o robadas.*

- *Cuando las tarjetas con chip reemplazan el efectivo, se reduce el riesgo de manejar y guardar dinero. El reemplazo de efectivo por tarjetas con chip reduce los riesgos que se corren al manejar y guardar efectivo.*

- *Las tarjetas con chip reducen el potencial de cometer errores y tener pérdidas porque eliminan la necesidad de hacer conciliaciones en papel. Los registros de las transacciones para los pagos de tarjetas con chip son totalmente electrónicos. Además cada transacción que sea aprobada o declinada deja un rastro digital denominado "Criptograma" que puede ser una herramienta muy útil para validar que la transacción fue genuina.*

- *Las transacciones con chip no dependen de los dependientes que no tendrán que tomar decisiones difíciles sobre la validación de la firma. Lo único que tienen que hacer es seguir las indicaciones de la terminal.*

Procesamiento más ágil

Las tarjetas con chip pueden ahorrarle tiempo y dinero al:

- *Reducir el papeleo, porque son menos los recibos firmados que se tienen que manejar y guardar.*

- *Reducir el procesamiento para el manejo de excepciones, referencias y contra cargos.*

Servicio a clientes más rápido y conveniente:

- *La tecnología de las tarjetas con chip puede dar como resultado un servicio más rápido, que puede significar clientes más satisfechos y un mayor volumen.*

- *Con frecuencia las tarjetas con chip no requieren de autorización adicional. En consecuencia, las transacciones se pueden procesar con mucha mayor velocidad.*

- *Cuando se combinan con el uso de un NIP, no siempre es necesario firmar o archivar un recibo de venta y la caja se abre con menor frecuencia, reduciendo el trabajo y el riesgo.*

- *El chip le proporciona la oportunidad de ofrecer a sus clientes un auto-servicio para que paguen sus productos sin tener que esperar.*

Fuente: http://www.mastercard.com/mx/merchant/es/chip.html

Desventajas

Hay quienes aseguran que con la tarjeta con chip se puede hacer el mismo fraude que con una tarjeta de banda magnética. Según esta teoría, es pura y exclusivamente una maniobra comercial y de marketing por parte de los sellos para migrar todas las tarjetas de crédito de banda magnética a chip con el objetivo de deslindarse responsabilidades en lo que a fraude concierne. Esto significa que de existir fraude con tarjeta de banda magnética será responsabilidad del tarjetahabiente o del respectivo comercio por no haberse adaptado a la nueva tecnología del chip.

Si bien por un lado es más difícil de falsificar que una tarjeta de banda magnética, por otro no es mucho más complejo copiarle los datos. Esto permitirá entonces, otra modalidad de fraude que es la de copiar los datos de una tarjeta con chip en un mercado donde éste está instalado para poder usarla en un mercado donde solamente existe banda magnética. Un claro ejemplo puede ser el de una tarjeta con chip a la cual se le copian los datos en determinado país donde esta tecnología está instalada. Luego de esto, el defraudador se traslada hacia otro lugar para utilizar la misma. Ya no existe la tarjeta con chip, sino que los datos que estaban en ésta fueron copiados y trasladados a una banda magnética que forma parte de una nueva tarjeta falsificada. El delincuente entonces, tratará de utilizar la misma en un lugar en el cual el sistema de chip no es obligatorio. Si se trasladara a otro lugar, en el cual solamente se exigiera tarjeta con chip, este tipo de fraude no podría ser cometido porque la banda magnética ya no sería aceptada.

En lo que respecta a compras por internet, se han detectado ciertas transacciones a través de las cuales no fue necesario utilizar el PIN para su respectiva autorización, lo cual permite su uso con solamente copiar los datos.

Por lo tanto, se ve que el chip no detiene sino que complica en alguna medida el fraude porque requiere que los criminales se actualicen en lo que respecta a esta nueva tecnología. Hay quienes han demostrado que el chip en ningún lado bajó significativamente el fraude total de tarjetas de crédito. Sí ha hecho que el mismo se mueva hacia otros tipos de fraude como Internet o que se mueva hacia países limítrofes que aún no han migrado al chip. Por lo tanto la tarjeta con chip no es impedimento para el fraude sino una complicación mayor para los delincuentes o un traslado geográfico del fraude.

Responsabilidad

Respecto a las reglas operativas que imponen los sellos a nivel internacional en cuanto a la responsabilidad ante casos de fraude, cada vez existe más presión hacia los países con tecnología más vieja (o sea la de banda magnética). Esto es, si la institución financiera

emitió la tarjeta con chip y el respectivo PIN, y el fraude se dio como consecuencia de haber usado solamente la banda, la responsabilidad será cien por ciento del comercio por haber aceptado ese tipo de tarjeta. De cierta manera se va ejerciendo cierta presión económica a los mercados que no migraron a tecnología de chip para que de una vez lo hagan.

A continuación se transcribirá un fragmento de la página web de la empresa EMSA S.A.[24] El mismo trata sobre el sistema EMV[25] para tarjetas de crédito y desarrolla el tema de la responsabilidad ante el fraude para algunos casos en Estados Unidos.

Establecer un cambio en la responsabilidad por fraudes con tarjetas falsificadas
Con vigencia a partir del 1ro de octubre de 2015 Visa se propone instituir en Estados Unidos un cambio en la responsabilidad por las transacciones de punto de venta (POS) domésticas y a través de fronteras realizadas con tarjeta presente con un plástico falsificado. Los comercios de venta de combustible tendrán dos años más, hasta el 1ro de octubre de 2017, antes que el cambio de responsabilidad cobre vigencia en el caso de las transacciones generadas en surtidores automatizados de combustible. Actualmente los emisores de tarjetas absorben la mayor parte del fraude con tarjetas falsificadas en el punto de venta. Con la implementación del cambio de responsabilidad, si se presenta una tarjeta de chip con contacto a un comercio que no haya adoptado, como mínimo, las terminales habilitadas para chip de contacto, la responsabilidad por el fraude con la tarjeta falsificada podría recaer en el adquirente del comercio. Este cambio estimula la adopción del chip, ya que cualquier transacción chip a chip (tarjeta de chip leída en una terminal de chip) proporciona autenticación dinámica de datos, la cual ayuda a brindar una mejor protección a todos los participantes.

En el futuro, a medida que la infraestructura de pago en el punto de venta evolucione de la banda magnética estática a dispositivos inteligentes como las tarjetas de chip EMV y los teléfonos móviles habilitados con la tecnología de comunicación de campo cercano, es crucial que los tarjetahabientes puedan continuar realizando pagos convenientes, seguros y confiables también en el caso de las transacciones con tarjeta no presente. Visa está diseñando su nueva billetera digital con la funcionalidad "clic para comprar", capaz de soportar la autenticación dinámica a través de múltiples canales que incluyen el ambiente de comercio electrónico. Visa también continuará mejorando las herramientas de

[24] EMSA S.A.: Empresa uruguaya que brinda servicios de soluciones integrales para el procesamiento de medios de pago.

[25] Tarjetas EMV: Europay MasterCard Visa, lleva el nombre de las tres compañías que han desarrollado el proyecto, el cual consiste en una tarjeta con chip que autentica pagos mediante tarjetas de crédito y débito.

detección de fraude inteligentes en la red como la Autenticación Avanzada de Visa y las alertas de transacción al tarjetahabiente, a fin de complementar los métodos de autenticación dinámica y basada en riesgo. Como siempre, la prevención eficaz del fraude requiere múltiples capas de seguridad.

Fuente: http://www.emsa.com.uy/macros/TextContent_M.jsp?contentid=276&version=1

Actualidad en nuestro país

Hoy en día en nuestro país todas las tarjetas de crédito poseen banda magnética y se está en un proceso de migración a la tarjeta con chip según información que nos fuera brindada tanto por las instituciones financieras bancarias como también por parte de los procesadores de los sellos Visa y MasterCard. Claro que aún no se sabe con exactitud cuándo nuestro país deberá "migrar" de la banda magnética al chip. Según las distintas versiones obtenidas, concuerdan en que hasta tanto el mercado latinoamericano no adopte la tecnología del chip, Uruguay no será la excepción. Esto significa básicamente que hasta tanto Brasil y México no lo hagan, nuestro país tampoco. Esto respecto a las instituciones financieras emisoras que son quienes tendrán que cargar con la engorrosa y costosa acción de reemplazar la totalidad de tarjetas de crédito de banda magnética de sus clientes, por tarjetas con chip. Asimismo, las mismas versiones indican que para la parte adquirente en cambio, más del ochenta y cinco por ciento de los comercios de nuestro país cuentan con terminales POS capaces de leer el mismo. De la conjunción de ambas, se puede concluir que dependerá solamente de las instituciones emisoras entonces, que nuestro país adopte dicha tecnología.

Sí hay que dejar en claro, que emitir una tarjeta con chip, puede llegar a ser hasta diez veces más costoso que emitir una tarjeta con banda magnética.

Como las tarjetas con chip no reemplazarán de forma inmediata las tarjetas con banda magnética, tendrán que aceptarse ambas tarjetas durante un tiempo. Las terminales (POS) de chip están diseñadas para funcionar con ambos tipos, para evitar la necesidad de tener dos terminales por separado.

BIBLIOGRAFÍA

ENTREVISTAS REALIZADAS

Entrevistas realizadas a instituciones financieras bancarias

Banco Santander:

- Marcelo Chuayre, Medio de Pago Banco Santander Uruguay
- Rubens Benítez, Medio de Pago Banco Santander Uruguay
- Daniel Gordiola, Medio de Pago Banco Santander Uruguay

Banco de la República Oriental del Uruguay:

- Gustavo González, Gerente Tarjetas de Crédito

Citibank:

- Marianela de Ávila, Supervisora del Área de Cobranzas y Fraudes
- Luis Esoin, Supervisor del Área de Crédito

Banco Itaú:

- Juan Pablo Fernández, Gerente Comercial Tarjetas de Crédito

Nuevo Banco Comercial:

- Daniel Pintos, Jefe de Seguridad

Entrevistas realizadas a instituciones financieras no bancarias

Pronto:

- Alejandra López, Responsable de Contabilidad y Reporting
- María Poladura, Encargada de Reporting

Creditel:

- Marcelo Parodi, Gerente de Préstamos y Tarjetas de Crédito

Oca Card:

- Lourdes Beltrame, Encargada de Cumplimiento

Entrevistas realizadas a procesadores

Sistarbanc:

- Rafael Saldain, Adscripto a Gerencia
- Walter Ascorreta, Encargado de Administración de Riesgos y Seguridad
- Diego Arias, Coordinador de Calidad
- Victoria Soffer, Encargada de Contracargo

First Data:

- Héctor Cabano, Gerente de Administración de Riesgo
- Luis Labadie, Gerente Tecnología y Procesamiento

Entrevista realizada a empresa de desarrollo de software para detección y prevención de fraude

PayTrue:

- Álvaro Rodríguez, Ingeniero de Sistemas
- Ana Laura Olmos, Analista en Marketing

PÁGINAS WEB CONSULTADAS

Banco Central del Uruguay: www.bcu.gub.uy

Banco Comercial: www.bancocomercial.com.uy

Banco Citi: www.citi.com.uy

Banco República: www.brou.com.uy

Banco Itaú: www.itau.com.uy

Banco BBVA: www.bbva.com.uy

Visanet Uruguay: www.visanet.com.uy

First Data Uruguay: www.firstdata.com.uy

Sistarbanc: www.sistarbanc.com.uy

MasterCard (Mexico): www.mastercard.com/mx/merchant/es/chip.html

Visa (U.S.A.): usa.visa.com/espanol/seguro/cero_responabilidad.html

Diario El País: www.elpais.com.uy

Diario El Observador: www.observa.com.uy

Diario La Red 21: www.lr21.com.uy

Security Standards Council (Normas P.C.I.):

- www.pcisecuritystandards.org/pdfs/pci_dss_spanish.pdf
- www.normapci.com/

Bussiness Identification Number: www.bindb.com

Sitios Web con servicio de venta on-line propio (Compra Segura):

- www.amazon.com
- www.copaair.com

Sitios Web con servicio de venta on-line tercerizado:

- www.notelapierdas.com.uy
- www.woow.com.uy

MATERIALES Y BIBLIOGRAFÍA CONSULTADOS

- Committee of Sponsoring Organizations of the Treadway Commission – Informe COSO (Resumen Ejecutivo, Marco de Conceptos y Herramientas de Evaluación)
- Control Interno – Integración de Conceptos.
  Material elaborado por la Cátedra de Control Interno y Organización de Sistemas Contables de la Facultad de Ciencias Económicas y de Administración de la Universidad de la República.
- Normativa Particular 3.8 y Comunicado 2006/195, emitidos por el Banco Central del Uruguay, para la exigencia de información a solicitar por parte de instituciones financieras por el otorgamiento de créditos.
- Definición y Clasificación de Fraude; extraídos del Manual de Operaciones de Visa Internacional, emitido en el año 2006.
- Definición de Fraude; Diccionario de la Real Academia Española, vigésima edición.
- Definición de Fraude; Diccionario Salvat, edición especial para el Diario El País, Montevideo, Uruguay.
- Definición de Fraude; Diccionario Durvan, primera edición.
- Requisitos de las PCI DSS y procedimientos para la evaluación de la seguridad, versión 2.0 Octubre de 2010. PCI Security Standards Council LLC Página 85.

ÍNDICE

Capítulo VII: Evaluación de riesgo de fraude y actividades de control

Capítulo VIII: Conclusiones

Anexos

Bibliografía