Medios de pago en Internet

Álvaro Gómez Vieites
agomezvieites@gmail.com
Profesor de la Escuela de Negocios Caixanova

RESUMEN DE LA PONENCIA

En la siguiente ponencia se pretende analizar el papel fundamental que juegan los medios de pago en el desarrollo del comercio electrónico.

Hay que tener en cuenta que en la actualidad uno de los principales aspectos que limitan la expansión del comercio electrónico es la percepción que tienen muchos potenciales clientes de que Internet todavía es una red insegura. Además, muchos medios de pago tradicionales no se adaptan a los nuevos requisitos de las transacciones en Internet.

Desde hace algunos años se han propuesto medios de pago específicamente creados para operar en Internet, con mayor o menor éxito en el mercado, según el caso.

Entre los requisitos que debería cumplir un medio de pago desarrollado para dar soporte a las transacciones electrónicas, podríamos destacar la necesidad de garantizar la seguridad de las transacciones; su fiabilidad; la escalabilidad; la adecuación a los distintos tipos de transacciones electrónicas; la necesidad de garantizar el anonimato para cierto tipo de compras; la facilidad de uso; la integración con los sistemas de gestión empresarial; la interoperabilidad con otros sistemas de pago; la divisibilidad de las unidades monetarias procesadas por el sistema; etc. Además, será necesario tener en cuenta el coste asociado al procesamiento de cada transacción.

En la práctica ha sido difícil combinar todas las características anteriormente citadas en un único medio de pago.

En esta ponencia se describen algunos de los medios de pago propuestos más destacados, y también se analiza el problema del fraude en Internet.

1. MEDIOS DE PAGO TRADICIONALES

En la actualidad es posible utilizar en Internet medios de pago "tradicionales", como el pago contrarreembolso y las transferencias bancarias. No obstante, el medio más extendido es el pago mediante tarjetas de crédito o de débito, soportado por los protocolos SSL y SET. En este caso, el comprador envía a través de una conexión segura (gracias al protocolo SSL o al protocolo SET) el número de su tarjeta de crédito o de débito, así como la fecha de caducidad. El vendedor solicitará confirmación a la entidad financiera emisora de la tarjeta y procederá a realizar el cargo del importe de la operación en la tarjeta de la que es titular el comprador.

Para la compra de determinado tipo de servicios, también se está recurriendo a los pagos a través de mensajes SMS de teléfonos móviles o mediante la utilización de "dialers" (marcadores telefónicos) y la conexión del equipo del usuario a números de tarificación especial. Sin embargo, en estos casos el vendedor debe afrontar el problema derivado de las elevadas comisiones cobradas por los operadores de telefonía.

En lo que se refiere a la utilización de las tarjetas de crédito, debemos tener en cuenta que desde que en 1950 Dinners Club emitió la primera tarjeta de crédito, la expansión del dinero de plástico ha sido tan espectacular que en 1992 Alix Hart, Presidente de MasterCard Internacional, llegó a afirmar que "el dinero de plástico va a sustituir totalmente al efectivo y a los cheques en un plazo de entre 30 y 40 años".

Según un estudio realizado por Activmedia en octubre de 2000, las tarjetas de crédito eran el medio seleccionado por los consumidores que realizaban compras en Internet en un 98,5% de los casos, si bien en dicho informe se dejaba entrever la posibilidad que los compradores de productos y servicios a través de Internet comenzarían a recurrir a otros métodos de pago en los próximos años.

Durante el año 2002 en España los pagos mediante tarjetas de crédito en las compras por Internet representaron el 53% de los casos. El uso de este medio de pago aumentó en 2003 hasta alcanzar el 85% de las transacciones del comercio electrónico español, según datos de la Comisión del Mercado de las Telecomunicaciones (CMT). Conviene destacar que del conjunto de operaciones efectuadas, casi la mitad se correspondían a compras realizadas en el extranjero.

2. MEDIOS DE PAGO PARA EL COMERCIO ELECTRÓNICO

Desde hace algunos años se han propuesto medios de pago específicamente creados para operar en Internet. Seguidamente se exponen algunos de los requisitos que debería cumplir un medio de pago desarrollado para dar soporte a las transacciones electrónicas:

1. Seguridad de las transacciones.
2. Fiabilidad.
3. Escalabilidad.
4. Adecuación a los distintos tipos de transacciones electrónicas.
5. Anonimato.
6. Facilidad de uso.
7. Facilidad de integración con los sistemas de gestión empresarial.
8. Interoperabilidad con otros sistemas de pago.
9. Divisibilidad de las unidades monetarias procesadas por el sistema.
10. Coste asociado al procesamiento de cada transacción.

En la práctica ha sido difícil combinar todas las características anteriormente citadas en un único medio de pago. Cualquier sistema propuesto necesita contar con el apoyo de las entidades financieras, diversos organismos gubernamentales y empresas especializadas en medios de pago, que suelen imponer sus propias reglas de juego.

En los siguientes apartados de esta ponencia se describen algunos de los medios de pago propuestos más destacados.

2.1. DINERO ELECTRÓNICO: "E-MONEY"

Podemos considerar que el dinero electrónico está constituido por una especie de "cibermonedas" que se pueden guardar en un ordenador o soporte informático y que son equivalentes a una determinada cantidad de dinero.

En el proceso de creación de dinero electrónico, el titular de una cuenta bancaria solicita a su entidad financiera la generación de una determinada cantidad de dinero electrónico ("cibermonedas"). Cada cibermoneda consiste en una secuencia de bits con un número de serie aleatorio que la identifica, la información sobre su valor económico y la firma electrónica del banco, mediante una técnica conocida como "firma electrónica ciega", desarrollada por el criptógrafo David Chaum. De este modo, el banco no conoce los números de serie de las cibermonedas que ha entregado al usuario, pero respalda su valor.

Las cibermonedas se guardan en el disco duro del ordenador del cliente, aunque también podrían ser depositadas en un dispositivo de almacenamiento (disquete, pendrive, tarjeta chip, etc.).

Para utilizar este dinero electrónico, el cliente debe enviar cibermonedas a la tienda online donde desea realizar una transacción. El vendedor remitirá las cibermonedas a la entidad financiera responsable de su emisión, quien se encargará de comprobar la validez del número de serie de cada cibermoneda (es decir, que todavía no ha sido utilizada), para a continuación abonar en la cuenta del vendedor el importe correspondiente a cada cibermoneda.

Para que este sistema funcione correctamente, la entidad financiera debe mantener una base de datos con la relación de números de serie de cibermonedas en circulación, con el objetivo de evitar que se pueda tratar de reutilizar una misma cibermoneda.

Se han propuesto varios sistemas para la creación y utilización de "cibermonedas", como ECash (http://www.ecashtechnologies.com) o NetCash (http://gost.isi.edu/info/netcash).

2.2. CHEQUES ELECTRÓNICOS: ECHECK, NETCHEQUE, NETCHEX

Sistemas como eCheck, NetCheque o NetChex han permitido desarrollar el concepto de cheque electrónico en Internet.

eCheck es un sistema de cheque electrónico desarrollado por el FSTC (Financial Service Technology Consortium), un consorcio de más de 90 miembros, principalmente bancos, que colaboran de forma no competitiva en el desarrollo de proyectos técnicos.

Este sistema emplea una tarjeta inteligente para implementar un "talonario de cheques electrónicos" seguro, que consiste en una relación de órdenes de pago firmadas digitalmente. ara su puesta en marcha contó con el respaldo de la administración estadounidense, que firmó en junio de 1998 su primer cheque electrónico usando este sistema.

A grandes rasgos, el funcionamiento de este sistema es el que se indica a continuación:

1. El comprador selecciona los productos que desea comprar y a continuación envía a través de Internet un cheque digital firmado con su clave privada.

2. El vendedor recibe el cheque, comprueba su validez y procede a firmarlo con su clave privada.

3. El vendedor envía el cheque firmado a la entidad financiera encargada de procesar la orden de pago.

Otros ejemplos de cheques electrónicos serían el sistema NetCheque, desarrollado por la Universidad del Sur de California, que reproduce en Internet el sistema usual de emisión de cheques y compensación entre bancos, y el sistema NetChex de la empresa Universal Payment Solutions.

2.3. FIRST VIRTUAL

Este protocolo de pago fue desarrollado en 1994 por la empresa First Virtual Holdings Inc, constituyendo una de las primeras alternativas para efectuar compras en Internet de forma segura. En agosto de 1998 la empresa abandonó definitivamente este sistema de pagos, al existir soluciones más robustas y eficaces en el mercado. En ese momento contaba con 2.000 comercios adscritos y más de 60.000 clientes registrados.

El sistema First Virtual proporcionaba a sus usuarios un identificativo personal, conocido como Virtual PIN, que debían facilitar en cada operación de compra al vendedor, en lugar del número de la tarjeta de crédito. Seguidamente, el vendedor remitía este Virtual PIN al servidor de First Virtual para solicitar la autorización de la operación. El servidor de First Virtual enviaba un mensaje de correo electrónico el cliente para pedir una confirmación de la operación, de tal modo que si éste la aceptaba respondiendo al mensaje con otro correo, First Virtual procedía a realizar el cargo del importe de la compra en la tarjeta del cliente.

Con este esquema de funcionamiento, este sistema presentaba la ventaja de evitar que el número de tarjeta de crédito tuviera que ser enviado a través de Internet (de hecho, sólo se almacenaba en el servidor de First Virtual) y de solicitar una confirmación expresa del usuario para cada operación.

Sin embargo, su principal problema residía en el hecho de utilizar una herramienta potencialmente insegura como el correo electrónico para la confirmación de las operaciones, sin recurrir a ningún tipo de sistema de encriptación que permitiera reforzar la seguridad de los mensajes de correo.

2.4. TARJETAS BANCARIAS COMO VIRTU@LCASH O E-CASH

La tarjeta "Virtu@lcash" es una tarjeta desarrollada por la entidad financiera española Banesto para la realización de pagos seguros en Internet. Inicialmente, en su primera versión se trataba de una tarjeta virtual, que no incorporaba ni chip ni banda magnética, por lo que el importe de las compras era cargado en una cuenta asociada que el titular debía tener abierta en esta entidad.

Esta tarjeta ha tenido una segunda versión conocida como "Virtual Cash Plus", presentada a comienzos del año 2000 y que permite un uso seguro y anónimo para realizar compras en Internet, sin que sea necesario disponer de una cuenta en Banesto para operar con ella. Virtual Cash Plus es una tarjetera monedero que se puede recargar en cualquier cajero de la red 4B.

A su vez, el Banco Santander Central Hispano lanzó al mercado en junio de 2001 a través de su red de banca minorista BCH una tarjeta virtual y de prepago denominada "BCH e-cash", que permite realizar compras a través de Internet y que está asociada a la MasterCard.

Esta tarjeta virtual ofrecía la posibilidad de recargar su saldo a través de la red de cajeros 4B, del servicio telefónico (BCH Línea) o de la Banca por Internet (BCH Internet).

2.5. CYBERCASH

Cybercash es un sistema desarrollado en 1994 para gestionar el pago mediante tarjetas de crédito. Se trata de uno de los pioneros y ha servido como base para el posterior desarrollo del sistema SET. En España se pudo utilizar desde 1995.

Cybercash constituía una pasarela de pago entre los comerciantes y las redes de las entidades financieras. Antes de empezar a operar, el

comprador debía descargar, registrar e instalar en su ordenador el programa "Cybercash Wallet", un monedero electrónico en el que podía introducir los datos de las tarjetas de crédito que pretendía utilizar para pagar sus compras en Internet. Posteriormente, este programa se encargaba de la generación y gestión de las claves utilizadas para encriptar el proceso de comunicación.

Por su parte, el vendedor que quisiera ofrecer este medio de pago también tenía que registrarse con Cybercash e instalar el software de servidor denominado "Cash Register", disponible para plataformas UNIX y Windows.

El proceso seguido para realizar un pago mediante el sistema de Cybercash constaba de los siguientes pasos:

1. El cliente seleccionaba los productos que deseaba incluir en su compra y utilizaba el programa Cybercash Wallet para generar una hoja de pedido electrónica, en la que se incluía el número de la tarjeta de crédito en que se iba a cargar el importe de la operación, su identificador de cliente, el importe de los productos solicitados y el domicilio para la entrega de estos productos. Esta hoja era firmada posteriormente con la clave secreta del cliente y con la clave pública del servidor de Cybercash.

2. El comerciante anotaba la forma de pago elegida por el cliente y el domicilio para la entrega, generaba un recibo de la operación de compra y, a continuación, enviaba al cliente una factura pro forma firmada con su clave privada.

3. El cliente, después de haber revisado el recibo de la compra, generaba y enviaba al comerciante un mensaje de aceptación del pago. Este mensaje estaba firmado electrónicamente e incluía una huella digital correspondiente a la factura pro forma y a las instrucciones de pago.

4. El comerciante remitía a Cybercash el contenido del mensaje de aceptación del pago y los datos del pedido.

5. Cybercash se encargaba de descifrar y comparar ambos mensajes. Si éstos coincidían, solicitaba confirmación de la aceptación del pago a través de la red financiera y enviaba la respuesta al comerciante para que éste cerrase la transacción.

6. El comerciante informaba al cliente de que el pago había sido aceptado, cerrando de este modo la operación de compra.

En condiciones normales todo este proceso tenía lugar en unos 20 segundos. Además, en este sistema los datos con la tarjeta de crédito del comprador se enviaban encriptados para que sólo pudieran ser leídos por Cybercash. De esta forma, el comerciante no tenía acceso a los datos de la tarjeta de crédito del cliente.

El sistema de Cybercash tuvo una importante aceptación en los primeros años de su existencia, al ofrecer una infraestructura bastante sólida, eficiente y segura para procesar pagos mediante tarjeta de crédito. Sin embargo, la posterior aparición y desarrollo de nuevos medios de pago electrónico, así como la publicación del protocolo SET como una versión más avanzada de Cybercash, avalada por Visa y MasterCard, restaron interés a este medio de pago. Finalmente Cybercash fue adquirido por la empresa de seguridad informática Verisign.

2.6. CYBERCOIN

Cybercash disponía también de un servicio específico denominado Cybercoin para la realización de pequeños pagos ("micropagos") en Internet, como el pago por acceso a bases de datos, compra de páginas de información, lectura de un periódico, etc.

Hay que tener en cuenta que para estos pagos de un importe reducido (menos de 3 €) no resulta rentable utilizar un medio basado en una tarjeta de crédito, por el elevado importe de la comisión aplicada, que puede ser superior al propio valor de la transacción.

Cybercoin era un monedero electrónico que se podía recargar a partir de una determinada tarjeta de crédito. Este monedero estaba ubicado en el servidor central de Cybercoin, desde donde se gestionaban los micropagos de cada uno de sus clientes, realizando las correspondientes anotaciones en las cuentas de sus respectivos monederos.

De este modo, para realizar un pago el cliente proporcionaba al comerciante un número de cuenta y una autorización para que se le cargase el importe correspondiente a la operación. El comerciante remitía estos datos al servidor central de Cybercoin y allí se deducía esa cantidad de la cuenta del cliente.

2.7. SISTEMA ECASH DE LA EMPRESA DIGICASH

DigiCash es una empresa holandesa fundada en 1990 por el famoso criptógrafo David Chaum. Esta empresa lanzó al mercado el sistema conocido como "ECash", un monedero digital que permitía almacenar una cierta cantidad de dinero en el disco duro del ordenador,

facilitando la realización de compras anónimas y seguras en Internet.

Para ser usuario de ECash era necesario abrir una cuenta en alguno de los bancos que trabajaban con este sistema, como el Mark Twain Bank de Missouri (Estados Unidos), uno de los primeros en adherirse al sistema. Seguidamente el usuario tenía que solicitar la cuenta ECash e instalar en su ordenador el programa de monedero electrónico.

Los vendedores que quisieran ofrecer esta modalidad de pago a sus clientes tenían que seguir un proceso similar para registrarse en el sistema: abrir una cuenta en una entidad financiera participante e instalar el programa de monedero electrónico.

A grandes rasgos, el sistema ECash funcionaba de la siguiente manera:

Cuando un usuario de ECash decidía retirar fondos de su cuenta en el banco, generaba por sí mismo una serie de monedas electrónicas ("cibermonedas"). Una moneda electrónica no es más que una secuencia de bits que contienen el valor de la moneda, acompañado de un número de serie único en el sistema ECash asociado a dicha moneda, que se utiliza para detectar copias ilegales de la moneda.

Seguidamente, el usuario presentaba estas "cibermonedas" al banco para que las firmase, respaldando así su valor. El banco se encargaba de firmarla utilizando la técnica de "firma electrónica ciega", desarrollada por el criptógrafo David Chaum. De este modo, el banco respaldaba el valor del dinero sin conocer los números de serie de las monedas, preservando así el anonimato en el uso de estas "monedas electrónicas".

Las "monedas electrónicas" podían ser utilizadas por el usuario para pagar sus compras en las tiendas de Internet participantes en el sistema ECash. Para ello, tenía que enviar al vendedor "monedas electrónicas" cuyo valor total resultase suficiente para saldar el importe de la compra que había realizado. A continuación, la tienda se encargaba de comprobar que dichas monedas eran auténticas, verificando la firma electrónica del banco emisor. Además, para comprobar que las monedas todavía seguían siendo válidas, es decir, para comprobar que no habían sido utilizadas ya en otras transacciones, la tienda debía enviar estas monedas a la entidad financiera.

Por este motivo, las entidades financieras participantes en el sistema ECash tenían que registrar en una base de datos todos los números de serie de las monedas electrónicas que habían recibido de las empresas y tiendas integradas en el sistema. Esta base de datos constituía un registro de las monedas electrónicas que ya habían sido utilizadas en alguna transacción y que, por lo tanto, habían quedado fuera de circulación.

Cuando la entidad financiera recibía una nueva moneda electrónica, se encargaba en primer lugar de comprobar su autenticidad mediante la verificación de su firma electrónica. A continuación, buscaba el número de serie de la moneda electrónica en su base de datos de monedas que ya habían sido utilizadas, de tal modo que, si el número de serie de la moneda se encontrase en dicha base de datos, la entidad financiera tendría que rechazar la moneda en cuestión por tratarse de una copia de otra que ya había sido utilizada en otra transacción, informando de esta circunstancia al vendedor para que procediera a anular la operación de venta.

Por el contrario, si el número de serie de una moneda electrónica recibida no se encontraba en la base de datos, la entidad financiera la daría por válida, aceptando el pago e incrementando el saldo de la cuenta del vendedor con en el importe registrado en la moneda. Asimismo, registraría el número de serie de la moneda en su base de datos para "retirarla de la circulación".

Este sistema garantizaba totalmente el anonimato para el usuario que efectuaba el pago, debido a que la entidad financiera firmaba las monedas con la técnica de "firma electrónica ciega". Esta técnica permite que un individuo u organización pueda firmar digitalmente un determinado documento en formato electrónico sin tener posibilidad alguna de conocer el contenido del mismo y, por este motivo, se dice que se firma "a ciegas".

De este modo, la entidad financiera conocía el valor de la moneda electrónica, pero no tenía acceso al número de serie que había generado la aplicación de monedero electrónico del equipo del usuario, por lo que cuando recibía las monedas enviadas por una tienda participante en el sistema ECash, no podía determinar la identidad del usuario que estaba realizando el pago de la transacción. Simplemente se limitaba a comprobar la validez de las monedas electrónicas, por lo que el sistema ECash se comportaba de un modo similar al dinero real en efectivo.

Sin embargo, esta característica impedía identificar a los usuarios que intentasen llevar a

cabo un uso fraudulento de las monedas electrónicas. Además, ECash no proporcionaba el anonimato para el vendedor que recibía el pago, ya que éste debía identificarse ante la entidad financiera para hacer efectivo el cobro, con el fin de que la entidad financiera pudiera incrementar el saldo de su cuenta.

Por otra parte, este sistema presentaba otro problema que limitaba de forma importante su escalabilidad: el tamaño de la base de datos en que se debían registrar los números de serie de todas las monedas electrónicas ya utilizadas. Además, se trataba de un sistema centralizado que requería de una conexión on-line de la tienda con la entidad financiera asociada para poder validar cada operación.

2.8. MILLICENT

Millicent era un sistema desarrollado por la empresa Digital en 1995 (hoy integrada en HP-Compaq) para realizar micropagos en transacciones dentro de Internet.

Este sistema empleaba una especie de cupón electrónico, denominado "scrip", que representaba un valor prepagado y era válido solamente para un vendedor específico. El "scrip" era emitido por intermediarios, que simplificaban la interacción entre los compradores y los vendedores.

Para poder realizar transacciones, los usuarios debían comprar "scrip" a un intermediario. El "scrip" genérico del intermediario podía cambiarse por "scrip" válido únicamente para realizar compras a un determinado vendedor. El "scrip" sobrante de una transacción se podía cambiar a través de un intermediario por "scrip" válido para otro vendedor.

Una importante ventaja de este sistema era su facilidad de uso, ya que las compras se podían confirmar con un simple clic de ratón desde el propio navegador. Para ello, era necesario instalar el programa monedero de Millicent, que se integraba en el navegador utilizado en el equipo del usuario.

El sistema permitía a sus usuarios realizar multitud de compras en Internet de pequeños importes, sin que éstos tuvieran que molestarse por los detalles de cada operación: bastaba con un simple clic de ratón para confirmar cada operación, si se poseía de suficiente "scrip" en su monedero para la tienda en la que se estaban adquiriendo los productos.

Por su parte, los vendedores que participaban en este sistema podían realizar transacciones con unos costes muy inferiores a los pagos con tarjeta de crédito. Se trataba, además, de un sistema de pagos totalmente descentralizado, cuya operatividad descansaba en el papel de los intermediarios y no en un servidor central responsable de la autorización de cada una de las operaciones.

Los intermediarios se encargaban de comprar "scrip" a los comerciantes y revenderlo posteriormente a un precio superior a los clientes, obteniendo sus ingresos de este margen de intermediación. El papel de estos intermediarios resultaba fundamental para evitar que cada comprador tuviera que mantener una cuenta específica con cada uno de sus clientes. Además, se encargaban de cargar el importe del "scrip" que había sido comprado por cada cliente en la cuenta o tarjeta de crédito facilitada por éste. De este modo, los intermediarios actuaban de puente entre el sistema de micropagos de Millicent y el sistema financiero tradicional.

Para reducir los costes de las transacciones, Millicent empleaba técnicas criptográficas débiles, más eficientes desde el punto de vista computacional. Dado que estaba pensado para realizar transacciones de un importe muy pequeño (micropagos), la seguridad no era un factor tan crítico como en otros sistemas, por lo que se consideró adecuado emplear técnicas criptográficas suficientemente robustas como para hacer que el coste de romper la seguridad de una transacción resultase muy superior al importe de la transacción en sí.

Por otra parte, en este sistema tampoco se emitían recibos ni justificantes de las transacciones ya que, debido al reducido importe de éstas, el riesgo de operaciones fraudulentas podía ser muy bajo.

2.9. PAYPAL

PayPal (www.paypal.com) es un medio de pago basado en el correo electrónico que ha adquirido una gran popularidad en Internet en estos últimos años, sobre todo para dar cobertura a las transacciones realizadas entre particulares en Websites de subastas como eBay.

PayPal es una compañía fundada en Palo Alto, California, en octubre de 1999 por los jóvenes Elon Musk y Peter Thiel, que tenían respectivamente 30 y 34 años en ese momento.

El funcionamiento de este sistema es simple y eficaz: cada usuario abre una especie de cuenta corriente en PayPal, deposita allí una determinada cantidad de dinero (mediante una tarjeta de crédito o un cheque) y luego lo puede utilizar para llevar a cabo transacciones, pagos a "cole-

gas" (de ahí el nombre del sistema) u empresas, o bien para participar en subastas on-line como las desarrolladas en eBay.

Se trata, por lo tanto, de un medio de pago muy útil para las transacciones entre particulares, ya que elimina la inseguridad e incertidumbre que supone aceptar pagos como cheques personales o tarjetas de crédito. PayPal actúa de intermediario financiero en este caso, garantizando que existe dinero disponible en la cuenta del comprador. A cambio de dar fe de ello, se queda con una pequeña comisión del 3%, inferior a la que suelen aplicar para estas transacciones las tarjetas de crédito.

Los fundadores comenzaron su proyecto con 24 usuarios experimentales y, debido a su espectacular crecimiento, a 31 de diciembre de 2001 contaban ya con 12,8 millones de usuarios (la mitad eran usuarios activos), alcanzando una facturación de 104,8 millones.

Atraídos por su éxito, en marzo de 2001 varias entidades financieras, entre las que se encontraba el banco español eBankinter, pasaron a forma parte del accionariado de PayPal al afrontar una ampliación de capital de 90 millones de dólares. La compañía salió a Bolsa en febrero de 2002, alcanzando una valoración de 1.200 millones de dólares.

Posteriormente, en julio de 2002 la empresa eBay adquirió PayPal mediante una operación de canje de acciones, por un importe total de 1.500 millones de dólares.

En octubre de 2005 el sistema PayPal contaba ya con más de 78 millones de cuentas activas, pertenecientes a usuarios registrados de 56 países de todo el mundo. PayPal cerró el año 2005 con un volumen total de transacciones por valor de 27.000 millones de dólares, sobrepasando los 1.000 millones de beneficios.

Debido a su gran éxito, numerosas empresas de la talla de Dell (el mayor vendedor de ordenadores PC del mundo) han incorporado este sistema de pago en sus tiendas de Internet. De hecho, en febrero de 2006 este sistema conseguía sobrepasar ya la cifra de más de 100 millones de usuarios, con un ritmo de crecimiento de 100.000 nuevos usuarios cada mes.

2.10. EPAGADO

El sistema "epagado.com" es un sistema de pago desarrollado en España por la entidad financiera eBankinter, que permite vincular una cuenta corriente bancaria y una dirección de correo electrónico.

Para ello, el usuario de este medio de pago electrónico tiene que vincular la cuenta "epagado.com" a una cuenta corriente de cualquier entidad desde la que se transferirán el importe para los pagos. Este sistema evita así que el cliente en una operación de compra tenga que proporcionar datos sensibles como el número de cuenta o la tarjeta de crédito, con lo que se eleva la seguridad de la transacción. La confirmación de la operación se realiza a través del correo electrónico registrado previamente por el usuario del sistema.

Según el propio eBankinter, este sistema ofrece a los comercios una importante ventaja frente a las tarjetas de crédito o las cuentas corrientes, ya que no existe posibilidad de repudio de la operación, puesto que el cobro se produce al instante, evitando el fraude. Además, tiene un coste inferior a otros sistemas y permite el cobro de cualquier importe, por pequeño que éste sea.

2.11. SISTEMAS BASADOS EN TARJETAS PREPAGO

En mayo 2003 se lanzaba Morsopay, un sistema basado en una tarjeta prepago, creado específicamente para las compras en Internet y orientada al pago de contenidos.

El cliente de este servicio puede adquirir la tarjeta por un importe de 5, 10 o 20 euros en uno de los puntos de venta autorizados de Morsopay: más de 6.000 en toda España, entre gasolineras, estancos, etc.

Al acceder al Website que ofrece los contenidos (noticias, juegos, páginas con contenidos para adultos, informes técnicos, cursos, etc.), el usuario debe introducir una de las claves contenidas en la tarjeta y en ese momento el sistema Morsopay validará el servicio, indicando cuál es el saldo remanente a su favor y notificando la validez de la operación al Website que proporciona los contenidos.

Sus creadores destacan las siguientes ventajas del sistema:

- Anonimato: no se facilitan datos personales.
- Seguridad: no se utilizan cuentas corrientes ni tarjetas de crédito.
- Comodidad y facilidad de uso.
- Reducción del riesgo de impagados o fraudes para el comercio en Internet.

Por otra parte, en octubre de 2005 se anunciaba el lanzamiento en España del sistema de

pago Ukash, también basado en una tarjeta prepago (denominada "cupón Ukash").

2.12. NUEVAS ALTERNATIVAS PARA LOS MICROPAGOS

En estos últimos años se han propuesto otros sistemas para la gestión de los micropagos en Internet y, en especial para la venta de contenidos como artículos de periódicos y revistas o capítulos de libros, entre los que podríamos citar Qpass, BitPass, PayStone, Firstgate o PepperCoin, entre otros.

Todos estos sistemas permiten agrupar los importes de varias microtransacciones para reducir los costes de las comisiones y de la tramitación de los pagos.

Así, por ejemplo, en el caso de Qpass, el usuario debe abrir una cuenta en este sistema, facilitando su nombre, dirección de correo electrónico y tarjeta de crédito. En un Website en el que los contenidos se encuentran protegidos mediante este sistema, el usuario puede adquirir y descargarse el contenido que le interesa haciendo clic en el icono de Qpass e introduciendo su número de identificación y contraseña. En ese mismo momento el sistema Qpass realiza una anotación de cargo en su cuenta y una anotación de abono en la cuenta del proveedor del contenido.

Al final de cada mes, el sistema Qpass procede a realizar un cargo contra la tarjeta del usuario por el importe total de las compras realizadas, así como un ingreso en la cuenta del propietario de los contenidos por el importe total de las ventas. Este sistema está siendo utilizado en periódicos digitales como el New York Times o el Wall Street Journal.

3. TARJETAS INTELIGENTES (*"SMART CARDS"*)

Las tarjetas inteligentes, "*smart cards*" o "tarjetas chip" se caracterizan por incorporar un circuito integrado ("chip"), que sustituye a la banda magnética de las tarjetas clásicas de plástico. Por este motivo, resultan mucho más seguras que las tarjetas de banda magnética, ya que son más difíciles de falsificar.

Algunas de estas "tarjetas chip" simplemente incorporan un pequeño circuito de memoria en el que se registran los datos del titular: son las conocidas como "memory cards" (tarjetas de memoria).

Sin embargo, los modelos de "tarjetas chip" más avanzados también incorporan un procesador criptográfico dentro del circuito integrado ("microprocessor cards"), que permite realizar internamente todas las operaciones criptográficas necesarias en protocolos para realizar transacciones seguras como el SET. En ese caso se habla de las tarjetas inteligentes propiamente dichas, más caras pero más seguras que las tarjetas de memoria, ya que todas las operaciones criptográficas se realizan dentro de la propia tarjeta.

Los detalles técnicos de estas tarjetas inteligentes (características eléctricas y físicas, tipos de contactos, etc.) se definen en el estándar ISO 7816. Además, los fabricantes de estas tarjetas suelen utilizar la interfaz de programación (API) definida en el estándar PKCS#11 (estándar "Crypto Token Interface").

Por otra parte, a principios de 2005 se han lanzado al mercado nuevos modelos de tarjetas inteligentes que incorporan la tecnología de radiofrecuencia (RFID), que permiten el pago "a distancia" en locales comerciales y máquinas expendedoras.

Una aplicación de las "tarjetas chip" es la tarjeta monedero, desarrollada como una interesante alternativa para solucionar el problema de los micropagos. Estas tarjetas incorporan un pequeño chip en el que se almacena un determinado valor monetario prepagado (un buen ejemplo lo encontramos en las tarjetas telefónicas de prepago), que puede ser gastado en cualquier comercio que haya instalado un lector adaptado a estas tarjetas.

De este modo, el importe de las compras puede deducirse de la tarjeta cada vez que el usuario realice un pago con ella, siendo este proceso muy rápido y sencillo para ambas partes.

Se trata, en definitiva, de un medio de pago ideal en transacciones de escaso valor (inferiores a 5 €) y que requieran de cambio exacto: compras en máquinas de autoventa (expendedoras de comida, refrescos o tabaco); transporte público; peajes; teléfonos públicos; etcétera.

Sin embargo, la existencia en el mercado de gran variedad de tarjetas incompatibles entre sí ha frenado su expansión. Para tratar de paliar esta situación y garantizar la interoperabilidad de las tarjetas monedero, se aprobaron en abril de 1999 las Especificaciones Comunes para Monederos Electrónicos (CEPS), realizadas por un grupo de trabajo integrado por Europay International, SERMEPA, Visa International y ZKA (Zentraler Kreditausschuss, de Alemania). Con esta iniciativa se pretende alcanzar la inter-

operabilidad de todas las tarjetas monedero en un futuro próximo.

El entendimiento entre las distintas tarjetas hará posible que un ciudadano de la Unión Europea, poseedor de una tarjeta interoperable, pueda recargar su monedero con dinero electrónico en cualquier punto de carga en bancos o quioscos que ofrezcan este servicio, además de poder gastarlo en establecimientos y servicios que tengan instalado un lector de "tarjetas chip".

En el estándar CEPS se definen varios tipos de transacciones que podrá realizar una "tarjeta monedero":

- Carga de dinero: los titulares de la tarjeta pueden cargar dinero en ella en cualquier terminal de carga (normalmente será un cajero convencional de la red de una entidad financiera) que ostente la marca del emisor de su tarjeta, en cualquier divisa soportada por la tarjeta. Para realizar esta operación el usuario deberá autenticarse previamente mediante la introducción de un Número de Identificación Personal (PIN).
- Descarga de dinero: en cualquier momento el titular podrá descargar dinero de su tarjeta y devolverlo a su cuenta bancaria, residente en la institución financiera del emisor de tarjetas. La descarga de dinero también puede incluir la capacidad de obtener efectivo del terminal de descarga, pero sólo en terminales del banco emisor.
- Intercambio de divisas: las tarjetas contarán con distintas "ranuras", en las cuales se podrá almacenar dinero en varias divisas. En cualquier momento se le permitirá al titular cambiar todo o parte del dinero almacenado en una divisa a otra divisa dentro de su propia tarjeta.
- Compra y retrocesión de la compra: el titular de la tarjeta podrá hacer uso de ésta en cualquier terminal de venta que tenga el sello de su marca de tarjeta. El terminal de venta mostrará al usuario el importe de la operación, pidiéndole su autorización antes de que ésta se haga efectiva. En caso afirmativo, el terminal de venta mostrará al usuario el balance de su tarjeta antes y después de la compra. Si por cualquier motivo la compra no puede realizarse con éxito (agotamiento del artículo que se desea comprar, etc.), se puede retroceder la operación y reintegrar el dinero a la tarjeta, sin perjuicio para su titular.
- Compra incremental: sucesión de compras de muy pequeño valor, como en el caso de los "pasos" en una llamada telefónica desde una cabina o el número de partidas completas en un juego online. Se trata, además, de un tipo de servicio muy útil para la acumulación de varios "micropagos" en Internet.
- Cancelación de la última compra: permite cancelar la última operación de compra realizada con la tarjeta, en el caso de que el usuario desee devolver el producto adquirido. Esta operación deberá realizarse en el mismo terminal en el que se completó la operación de compra y sólo podrá tener lugar una vez.

Además, el titular podrá consultar en cualquier momento el balance de su tarjeta, utilizando un dispositivo lector adecuado, así como un registro de los últimos movimientos.

Por otra parte, para facilitar su utilización en las compras a través de Internet, está prevista la incorporación de dispositivos lectores de tarjetas inteligentes en los teclados de los ordenadores.

A finales de 2005 se daba a conocer el gran éxito de los monederos electrónicos en Japón, hasta el punto de que uno de cada cinco japoneses poseía una tarjeta monedero y cada día se registraban 500.000 transacciones con este sistema de pago. La empresa Bitwallet, que gestiona el monedero electrónico EDY (Euro Dollar Yen) lanzado en el año 2001, había distribuido en Japón unos 15,4 millones de tarjetas hasta principios de febrero de 2006, de los que 2,4 millones eran tarjetas virtuales directamente integradas en un chip electrónico de los teléfonos móviles.

No obstante, a pesar de la mejora sustancial de la seguridad frente a las tarjetas clásicas basadas en las bandas magnéticas, se han propuesto varios tipos de ataques contra las "tarjetas chip": así, por ejemplo, un atacante podría tratar de comprometer los equipos de lectura o el software específico instalado en el ordenador del usuario, el cual, de este modo, podría mostrar información errónea al usuario en pantalla o bien facilitar la manipulación de los datos que se envían o reciben de la tarjeta.

Por otra parte, se han descubierto vulnerabilidades en los protocolos diseñados para inter-

cambiar datos desde los dispositivos lectores con las "tarjetas chip". También se han dado conocer posibles vulnerabilidades a nivel del diseño eléctrico de las tarjetas, que permitirían que un atacante aplicase determinados voltajes a la tarjeta para conseguir que se eliminasen las claves criptográficas almacenadas en la memoria de una tarjeta afectada por un mal diseño.

De un modo similar, se han propuesto ataques contra tarjetas criptográficas basados en el análisis de la cantidad de energía eléctrica consumida por el chip (o también en el tiempo de cálculo) al realizar las distintas operaciones con los datos y las claves criptográficas.

Por todo ello, en los últimos años se han desarrollado "tarjetas chip" más seguras, que incorporan mecanismos anti-intrusión (tarjetas "Tamper-Resistant") para poder resistir los intentos de manipulación y de intrusión, así como la monitorización externa de la actividad de la tarjeta.

4. EL TELÉFONO MÓVIL COMO INSTRUMENTO DE PAGO

En los últimos años, gracias al desarrollo de las comunicaciones y los servicios inalámbricos, han cobrado especial importancia las plataformas de gestión de pagos a través del teléfono móvil, mediante una cuenta asociada a un número de abonado.

Con estos sistemas se pretende que el teléfono móvil funcione como un monedero virtual para el pago de productos y servicios, facilitando las compras en tiendas de Internet, en máquinas expendedoras, en taxis, en restaurantes, en gasolineras, etc. De hecho, a finales del año 2000 se presentaron varias de estas plataformas en España:

- Caixamóvil, desarrollado por La Caixa y restringido sólo para sus clientes y para la realización de pagos en Internet.
- Paybox, del Deutsche Bank, que permitía operar con cualquier entidad bancaria instalada en España, previo abono de una cuota anual de cinco euros. Se cobraba además una comisión por cada transacción realizada.
- Movilpago, de Telefónica Móviles y el BBVA. En este sistema las operaciones invertían un tiempo de 10 segundos en ser aceptadas, tras marcar el número de abonado y un código personal. Además, Movilpago pretendía ser aceptado como medio de pago en máquinas expendedoras, en la compra por catálogo, así como en los sistemas de pago por visión de películas y programas.
- Pagomovil, plataforma similar a la anterior desarrollada por Vodafone, el BSCH y el sistema de pagos 4B.

A finales de mayo de 2001 las plataformas Movilpago y Pagomovil acordaron su integración en una sola, dando lugar al nacimiento de Mobipay. Con esta decisión pretendían evitar la competencia entre varios sistemas de pago diferentes e incompatibles entre sí.

La alianza entre entidades financieras y operadoras de telecomunicaciones no es fruto de la casualidad. Si tienen aceptación en el mercado, estos sistemas de pago por móvil podrán generar importantes comisiones a los socios financieros, así como un incremento de la facturación de las operadoras. Sin embargo, su utilización podría ir en detrimento del uso de las tarjetas de crédito y de débito.

Por otra parte, en octubre de 2002, la compañía de telecomunicaciones japonesa NTT DoCoMo comenzó las pruebas de un nuevo servicio de pago electrónico con teléfono móvil, bautizado como FOMA ("Libertad de Acceso Móvil Multimedia"), que permite agilizar las compras gracias a la tecnología inalámbrica. Para ello, los teléfonos móviles incorporan un chip emisor especial y los propietarios de estos teléfonos deben tener una cuenta bancaria (u otro medio de pago, como una tarjeta de crédito) asociada a dicho chip. Cuando el usuario del teléfono móvil desee adquirir un producto en una de las tiendas que soporten este sistema de pago, tan sólo tendrá que pasar el teléfono cerca de los dispositivos lectores y, si confirma la operación, el importe del producto se cargará en su cuenta.

En septiembre de 2003, las empresas Nokia y Visa firmaron un acuerdo de colaboración en el segmento de los pagos a través de móvil, para potenciar el uso de una nueva aplicación de "monedero electrónico" de los terminales de Nokia y el servicio "Verificado por Visa", con el objetivo de facilitar la realización de operaciones seguras y cómodas. La nueva versión de la aplicación "monedero electrónico" de Nokia permite almacenar información personal, como nombres de usuario, contraseñas, número de tarjeta de crédito, bonos de transportes, direcciones de entrega y otros datos necesarios para realizar compras a distancia.

También podemos destacar que en febrero de 2005 Nokia presentaba la tecnología NFC

("Near Field Communications"), que permite que el teléfono móvil pueda interactuar con puntos de venta y máquinas de expendedoras para realizar transacciones locales con cargo a la factura mensual del teléfono móvil.

4.1. MOBIPAY

Mobipay es un sistema que permite activar distintos medios de pago (tarjetas bancarias físicas o virtuales, de crédito, débito o de prepago) desde un terminal de telefonía móvil, para realizar una gran variedad de pagos y operaciones, invirtiendo menos de 15 segundos en la confirmación de cada transacción. De este modo, los creadores de Mobipay pretenden que el teléfono móvil presente en el bolsillo de muchos ciudadanos se convierta en la forma de pago habitual para muchas de las compras de cada día.

Mobipay nació en julio de 2001, como fruto de la fusión de dos iniciativas paralelas que pretendían crear un medio de pago a través del teléfono móvil, desarrolladas por BBVA y Movistar (plataforma Movilpago), por una parte, y por el BSCH, Vodafone y Amena (plataforma Pagomovil), por la otra. Mediante la integración de ambas plataformas, inicialmente incompatibles entre sí, se pretendía desarrollar un sistema interoperable que resultase mucho más atractivo para clientes, comercios y las entidades financieras y operadores de telefonía participantes.

Se crearon entonces dos compañías. La primera es Mobipay España, que está participada en un 48% por casi 90 entidades financieras (BBVA, Santander, Bankinter, Banco Popular, Banesto, Barclays, Caja Madrid, el grupo de cajas rurales...), un 40% es de las tres operadoras de telefonía móvil españolas (Telefónica Móviles, Amena y Vodafone), mientras que las sociedades de medios de pago Sermepa (Grupo Servired), Sistema 4B y Euro6000 poseen el 12% restante.

La otra compañía es Mobipay Internacional, pero su origen directo es el proyecto Movilpago, así que sus accionistas son únicamente BBVA y Telefónica Móviles.

El funcionamiento del sistema Mobipay es muy sencillo: el comprador de cualquier artículo en una tienda física debe proporcionar al vendedor su número de teléfono o un alias que lo identifique dentro del sistema. A continuación, el vendedor introduce estos datos en un terminal similar al utilizado en el pago con tarjetas de crédito (datáfono) y, una vez procesados por el sistema Mobipay, el cliente recibe un mensaje en su teléfono móvil con el importe de la operación. Éste da su aceptación introduciendo una clave secreta que sólo él conoce (PIN) y la transacción queda entonces confirmada. Cabe destacar que todo este proceso ocurre en apenas 15 segundos.

Cuando se realiza una compra a través de Internet en una tienda on-line, el usuario suscrito al servicio Mobipay también debe escribir su clave secreta en el teléfono móvil para confirmar la operación.

Debemos tener en cuenta, además, que ya existen teléfonos móviles que incorporan distintas técnicas biométricas para reforzar la seguridad en operaciones como las descritas: lectores de huellas dactilares o sistemas de reconocimiento de patrones faciales a partir de la cámara digital integrada, que permitan combinar la biometría con la utilización de una clave de identificación personal (sistema de identificación basado en dos factores).

Un usuario se puede dar de alta en el servicio Mobipay a través de una entidad financiera o de su operadora de telefonía móvil, pudiendo especificar en ese momento una lista de nueve posibles medios con los que pagar las operaciones, entre los que se incluyen tarjetas de crédito, tarjetas de débito, domiciliación en cuenta corriente, etc. Cada vez que realice un pago mediante Mobipay, el sistema le dará a elegir cuál de ellos quiere utilizar en esa ocasión. Las compras de pequeña cuantía, como las realizadas en máquinas expendedoras, las microtransacciones en tiendas de Internet o la recarga del teléfono si es de prepago, se cargan directamente a la cuenta del propio teléfono móvil.

Las aplicaciones del servicio Mobipay como medio de pago se pueden extender a todo tipo de compras: desde las realizadas en tiendas físicas, pasando por el pago en taxis y otros servicios de transporte (como los autobuses urbanos, sistema ya implantado en algunas ciudades como Málaga), compra en máquinas expendedoras de bebidas o tabaco, compra de entradas de espectáculos, pago de facturas de servicios como la luz o el agua, pago de parquímetros (en ciudades nórdicas como Estocolmo), servicios "pay per view", pedidos encargados a establecimientos de comida rápida, otros servicios a domicilio, etc.

Así, por ejemplo, Mobipay firmó en junio de 2003 un acuerdo de colaboración con el fabricante de taxímetros Taxitronic, con el fin de implantar en el sector del taxi el pago por medio del móvil. En virtud de este acuerdo, los clientes podrán pagar a través de sus teléfonos

móviles en más de 10.000 taxis, repartidos entre veinte ciudades españolas. El taxista que instale este sistema sólo tendrá que marcar en su terminal el importe del recorrido y el número del móvil del usuario, que recibirá un mensaje donde se le pedirá la confirmación de la operación. De este modo, a partir de noviembre de 2003 unos 1.400 vehículos de "Radio Teléfono Taxi" y "Radio Mercedes de Madrid" comenzaron a implantar en sus coches el estándar de pago por móvil Mobipay, mediante los terminales Taxitronic.

Posteriormente, en enero de 2004 se anunciaba el acuerdo entre Mobipay y la empresa Kilowatt para utilizar el sistema en máquinas expendedoras. Kilowatt tiene instalados en España más de 10.000 módulos de máquinas expendedoras de productos como los refrescos de Coca Cola o los helados de Camy. Además, se prevé que el sistema de pago Mobipay pueda ser implantado en la venta de otros productos o, incluso, en máquinas recreativas.

En el caso de las máquinas expendedoras o de autoventa, para pagar con su teléfono móvil el usuario debe introducir el código mostrado en la máquina expendedora y, tras ser informado en la pantalla del móvil de la compra que está realizando, autorizar la operación desde su propio terminal. También debemos tener en cuenta que con la incorporación de cámaras digitales de alta resolución y software de procesado de imágenes y reconocimiento de caracteres, los propios teléfonos móviles podrían reconocer el código de la máquina expendedora al ser leído éste directamente mediante la cámara digital integrada.

El importe del producto obtenido de la máquina expendedora se incluirá en la factura mensual del teléfono móvil, en el caso de ser cliente de contrato, aunque también se podría descontar directamente del saldo de su tarjeta si se tratase de un usuario de prepago.

En enero de 2005 se extendía el servicio de pago Mobipay a 60 máquinas expendedoras de bebidas y alimentos situadas en aeropuertos, estaciones de tren, centros comerciales y universidades de las provincias de Madrid y de Sevilla.

Por otra parte, en junio de 2004 Mobipay firmó un acuerdo con las empresas Consultrans y ENQ (Grupo Etra) para extender esta modalidad de pago en el transporte interurbano de pasajeros en España, ofreciendo a sus usuarios la posibilidad de realizar las reservas y el pago de los billetes a través del móvil.

En agosto de 2005 el sistema Mobipay cumplía los cuatro años de actividad en España, contando en esa fecha con 250.000 usuarios registrados y 7.600 comercios adheridos. La compañía aseguraba que en su plataforma se estaban realizando unas 80.000 transacciones al mes y preparaba ya su desembarco en América Latina, comenzando por México, Chile y Perú.

Sin embargo, cuando se presentaba el sistema en 2001, las previsiones iniciales eran mucho más optimistas, ya que sus responsables esperaban tener beneficios y contar con cuatro millones de clientes en el año 2004. La realidad es que a mediados de 2005 el sistema Mobipay tan sólo contaba con 250.000 usuarios y, según reconocía la propia compañía, no esperaban obtener beneficios en el corto plazo.

La consultora Arthur D. Little reflejaba en un estudio realizado durante 2004 que no sólo en España se han incumplido las grandes expectativas surgidas en torno a esta nueva modalidad de pago. Las predicciones indicaban que para 2003 el mercado mundial de pagos a través de teléfonos móviles podrían alcanzar los 15.000 millones de dólares, cuando realmente sólo se generó un volumen de negocio de 3.200 millones de dólares.

De hecho, en muchos países la existencia de varios sistemas incompatibles entre sí, lanzados por distintos operadores y entidades financieras, explica en parte la escasa aceptación del sistema. En el caso español, los analistas destacan que el principal problema ha sido que las propias entidades financieras no han creído en esta nueva tecnología y, en consecuencia, apenas la han dado a conocer a sus clientes.

A nivel europeo se anunciaba en 2003 el lanzamiento de una nueva plataforma denominada SIMPAY, fruto de la colaboración de los cuatro mayores operadores de telefonía móvil de Europa: Movistar, Vodafone, Orange y T-Mobil. Esta plataforma se daba a conocer en España en febrero de 2005, siendo compatible con el sistema Mobipay. Sin embargo, poco después sus socios decidían "aparcar temporalmente" este proyecto, a la espera de una situación más propicia en los mercados.

5. EL PROBLEMA DEL FRAUDE EN INTERNET

En la actualidad, para realizar muchas compras en Internet basta con facilitar un número válido y una fecha de caducidad de una tarjeta de crédito, sin ningún otro tipo de requisito para la identificación del poseedor de la tarjeta. Además, el protocolo SSL, el más extendido

entre los comercios electrónicos, no permite garantizar en muchos casos la identidad del comprador, al no emplear certificados digitales de cliente (sólo se utilizan en la parte del servidor Web del comercio).

Además, los distintos estudios realizados en estos últimos años coinciden en señalar que la principal preocupación de los usuarios de Internet es la falta de confianza en la seguridad en las transacciones realizadas en tiendas on-line.

En un informe de Gartner Group publicado en julio de 2000, se señalaba que el índice de operaciones fraudulentas en las compras con tarjetas de crédito por Internet multiplicaba por 12 el del comercio tradicional.

En 1999, MasterCard sufrió fraudes por 740 millones de euros, un tercio más que en 1998, mientras que VISA vio crecer el fraude un 28%, hasta los 1.985 millones de euros.

Según los resultados de otro estudio publicado en Francia en marzo de 2002 y realizado por el instituto Gartner Group, el fraude detectado en los pagos con tarjeta de crédito por Internet se elevaba al 1,1%, mientras que el nivel de fraude en el conjunto de los pagos con tarjetas era de sólo el 0,026%. En la opinión de los autores, el riesgo de fraude en los pagos por Internet es "potencialmente elevado" y los métodos utilizados para las transacciones on-line tienen problemas "a menudo inquietantes".

El consumidor está protegido del fraude siempre que rechace a tiempo el cargo no reconocido en el extracto mensual de la tarjeta de crédito. Sin embargo, la "cibercriminalidad" hace aumentar los tipos de interés de las tarjetas y provoca que las comisiones cobradas a los vendedores on-line sean muy superiores a las que pagan los comercios tradicionales, por lo que a la postre termina perjudicando al usuario.

Además, en muchos casos los comercios virtuales deben cargar con todas las responsabilidades y los costes asociados a las operaciones en caso de fraude, mientras que las entidades emisoras de las tarjetas son las que normalmente asumen el importe del fraude cuando se trata de comercios tradicionales.

El fuerte crecimiento del fraude en el negocio de las tarjetas se debe, en parte, al software distribuido por piratas informáticos a través de Internet que permite que cualquier usuario con unos mínimos conocimientos de informática (basta con instalar y ejecutar dicho programa en su ordenador) pueda generar números de tarjetas de crédito perfectamente válidos.

En otros casos, la sustracción de los datos de los clientes, incluidos sus números de tarjetas de crédito, de ordenadores conectados a Internet que han sido víctimas de ataques informáticos constituye otro de los medios utilizados para obtener los datos necesarios para realizar operaciones fraudulentas en Internet.

Podemos citar numerosos incidentes relacionados con la falta de seguridad de las tarjetas de crédito. Así, por ejemplo, en el año 1999, un "cracker" localizado en Rusia consiguió hacerse con los datos de más de 300.000 tarjetas de crédito de los clientes que figuraban en la base de datos de CD Universe, un distribuidor de Compact-Disc a través de Internet.

En diciembre de 2000 la empresa Creditcards.com, dedicada a la refinanciación de deudas en los pagos mediante tarjeta de crédito, sufrió el robo de la información de otros 55.000 clientes suyos.

También en diciembre de 2000 unos "crackers" conseguían acceder a la base de datos de la empresa Egghead.com, dedicada a la venta de material informático y electrónico por Internet, con sede en la ciudad californiana de Menlo Park (Estados Unidos). Los archivos asaltados contenían información de sus 3,7 millones de clientes e incluían los datos de sus tarjetas de crédito.

En febrero de 2001 un grupo militante contra la globalización consiguió violar la seguridad del sistema informático del Foro Económico Mundial de Davos (Suiza), por lo que pudo tener acceso a los datos de 1.400 tarjetas de crédito de destacados participantes en las distintas ediciones del evento, así como otros datos personales y económicos (números de pasaporte y de teléfono móvil, direcciones de correo electrónico, claves de entrada, etc.) de personalidades como el ex-presidente estadounidense Bill Clinton, el fundador de Microsoft, Bill Gates, o el primer ministro chino Li Peng. El dominical suizo Sonntagszeitung recibió como prueba un CD-ROM enviado por los piratas con 165 Mbytes de datos sustraídos sobre los participantes. Las empresas de tarjetas de crédito tuvieron que bloquear inmediatamente las tarjetas afectadas, para evitar que los piratas pudieran realizar compras con ellas.

Posteriormente, en febrero de 2003 otro "cracker" consiguió burlar el sistema de seguridad de la empresa Data Processors International, que procesa las transacciones comerciales por correo de las compañías VISA y MasterCard, por lo que pudo acceder a los datos de ocho

millones de tarjetas de crédito en Estados Unidos.

Asimismo, las técnicas de "skimming", consistentes en la duplicación de una tarjeta de crédito cuando se registran sus datos en un falso lector incorporado a un datáfono o en la puerta de un cajero automático, permiten a bandas de delincuentes perfectamente organizados (generalmente procedentes de países del Este de Europa) sustraer este tipo de datos para realizar posteriormente operaciones fraudulentas, tanto dentro como fuera de Internet.

De hecho, en 2003 sólo en la ciudad de Madrid se registraron casi ocho denuncias diarias de usuarios estafados por la clonación de su tarjeta ("skimming"), según fuentes policiales.

Según informaba en mayo de 2002 el periódico The New York Times, el mercado de venta de números de tarjetas de crédito estaba alcanzando unas dimensiones alarmantes. Los datos robados de decenas de miles de tarjetas de crédito se estaban ofreciendo al mejor postor en Websites operados en su mayoría por residentes de la antigua Unión Soviética o de otros países de Europa del Este.

El precio por tarjeta podía oscilar entre los 40 centavos de dólar y los 5 dólares, dependiendo del nivel de autentificación logrado. Normalmente, los datos se ofrecían en paquetes de, por ejemplo, 5.000 tarjetas a 1.000 dólares, y se cobraban a través de cuentas on-line en determinados Websites como www.webmoney.ru. Estos datos se estaban empleando para realizar compras fraudulentas en tiendas on-line, así como para la extracción fraudulenta de dinero en cajeros automáticos.

Por todo ello, VISA y MasterCard han decidido reforzar la seguridad de las tarjetas de crédito, mediante la incorporación un chip que solicitará al poseedor un código secreto para cada operación. Esta reconversión de las tarjetas de crédito, que pretende frenar la desconfianza de los consumidores ante el espectacular crecimiento del fraude en Internet, supondrá una fuerte inversión para las empresas responsables de la gestión de tarjetas de crédito y de débito, como VISA, MasterCard, 4B, Red 6000, Dinners y American Express.

VISA y MasterCard han acordado una medida previa, implantada ya en algunos países como el Reino Unido, por la cual los emisores de las tarjetas de crédito deben incluir tres dígitos en la parte posterior de las mismas. De este modo, los consumidores tendrán que facilitar estos tres dígitos cuando realicen sus compras por teléfono o por Internet. También se les solicitarán detalles sobre su dirección, una medida desconocida en Europa pero habitual en Estados Unidos, país en el que se ha desarrollado con éxito el sistema AVS (Address Verification Service, Servicio de Verificación del Domicilio) para reducir el número de operaciones fraudulentas.

Podemos destacar otros dos nuevos servicios de VISA y MasterCard para reducir el fraude en la compra mediante tarjetas de crédito.

Así, mediante el servicio "Verified by Visa" (www.verifiedbyvisa.com), presentado en abril de 2002 y disponible inicialmente en Estados Unidos, el titular de la tarjeta de crédito debe registrar en el Website de Visa una contraseña que asocia a su tarjeta y que sólo él mismo conoce. Para poder comprar con la tarjeta en las tiendas on-line asociadas a este programa será necesario introducir los datos de la tarjeta y la contraseña creada por el titular.

Por otra parte, el servicio bautizado como "SecureCode" de la empresa MasterCard (www.mastercardmerchant.com/securecode/), lanzado en octubre de 2002 para las tarjetas que llevan las marcas MasterCard y Maestro, tiene un esquema de funcionamiento similar al anterior.

En este caso, el titular de la tarjeta debe registrar su propio código de seguridad a través de Internet o por teléfono. Este código es otorgado y gestionado directamente por la entidad financiera emisora de la tarjeta MasterCard o Maestro y nunca será facilitado a los comercios donde se utilice dicha tarjeta. A la hora de confirmar una operación de compra en Internet, MasterCard SecureCode solicitará al titular de la tarjeta que realiza la compra que introduzca su código secreto en una ventana que aparecerá en la pantalla de su ordenador o en su teléfono móvil, para poder completar de forma segura la transacción. Este proceso es equivalente al recibo firmado por el titular de la tarjeta, por lo que garantiza la autorización de la operación basada en la autenticación del titular a través del código secreto.

Debemos destacar, a modo de conclusión de este capítulo, que los principales problemas de operaciones fraudulentas a través de Internet vienen motivados por la utilización de un medio de pago, la tarjeta de crédito, que inicialmente no estaba pensado para la realización de compras on-line.

Además, las actuales tarjetas de crédito basadas en una tarjeta de plástico con banda magnética son muy fáciles de falsificar (mediante técnicas como el "skimming" en los cajeros automáticos) y, en muchos otros casos, estos datos se encuentran al alcance de un experto informático que pueda acceder a la base de datos del servidor de una tienda, aprovechando alguno de los fallos de seguridad que afectan a miles de ordenadores con una configuración y un mantenimiento inadecuados y que están conectados a Internet.

Los datos enviados a través de una conexión segura, mediante el protocolo SSL o SET, son muy difíciles de desencriptar utilizando los medios informáticos disponibles en la actualidad. De hecho, no se encuentra aquí la raíz del problema, sino que en muchos casos los datos de las tarjetas de crédito se obtienen a través de otras fuentes: se recopilan de tickets y recibos de compra impresos en papel en los que se incluyen el número de la tarjeta y su fecha de caducidad, se obtienen mediante la técnica de "skimming" en cajeros automáticos, se roban de bases de datos de ordenadores vulnerables a ataques informáticos o, incluso, se obtienen mediante engaños y técnicas de "ingeniería social", como podrían ser falsas llamadas telefónicas al titular de una tarjeta o cuenta bancaria para solicitar sus claves en nombre de la entidad emisora. Además, el "pharming" y el "phishing" también pueden ser empleados para robar y utilizar de forma fraudulenta números de tarjetas de crédito.

La sustitución de las tarjetas de banda magnética por "tarjetas chip", la utilización de certificados digitales de cliente y no sólo de servidor, así como el recurso a protocolos para gestionar las transacciones como SET o como SSLv3, constituyen algunas de las medidas de seguridad que deberían impulsar las entidades financieras y las empresas emisoras de las tarjetas de crédito, como VISA y MasterCard.

Además, las campañas de sensibilización y formación dirigidas a usuarios y comerciantes contribuirían a evitar la mayor parte de los casos de utilización fraudulenta de las tarjetas de crédito y otros medios de pago.

6. REFERENCIAS DE INTERÉS

- eCheck: http://www.echeck.org/
- NetCheque: http://www.netcheque.org/
- NetChex: http://www.netchex.com/
- Cybercash: http://www.cybercash.com
- eCash: http://www.digicash.com
  http://www.ecashtechnologies.com
- PayPal: http://www.paypal.com
- ePagado: http://www.epagado.com
- Morsopay: http://www.morsopay.com
- Qpass: http://www.qpass.com
- BitPass: http://www.bitpass.com
- PayStone: http://www.paystone.com
- Firstgate: http://www.firstgate.com
- PepperCoin: http://www.peppercoin.com
- Mobipay: http://www.mobipay.com
- Verified by Visa: http://www.verifiedbyvisa.com
- MasterCard Secure Code: http://www.mastercardmerchant.com/securecode/

RESEÑA CURRICULAR DEL AUTOR

Álvaro Gómez Vieites

Ingeniero de Telecomunicación por la Universidad de Vigo. Especialidades de Telemática y de Comunicaciones. Número uno de su promoción (1996) y Premio Extraordinario Fin de Carrera.

Ingeniero Técnico en Informática de Gestión" por la UNED (2004-2006). Premio al mejor expediente académico del curso 2004-2005 en la Escuela Técnica Superior de Ingeniería Informática de la UNED

"Executive MBA" y "Diploma in Business Administration" por la Escuela de Negocios Caixanova.

Ha sido Director de Sistemas de Información y Control de Gestión en la Escuela de Negocios Caixanova. Profesor colaborador de esta entidad desde 1996, responsable de los cursos y seminarios sobre Internet, Marketing Digital y Comercio Electrónico.

Socio-Director de la empresa SIMCe Consultores, integrada en el Grupo EOSA.

Autor de varios libros y numerosos artículos sobre el impacto de Internet y las TICs en la gestión empresarial.