Evolución y estructura de los medios de pago

Equipo Técnico de ADICAE

Los medios de pago constituyen la herramienta que los agentes de una economía requieren para transferir valor monetario a fin de pagar por los bienes, servicios y activos financieros que adquieren. Para cualquier economía es fundamental contar con sistemas de pago eficientes y seguros. En la búsqueda de sistemas de pagos eficientes, muchos países se han orientado hacia la rápida adopción de sistemas de pago electrónicos. Las autoridades financieras los han promovido para reducir el riesgo sistémico. Las instituciones bancarias también los han fomentado para proveer un mejor servicio a sus clientes y para reducir sus costos de transacción. Asimismo, muchas empresas e individuos han adoptado medios de pago electrónicos por su flexibilidad, confiabilidad y conveniencia. Aún más, el desarrollo del Internet ha añadido una nueva dimensión al uso de algunos pagos electrónicos tradicionales y ha preparado el terreno para la adopción de nuevos mecanismos tales como el dinero electrónico, los cheques electrónicos y las tarjetas con chip. De este modo los pagos electrónicos han venido ganando terreno.

La gran evolución de los principales medios de pago que se utilizan en España se ha producido, debido especialmente a los avances tecnológicos. Se diferencian medios de pago tradicionales, tales como son los cheques y las tarjetas, y medios de pago no tradicionales, como las transferencias electrónicas. Se aprecia que se ha reducido la importancia de los medios de pago tradicionales mientras que los pagos electrónicos han ganado relevancia. Las tarjetas han registrado un elevado crecimiento apoyado tanto en el desarrollo de la red de cajeros automáticos, como en su amplísima aceptación como medio de pago en puntos de venta. Es notable la pérdida de importancia de los cheques tanto en número como en valor de las transacciones

La adopción de los medios de pago electrónicos se ve condicionada por la capacidad de la población del acceso a nuevas tecnologías, o en su defecto la participación de intermediarios financieros. Del mismo modo, el sistema legal también puede beneficiar o restringir el desarrollo de algunos medios de pago por la lentitud con que se resuelven las controversias; por tanto, el uso de aquellos medios que involucran un mayor elemento de riesgo, como los cheques, se ve afectado negativamente. Los cambios en la regulación también han influido en el uso de los distintos medios de pago. Por ejemplo, los cambios de regulación orientados a fomentar la adopción de pagos electrónicos han dado lugar a un impulso en el uso de las transferencias electrónicas y a un desplazamiento de los cheques o incluso del efectivo frente a las tarjetas de crédito o débito.

Es conveniente señalar la diferencia conceptual que existe entre sistemas y medios de pago. El sistema de pagos es el conjunto de instrumentos, procedimientos bancarios e infraestructura para transferir fondos entre bancos, que garantiza la circulación de recursos; los medios o instrumentos que los propios agentes utilizan para pagar por los bienes, servicios y activos financieros que adquieren, constituyen componentes centrales de los sistemas de pago. Existe una correspondencia entre el desarrollo de un sistema y el uso de los medios de pago asociados con dicho sistema, pues podría pensarse que los medios fluyen a través de la infraestructura de los sistemas.

Se observa que se ha reducido la importancia de los medios de pago tradicionales distintos al efectivo, mientras que los pagos menos tradicionales han ganado participación en el mercado. En el caso de los pagos de alto volumen, las tarjetas han registrado un elevado crecimiento por su absoluta aceptación como medio de pago en puntos de venta. Del mismo modo, los pagos interbancarios han experimentado un incremento significativo. En el caso de los cheques es notable la pérdida de importancia tanto en el número como en el valor de las transacciones.

Los cheques y las tarjetas son los medios de pago distintos al efectivo más tradicionales, sin embargo sigue sin existir una absoluta confianza relacionada con el nivel de riesgo que su uso implica y con el sistema legal que aún no protege claramente al consumidor y que no permite una pronta resolución de los problemas de pago. En contraste los Pagos Interbancarios - cuyas características intrínsecas generan un riesgo menor - están completamente asentados.

El efectivo

El efectivo es el medio de pago más tradicional en el mundo. A pesar ello la información sobre el va-

lor y el número de las transacciones que se realizan en efectivo no está disponible. Este problema se relaciona con la falta de encuestas que permitan el desarrollo de estimaciones adecuadas.

El efectivo posee varias ventajas sobre otros medios de pago. En primer lugar, el efectivo es muy práctico, es divisible y es aceptado en todas partes. En segundo lugar, las transacciones que se pagan en efectivo, son finales; exceptuando la falsificación, no existe un riesgo adicional en una transacción en efectivo y los recursos pueden ser utilizados de inmediato. Esto significa que el efectivo resulta un medio de pago eficiente y seguro para llevar a cabo transacciones de bajo valor. Sin embargo, cuando las transacciones son de un monto considerable, el uso de efectivo presenta ciertas desventajas. En general, no es práctico que los consumidores lleven consigo grandes cantidades de efectivo.

Cajeros Automáticos

Los cajeros automáticos no constituyen un medio de pago, pues no permiten que se realicen pagos entre distintos agentes. Sin embargo, la infraestructura de cajeros puede hacer accesibles las disposiciones de efectivo, por medio, principalmente, de tarjetas. Los cajeros automáticos tienen un doble efecto en las tenencias de efectivo de los individuos. En primer lugar, les permite mantener un saldo más alto en sus cuentas bancarias por medio del retiro de montos más pequeños con más frecuencia - esto reduciría las tenencias de efectivo. En segundo lugar, les permite un fácil acceso al dinero; es decir, el tamaño de la red de cajeros automáticos guarda una relación directa con la probabilidad de que una transacción se lleve a cabo con efectivo, lo cual aumentaría las tenencias. En todo caso, estos dos efectos se contrarrestan; por tanto, la extensión de la red de cajeros automáticos no parece afectar las tenencias de efectivo individuales.

Una operación particular en un cajero automático, involucra al consumidor poseedor de la tarjeta, al banco emisor de la tarjeta, al propio cajero automático -que puede o no ser propiedad del banco que emite la tarjeta- y a la red a la cual tanto el banco emisor como el cajero automático específico están conectados. Los cajeros permiten a los consumidores retirar fondos que son inmediatamente deducidos de sus cuentas bancarias.

La liberalización de los servicios bancarios incrementó el nivel de competencia en la industria; uno de los instrumentos de competencia que los bancos han utilizado para atraer clientes es la extensión de sus redes de cajeros automáticos. En segundo lugar, conforme ha pasado el tiempo, un mayor número de usuarios se ha dado cuenta de la conveniencia de utilizar esta red y se ha familiarizado con ella. De ahí la casi total extensión de este servicio.

Cheques

Los bancos reciben depósitos en forma de cheques de otros bancos para posteriormente realizar la compensación en cámaras de compensación regionales.

Tarjetas de crédito

En una transacción pagada con tarjeta de crédito participan cuatro agentes: el consumidor usuario de la tarjeta que realiza el pago, el banco emisor de la tarjeta, el comercio receptor del pago y el banco del comerciante, denominado banco adquiriente. El banco adquiriente cobra al comercio afiliado un porcentaje del valor de la transacción; el banco adquiriente, a su vez, transfiere la mayor parte de ese porcentaje al banco emisor de la tarjeta puesto que es éste último el que incurre en el riesgo de crédito.

Tarjetas de débito

Los bancos emiten tarjetas de efectivo vinculadas a cuentas de corrientes y de ahorro, estas tarjetas, además de poder usarse como tarjetas de retirada de efectivo, tienen la capacidad de ser un medio de pago directo en multitud de comercios.

Pago Interbancario

Las transferencias de fondos constituyen una importante categoría entre los pagos electrónicos. El Pago Interbancario se utiliza para realizar pagos Cabe destacar que la reciente introducción de la "Banca por Internet" permite a los clientes de los bancos realizar transferencias de fondos electrónicas; estas transferencias están contribuyendo al aumento en el uso del Pago Interbancario, pues se transmiten a través de este sistema.

La protección de los usuarios ante los medios de pago

El uso de medios de pago diferentes al efectivo por parte de los consumidores requiere una confianza en su seguridad, a mayor confianza mayor uso. Los operadores del mercado deben de ser conscientes de este hecho y facilitar a los consumidores

Existen en la actualidad, especialmente por el uso de nuevas tecnología, cada vez más posibilidades de uso de medios de pago, si bien estos medios continúan, debido a la falta de seguridad, sin conseguir una implantación notoria.

La protección de los usuarios frente a los medios de pago continúa siendo insuficiente y en la mayor parte de los casos es el propio consumidor el que debe de iniciar reclamaciones y quejas para defender sus derechos y no ser el último perjudicado por el robo y/o fraude que pueda afectar a su medios de pago.

La protección al consumidor en lo que se refiere a la vía extrajudicial se realiza a través del sistema de Defensor del Cliente (sistema interno de los bancos, que por supuesto no favorece la confianza de los consumidores) y del sistema no vinculante del Servicio de Reclamaciones del Banco de España, además por supuesto de poder operar por la lenta y costosa vía judicial.

Consejos de ADICAE sobre los medios de pago

Equipo Técnico de ADICAE

Además del pago en efectivo, los medios de pago más utilizados por los consumidores son las tarjetas de crédito, aunque no podemos olvidarnos de otras formas de pago como las letras de cambio o los cheques, mucho menos utilizados por los consumidores:

1 Si va a optar por utilizar tarjeta, sepa que existen dos modalidades, las de crédito, que sirven para el pago aplazado, ya que incorporan la posibilidad de solicitar un crédito; y las de débito, que sólo sirven para pagar y no puede solicitarse con ellas un crédito a cuenta. Una tercera clase es la de las tarjetas comerciales, que están orientadas a pagar lo que usted compre en un determinado establecimiento comercial o agrupación de comerciantes.

2 A la hora de solicitar su tarjeta, tenga en cuenta su perfil de gasto mensual, sopese el uso que hará de ella, y decida en consecuencia. Valore, por ejemplo, cuánto acostumbra a gastar, en qué cajeros suele sacar efectivo y si viaja, o no al extranjero.

3 Debe memorizar su número personal nada más recibir la tarjeta y deshacerse cuanto antes del escrito de la entidad en el que se comunica la clave. Si anota el número en la tarjeta, no lo lleve en la cartera o en el bolso.

4 Lleve siempre consigo el número de teléfono al que es necesario llamar para anular la tarjeta en caso de robo o pérdida. Recuerde que una actuación rápida puede ahorrarle muchos disgustos.

5 Si quiere contratar una tarjeta comercial, infórmese bien antes de decidir hacerse con una. Los comercios no cesan de destacar sus innumerables ventajas (gratuidad, descuentos, regalos...), pero no dicen nada sobre sus altísimos intereses en caso de compras a crédito o si limitan la responsabilidad por uso fraudulento en caso de robo o pérdida (no todas lo hacen).

6 Compruebe que el extracto bancario coincide con la cantidad real a pagar. Si usted tiene domiciliado sus pagos a las compañías de agua, teléfono o gas. Los errores son más comunes de lo que parece. Vigilar que las cantidades coincidan cuesta apenas unos minutos y haciéndolo pueden evitarse sorpresas muy desagradables.

7 Si usted opta por pagar a través de una letra de cambio, sepa que poner la firma le hace responsable del pago, aunque luego tenga problemas con lo que ha comprado y quiera cambiarlo o no se le haya entregado. Una excesiva alegría al firmar, en una sociedad de consumo como la actual, puede ponerle en serios aprietos. El impago abre una vía peligrosa: la vía ejecutiva o el embargo inmediato tras un aviso judicial de pago.

CONSEJOS SOBRE TARJETAS DE COMPRA

1 Antes de contratar una tarjeta de compra, infórmese bien, compare y decídase por aquella que usted considere más adecuada a sus necesidades.

2 Lea bien todas las condiciones antes de firmar, pues una vez firmados la tarjeta y el contrato suponen la plena aceptación de todas las condiciones;

3 Si no entiende algo, exija que se lo expliquen. Si no está de acuerdo con alguna de las condiciones estipuladas, no firme la tarjeta.

4 Al firmar el contrato, observe la existencia de alguna cláusula por la que si usted lo desea, no recibirá publicidad por correo. Muchas entidades le enviarán información y publicidad de todas las empresas o establecimientos del grupo, debido a que sus datos entran a formar parte de la base de datos de la entidad.

5 Siempre que tenga que satisfacer un interés, exija que le faciliten el tipo de interés mensual y la TAE, pues en la mayoría de los casos un tipo de interés mensual bajo puede conllevar una TAE alta. Recuerde que el TAE incluye los intereses anuales junto con las comisiones y demás gastos financieros.

6 Casi todas las entidades mandan un extracto a su domicilio a principios de cada mes, con todos las operaciones realizadas con la tarjeta de compra durante el mes anterior, así como con el saldo pendiente.

7 Si se modificaran los tipos de interés o comisiones o las cláusulas, deberá exigir la información sobre estos cambios por parte de la finan-

ciera. Muchas entidades publican estos datos sobre los tipos de interés en diarios de ámbito nacional con anterioridad a su entrada en vigor. Otras se lo remiten a casa.

8 Ante cualquier cambio o modificación de sus datos personales no olvide comunicarlos a la entidad.

9 En cuanto pierda o le sustraigan la tarjeta, notifíquelo al Servicio de Atención al Cliente que dicha entidad posea, con la mayor brevedad posible. Casi ninguna entidad se hace cargo del uso fraudulento que puedan hacer los terceros hasta el momento de la notificación.

10 En época de rebajas, infórmese de si puede utilizar la tarjeta de compra, y si las condiciones de uso son las mismas que en el resto del año.

11 En la mayoría de los casos, las entidades fijan en las condiciones generales el ámbito judicial en Madrid y en muy pocos se establece el foro de la ciudad donde se firma el contrato.

12 Se puede anular el contrato cuando usted lo desee. Lo recomendable es intentar hacerlo en el momento de no tener ninguna deuda, pues en caso de tenerla deberá hacer frente a ella con los correspondientes intereses que figuren en el contrato de adhesión. Además deberá devolver la tarjeta.

CONSEJOS DE BANCA VIRTUAL:

En la actualidad, está de moda el realizar nuestras compras o solicitar nuestros servicios financieros a través del comercio electrónico. Son muchas las ventajas, pero debemos tener en cuenta una serie de consejos:

1 Antes de comprar seleccione muy bien las "tiendas virtuales" en las que va a hacerlo. Adquiera productos solamente en aquellas que le inspiren una cierta confianza, por ser conocidas o por tener algún tipo de certificación. Averigüe quién está detrás de la web y su dirección física. Busque estos datos detrás de enlaces como "información general", "¿quiénes somos?", o similares. Con estos datos, podrá reclamar en caso de fraude. Si no los puede encontrar, desconfíe.

2 La empresa o profesional que ofrezca la contratación electrónica tiene que aportar con facilidad y de forma directa y efectiva como mínimo:

- Nombre o razón social.
- Dirección
- Datos para poder contratar con la empresa o profesional rápidamente y de forma directa y efectiva.
- Si se halla inscrita en algún registro público (ej. Registro Mercantil), especificará en cuál de ellos y su número de inscripción.
- Los precios, estarán claramente indicados, sin ambigüedades, constando expresamente si se incluye impuestos y gastos de envío.

3 Compruebe siempre que las páginas en las que va a realizar sus compras u operaciones financieras están protegidas. Para ello, observe si en el ángulo inferior izquierdo de la web aparece un icono que representa un candado cerrado. Si no es así, desista de su operación y no envíe ningún dato personal, ni mucho menos, de su tarjeta de crédito. Esta información podría ser interceptada por cualquier internauta.

4 Debe informarse siempre de las medidas de seguridad utilizadas por los bancos en sus sucursales virtuales, antes de decidirse a suscribir un servicio financiero on-line. Todos dicen ser los más seguros, pero muchos todavía no están a la altura de las circunstancias.

5 Una vez contratado el servicio con la entidad financiera, memorice sus claves de acceso y su firma electrónica, guárdelas en un lugar seguro. Si le ofrecen la posibilidad, modifíquelas con cierta frecuencia para evitar problemas.

6 Intente operar siempre desde el ordenador de su casa. Si no le es posible, y lo hace desde su trabajo u otros lugares concurridos, como cybercafés, tenga cuidado. No pierda de vista ni un minuto el terminal, sobre todo, después de haber conseguido el acceso a sus productos. Alguien podría suplantarle y operar fraudulentamente.

ADICAE ha participado en las sesiones del "Grupo de Expertos en el Fraude en medios de pago" de la Dirección General de Mercado Interior de la Comisión Europea. En las sesiones del Grupo se valoraron los avances de las diferentes acciones que en los diversos estados y a nivel internacional se llevan a cabo. Son especialmente reseñables los siguientes datos:

El continuo crecimiento del fraude en medios de pago, principalmente en tarjetas.

El retraso de una de las soluciones al fraude: las tarjetas con chip, que en principio se retrasaran hasta el año 2008 (cuando en principio estaban previstas para el 2005).

La firme decisión de la Comisión Europea de regular la responsabilidad de los consumidores por uso indebido de tarjetas en caso de robo o pérdida (actualmente está regulación se encuentra en una recomendación que las entidades financieras no cumplen).

Prevenir el fraude con tarjetas de crédito

Folleto de Consumer's Union, Asociación de consumidores EEUU

Le daría Usted las llaves de su casa a un desconocido?

Claro que no - si le interesa la protección y la seguridad de sus pertenencias.

Proteja de la misma forma sus tarjetas de crédito o el número de las mismas. Un ladrón con el número y fecha de vencimiento de su tarjeta de crédito puede cargar miles de dólares en pocos minutos.

Anualmente,el fraude por tarjetas de crédito cuesta a las empresas miles de millones de dólares, pérdidas enormes que todos pagamos en la forma de aumentos en los costos de las tarjetas de crédito. Afortunadamente el fraude por tarjeta de crédito es una de las formas de robo más fácil de evitar.

La mayoría del delito por tarjeta de crédito ocurre por tarjetas perdidas o robadas. El ladrón puede obtener sus tarjetas robándole la billetera o entrando a robar a su casa.

Los delincuentes también pagan a empleados de tiendas por obtener números de tarjetas de crédito y crear tarjetas de créditos falsas para revender en el mercado negro.

Para los ladrones de tarjetas de crédito no es necesario tener la tarjeta en sí para robar de su cuenta. Si encuentran un recibo con su número de cuenta y fecha de vencimiento, podrían aprovechar de su cuenta.

Los telemercaderes delincuentes pueden llamarlo con ofertas muy tentadoras de mercadería rebajada o decirle que se ganó un premio. Le piden un número de tarjeta de crédito para los cargos de envío o por algún otro motivo falso. Le pueden enviar artículos falsos o sin valor o cobrarle a su cuenta de tarjeta de crédito sin enviarle nada.

A veces los delincuentes se quedan cerca de los teléfonos públicos y tratan de escuchar cuando usted dice su número de cuenta para hacer una llamada.

Los delincuentes se roban también las tarjetas de crédito de los buzones o centros postales antes de que usted las reciba. Como protección, la mayoría de las empresas que emiten tarjetas de crédito ahora requieren que llame desde su casa para activar la tarjeta antes de usarla.

El fraude por tarjeta de crédito ha aparecido en el Internet, aunque afortunadamente no resulta tan difundido porque los sitios de ventas al por menor utilizan una modalidad de conexión "segura" para las operaciones. Esto significa que mezclan los números de tarjetas de crédito para disfrazarlos antes de enviarlos por el Internet.

- Lleve sólo una o dos tarjetas, de esa forma si las pierde o se las roban, tiene menos que notificar como perdidas.

- Anote los números sin cargo donde notificar en caso de que pierda o le roben las tarjetas y guarde el número en su casa, en la cartera o en la billetera y en su oficina para que pueda llamar inmediatamente si fuera necesario.

- Nunca desatienda su cartera o su billetera en un lugar público. Tenga cuidado de los carteristas.

- Siempre verifique que le devuelvan su tarjeta de crédito después que haga una compra.

- En casa, guarde las tarjetas en un lugar seguro que no sea obvio para los ladrones.

- Siempre firme su tarjeta con tinta lo antes posible después de recibirla.

- Nunca le preste a nadie su tarjeta. Si desea permitir que alguien use su tarjeta para comprar algo, realice la operación usted mismo.

- Tenga presente cuándo le deben llegar las tarjetas nuevas o reemitidas, y llame a la compañía que las emite cuando no lleguen a tiempo.

- Tenga cuidado de que su buzón sea seguro, y que sólo usted y el cartero tengan acceso.

- Rompa todos los recibos de cargos de tarjetas de crédito y cualquier correspondencia que le ofrezca tarjetas de crédito preaprobadas en pedacitos pequeños antes de echarlos a la basura. Guarde las facturas en un lugar seguro.

- Antes de devolverle una tarjeta de cuenta a la empresa que la emitió para cerrar la cuenta, córtela en varios pedazos.

Cuando utilice la tarjeta de crédito electrónicamente por ordenador, asegúrese de estar utilizando un sitio de Internet seguro. Busque un símbolo de llave y candado pequeño en el lado inferior izquierdo de la ventana de su navegador.

- Nunca le dé a desconocidos o a televendedores que lo llamen por teléfono el número de su tarjeta de crédito.

- Si gente que no merece su confianza consigue el número y fecha de vencimiento, pueden comprar mercadería por teléfono cargan-

do a su cuenta, o también ordenar una tarjeta nueva a nombre suyo.

- El robo de identidad es un crimen muy difundido en el que el delincuente utiliza su información personal, como nombre, dirección y número de Seguro Social para establecer cuentas de crédito fraudulentas a nombre suyo.

- Nunca le dé el número de su tarjeta a desconocidos que lo llamen, por más genuinos que parezcan. Nunca puede estar seguro que un telemercader desconocido sea honrado. No divulgue el número de su tarjeta de crédito a menos que haya sido usted el que inició la llamada.

- No deje correspondencia, recibos o facturas que tengan el número de su tarjeta de crédito sin guardar en su oficina o su casa de forma que alguien los lea. Sepa cuándo debe recibir la factura y llame a quien le emitió la tarjeta de crédito si no llega puntualmente. Un ladrón puede sacar el número de su tarjeta de crédito de la factura.

- Lleve una lista completa de todos los números de su tarjeta de crédito en un lugar seguro. (Nunca la lleve en la billetera). De esta forma será más fácil notificar si la pierde o se la roban.

- Guarde los recibos de todas las compras con tarjetas de crédito y compare la factura mensual con los recibos para verificar si hay algún cargo que usted no haya hecho. Es la mejor forma de asegurarse que nadie más que usted utilice el número de la tarjeta de crédito.

- Nunca anote el número de su tarjeta en una tarjeta postal o en el exterior de un sobre.

- No permita que en los comercios anoten el número de su tarjeta como confirmación en los cheques. En muchos estados es ilegal que los comerciantes soliciten tarjetas de crédito como identificación cuando usted paga con cheque.

- Memorice el número de su identificación personal (PIN); es el código secreto que usted utiliza al retirar dinero en efectivo del cajero automático. No lo anote en la parte posterior de la tarjeta ni lo guarde en su billetera. Guarde una copia del número en un lugar seguro en su casa. No utilice el mismo número de identificación personal en todas sus tarjetas, no use su fecha de nacimiento ni otro número que sea fácil de identificar que podría figurar en otra parte de su billetera.

- Si lo llama alguien diciendo ser representante del banco y le pide su número de identificación personal, no se lo dé. Denuncie la llamada a la policía y a la compañía que emite la tarjeta de crédito.

- Proteja su tarjeta de crédito o de llamada cuando haga una llamada de larga distancia desde un teléfono público. También cubra el panel de discado cuando marque el número de la tarjeta. Asegúrese que no lo estén escuchando cuando le diga su número de tarjeta a la operadora.

- En cuanto se dé cuenta que le falta la tarjeta, actúe rápidamente para notificar sobre esto. Tenga el número de la compañía que emitió la tarjeta, en la oficina o en el directorio personal que lleva encima, y también en su casa para que pueda llamar sin demoras. Si no tiene el número de teléfono llame sin cargo a la operadora de información para averiguarlo. (Vea, "Dónde obtener asistencia.")

- Para proteger sus derechos, debe notificar la pérdida o el robo de su tarjeta en cuanto se dé cuenta que le falta o que fue utilizada sin su permiso. La ley federal limita la cantidad de dinero que puede perder como resultado del uso fraudulento de su tarjeta de crédito.

- Si usted notifica a la compañía que emite su tarjeta antes de que ésta sea utilizada, no tendrá ninguna responsabilidad por el pago de cargos no autorizados. Si la tarjeta fue utilizada de forma fraudulenta antes de que usted notifique a la compañía que la emitió, es posible que se le requiera pagar hasta 150 euros por tarjeta por dichos cargos.

- Si se usó su número de cuenta pero no la tarjeta en sí, usted no es responsable por ninguna cantidad.

- No utilice la tarjeta después de haber notificado que fue robada o perdida.

- Después de llamar para notificar el problema, debe enviar una carta a la compañía emisora explicando que se realizó un cargo sin autorización. Esta documentación por escrito de su notificación también puede limitar su responsabilidad.

- Llame a la compañía emisora de su tarjeta de crédito inmediatamente si nota algo sospechoso en su factura. De esta forma podría asistir a la compañía a descubrir un fraude - y ahorrarse el pago de cargos no autorizados.

- Llame a la compañía que emitió su tarjeta de crédito tan pronto le sea posible para notificar la pérdida o el robo de su tarjeta. También llame siempre que tenga preguntas sobre su cuenta. La mayoría de las compañías que emiten tarjetas de crédito tienen números sin cargo que puede obtener con la operadora de información. Llame a la policía para denunciar todo robo o actividad delincuente.

La lucha contra el fraude en medios de pago, grave riesgo para la economía europea

Conclusiones del Grupo de Trabajo de expertos en medios de pago de la Dirección General de mercado interior, Comisión Europea

Material:

■ Decisión Marco 28 de mayo 2001 sobre la lucha contra el fraude y la falsificación de medios de pago distintos al efectivo.

■ Un posible marco legal para un area única de pagos en el mercado interior (MARKT/208/02) 07/05/02.

■ Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Banco Central Europeo, al Comité Económico y Social y a Europol.

Notas:

Las autoridades francesas ya han estructurado legislación: "La Ley de Seguridad Cotidiana".

Progreso del Plan Contra el Fraude:

El Plan comenzó en febrero del año 2001. Es un plan de acción no legislativo, basado en la iniciativa nacional. Al fin del año 2003 debemos valorar el funcionamiento del plan. La clave es la cooperación entre todos los organismos interesados. Principalmente el sector de los pagos (Industria) y con todos los demás implicados, con una idea de cooperación, sirviendo la Comisión Europea como catalizadora.

¿Que se ha conseguido con el plan hasta ahora?

2 Acciones:

Legislación Penal.

Medidas preventivas, no legislativas, buscando un enfoque global.

Areas de trabajo: a) Mejoras tecnológicas b) Intercambio de información c) Cooperación educacional d) Cooperación con terceros países.

Medidas:

■ Estudio de medios de pago electronicos.

■ Conferencia a principios de 2003, con el enfoque de ver cual sería el medio de dar seguridad al público.

■ Intercambio de información.

■ Respecto a protección de datos, contamos con la Directiva, que no pretende ser absoluta, se basa en la certeza absoluta de que es lo que se permite y lo que no.

■ Creación de página web contra el fraude.

Grupo de Trabajo:

Será el Grupo Director del Plan y asistente de las actividades. Se pretende crear una concienciación de jueces y fiscales (y los organismos extrajudiciales de resolución de conflictos?). Aún no se ha empezado a trabajar en serio y una de las principales cuestiones es como informar a los consumidores y fortalecer la formación. Se proyecta la creación de un número de teléfono único. La próxima reunión será en noviembre.

Terceros países: el 1 de enero de 2004 surgirán 10 nuevos países, concienciación para que puedan adaptar su normativa.

Sensibilizar a los consumidores, ya que el fraude es superior en el ambito entre los países que dentro de los propios países.

Plantear una dimensión nacional: Quizás a través del Ministerio de Economía, con un papel de centralización, que colaborase con la Europol y Banco Central Europeo. Aunque es clara la dificultad de relación entre lo publico - lo privado - lo social (Se debería de prever un papel de lo administrativo previo a lo policial o a lo judicial).

Debe de existir un equilibrio entre prevención y represión. Se debería de realizar publicidad por parte de la Comisión de cara a los consumidores.

Balance de aplicación de la decisión marco:

La Decisión de 28 de mayo de 2001 señala que en los ordenamientos jurídicos nacionales existen lagunas, sobre todo de persecución de actividades transfronterizas y una cierta unificación de delitos penales.

Distinción entre instrumentos de pago: a) corpóreos y b) virtuales. Según esta distinción se buscan sanciones más eficaces. Los casos más graves serían con extradición. Se debería de apoyar fuertemente las reglas de extradición.

Creación de puntos de contacto (siguiendo el criterio de aprovechamiento de estructuras preexistentes).

El 2 de junio de 2003 es la fecha límite de transposición de esta decisión. Presentation de la "Loi de securite quotidienne" (Octubre de 2001): Crea

una tipología de fraudes, había cosas que no se podían penar, ahora si (por ejemplo: la tenencia de números de tarjetas de crédito no propias). La ley atúa en tres líneas: a) Controles (Observatorios, órganos administrativos, etc.) b) Refuerzo de garantías de consumidores (en el 2004: Perdida/robo, salvo falta grave, límite de 150 Euros y exención de responsabilidad de 70 días en casos de e-commerce) c) Ampliación de represión.

Puntos de contacto: Artículo 12 (Nacionales). Intercambio de información u otras funciones. Coordinar la lucha, también contra el delito informático. Probablemente haría falta un punto de contacto central. El dinero electrónico no es dinero emitido por la administración, ¿qué control tendrá sobre él?.

Interpol: Mejora de la seguridad de pagos electrónicos:

Interpol tiene una página web sobre falsificación de tarjetas. Tiene un convenio con las empresas de tarjetas para represión del fraude, contenido: material de formación para detallistas: Boletín, sistema de contraseñas, etc. (http:interpol.int https://sigadiv:1443/). Sistema de base de datos de tarjetas falsificadas en la web. Proyecto: Interpol asocia grupos: de fabricantes de tarjetas, administraciones, etc.) para formación de forenses y creación de una base de datos dinámica; beneficios: Economías de escala que beneficiarían al sector, reducción de costes de viajes de expertos, reducción de los costes de emisiones de tarjetas. Uno de los objetivos especialmente buscados es: un call center, las 24 horas al día.

Punto de contacto de fraude en Holanda:

(En asociación el sector público y privado: Asociaciones de consumidores, Policia, PYMES y Bancos), su finalidad última es conseguir confianza en el comercio electrónico.

Métodos de la mejora de confianza: a) Punto de contacto da información b) Contesta quejas c) Hace llegar información a todas las organizaciones.

Funciones: a) Prevención (10 normas de oro + novedades en prevención) b) soportar quejas de los consumidores c) Dar a la policía toda la información que exista.

Ideas: Enseñar a los consumidores donde esta este punto y darle publicidad. Dar respuestas en el más breve espacio de tiempo posible. Centralizar la información: sectorializada no vale nada.

Medidas tácticas para reducir el fraude hasta la llegada de la tecnología del chip:

VISA: el chip (quizás en el 2005) será un cambio brutal en tarjetas, no solo porque será más dificil el fraude, sino porque se incrementarán los beneficios para los clientes (sobre todo, esto aumentará la confianza). Los elementos innovadores serán: Chip + autentificación para e-commerce. Hasta el momento de llegar a la tecnología "chip" es necesario cubrir las lagunas. Para que la tecnología del chip impida el fraude habrá que trabajar también en el e-commerce y habrá que cambiar toda la tecnología.

Elementos del plan intermedio para luchar contra el fraude: a) Falsificación b) Fraude sin tarjeta c) Fraude transfronterizo (muy importante). "Buenas prácticas", en el tema de fraude de tarjetas se puede conseguir un gran avance a través de las buenas prácticas.

Elementos de trabajo: a) Control de transacciones b) Puntos comunes de compra (lugares donde se pone en peligro la compra) c) Se producira evolución de fraude con los números de tarjetas (es decir, tarjetas no presentes), fraude por teléfon, internet, etc.

Conclusión: Existe demasiado farude, que supone demasiado gasto, hay que encontrar otro modelo, las medidas pueden haber supuesto 4.475 millones de euros.

Vías de acción: Más rapidez de comunicación en el fraude. Diseminar bases de datos de fraude. Alertas on-line de Visa.

Mejores prácticas manuales: 70% del fraude es "aceptado" por el consumidor: Visa prepara manual, todavía hay mucho por hacer en formación. Normativización y sanciones para los estados que no cumplan.

La seguridad en los pagos electrónicos:

VISA: Las Bases de Datos son atacadas por delincuentes, existe un problema de seguridad en los datos (hay unos 4 millones de clientes en peligro y unas 40 empresas). Visa introdujo en 2000 un nuevo proceso: datos guardados en forma segura por los operadores. Se ha preparado un programa que el banco debe de poner en funcionamiento con el vendedor. Se trabaja por zonas. Se ha creado una web en la que cualquiera puede ver que hay que hacer para dar seguridad a su negocio en Internet.

MASTERCARD: Con Internet se llega a un entorno no necesariamente seguro. Los hackers pueden coger una base de datos entera, para ello Master Card tiene un sistema para bloquear las cuentas de toda una Base de datos. Se debería de sancionar a los compradores o vendedores que no protegan sus datos. Se crea un sistema por el que se da la posibilidad de conocer al consumidor sus puntos flacos y cubrirlos. Se crea un programa de control de riesgos en e-commerce, es como un test con recomendaciones.

Hurto de Identidad:

Master Card: En Europa, ahora, ya no es importante, en el futuro lo será. En USA es muy habitual (3.100 casos por día, se necesitan 400 horas para solucionarlo). Del 2000 al 2001 en Europa el incremento es del 0% en USA del 54%. Se prevé incremento en Europa.

2 elementos: a) Persona que necesita DNI (depende de los gobiernos) b) Verificación de si la persona es la apropiada.

Alguien puede usar el nombre de otro para realizar acciones financieras (por ejemplo: pedir crédito a su nombre). Hay páginas donde se pueden

encontrar DNIs falsos (en USA hay leyes sobre este tema).

2 Versiones: a) Solicitud fraudulenta (petición de tarjetas bajo identidad falsa) b) Uso de una cuenta.

Usurpación de personalidad permite tambien actividades delictivas como: fraudes, estafas, blanqueo de dinero, etc.

Se deberían de buscar medidas preventivas antes de que la tasa de usurpación se dispare:

- Normativización.
- Incremento de posibilidades de verificación.
- Convertirlo por Comisión Europea en punto focal de sus acciones.

Sistemas para evitar el fraude en el crédito:

CIFRAS:

Asociación Reino Unido para prevención del fraude (empresas sin fines de lucro) , son 240 miembros entre aseguradoras, compañías de leesing, empresas de inversión, bancos, etc. El 75% del fraude se puede prevenir.

Elementos:

Proporciona intercambio de información sobre fraude y alertas de seguridad.

Antirrobos

Grupos de inteligencia para el fraude internacional.

2.500 personas trabajando

Fraudes + Usurpación de la personalidad 1991 (5330 casos) - 2001 (53.536 casos)

La apropiación de cuentas es otro tipo de usurpación que va en aumento.

Fraude de uso de la dirección anterior y se da una dirección nueva (para recibir todo lo que se compra a prestamo o distancia). También se da la "clnación de empresas", con cambios en los registros.

Prevención:

Concienciación de consumidores: cuidar sus documentos (antes de abrir una cuenta determinar perfectamente quien es)

Entidades:

■ Conocer al cliente

■ Se puede comprobar a través de un "estadillo" del banco: nombre, dirección, antiguedad de la cuenta.

Cooperación en aplicación de leyes

VISA: Se trata de la presentación de un paquete de formación para la prevención y cooperación en el ámbito de aplicación de las leyes de represión del fraude.

El dinero electrónico como nuevo medio de pago: nuevas posibilidades nuevos problemas

Informe del Banco Central Europeo (B.C.E.) sobre el dinero electrónico

El B.C.E. (Banco Central Europeo) ha publicado un informe en el cual se estudia y analiza los posibles riesgos que conllevará la emisión de dinero electrónico. Este dinero electrónico consistirá en la emisión de tarjetas de pre-pago o en programas especializados y dirigidos a desarrollar los pagos a través de Internet.

El mencionado informe concluye con una serie de conclusiones de las que, por su importancia, destacan:

La emisión de dinero electrónico tendrá una importante incidencia en la política monetaria y obligará a asegurar la estabilidad de los precios y la función del dinero como unidad de cuenta.

Necesidad de desarrollar nuevas normas que garanticen, por un lado la confidencialidad, el funcionamiento de los sistemas de pagos y la estabilidad de los mercados financieros, y por otro lado, la protección de los consumidores y usuarios y la protección contra los posibles delitos.

Deberán establecerse los requisitos que deberá cumplir la emisión de dinero electrónico.

Será necesario incrementar la cooperación entre las autoridades de supervisión de los países implicados para evaluar la integridad de los sistemas de dinero electrónico, en especial, en las operaciones transfronterizas.

Conseguir la interoperabilidad de los diferentes sistemas de dinero electrónico.

Limitar la emisión de dinero electrónico a las entidades de crédito, tal como las define el artículo 1 de la primera Directiva sobre coordinación bancaria.

Riesgos en la banca electrónica

Internet es un entorno en el que pueden producirse comunicaciones seguras, esta seguridad se alcanza cuando existen unos requisitos tales como la confidencialidad, la integridad o garantía de inalterabilidad, autenticidad sobre la autoría y el "no rechazo" o no repudio ni del envío por parte del remitente ni de la recepción por parte del destinatario.

Seguridad

En la banca electrónica que un tercero pueda tener acceso a los datos de los usuarios entraña un grave riesgo a la seguridad económica de éste puesto que el hecho de tener este accesp a las distintas operaciones financieras abre la puerta a los delincuentes para obtener la información necesaria sobre, contraseñas (passwords), tarjetas de crédito etc. lo que podría suponer un marco idóneo para la utilización fraudulenta de ests datos.

De igual modo este acceso ilícito puede acarrear consecuencias negativas al existir la posibilidad de manipulación de los datos en el momento de su transferencia o mientras se hallen estacionados en un sistema informático.

Autentificación

Es imprescindible tener la posibilidad de identificación de los diferentes usuarios para poder apreciar sin error ninguno la base o legitimidad con la que pretende realizar las operaciones a través de la banca electrónica pues de otro modo existiría la posibilidad de suplantar al verdadero usuario de un producto determinado.

Hasta la fecha el mecanismo que tiene una mayor seguridad es la firma electrónica avanzada.

No repudio

Conectando con el apartado anterior, podemos concluir que la identificación de cada una de las partes debe tener la más completa y absoluta seguridad de que está llevando a cabo una operación con la persona o entidad correcta sino nos encontraríamos que cualquiera de las dos partes pueda repudiar dicha operación.

Arquitectura y diseño del sistema

La arquitectura abierta de Internet permite ataques contra la seguridad del sistema desde cualquier parte del mundo, utilizando servidores intermedios que permiten ocultar el origen real de la acción. Junto a los protocolos de simple lectura existen otros que permite modificar o destruir la información financiera que se suministra al público. En otros casos, se puede generar un número de solicitudes de información tan alto, que provoca la caída del sistema.

Programas de defensa

En la actualidad contamos con una serie de programas encaminados a la prevención de los posibles atques por parte de un terecero mediante la locaclización de los puntos débiles de la seguridad.

Controles en los accesos

Los passwords de acceso pueden ser obtenidos mediante "spoofing", dirigiendo a los usuarios de una entidad financiera a otro web en el que se ha instalado una réplica del original, de manera que se pueda monitorizar la entrada de los datos identificativos. También pueden producirse ataques por fuerza bruta, mediante programas que generen passwords repetitivamente. También pueden obtenerse passwords con "sniffers" y a través de la memoria caché.

Agujeros de seguridad

Una vez que se localiza un fallo en el sistema de seguridad debemos pensar que debido a la rapidez de la web se conocerá de inmediato con lo cual estamos asumiendo un riesgo de un atque inmediato. En este supuesto el Federal Deposit Insurance Corporation en un informe publicado en Diciembre de1997aconseja:

- mantener un estrecho contacto con los desarrolladores para recibir los parches de forma inmediata.
- suscribirse a servicios de alerta como el del CERT.

Virus y programas maliciosos

Ante un posible ataque de virus o programas maliciosos que puedan afectar la seguridad e integridad de los datos acumulados se debe aplicar una política de prevención adecuada, que utilice sistemas anti-virus y otras medidas de protección de datos.

Recomendaciones

- La educación del usuario en el uso de los passwords.
- Passwords de un solo uso.
- La utilización de tarjetas inteligentes.
- La posible utilización de identificadores biométricos.
- Mayor relevancia a la firma electrónica avanzada.

El dinero móvil

Con el teléfono móvil se podrá pagar lo que compre, recargar la tarjeta y prestar dinero. Existen dos plataformas de pago por móvil. Paybox y Mobipay, Los dos sistemas sirven para lo mismo: nada de billetes, nada de tarjetas, a la hora de pagar use el móvil. El procedimiento es sencillo. Basta con indicar al vendedor que se va a pagar con el teléfono. Éste introduce el número del móvil en el terminal punto de venta (TPV) igual que haría con una tarjeta de crédito. En pocos segundos, el comprador recibe un mensaje pidiendo su autorización. Por último, se introduce la clave secreta y se confirma la operación. El importe ya ha sido cargado en la tarjeta o cuenta bancaria asociada al número telefónico.

En teoría, todo lo que se puede comprar con dinero también se podrá adquirir con el teléfono. Tanto las tiendas de toda la vida como los negocios on line han mostrado su interés por el sistema. Paybox cuenta con 1.000 establecimientos afiliados, la mayoría de Internet. Mobipay, aun antes de su lanzamiento oficial en todo el país, ya dispone de 4.100 comercios que aceptan esta modalidad de pago.

En la práctica, "hoy en día, los servicios con más éxito son las descargas de tonos y la recarga de los móviles prepago", La compra on line de libros, música o informática aparece en el segundo lugar.

El teléfono podría acabar con los problemas de calderilla. En los próximos meses, las máquinas expendedoras llevarán un código para cada producto. Bastará con marcar la referencia en el móvil para que la máquina se lo suministre.

El sistema convierte el teléfono en un pequeño cajero automático desde el que se puede realizar de forma segura todo tipo de pagos, recargas y consultas Un punto clave es la seguridad. La información viaja encriptada por la red GSM. Además, para convalidar cada operación hay que teclear el número de identificación personal.

Las expectativas de éxito no se han cumplido todavía, por ahora, todas las llamadas para las transacciones son gratuitas. Los comerciantes, que pagan un recargo en torno al 3%, soportan el sistema. En el caso de Mobipay, cada uno de los bancos colaboradores tiene sus propias tarifas. Pagar hoy no es viable pero lo será en el futuro.

Paybox y Mobipay están reestructurando el sistema para hacerlo más sencillo y relanzarlo, por otro lado, las operadoras no quieren dejar el negocio en manos de los bancos.

Un mercado único de servicios financieros: los servicios financieros a distancia en Europa

El complejo proceso de construcción de un mercado único de los servicios financieros en la Unión Europea comienza con el nacimiento de la Comunidad, se concreta en Junio de 1998, en el Consejo Europeo de Cardiff, cuando los jefes de gobierno de la Unión Europea encargaron a la Comisión la elaboración de un Plan de Acción (PASF) para conseguir la unificación de los mercados financieros comunitarios.

El Plan de Acción comprende 43 medidas -legislativas y no legislativas-, entre las que podemos destacar la publicación de la Directiva relativa a la comercialización a distancia de servicios financieros destinados a los consumidores que, en materia financiera deberá aplicarse en conjunción a la Directiva 2000/31/CE sobre el comercio electrónico.

El objetivo primordial de esta norma es establecer un marco jurídico armonizado y adecuado para los contratos a distancia en materia de servicios financieros, siempre manteniendo un nivel adecuado de protección de los consumidores. Es precisamente este pretendido alto nivel de protección el que se espera aumente la confianza al poder acceder, sin discriminación, a una gama más amplia de servicios financieros disponibles en la Unión Europea. La falta de armonización de la normativa de los países miembros en el ámbito de servicios financieros, y en particular en el ámbito de medios de pago, es patente.

La Directiva 2002/65/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de septiembre de 2002 relativa a la comercialización a distancia de servicios financieros destinados a los consumidores, es de aplicación respecto de un nuevo concepto armonizado de los servicios financieros entendidos en sentido amplio (bancario, de crédito, de seguros, de jubilación personal, de inversión o de pago) establece importantes medidas tendentes a la protección del consumidor final cuya naturaleza no estará ausente de interpretaciones al concretarse que éste será persona física omitiéndose referencia a las jurídicas. Se ha pretendido lograr un nivel de protección más alto de los consumidores mediante la introducción de determinados derechos para los mismos a la hora de contratar servicios financieros a distancia, obligando igualmente a los Estados miembros a establecer procedimientos apropiados y eficaces de reclamación y recurso para la resolución de eventuales litigios entre proveedores y consumidores.

De las medidas tendentes a proteger al consumidor, destacan las relativas a la información previa a la celebración del contrato, el derecho de resolución, el pago mediante tarjeta y los servicios y comunicaciones no solicitadas. En cuanto al objetivo de velar por el establecimiento de procedimientos eficaces y adecuados, la Comisión Europea trabaja en el proyecto "FIN-NET", una red de denuncias transfronterizas extrajudiciales en el ámbito de servicios financieros en el Espacio Económico Europeo.