PROYECTO INTERNACIONAL ADICAE

Ciclo de Seminarios Europeos contra el fraude en medios de pago

El fraude a debate entre los consumidores europeos

Conclusiones y propuestas de los seminarios realizados en toda Europa

Organiza:

ADICAE
Asociación de Usuarios
de Bancos, Cajas y Seguros

Con la colaboración de:

DG JUSTICIA, LIBERTAD Y SEGURIDAD
Comisión Europea

Edita:

ADICAE
Asociación de Usuarios de Bancos, Cajas y Seguros

Servicios Centrales

c/ Gavín, 12 local - 50001 Zaragoza
Tel.: 976 39 00 60
Fax: 976 39 01 99
email: aicar.adicae@adicae.net
www.adicae.net

A-S 200107

Indice

PARTE 1 - UN PROYECTO PARA TODOS LOS CONSUMIDORES DE MEDIOS DE PAGO

Presentación del libro 4
Organización de partners 5

PARTE 2 - EXPERIENCIA DE LOS PAÍSES EUROPEOS EN LA LUCHA CONTRA EL FRAUDE

Seminarios países partners 9
Fraude en los medios de pago: El gran reto de los consumidores europeos . 10
Seminario República Checa 16
Seminario Lituania 20
Seminario Bulgaria 24
Seminario Italia (1) 28
Seminario Italia (2) 32
Seminario Rumanía 36
Seminario República Eslovaca 40
Los consumidores ante el fraude en los medios de pago 44

PARTE 3 - CONCLUSIONES Y PROPUESTAS DE ADICAE

Conclusiones 50
Propuestas de ADICAE para la lucha contra el fraude en medios de pago 51

PARTE 1

Un proyecto para todos los consumidores de medios de pago

Presentación del libro

PRESENTACIÓN DEL LIBRO

En la actualidad, y cada vez más, es indiscutible el avance del uso de instrumentos que posibilitan que el consumidor pueda pagar sus adquisiciones de bienes y servicios sin utilizar monedas y billetes, es decir, los medios de pago distintos al efectivo.

Tarjetas, transferencias, cheques, banca electrónica, pago a través de telefonía móvil y otros muchos instrumentos están al alcance de casi todos los consumidores y su mercado ha experimentado un notable aumento en los últimos años. Sólo por poner un ejemplo, en la zona euro existen actualmente más de 350 millones de tarjetas en circulación que en total se utilizan en más de 12.000 millones de operaciones de pago.

Si parece desorbitado el avance mundial de los distintos medios de pago más lo es el avance de los fraudes en éstos. Los fraudes en los medios de pago distintos al efectivo son delitos de índole económico cometidos generalmente por bandas organizadas que se basan en la violación de los mecanismos de seguridad de estos instrumentos para así disponer de la capacidad de usarlo en beneficio propioen perjuicio del consumidor, que en numerosas ocasiones El uso de códigos maliciosos y programas informáticos especializados en el robo de información está proliferando de manera preocupante, al igual que las bandas organizadas que tienen sus redes extendidas por todo el mundo y que hacen de estos fraudes y otros delitos su medio de vida.

ADICAE, la única asociación de consumidores española especializada en Bancos, Cajas y Seguros, preocupada por la situación de desprotección en la que están los usuarios de estos medios de pago, ha capitaneado el proyecto internacional "Ciclo europeo de seminarios para la prevención del fraude en medios de pago en colaboración con las autoridades policiales, judiciales, asociaciones de consumidores y entidades profesionales" subvencionado por la Dirección General de Justicia, Libertad y Seguridad de la Comisión Europea y en el que colabora con otras 8 asociaciones de consumidores europeas. ADICAE y las demás asociaciones de consumidores celebraron diversos Seminarios en los diferentes países en los que se llevó a cabo el Proyecto.

La intención de esta publicación es informar sobre los Seminarios que tuvieron lugar a lo largo de toda Europa en el marco de este Proyecto, planteando en los diversos países un interesante debate entre los diferentes agentes que intervienen en el sector (entidades financieras, proveedores de tarjetas, cajeros o lectores, empresas de seguridad informática, cuerpos policiales, reguladores, Administración, etc) para llegar a poner en marcha mecanismos que garanticen la defensa del consumidor y hagan que progreso y seguridad vayan de la mano. Podemos decir que otro de los objetivos principales del Proyecto organizado por ADICAE es informar a los usuarios para prevenir de los riesgos al utilizar estos intrumentos de pago, ya que a lo largo de nuestra dilatada experiencia en el campo de la defensa del consumidor hemos observado cada mez mayores problemas en cuanto al conocimiento del uso de los medios de pago y conflictos generados entre entidades financieras y consumidores en su relación como proveedor y usuario de medios de pago.

Consideramos desde ADICE que esta publicación, como las del resto del proyecto, son una herramienta tremendamente útil y actual tanto para usuarios de medios de pago como académicos, técnicos de consumo, autoridades judiciales y policiales y en general profesionales interesados en la temática del consumo, comercio electrónico e instrumentos de pago distintos al efectivo.

ORGANIZACIONES PARTNERS

ADICAE

Asociación de Usuarios de Bancos, Cajas y Seguros de España

Bulgaria: "Asociación nacional búlgara de consumidores (BNAP)""

Eslovaquia: "Asociación nacional eslovaca de consumidores (ASC)""

Italia: "Associazione per la difesa de consumatori e ambiente (ADICONSUM)" "Movimiento Difesa del Cittadino (MDC)"

Lituania: "Lithuanian National Consumer Federation (LNCF)"

República Checa: "Sdružení českých spotřebitelů (SČS)"

Rumania: "Asociatia Nationala pentru Protectia Consumatorilor si Promovarea Programelor si Strategiilor din Romania (ANPCPPS)"

PUBLICACIONES DEL PROYECTO

Estudio jurídico sobre el fraude

Libro seminario internacional del proyecto

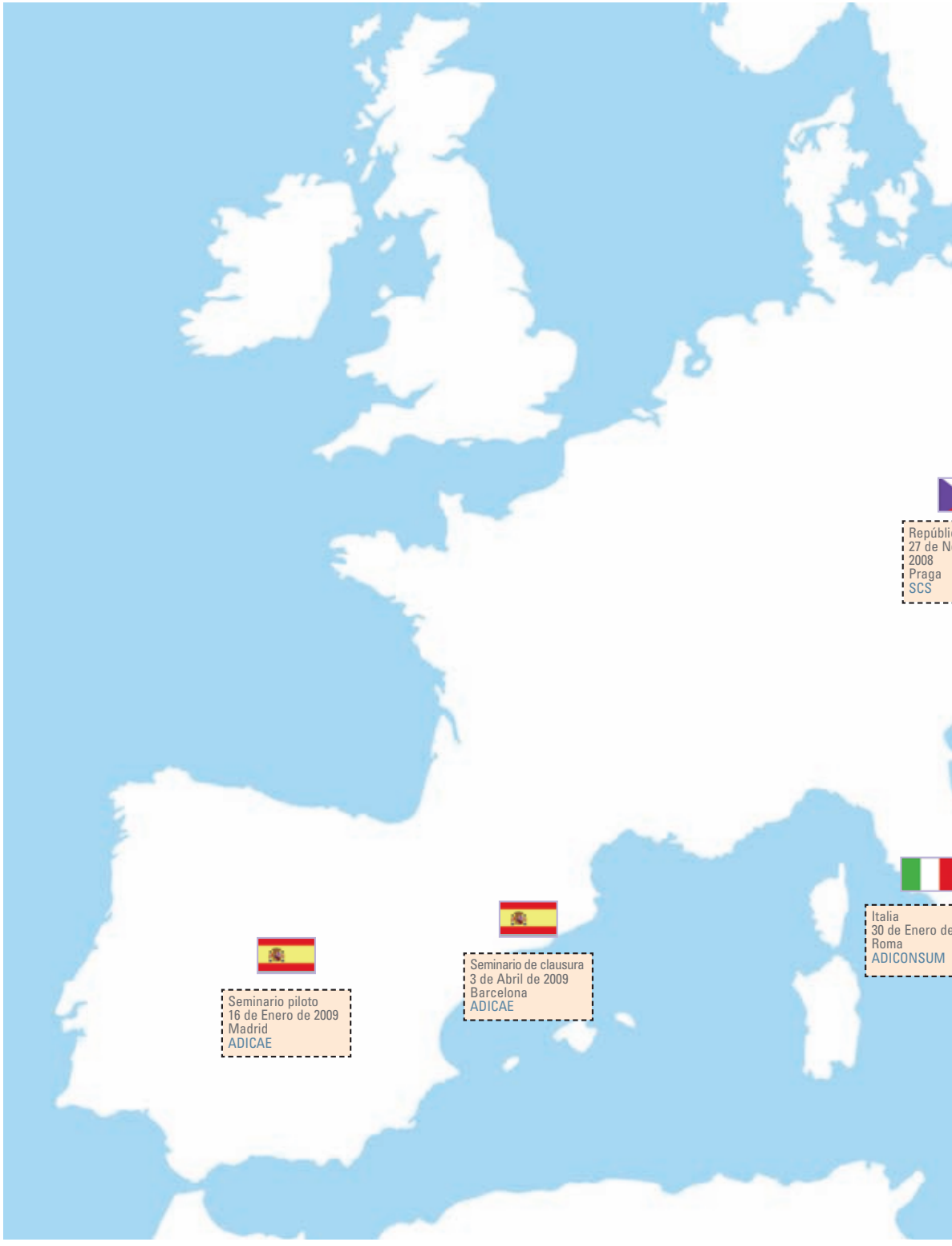
Página web del proyecto

Simulador informático contra el fraude

PARTE 2

Experiencia de los países europeos en la lucha contra el fraude

Seminarios países partners


Seminario piloto
16 de Enero de 2009
Madrid
ADICAE
Seminario de clausura
3 de Abril de 2009
Barcelona
ADICAE
Italia
30 de Enero de
Roma
ADICONSUM

Lituania
16 de Diciembre de 2008
Vilnius
LNCF

ca Checa
oviembre de

República Eslovaca
7 de Abril de 2009
Bratislava
ZSS

Rumanía
23 de Marzo de 2009
Bucarest
ANPCPPSR

Bulgaria
28 de Enero de 2009
Sofía
BNAP

e 2009

Italia
13 de Febrero de 2009
Roma
MDC

"FRAUDE EN LOS MEDIOS DE PAGO: EL GRAN RETO DE LOS CONSUMIDORES EUROPEOS"

Seminario piloto del proyecto

- Organizado por ADICAE
- Fecha: 16 de Enero de 2009
- Lugar: Hotel Convención, Madrid.

Ponentes:

D. Emilio Vicente Quintano,
Inspector Jefe del Cuerpo Nacional de Policía, jefe de la sección de Medios de Pago y contacto designado por la Dirección General de la Policía y la Guardia Civil para la colaboración con ADICAE.

Javier Berciano Alonso,
Coordinador Área - Servicios Reactivos y Operaciones INTECO-CERT (Instituto de Tecnologías de la Comunicación acudió eConfianza / Dirección de Programas. Sustituyó a Elena García, el contacto en INTECO de ADICAE. INTECO es un Instituto oficial dependiente del Ministerio de Industria que se mantiene muy activo en este tipo de cuestiones.

D. Javier Díaz Martín,
Director de Negocio de MobiPay. MobiPay es una empresa que gestional la logística y la seguridad del pago por móvil, servicio ofrecido por algunas entidades financieras como BBVA, Santander, Caja Madrid, Banesto y Banco Popular.

PRESENTACIÓN DE RESULTADOS DEL ESTUDIO SOBRE FRAUDE LLEVADO A CABO POR ADICAE

Como punto de partida a la celebración de los distintos seminarios nacionales e internacionales, se elaboró un estudio con distintas partes (jurídica, sociológica, estadística) analizando de forma pormernorizada el fenómeno de la proliferación del fraude y sus causa.

En un primer análisis se detectó que los prejuicios más comunes sufridos por los usuarios víctimas de un fraude, mediante diversos mecanismos, eran los siguientes: cargos por compras no realizadas (de forma presencial y por Internet), transferencias fraudulentas por Banca Electrónica, engaño y extorsión desde terceros países, además de la suplantación de personalidad.

El estudio de ADICAE analizó fundamentalmente contratos de tres tipos: tarjetas de crédito y de débito (tanto en su uso presencial como por Internet), banca electrónica y otros medios de pao (transferencias, domiciliaciones, pago por móvil y cheques). Se analizaron 39 tipologías distintas de contratos de medios de pago, pertenecientes a las 20 entidades financieras más importantes que los comercializan en España.

Algunas de las entidades estudiadas fueron BANCO SANTANDER-CENTRAL-HISPANO, BBVA, BARCLAYS, CITIBANK,BANCO CAIXA GERAL, BANESTO, OPENBANK, CAJASOL, CAIXA GALICIA, IBERCAJA, CAJA LABORAL POPULAR, LA CAIXA, CAIXA CATALUÑA, CAJA INMACULADA, CAJA VITAL KUTXA, CAJA ESPAÑA, CAJA DUERO, CAJA RURAL DEL SUR.

El problemas de las cláusulas abusivas

Es evidente que existen y seguirán existiendo cláusulas abusivas en los contratos de los medios de pago, que contravienen tanto Recomendaciones (normativa no vinculante a nivel europeo) como Códigos de Buena Conducta adoptados por la industria. Por esta razón se deduce, al contrario de lo que afirman las entidades financieras, que la autorregulación y la normativa "blanda" no son auténticas soluciones a este problema, sino que sólo contribuyen a alargar la situación de indefensión del consumidor. En cuanto a las claúsulas abusivas, uno de los principales factores que posibilitan su existencia, legitimando así las malas prácticas de las entidades financieras, es la escasez de educación financiera (la cual por otro lado, poco o nada hacen las entidades por mejorar); gracias a la profunda experiencia de ADICAE se ha comprobado que los consumidores en general no se leen de forma exhaustiva los contratos ni entienden qué es exactamente lo que están firmando y, por tanto, a qué se compromenten.

También se ha podido ver la ausencia de control de los contratos de adhesión en servicios ofrecidos por las entidades financieras, principalmente por su organismo regulador (Banco de España); además de contravenir la Ley de Condiciones Generales de Contratación, quedando las mismas recogidas en un Registro regulado por el Ministerio de Justicia . Por último, cabe destacar la ausencia de vías preventivas de la comercialización de contratos con este tipo de cláusulas que socavan los derechos de los usuarios.

Como primeras medidas para que el usuario pudiese protegerse ante esta situación abusiva establecida por las entidades financieras, destacan la negociación colectiva y previa para la supresión de las cláusulas abusivas, la contratación de mecanismos de seguridad adicionales por parte de las entidades que reduzcan el propio fenómeno del fraude, la comparación entre las diferentes condiciones ofrecidas por las entidades financieras, además de la solicitud de asesoramiento profesional e independiente a una Asociación de Consumidores en cualquier momento (anterior o posterior) de la contratación.

En el peor de los casos, cuando ya se ha sufrido el perjuicio se debe reclamar a la entidad financiera por medio del sistema extrajudicial de resolución de conflictos existente, que contempla reclamar ante el Banco de España ante una reclamación no resuelta satisfactoriamente por el Servicio de Atención al Cliente de la Entidad, aunque este sistema posee numerosos defectos y lagunas como viene denunciando ADICAE desde hace muchos años.

LA EXPERIENCIA DE ADICAE EN LA LUCHA CONTRA EL FRAUDE

El conocimiento de la realidad de ADICAE pone de manifiesto que es necesario que se garanticen los derechos básicos de los usuarios ante los fraudes en medios de pago. Éstos suponen indudables beneficios y comodidades para los consumidores aunque sólo en el caso de ser bien entendidos y utilizados. Los fraudes en medios de pago alcanzan unos 4.122 millones de Euros anualmente, lo que hace que incluso la polícia se declare rebasada y sobrepasada ante estos fraudes.

En la actualidad, puede destacarse que en materia de protección de los consumidores en materia de fraude en medios de pago la principal regulación existente es la Recomendación del 30 de Julio de 1997: Se limita la responsabilidad del usuario en los primeros 150€ en caso de fraude, salvo negligencia en la custodia o uso de la tarjeta. También es notoria la insuficiencia (si no ausencia) normativa para la Banca Electrónica; por lo que podemos decir que la Legislación favorable a las entidades.

Sin embargo, podemos entrever algunas mejoras en cuanto a la legislación que próximamente va a adoptarse, como es el caso de la Directiva de Medios de Pago (2007), actualmente en proceso de transposión, que establece que son las entidades quienes deben probar la falta de diligencia en el uso de la tarjeta de crédito. Podemos destacar en cuanto a principal punto negativo la Incertidumbre en cuanto a la protección del consumidor en los nuevos medios de pago que surjan en el futuro.

La nueva problemática del fraude en medios de pago

En el pasado, los fraudes eran cometidos normalmente por hackers que actuaban por su cuenta sin interactuar con otros criminales, muchas veces sin motivación económica; sin embargo, en la actualidad los fraudes en medios de pago son cometidos por bandas criminales muy jerarquizadas, con intenciones lucrativas y que invierten las ganancias de su actividad en cuestiones como el terrorismo, tráfico de drogas y de armas, etc.

Los fraudes en medios de pago en la actualidad no están focalizados en determinados puntos como antes, sino que se cometen a nivel transnacional o incluso transcontinental (por ejemplo, se roban los datos en un país determinado y las tarjeta se clona en un país diferente). Por ello, se considera que la lucha contra el fraude debe llevarse a cabo a nivel transnacional y con la cooperación de todos afectados.

Iniciativas europeas en la luchas contra el fraude

En cuanto a las iniciativas que se han tomado a nivel europeo en cuanto a la lucha contra el fraue, cabe destacar diversas cuestiones: la existencia de diversa legislación a nivel europeo (que ya hemos comentado), la cooperación entre la policía de los diversos países a través de Europol., la creación de diversos grupos consultivos de expertos, el desarrollo de la SEPA y los planes de acción llevados a cabo por la Comisión Europea (cabe destacar el Plan de Acción 2004-2007)

Concretamente, las prioridades del Plan de Acción para la Prevención del Fraude elaborado por la Comisión Europea son:

1. La seguridad de los productos y sistemas de pago.

2. La cooperación entre las administraciones públicas y el sector privado.

3. La integración de los nuevos estados miembros en el nuevo marco para la prevención del fraude en la Unión Europea.

4. El estrechamiento de lazos con los países vecinos a la Unión Europea que afectan a la situación del fraude.

Cómo se puede apreciar, la iniciativa llevada a cabo por ADICAE se adecúa especialmente al Proyecto de ADICAE.

ADICAE tiene una larga experiencia en cuanto a acciones para la lucha contra el fraude. Desde el ECCG (Grupo Europeo Consultivo de consumo), subgrupo FSCG (Crupo de Consumidores de Servicios Financieros). ADICAE también participa en el FPEG (Grupo de expertos en la Prevención del Fraude) con proveedores de medios de pago (VISA, Mastercard), Comisión europea, Instituciones nacionales, asociaciones de bancos e, industria de medios de pago y asociaciones de consumidores.

ADICAE ha detectado que los usuarios de medios de pago tienen numerosos conflictos con las entidades financieras que prestan estos servicios; podemos dividirlo en dos categorías principales:

CLAUSULAS ABUSIVAS

- No inclusión de límites de responsabilidad (Recomendación 150€). No inlcusión de límites de responsabilidad (Recomendación 150€).
- Carga de la prueba trasladada al consumidor.
- Presunción de culpabilidad del usuario.

MALAS PRÁCTICAS BANCARIAS

- No cumplimiento de las Sentencias del Banco de España al respecto.
- Retraso de la migración al esquema Chip-EMV.
- Sistemas de seguridad no óptimos.
- Asociaciones de Consumidores ninguneadas a pesar de ser los representantes autorizados

Por tanto, como conclusiones a la exposición destacamos las siguientes:

■ Deben encontrarse ante la problemática del fraude:
- Soluciones jurídicas.
- Solutions técnicas y económicas
- Las Entidades Financieras deben apostar por el fin de este problema, como uno de los agentes que más intervienen en el mismo.
- Los Consumidores deben tener a su alcance verdaderas herramientas para su protección efectiva, y unirse a una asociación de consumidores que velen por sus derechos y realicen una defensa eficaz en esta materia.
- No puede haber un auténtico desarrollo de los medios de pago distintos al efectivo sin la confianza de los consumidores

Consejos ADICAE para evitar el fraude

Desde ADICAE se ofrece una serie de consejos que pueden ser útiles a los ciudadanos para prevenir cualquier fraude.

- Desconfíe de promesas de dinero rápido.
- Evite acceder a servicios de banca electronica desde ordenadores públicos.
- Sanee su ordenador periódicamente.
- Compruebe de vez en cuando la cuenta periódica asociada a la tarjeta.
- Ojo con hacer click en enlaces o descargar programas desconocidos.
- Nueva contraseña para acceder al banco: Cambie periódicamente sus claves.
- Filtre los mensajes de desconocidos.
- Identifique al interlocutor o prestador de servicios.
- Asegurese al hacer alguna operación con datos bancarios o tarjeta del certificado de la empresa.

LA LUCHA CONTRA EL FRAUDE POR PARTE DE LA ADMINISTRACIÓN ESPAÑOLA

La experiencia de INTECO

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), organismo promovido por el Ministerio de Industria, Turismo y Comercio, es una plataforma para el desarrollo de la Sociedad del Conocimiento, dirigida a Ciudadanos y Pymes a través de proyectos del ámbito de la innovación y la tecnología. INTECO tiene un doble objetivo: contribuir a la convergencia de España con Europa en la Sociedad de la Información y promover el desarrollo regional, enraizando en León un proyecto con vocación global. INTECO desarrolla, entre otras, iniciativas de seguridad tecnológica, accesibilidad e inclusión en la sociedad digital y soluciones de comunicación para particulares y empresas.

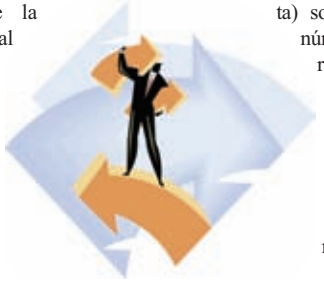
El Instituto lleva a cabo diferentes programas:

Seguridad

- Centro de Respuesta a Incidentes Informáticos en Tecnologías de la Información para PyMEs y Ciudadanos

- Observatorio de la Seguridad de la Información: tiene como misión principal la de analizar, describir, asesorar y difundir la cultura de la seguridad y la confianza en la Sociedad de la Información.

- Centro Demostrador y potenciador de Seguridad para la PyME



Accesibilidad

Busca garantizar el derecho de ciudadanos y empresas a relacionarse electrónicamente con las AAPP:

- Centro de Referencia en Accesibilidad y Estándares Web: tiene como misión principal el impulsar las técnicas de construcción de sitios Web en la Administración Pública teniendo en cuenta requisitos de accesibilidad, facilidad de uso y adopción de estándares de construcción.

Las nuevas formas de fraude en tarjetas de crédito

En Cajeros Automáticos

El ladrón consigue ver el PIN que el usuario teclea, que utiliza posteriormente, robándole a este la tarjeta.

Manipulación del cajero mediante dispositivos en la ranura de la maquina y una micro-cámara oculta: al introducir la tarjeta en el lector del cajero se graban los datos de la tarjeta y al marcar el PIN los números son grabados por la micro-cámara.

Bloqueo de la tarjeta en el cajero: un extraño le dice que vuelva a introducir el PIN. Este lo memoriza y lo utiliza después con la tarjeta todavía bloqueada.

Telefónicamente:

Cuando recibimos una llamada ofreciéndonos algo y nos piden su información de la tarjeta.

Haciéndose pasar por la entidad emisora de la tarjeta y solicitar algunos datos de confirmación.

De otra entidad, ofreciéndonos una oferta, para lo cual necesitan transferir los fondos a la nueva tarjeta.

Informándonos de que hemos ganado un premio y que necesitan nuestros datos para cobrarnos los gastos de envío.

El auge del fraude por internet

-"Phishing": entidad financiera o comercio falsos o suplantados: realizamos una compra en una web que aparenta ser un comercio, pero que en realidad es un cebo para hacerse con nuestros datos o recibimos un correo electrónico supuestamente de nuestra entidad financiera (suplantación fraudulenta) solicitando nuestros datos (claves de acceso, números de tarjeta, pines,…).Una entidad bancaria NUNCA va a solicitar por correo electrónico nuestros datos de identificación.

-Realizamos una operación en un comercio y posteriormente nos pasan adeudos no autorizados previamente (p.ej. suscripciones a determinados servicios).

-Comercio falso o suplantado: realizamos una compra en una web que aparenta ser un comercio, pero que en realidad es un cebo para hacerse con nuestros datos (phishing).

-Fraudes de subastas: las estafas relacionadas con subastas se han convertido en el tipo más común de fraude por Internet, y representan el 42% de todas las quejas recibidas por la Unidad de fraudes en Internet de la Liga nacional de consumidores de EE.UU. en los últimos años. Los fraudes de subastas se producen en los casos en los que un artículo que ha ganado en una subasta en línea no le llega nunca, o bien cuando sus características se han falseado de forma significativa.

- Artículos no entregados: los consumidores simplemente no reciben los artículos que han adquirido en Internet. Después de los fraudes en las subastas, éste es el segundo tipo más común de estafa en línea.

- Ofertas económicas falsas: es muy probable que ya haya recibido mensajes de spam con este tipo de propuestas. Una persona, quizá de Nigeria, se pone en contacto con usted porque, al parecer, es el heredero de una importante suma económica. Todo lo que tiene que hacer es propor-

cionar los datos de su cuenta bancaria y abonar una pequeña cantidad de dinero.

- Cheques falsos para la compra de productos o servicios en este caso, el estafador compra un producto o un servicio, envía al vendedor un cheque por una cantidad superior al precio, y le pide que haga una transferencia por valor del dinero sobrante. El cheque original se rechaza y el vendedor no sólo se queda sin recibir el pago, sino que además pierde el dinero que ha mandado en la transferencia.

- Planes de trabajo en casa y esquemas piramidales: en estos esquemas, se prometen grandes cantidades de dinero a cambio de trabajos realizados en su propia casa o si consigue más distribuidores para un producto determinado. A cambio, la víctima paga por kits de trabajo que nunca recibe, o compra grandes cantidades de un producto que no quiere nadie, o bien invierte en una pirámide que se desmorona antes de obtener ningún tipo de compensación. En todos los casos, el desembolso de dinero supera con creces el beneficio obtenido.

- Préstamos falsos o pago de una cuota para obtener créditos: a menudo basados en mensajes de spam, se trata de falsas promesas de concesión de préstamos, sobre todo para ayudar a ciertos consumidores a saldar sus deudas o a mejorar su situación de crédito. En estas estafas, el prestamista pide una cuota para sufragar los gastos de solicitud del crédito y luego desaparece del mapa.
- Fraudes relacionados con organizaciones benéficas: suelen aparecer cuando se producen desastres naturales y otras tragedias, que algunos embaucadores aprovechan para hacerse pasar por organizaciones benéficas legítimas en correos electrónicos y sitios Web destinados a obtener el dinero de donantes bien intencionados.

El nuevo fenómeno de la inversión a través de Internet

Se ha generalizado en los últimos años la banca a distancia y más aún, las entidades que sólo operan por internet. Algunas entidades sólo funcionan como cuentas de ahorro y no admiten servicios tan comunes como domiciliacion de cobros; otras sí que permiten las operaciones habituales (transferencias, disponer de tarjetas de cajeros automáticos, etc.)

Precauciones del consumidor con los servicios financieros on-line

- Actualizar el software de nuestro ordenador regularmente, comprobar periodicamente el nivel de seguridad con el que estas conectado (scan de pertos, antivirus, firewall, datos sensibles en la configuración de cuentas...).

- Realizar periódicamente copias de seguridad de tus datos.

- Introducir información susceptible de generar peligros, como por ejemplo nuestro número de cuenta, sólo cuando la página que lo solicita sea segura. (por ejemplo aquellas que empiecen por “https”.) y encriptar los mensajes y ficheros más importantes.

Consejos ADICAE para evitar estos fraudes

A la hora de tratar con productos, servicios, oportunidades de inversión y donaciones en Internet, la palabra clave es precaución. Los consejos que aparecen a continuación pueden ayudarle a identificar y a evitar algunas de las estafas más comunes en Internet:

- No haga negocios ni envíe dinero a organizaciones en las que no confíe o cuya veracidad no pueda comprobar.

- Acuda a la agencia de protección al consumidor de su ciudad y consulte en la oficina de buenas prácticas comerciales para comprobar que no existe ninguna queja relacionada con una organización que le resulte desconocida.

- Confirme los supuestos datos de contacto de las organizaciones con las que no esté familiarizado, como por ejemplo las direcciones físicas, los números de teléfono y los domicilios sociales. No establezca ningún tipo de contacto comercial con las organizaciones que no proporcionen esta información sin ningún tipo de restricción.

- Antes de pujar por un artículo, haga todo lo que esté en su mano para confirmar el historial y los datos de contacto del vendedor en la subasta.

- No adquiera piezas de coleccionista o artículos únicos en las subastas por Internet. Si no puede examinar el artículo de antemano, ¿cómo puede estar seguro de que es auténtico?

- No envíe dinero en efectivo ni realice transferencias para comprar productos o servicios en línea o en subastas.

- Insista en recibir un recibo por el valor exacto de los productos o servicios que ha vendido por Internet. No ingrese nunca un cheque que haya recibido por un valor superior al precio negociado.

- Incluso si conoce a la organización benéfica, confirme por teléfono su solicitud en línea antes de realizar la donación.

- Utilice el sentido común cuando responda a ofertas para conseguir dinero fácil. Si parece ser demasiado bueno para ser verdad, es más que probable que sea una estafa.

- Extreme las precauciones si recibe peticiones no solicitadas para el pago de sumas de dinero por adelantado por parte de supuestos prestamistas, agencias gubernamentales u otras organizaciones.

- Realice todas las transacciones en línea con tarjetas de crédito en sitios Web seguros. Incluso si ha tomado todas las precauciones debidas y ha decidido realizar un negocio con una persona, no hay ningún motivo que le impida usar el método de pago más seguro.

PAGOS A TRAVÉS DEL MÓVIL

La propuesta de Mobipay

El sistema Mobipay trata de resolver muchas de las carencias en cuanto a operabilidad y seguridad de las demás formas de pagar sin utilizar monedas y billetes y que utiliza el pago a través del móvil. MOBIPAY España S.A es la plataforma española estándar para realizar pagos y otras transacciones de forma segura a través del teléfono móvil

Funcionalidades y Tipología

MOBIPAY permite activar a través del teléfono móvil diferentes medios de pago financieros (tarjetas Visa, Mastercard,…) así como activar pagos contra la cuenta del teléfono móvil, convirtiendo a éste en un canal transaccional para la realización de todo tipo de pagos en remoto.

¿Cómo funciona el pago por móvil?

- El consumidor tiene asociado a su teléfono móvil una "cartera" en la que puede activar varios medios de pago de distintos emisores.

- En cada transacción, el usuario puede elegir pagar con cualquiera de los medios de pago que tiene activados en su cartera y son admitidos en el establecimiento.

- Existe una "clave de autorización personal" (PIN) por cada medio de pago que es gestionada por la entidad emisora:
- Sólo es conocida por el titular.

- El usuario autoriza cada transacción mediante la introducción del PIN o el código que le indique en cada caso el emisor del medio de pago, siendo equivalente a la firma manuscrita.

En la actualidad la operativa de servicios que se ofrece es: Pago de compras (remotos y en proximidad), traspaso de fondos, consultas, etc.

Grandes incógnitas y problemas en la seguridad

Problemas de funcionalidad en el caso de que el consumidor perdiera la cobertura o la batería de su móvil ya que impediría al usuario realizar la transacción con los problemas que ello conllevaría.

En caso de robo físico del móvil ¿habría algún problema para dar de baja el servicio?

Por parte de la entidad no se aclara lo que ocurre si el consumidor tuviera un virus en su teléfono móvil o la señal estuviera siendo captada por otro terminal

SEMINARIO REPÚBLICA CHECA

- Organizado por SCS, Asociación Checa de Consumidores
- Praga, 27 de Noviembre de 2008
- Hotel Beránek, salón Václav (C/ Belehradska, 110)

Sdružení českých spotřebitelů (SČS). La Asociación Checa de Consumidores, establecida en 1990, estableció como prioridad el desarrollo de actividades enfocadas a apoyar un enfoque preventivo y dotar de herramientas relacionadas con la protección del consumidor. Estas actividades tienen como principal objetivo mejorar las relaciones entre proveedores de servicios y consumidores, intentando contribuir y apoyasr el desarrollo de mercados de libre competencia además de mecanismos efectivos para la protección del consumidor.

PROGRAMA:

10:00 APERTURA Libor Dupal, Presidente Sdružení českých spotřebitelů (Asociación Checa de Consumidores)

10:15 MESA REDONDA: SITUACIÓN DE LOS MEDIOS DE PAGO Y FRAUDES EN LOS MISMOS EN LA REPÚBLICA CHECA
František Klufa, Árbitro Financiero
Libor Dupal, Presidente Sdružení českých spotřebitelů (Asociación Checa de Consumidores)

11:00 MESA REDONDA: OPINIONES DE LOS AGENTES SOCIALES(I)
Jiří Beran, Ministerio de Economía y Finanzas
Michal Hradecký, Jefatura de Policía de la República Checa;
Karel Kuchařík, Jefatura de Policía de la República Checa;
Michaela Kolzová, Colegio de Abogados de la República Checa

12:00 MESA REDONDA: OPINIONES DE LOS AGENTES SOCIALES(II)
David Pikálek, Responsable de Seguridad de Banca Electrónica de la entidad financiera Česká spořitelna
Ladislav Pauker, representante de la Asociación Checa de Bancos
Karel Kadlčák , Presidente del Comité de Seguridad de la Asociación para las Tarjetas Bancarias
Hanka Michovská, representante de la Asociación de Electrónica de Consumo

13:00 MESA REDONDA:
Ponentes de las anteriores mesas, invitados y demás asistentes al Simposio

ASISTENTES: Más de 40 personas en total; con representantes de la Policía, representantes de diversos Ministerios, sector bancario (Asociación Checa de Bancos, Česká spořitelna), representantes de organizaciones empresariales (Confederación Checa de Comercio y Turismo, Oficina Local de Comercio-Brno), representantes de insituciones de Consumo (Agencia Estatal de Inspección de Consumo- Brno, asesores financieros, etc), sindicatos (ČMKOS), representantes de Universidades

DIFUSIÓN : Acudieron medios de prensa generalistas como las cadenas de televisión TV1 y TVZ1, donde el señor Dupal y el señor Klufa realizaron sendas entrevistas para divulgar los contenidos del Proyecto. Asimismo, se emitió la correspondiente nota de prensa.

Datos estadísticos R. CHECA

■ El aumento del acceso a Internet de los usuarios checos ha sido enorme en los últimos años, puesto que se pasó del 29% de los hogares en República Checa conectados a Internet en 2006 al 46% de los mismos en 2008.
■ Si observamos el avance de la banda ancha en República Checa, podemos observar que el mismo también es notable: pasamos de un 17% en 2006 a un 36% en 2008.
■ Como principales actividades para las que los usuarios checos se conectan a Internet, encontramos la lectura de noticias y periódicos on-line (33% de los usuarios) y la contratación de viajes y alojamiento (26%). La actividad que menos les interesa entre las consideradas es la búsqueda de trabajo y envío de solicitudes de empleo, ya que sólo un 5% de los usuarios checos utilizan este recurso.

SITUACIÓN LEGISLATIVA DEL FRAUDE EN MEDIOS DE PAGO EN REPÚBLICA CHECA

La transposición de la Directiva sobre Medios de Pago

La Directiva sobre servicios de pago 2007/64/CE fue aprobada a finales de 2007 (aunque su diseño ha sido preparado durante varios años). Su objetivo es armonizar la regulación de los servicios de pago en la UE. Consta de una parte relativa a disposiciones de carácter más público (las provisiones de acceso a la prestación de estos servicios por parte de empresas) y de una parte de carácter más privado (por ejemplo, relativo a los derechos mutuos de los proveedores de medios de pago y usuarios)

Esta Directiva es fruto de un complicado compromiso mutuo negociado entre las diversas partes (y respetando la discrecionalidad nacional de los Estados Miemebros) En virtud del principio de la plena armonización (artículo 86 de la presente Directiva), los Estados Miembros no pueden modificar la Directiva (tanto moderada como estrictamente)

Calendario de la Transposición en la República Checa

- Primavera 08: Consulta a los diferentes agentes sociales y económicos
- Octubre de 2008: Inicio preparación del texto
- Noviembre-Diciembre 2008: Periodo de Alegaciones
- Enero-Febrero 2009: Borrador remitido al Consejo Legislativo y a la Comisión de Gobierno
- Marzo 2009: Borrador remitido Gobierno
- Abril-Junio 2009: Votación por la Cámara de Diputados
- Agosto 2009: Aprobación por parte del Senado, Presidente de la República
- 1 Noviembre de 2009: Eficiencia (fin del plazo de transposición)

Proyecto de Ley sobre los sistemas de pago: Un reto para las entidades financieras y emisores de medios de pago

La nueva Ley de Sistemas de Pago supone la transposición de la Directiva europea de Servicios de Pago, y por tanto la regulación de la emisión de dinero electrónico y gestión de sistemas de pago por parte de empresas privadas.

A destacar 6 de las 146 secciones:

- Disposiciones generales (comunes, transitorias y finales).
- Los sistemas de pago.
- Derechos y obligaciones para la prestación de sistemas de pago.
- Sección empresas privada (título III y IV de la Directiva).
- Las infracciones administrativas.
- Disposiciones comunes, transitorias y finales.

En cuanto a las Disposiciones generales establecidas por la Directiva, cabe destacar que se pueden definir los servicios de pago (de conformidad con el anexo de la Directiva) como:

- Operaciones de pago (depósitos, retiros, transferencias)
- Remesas.
- Emisión y gestión de medios de pago.
- Pagos por instrumentos a distancia.

En cuanto al Ámbito de aplicación, consideramos que son todas las transacciones realizadas por un medio de pago distinto al efectivo, que sean:

- Directamente del ordenante al beneficiario.
- Transvase de fondos.
- Documentos de instrumentos de pago (cheques, facturas, comprobantes y gastos de envío).

En éstas disposiciones también se establece quién puede prestar servicios de pago: los Bancos, cooperativas de crédito, entidades de dinero electrónico, proveedores de medios de pago de pequeña escala, titulares de licencia postal y Banco Nacional Checo.

De conformidad con el artículo 26 de la Directiva, los proveedores de medios de pago de pequeña escala:

- Puede proporcionar servicios de pago de hasta 3 millones de € / mes.
- Personas físicas y jurídicas sobre la base de la inscripción en el Banco Nacional Checo (lo permite procedimiento simplificado).

Cabe destacar el Artículo 81 de la Directiva, que establece como supervisor de los proveedores de servicios de medios de pago al Banco Nacional Checo

También aparecen diversas infracciones administrativas establecidas por la nueva Ley con multas por el incumplimiento de los preceptos establecidos por la presente normativa.

Nueva normativa referente a transacciones no autorizadas

La trasposición de la Directiva de Servicios de Pago establece consideraciones relevantes en cuanto a las transacciones no autorizadas, dividiendo las responsabilidades entre el ordenante y el proveedor de servicios de medios de pago

La operación está autorizada si cuenta con el consentimiento del ordenante - debe presentarse el formulario o justificante de consentimiento. Si el proveedor es responsable de la pérdida, estará obligado a devolver la cantidad que el ordenante o acreditados haya perdido a una cuenta de titularidad del ordenante. Este compromiso es exigible de inmediato.

El alcance de la responsabilidad está graduado para el proveedor, dependiendo de si el contribuyente tiene una cierta parte de la culpa con respecto a la operación de pago no autorizada.

Debemos recordar que ya existe normativa europea (aunque no vinculante) que establece que salvo cuando es completamente responsable el ordenante, ante las pérdidas, robos, etc. le corresponde al mismo asumir sólo los 150 primeros Euros de la pérdida. Después de la notificación de pérdida, robo, etc corresponde al proveedor en su totalidad, salvo en los casos de engaño por el ordenante como hemos dicho.

El proyecto de ley contiene una disposición destacable: al utilizar un medio de pago (tarjetas de crédito y otros) que haya registrado la operación un prestador de servicios no significa necesariamente que la operación fue autorizada por el ordenante o que haya actuado de forma fraudulenta; o que intencionalmente o por negligencia grave, o violación de cualquiera de sus obligaciones en relación con el pago. Al mismo tiempo, en caso de litigio serán de aplicación aquí el principio de la libre evaluación de las pruebas por un tribunal, en virtud de la Sección 132 del Procedimiento Civil.

En cuanto a la carga de la prueba, se establece la obligación del prestador de presentar los documentos si el usuario reclama ante la operación de pago, por considerar que ha sido autorizada o aplicada indebidamente.

La esencia de este requisito es la prueba de ciertos hechos (verificada, debidamente registrada, consideración de fallos técnicos); aunque no se trata, sin embargo, de la carga de la prueba tradicional en términos de derecho procesal.

La diferencia con la carga de la prueba clásica es que si el proveedor no cumple con su obligación, sólo por esta razón no perdería cualquier disputa, por ejemplo; pero podría ser directamente considerado responsable de los daños. No nos encontramos ante una transferencia automática de la carga de la prueba.

La causa de esta disposición es que el usuario no tiene capacidad material de demostrar estos hechos para así poder defenderse, al contrario de lo que comunmente establecen los contratos de medios de pago (cláusulas abusivas).

LA VISIÓN DE INDUSTRIA Y ENTIDADES PRIVADAS:

Primeras medidas de las entidades financieras de la República Checa en la lucha contra el fraude en medios de pago

Česká spořitelna, la principal Caja de Ahorros de la República Checa (y presente en muchos otros países del Este de Europa) ha desarrollado mecanismos para la protección de sus clientes contra los fraudes en medios de pago. Ha habido un aumento significativo de la protección de sus clientes por las medidas de seguridad adicionales que ha introducido en los últimos años, como la tecnología 3D Secure. También la cooperación con las empresas de seguridad fabricantes de antivirus para buscar maneras de bloquear el spam de forma efectiva ha sido otra de las estrategias llevadas a cabo por esta entidad financiera.

Otra de sus políticas ha sido cambiar las prácticas bancarias para lograr una mayor protección del cliente. Anteriormente, había transacciones que no necesitaban autorización, pero que ahora sí la requieren. Para otras transacciones, en el pasado era sólo necesario un código de autorización del cliente (por ejemplo, para cambiar la aplicación de alertas SMS); pero ahora es necesario personarse en la sucursal para poder configurar este servicio.

La Caja de Ahorros Checa opera principalmente en países del Este. Más de 1,2 millones de clientes utilizan la banca directa (por Internet, teléfono móvil u otros medios telemáticos) de la Caja de Ahorros Checa; dispone de varias opciones para que los clientes puedan operar en su cuenta: en persona -en la sucursal-, a través de teléfono, Internet, cajeros automáticos y por teléfono móvil;

Como principales canales de banca directa de la Caja de Ahorros Checa -SERVIS 24- cabe destacar Internet, teléfono y GSM. Los clientes de esta entidad financiera son sobre todo clientes individuales, pequeñas y medianas empresas, municipios y grandes corporaciones.

CONCLUSIONES

- A pesar de que ya existen algunos foros para la discusión de esta problemática, como una Comisión para la Seguridad en la que las principales entidades fiancieras que operan en la República Checa participan; es necesaria una aún mayor cooperación entre los diversos agentes, incluyendo en el diálogo a los representantes de las asociaciones de consumidores, excluidos hasta este momento de ese proceso.

- Gracias a la nueva normativa europea, en República Checa además de en toda Europe parece que se va a solucionar la problemática de la carga de la prueba en casos de fraude en medios de pago. Se establece, en virtud de la Directiva sobre Medios de Pago, la obligación del prestador de presentar los documentos si el usuario reclama ante la operación de pago, por considerar que ha sido autorizada o aplicada indebidamente.

- Las entidades financieras introducen nuevos mecanismos para la protección de los instrumentos de pago utilizados por los consumidores. No obtante, esto no significa ni mucho menos que la inversión en seguridad sea óptima, que se vayam a erradicar los fraudes en medios de pago o que los consumidores tengan los conocimientos necesarios para efectivamente aprovechar estos nuevos mecanismos que mejoran su protección.

SEMINARIO LITUANIA

- Organizado por LNCF, Federación Nacional de Consumidores Lituanos
- Vilnius, 16 de Diciembre del 2008
- Sede del Ministerio de Justicia de Lituania

Federación Nacional Lituana de Consumidores (LNVF): LNVF se fundó en el año 2000, tiene su sede en Vilnius. Sus objetivos son proteger los derechos e intereses sociales y económicos de los consumidores; educar a los consumidores y empresarios sobre cuestiones de política de consumo y buscar el progreso de la seguridad de los consumidores de Lituania y de la UE. LNVF ofrece consejo a los consumidores en sus oficinas, por correo electrónico y telefónicamente informándoles de la legislación relativa a cualquier tipo de disputa con empresas proveedoras de bienes y servicios, además de efectuar labores de mediación en conflictos de consumo.

PROGRAMA:

10.00 APERTURA: Raimundas Jurka, Ministro de Justicia de la República de Lituania

10:15 PRESENTACIÓN DEL ESTUDIO SOBRE EL FRAUDE EN MEDIOS DE PAGO EN LITUANIA:
Zilvinas Jancoras, Experto LNCF

10.30 PERSPECTIVA DEL FRAUDE EN MEDIOS DE PAGO SEGÚN EL BANCO NACIONAL DE LITUANIA
Algimantas Sodeika, Director de la Currency Examination Division (División de Comprobación de la Moneda - Departamento de dinero en efectivo del Banco de Lituania)
Liutauras Zygas, Director de Jurisprudencia del Banco de Lituania

11.10 INICIATIVAS ACADÉMICAS EN LA VERIFICACIÓN DE MEDIOS DE PAGO
Raimondas Vasiliauskas, Facultad de Seguridad Pública de la Universidad Mykolas Riomeris en Kaunas

11:30 LA LUCHA CONTRA EL FRAUDE EN MEDIOS DE PAGO EN EL MARCO DE LA DEFENSA NACIONAL
Teniente Coronel Saulius Japertas, Director del Servicio de Sistemas de Información y Servicio de Defensa Nacional de las Comunicaciones de la República de Lituania

12:10 INICIATIVAS DE LA ADMINISTRACIÓN REGULADORA EN MATERIA DE PREVENCIÓN DE LOS FRAUDES EN MEDIOS DE PAGO
Rytis Rainys, Director de la División de Seguridad de la Información en la Agencia Reguladora de las Comunicaciones

13:00 LUCHA POLICIAL Y COOPERACIÓN CON DEMÁS AGENTES PARA LA PREVENCIÓN DEL FRAUDE EN MEDIOS DE PAGO
Vytautas Gailiusas, Departamento de la Policía Criminal, Policía Nacional Lituana
Aurelijus Banys, Director del Departamento de Investigación de Delitos Económicos de la Comisaría de Policía en Kaunas

Datos estadísticos LITUANIA

- Aumento del beneficio del mercado electrónico: desde el 2003 ha aumentado desde un 6 a un 11,5%).
- Más de la mitad de los encuestados había intentado usar tarjetas electrónicas de otras personas y alrededor del 80% no tuvo ninguna dificultad para ello.
- Más del 60% de los encuestados piensan que la protección de los medios de pago electrónico es incierta y pobre, sobre el 70% aprueba la instalación de escáner de códigos PIN en todas las tiendas.

NUEVOS MECANISMOS PARA LA VERIFICACIÓN DE MEDIOS DE PAGO

Las instituciones académicas como precursoras de nuevos métodos para la lucha contra el fraude en medios de pago

La Facultad de Seguridad Pública de la Universidad Mykolas Riomeris en Kaunas cuenta con una notable experiencia en cuanto a la lucha contra el fraude en diversos ámbitos. Esta institución ha desarrollado un nuevo método para verificar la autenticidad de documentos (que, por ejemplo, puede ser utilizada para los medios de pago) utilizando un sistema conocido como “ondas radiantes específicas” (en Lituano, Kriminalistinės holografinės interferencijos metodas).

Este nuevo método se basa en la grabación de gráficas del volumen de objetos, de tal forma que se proteger documentos (y que, como hemos dicho, puede aplicarse a medios de pago) ante intentos de fraude.

Las ventajas de la implantación de este nuevo método son, entre muchas otras, que se garantiza la conservación del estado del objeto original. Además, el citado método permite conseguir copias del objeto o impresiones que corresponden por completo a sus rasgos tridimensionales de forma que se mantiene la seguridad y permanencia de los rasgos individuales de cada uno de esos métodos y que podría permitir usar hologramas como prueba en los tribunales.

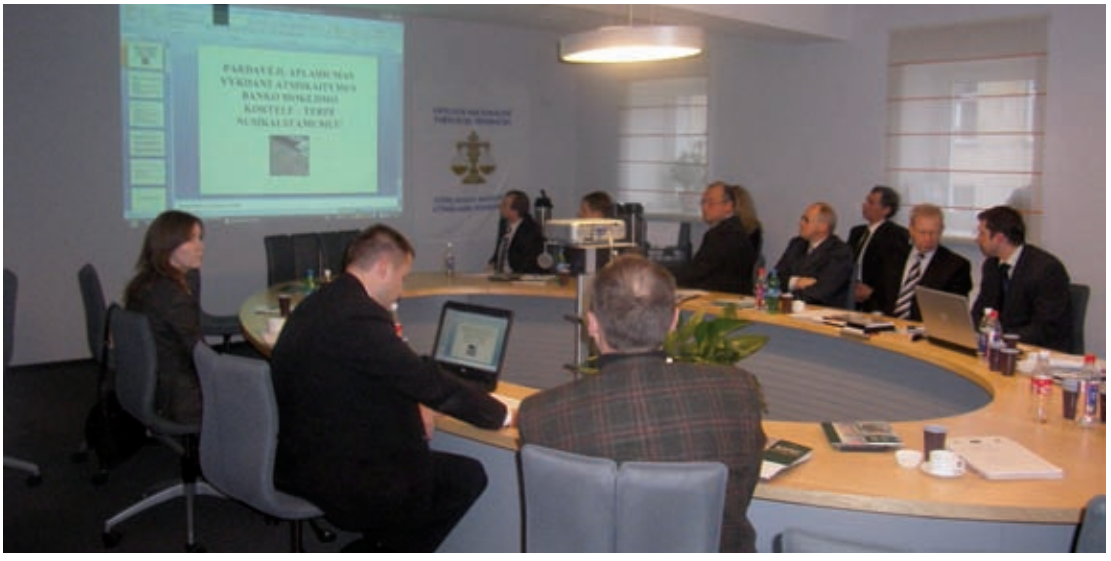
Los investigadores fueron financiados por el "Twins Project" (Proyecto Gemelos) aunque todavía no se han publicado oficialmente los resultados. Representantes de la citada Universidad esperan que este método ayude a la proceso de fabricación de monedas y billetes de Euro y en la investigación contra la falsificación de otros sistemas de pago distintos al efectivo.

EXPERIENCIA POLICIAL EN LA LUCHA CONTRA EL FRAUDE EN MEDIOS DE PAGO:

DEFICIENCIAS EN LA PROTECCIÓN DEL CONSUMIDOR

Existen una serie de actores en lo que a la circulación de tarjetas de pago electrónicas se refiere: policía, fiscales, tribunales, bancos centrales y comerciales, empresas que producen y autorizan tarjetas electrónicas, sujetos que realizan funciones de control y educativas y organizaciones internacionales.

Hubo un gran caso de fraude en medios de pago distintos al efectivo cometido por un grupo delictivo de Sri Lanka e individuos lituanos. Este fraude consistió en que los criminales estuvieron usando tarjetas electrónicas falsas para extraer dinero de los cajeros automáticos. Produjeron unos daños de alrededor de 35.000 euros.



Sin embargo, la mayoría de los delitos comunes son llevados a cabo por el uso de tarjetas electrónicas verdaderas que han sido robadas mientras se estaba pagando algo o se intentaba sacar dinero.

La policía opina que no hay suficientes normas explícitas sobre quién tendría que ser indemnizado en caso de fraude (banco, tienda, etc).

LA LUCHA CONTRA EL FRAUDE EN MEDIOS DE PAGO EN EL MARCO DE LA DEFENSA NACIONAL

Experiencias de la policía en cooperación con demás agentes

Actualmente, la Policía participa en diversos grupos de trabajos interdepartamentales, donde conjuntamente con los representantes de diferentes entidades (Bancos, Ministerio de Defensa Nacional, Ministerio de Asuntos Exteriores, Ministerio de Transporte y Comunicaciones, Banco Nacional, Ministerio del Interior, Departamento de Seguridad del Estado, Ministerio de Finanzas y departamentos correspondientes, etc) formulan propuestas para el Gobierno para consolidar la seguridad informática.

Actualmente, uno de esos grupo de trabajo presidido por el Director de Política de Defensa y del Departamento de planificación del Ministerio de Defensa Nacional, está centrado en la creación de una base legal en seguridad cibernética; el desarrollo de un sistema de coordinación nacional; la prevención de amenazas; la creación de sistemas de respuesta; la persecución de las infracciones cometidas; la consecución de estándares de seguridad en implantación de tecnologías de seguridad; la cooperación internacional y la formación de la cultura de seguridad nacional cibernética.

INICIATIVAS DE LA ADMINISTRACIÓN PÚBLICA EN MATERIA DE PREVENCIÓN DE LOS FRAUDES EN MEDIOS DE PAGO

La Autoridad Regulatoria de las Comunicaciones es la principal institución que defiende los derechos de los consumidores asegurando la competición de los mercados en enlaces electrónicos, el envío y la entrega de servicios de calidad.

La misión de esta institución es asegurar la variedad de las comunicaciones electrónicas asequibles, tecnológicamente progresivas, de alta calidad y seguridad y los servicios postales (productos) a todo ciudadano de Lituania como requisito previo para el desarrollo de la sociedad de la información.

Además, la Autoridad Regulatoria de las Comunicaciones es una institución que participa en procesos de resolución extrajudicial de conflictos entre consumidores y proveedores de servicios.

CONCLUSIONES

- A diferencia de otros países, Lituania no está preparada para protegerse de posibles ataques, ya que no hay sistema de defensa internacional y cada país es responsable de proteger su mecanismo económico y administrativo.
- Al igual que en el resto de los países de la UE, se considera que en general que hasta el momento ha habido una escasez de normas claras sobre la asunción de responsabilidad en caso de fraude (entidad financiera, emisor del medio de pago o usuario)
- La promoción de actividades de I+D relacionadas con los mecanismos técnicos de seguridad en medios de pago son vitales para la lucha contra los crímenes económicos asociados a estos instrumentos.

SEMINARIO BULGARIA

- Organizado por BNAP, Asociación Nacional Búlgara de Consumidores
- Sofia, 28 de Enero de 2009
- Radisson Hotel, Sala de Conferencias "Alexander"

La Asociación Nacional Búlgara de Consumidores es una organización no gubernamental fundada en 1998 que tiene como principal fin la protección de los derechos de los consumidores en Bulgaria. A tal fin proporciona información para que los consumidores puedan realizar mejores elecciones entre los productos, ofrece un servicio de asesoría jurídica para efectuar reclamaciones judiciales y extrajudiciales y está presente en los procesos legislativos representando los derechos de los consumidores.

PROGRAMA:

09:00 APERTURA DEL SIMPOSIO POR DANIELA IVANOVA, PRESIDENTA DE LA ASOCIACIÓN NACIONAL
BÚLGARA DE CONSUMIDORES
COMUNICACIÓN POR LA COMISARIA EUROPEA DE CONSUMO, MEGLENA KUNEVA

09:55 VULNERABILIDADES DE LAS TARJETAS MAGNÉTICAS Y ANÁLISIS FORENSE
Catalin Grigoras, Experto Forense de Rumanía.

10:15 LEGISLACIÓN PARA LA PROTECCIÓN DEL USUARIO EN FRAUDES INFORMÁTICOS
Doctor Georgi Dimitrow, Fundación Ley e Internet.

10:35 TIMOS POR INTERNET Y RETOS EN ISRAEL PARA LA PREVENCIÓN DEL FRAUDE
Avi Linden, Experto para la Protección contra el Fraude, Israel

11:30 PRESENTACIÓN DEL ESTUDIO SOBRE EL FRAUDE EN MEDIOS DE PAGO EN BULGARIA
Bogomil Nikolov, Director de la Asociación Nacional Búlgara de Consumidores

11:50 PUNTO DE VISTA DE LAS ENTIDADES FINANCIERAS EN BULGARIA
Eleonora Hristoforova, Abogada de la Asociación de Bancos en Bulgaria

12:05 LA LUCHA CONTRA EL FRAUDE DE LAS ADMINISTRACIONES PÚBLICAS
Yavor Koev, Director de la Sección de Delitos Informáticos, Subdirección de Lucha contra el Crimen Organizado
del Misterio del Interior

Datos estadísticos BULGARÍA

■ Inseguridad, problemas e insatisfacción de los usuarios búlgaros de medios de pago.

■ El 60% de los consumidores búlgaros han tenido problemas con pagos por tarjeta.

■ Hasta el 22% de los consumidores no consideran completamente seguros los pagos que no se efectúan en metálico.

■ Hasta el 29% de los consumidores encuentran que el coste de los pagos que no se efectúan en efectivo es alto, mientras que el 63% piensa que es normal.

ESTUDIO SOBRE EL FRAUDE EN MEDIOS DE PAGO EN BULGARIA

Existen disposiciones relativas a la protección de los usuarios de medios de pago ante los fraude en diversa legislación búlgara:

• Constitución de Bulgaria.

• Ley de Protección de los Consumidores.

• Ley sobre Provisión a distancia de servicios financieros.

• Ley sobre el Comercio Electrónico.

• Ley sobre las transferencias de dinero, los instrumentos de pago electrónicos y los sistemas de pago.

En la resolución extrajudicial de discrepancias entre usuario y empresa, es la Comisión de Conciliación en Conflictos por Pagos el órgano encargado de mediar entre ambas partes.

La Comisión de Conciliación en Conflictos por Pagos es una de las herramientas para resolver conflictos en Bulgaria fuera de los tribunales. Es un cuerpo independiente, que consta de dos representantes de la Asociación de los Bancos Comerciales y dos representantes de la Comisión de Protección al Consumidor. El presidente es un representante del Banco Nacional Búlgaro, es decir, él o ella no está comprometido con ninguna de las dos partes del conflicto.

La Comisión de Conciliación se crea bajo la Ley sobre transferencia de dinero, medios y sistemas de pago electrónicos y tiene potestad para actuar bajo las siguientes circunstancias:

• Conflictos sobre transferencias de dinero entre bancos y otros operadores autorizados, por una parte, y sus clientes por otra;

• Conflictos sobre temas de medios de pago electrónicos (sobre todo tarjetas bancarias) entre bancos y otros operadores autorizados por una parte, y sus cliente por otra.

Encontramos ya jurisprudencia en tribunales búlgaros en cuestión de fraude en medios de pago, aunque aún son pocos los casos. A este respecto, encontramos la sentencia número 252/14.05.2007 del Tribunal Superior de Apelación sobre el robo de identidad y falsificación de una tarjeta de crédito y daño económico por 10.964,90 levas (unos 5.595 euros). Se le sentenció al acusado a 5 años y 6 meses de prisión.

LEGISLACIÓN PARA LA PROTECCIÓN DEL USUARIO EN FRAUDES INFORMÁTICOS

- Protección penal: Este tipo de protección se contempla en el Código Penal de Bulgaria, bajo el Capítulo V, Sección IV.

- Protección Civil: La responsabilidad de los proveedores de Internet se recoge en la la Ley del Comercio Electrónico Búlgaro.

- Protección administrativa: El trabajo de la Comisión de Protección a los Consumidores se ha centrado en este aspecto. La pena por enviar estafas a personas o compañías, bajo la Ley del Comercio Electrónico Búlgaro, varía entre los 500 levas y los 2000 (250 – 1000 euros).

En la Ley de Comisión de Protección, se recogen penas por el caso de competencia desleal relacionada especialmente con los casos de fraudes comerciales.

VULNERABILIDADES DE LAS TARJETAS MAGNÉTICAS Y ANÁLISIS FORENSE

Las vulnerabilidades de las tarjetas magnéticas puden analizarse desde un punto de vista forense, tal y como expuso Catalin Grigoras, Experto Forense de Rumanía.

Las tarjetas magnéticas se rigen por la norma ISO 7810, que es un estándar que define las características físicas de las tarjetas de identidad o identificación.

Formato	Dimensión
ID-1	85.60 × 53.98 mm
ID-2	105 × 74 mm
ID-3	125 × 88 mm
ID-000	25 × 15 mm

El estándar define cuatro tamaños diferentes de tarjetas: ID-1, ID-2, ID-3 and ID-000.

La falsificación de la banda magnética y su uso fraudulento.

Los principales métodos de falsificación de las tarjetas magnéticas y su consiguiente uso fraudulento consisten principalemente en la lectura del contenido original de la banda magnética y su grabación, captura del código PIN introducido en el teclado así como posterior copia del contenido de la tarjeta intervenida en una nueva tarjeta (que puede ser bien una tarjeta robada o una tarjetas virgen).

En la práctica, se dan casos de sustracción de datos en el momento de la lectura de la tarjeta (skimming) en los aparatos de lectura (cajero automático, terminal de punto de venta). Al comprobar visualmente el citado aparato, debemos ver un solo lector de tarjeta; si hay dos, esto podría ser que hay un aparato con el cual pretender llevar a cabo técnicas de substracción de datos por lectura.

Alguna de las soluciones técnicas contra la falsificación de tarjetas de crédito por este método son las tarjetas inteligentes (que establecen mecanismos adicionales de verificación) o las tarjeta sin contacto.

TIPOS DE FRAUDE POR INTERNET Y RETOS EN CUANTO A SU PREVENCIÓN

LA VISIÓN DE LA EMPRESA PRIVADA EN ISRAEL Y EUROPA

Los responsables del departamento de Riesgos en diversas instituciones financieras se enfrentan a numerosos desafíos: unas normas regulatorias dinámicas y cada vez más rigurosas, un sistema empresarial altamente competitivo, amplia adopción de la banca electrónica y pagos electrónicos, infraestructuras de datos complejas y una evolución continua y migración del fraude.

Como resultado, estos responsables necesitan soluciones que les proporcionen aptitudes de liderazgo en estos aspectos.

¿Cuáles son los fraudes que más preocupan a las entidades financieras en Israel?

1. Fraude en los cajeros automáticos / tarjetas de débito.

Uno de los retos es poder descubrir más fraudes a tiempo real y poder proteger a los consumidores a través de los productos y canales comercializadores: esta acción actuación debe estar basada en la cooperación entre las diversas entidades financieras, y contando con las aportaciones de los consumidores.

Algunos incidentes relacionados con el gran volumen de ciertas informaciones comprometidas de titulares de tarjetas tienen preocupados a los consumidores, a los legisladores y la industria de las tarjetas. Bajo esta presión de realizar acciones al respecto, los emisores de tarjetas se están viendo forzados a tomar medidas diversas, a las que debe sumarse el coste de reemplazamiento de cantidades enormes de tarjetas.

Ciertos ataques por intentos de fraude transnacionales continúan influenciando las estrategias de lucha contra el fraude por parte de las entidades, resultando ello en un mayor impacto a los titulares de tarjetas que viajan al extranjero.

Las tarjetas de débito se usan cada vez más para compras online y ciertos fraudes con tarjetas no presenciales continúan siendo el tipo de fraude que está aumentando de forma más rápida en los ultimos años. Estos factores representan un reto significativo para las instituciones ya que deben seguir todas las novedades en cuanto a nuevos casos de fraude, siendo que estos evolucionan con una rapidez cada vez mayor.

2. Fraude de los empleados.

Las entidades financieras están bastante preocupados con algunos fraudes provocados con el consentimiento, cooperación o mala fe de sus empleados. Entre ellos se pueden considerar la autocontratación, malversación, robo de información, violaciones de política de la empresa y otros cuestiones similares; ellos representan un reto significativo para las instituciones financieras. Una encuesta reciente sobre la industria de servicios financieros revela que el 65 por ciento de los

encuestados creen en un aumento en la amenazada de fraudes por empleados; incluso más del 60 por ciento cree que sus habilidades para la detección de fraudes por empleados es menor de lo que sería aceptable.

3. La prevención del fraude a empresas – Soluciones comunes entre empresas.

La prevención del fraude es una actividad continua y evolutiva, ya que las delicuentes cambian de tácticas y desarrollan nuevas estrategias. Los sistemas de detección compartimentados o inconexos son ineficientes, costosos y descubren menos fraudes que las soluciones múltiples que potencia una sola plataforma. Para evitar pérdidas, intervenciones regulatorias y daños a marcas, las empresas necesitan amplias habilidades de prevención del fraude empresarial que ofrecen una plataforma común para reducir índices positivos falsos y procesos manuales autómatas.

4. Fraudes bancarios aislados – protección a través del producto y a través del canal.

El rápido crecimiento en el número de canales de acceso y complejidad en la banca ha creado nuevas oportunidades de negocio para empresas de servicios financieros, pero también ha creado nuevos retos ante el fraude. Los estafadores se dirigen sistemáticamente a una variedad de canales de acceso amplia, como centro de llamadas, sitios online, banca móvil y sistemas de respuesta de voz interactiva. Debido al carácter anónimo de estos canales y el variedad creciente de servicios que se ofrecen a través de estos canales remotos, las instituciones financieras se enfrentan a retos únicos y deberían no sólo envitar pérdidas monetarias, sino a enviar la erosión de la confianza del usuario final en los sistemas de pago.

PROPUESTAS PARA LA LUCHA CONTRA EL FRAUDE DE LAS ENTIDADES FINANCIERAS EN BULGARIA

La Asociación de Bancos en Bulgaria ha llevado a cabo diversas propuestas legislativas en esta materia, interviniendo activamente en los procesos legilativos en Bulgaria; además de otras actuaciones encaminadas a mejorar la coordinación entre bancos y las autoridades búlgaras.

La Asociación de Bancos en Bulgaria lucha contra los fraudes económicos a través de su Comité de Seguridad, realizando propuestas que son en general tomadas en consideración y aceptadas por las entidades financieras miembros de esta institución.

LA LUCHA DE LAS ADMINISTRACIONES PÚBLICAS CONTRA EL FRAUDE

- La sección de Delitos Informáticos trabaja para le persecución y erradicación del robo de certificados bancarios por parte de grupos delictivos búlgaros e internacionales.

- Existe un proyecto común del Ministerio y Microsoft, la web Cybercrime.bg, que aborda algunas de las cuestiones de las que se trata en el Simposio. Esta web fue diseñada por estudiantes de la Escuela Vocacionesl de Electrónica John Atanasov, conjuntamente con el Cuerpo para la Lucha contra el Crimen Organizado, y con el apoyo financiero de la Asociación de Veteranos de la Policía.

En esta web se ofrecen consejos para los usuarios en cuanto a protección contra diversos timos informáticos, como el phishing

CONCLUSIONES

- Las estafas en medios de pago distintos al efectivo son un problema común para los consumidores, bancos e instituciones y cada vez de mayor relevancia en Bulgaria, a pesar de que en a actualidad se puede considerar que los niveles de partida son más bien bajos.

- La coordinación entre los bancos para garantizar el acceso seguro de los usuarios a la banca electrónica tiene una importancia capital

- La lucha contra los fraudes en medios de pago es vital no sólo en relación a garantizar los derechos de los consumidores, sinode los ciudadanos en general y el Estado de derecho . Este tipo de delitos económicos vienen comunmente asociados a casos de blanqueamiento de dinero negro, tráfico de drogas y armas, terrismo, etc.; por lo que combatiéndolos también se está luchando contra muchos otros tipos de actividades delictivas.

SEMINARIO ITALIA (I) ADICONSUM

■ Organizado por ADICONSUM, Asociación para la Defensa del Consumidor y el Medio Ambiente
■ Roma, 30 de Enero de 2009
■ Centro de Conferencias Cavour.

ADICONSUM: La Asociación para la Defensa de los Consumidores y el Medio Ambiente, es una asociación de consumidores que cuenta con 122.000 asociados constituida en 1987 por iniciativa del CISL (Confederación Italiana de Sindicatos de Trabajadores). ADICONSUM defiende los intereses de los consumidores de manera totalmente independiente de empresas, partidos políticos, Gobierno y sindicatos. Está presente en todas las regiones italianas con 283 centros de información y asesoría a consumidores en las principales ciudades. Cuenta con 35 trabajadores a tiempo completo, 105 trabajadores a tiempo parcial y cientos de voluntarios.

PROGRAMA:

APERTURA: Paolo Landi, Secretario General de ADICONSUM

LA VISIÓN DE INSTITUCIONES Y FUERZAS DE SEGURIDAD
Antonio D'Onofrio, Director del departamento de Cibercrimen de la Unidad Especial de la Policía Financiera para el Fraude Telemático (G.A.T.);
Giovanni Pollastrini Director del Área de Pagos con Tarjeta y Crédito al Consumo, UCAMP (Oficina Central Antifraude de Medios de Pago del Ministerio de Finanzas y Economía)

LA VISIÓN DE INDUSTRIA Y ENTIDADES PRIVADAS
Alessandro Zollo, Director de ventas y medios de pago de la Asociación Bancaria Italiana (ABI);
Enrico Lodi Director de la Oficina del Servicio de Crédito del CRIF (Sistema de Información Crediticia);
Vincenzo Leggiero Director de Márketing de Consum.it - Grupo Monte dei Paschi di Siena;
Raffaele Panico Gestión del Fraude, Poste Italiane Antonio Caricato, Director de Seguridad y Negocio del Instituto Central de Bancos Populares Italianos

LA VISIÓN DE LOS ACADÉMICOS
Fabio Picciolini, Experto en Banca y Finanzas
Mara Mignone, Investigadora del Centro de Investigación sobre Seguridad y Crimen (RISSC)

Datos estadísticos ITALIA

■ Italia es un país que presenta unas cifras relativamente bajas de aprovechamiento de los diferentes servicios que Internet pone a disposición de los usuarios:
■ El 20% de los usuarios de Internet italianos lo utiliza para buscar viajes y alojamiento.
■ El 17% de los usuarios de Internet italianos lo utiliza para leer periódicos y noticias.
■ Sólo el 7% de los usuarios de Internet italianos lo utiliza para buscar trabajo o para adquirir bienes o servicios. Esta cifra es preocupante para la Comisión Europea, ya que va en sentido contrario a la cada vez mayor integración comercial y laboral entre los países miembros.

EXPERIENCIA Y ACTIVIDADES DE LAS ASOCIACIONES DE CONSUMIDORES ITALIANAS EN LA ERRADICACIÓN DE LOS CRÍMENES ECONÓMICOS RELATIVOS A LOS SISTEMAS DE PAGO DISTINTOS AL EFECTIVO

Los fraudes en medios de pago se han convertido en parte de las vidas de muchos italianos. Se han descubierto más de 22.000 casos de fraude y, lo que es mas preocupante, este tipo de casos se han doblado en muy pocos años.

Existe una amplia multitud de diferentes tipos de fraude, desde el relativamente simple robo de tarjetas de crédito hasta otros fraudes más complejos como el robo de identidad.

ADICONSUM lleva tiempo trabajando en la protección de los consumidores ante los fraudes en medios de pago; concretamente ha intervenido activamente en el proceso consultivo de diversos textos lecgislativos relartivos a esta materia:

- Texto unificado adoptado por la Comisión Permanente (Proyectos de Ley nº414 y 507) Disposición para la lucha contra el robo de identidad y sobre la prevención del fraude en el sector del crédito al consumo, pagos diferidos del sector asegurador

- Alegaciones de ADICONSUM a las Leyes 414 y 507 sobre Prevención del Fraude en Crédito al Consumo y Pagos diferidos, remitidos al Comité Financiero del Senado de la República Italiana.

LA VISIÓN DE INSTITUCIONES Y FUERZAS DE SEGURIDAD

El sector bancario y postal han llevado a cabo grandes esfuerzos llevados a cabo por estos organismos para intentar reducir el perjuicio económico que los usuarios sufren cuando son víctimas de este tipo de fraude. Por parte de estas instituciones se opina que deben dedicarse mayores recursos a las investigaciones policiales para poder reducir las consecuencias de este tipo de crímenes.

Existe predisposición manifestada del sector público en cuanto a la protección de los usuarios así como la supervisión y control de este tipo de crímenes. A este respecto, algunas de las medidas del Gobierno mejor acogidas por todos los agentes involucrados en esta problemática son la creación de una base de datos que recopilará información sobre tarjetas de crédito y la reanudación del debate parlamentatio sobre un sistema eficaz para poder combatir el fraude en creédito al consumo.

INICIATIVAS DE LA INDUSTRIA Y ENTIDADES PRIVADAS EN LA PREVENCIÓN DEL FRAUDE EN MEDIOS DE PAGO

La Asociación de Bancos Italianos llegó a un acuerdo con el Consorcio Bancomat por el cual van a sustituir todos los TPV (Terminal de Punto de Venta) por otros con verificación por sistema Chip-EMV, mucho más seguros, poniendo a disposición de la banca el sistema “Presidio Sicurezza Monetica”. A partir del 2007 el fonómeno del fraude, gracias a estas iniciaivas, ha invertido su tendencia, al decrecer un 30% al año siguiente.

No obstante, el fraude en el territorio nacional supone una pequeña parte en en cuanto a la totalidad de los casos de frau-

de registrados; por ello, el Consorcio Bancomat ha previsto, en el marco del Programa estratégico, la creación de un "Centro de Competencia Antifraude" el cual tendrá una influencia positica en cuanto a la prevención del fraude con tarjetas de crédito en todo el mundo.

También la creación del SIPAF, archivo informático sobre el que se habló en el segundo Seminario en Roma, es una iniciativa relevante en cuanto a la prevención del fraude en medios de pago en Italia.

Dos de los ponentes -un criminólogo y un oficial de la Guardia di Finanza (la policía financiera de Italia) realizaron aportaciones de gran interés. En concreto, el representante del GAT -la unidad especial para el Fraude Telemático de la Policía Financiera- explicó que existen otras muchas maneras para engañar a los usuarios que no se muestren alerta, aunque es también posible implementar un gran número de medidas que tengan un efecto real en cuanto a minimizar los daños causados por el fraude.

CRIF es una empresa Italiana que realiza servicios para operadores financieros, empresas y ciudadanos tanto a nivel nacional como internacional; de forma que puedan contar con información veraz y constatable.

En Italia, más de 10.000 consumidores están abonados al servicio de protección de datos personales contra el fraude crediticio ofrecido por CRIF (IDENTIKIT), que se sirve de la abundante información y experiencia en esta materia de CRIF. Éste sistema proporciona un servicio de alertas en cuanto se produce una variación en cuanto a la situación crediticia del cliente, por un eventual intento de fraude crediticio por uso ilegítimo de datos del cliente.

LA VISIÓN DE LOS ACADÉMICOS: LA CONFIANZA DEL CONSUMIDOR SE RESQUEBRAJA

Dª Mara Mignone, criminóloga representante del RISSC (Centro de Investigación y Estudio sobre Seguridad y Criminalidad) realizó una ponencia de carácter técnico donde definió según el punto de vista criminólogo las características de los medios de pago distintos del efectivo, moneda electrónica y el fraude que pueden sufrir los mismos como fenómeno delictivo.

La sra. Mignone comentó algunos datos que obtuvieron en el marco del Proyecto NESSUNO, realizado por RISSC en colaboración con CRIF y CCP Italia en 2007, como los siguientes:

- Cerca del 88% de los entrevistados utilizaban el cajero automático, aunque el porcentaje se rebaja al 65% para los entrevistados que utilizaban tarjeta de crédito
- La mayoría de los encuestados tienen una frecuenca de uso de cajero automático de "varias veces a la semana" o "varias veces al mes". La tarjeta de crédito es sobre todo utilizada "de vez en cuando".
- El titular de la tarjeta de crédito o usuario de cajero automático una "inseguridad significativa" en el uso de la tarjeta de crédito como alternativa al dinero en efectivo. Esta inseguridad condiciona, no obstante, de modo diverso los hábitos y modalidades de pago y de uso de estos medios de pago electrónicos.

- El usuario de cajero automático no utiliza la tarjeta de crédito porque no se siente seguro. Sólo en cuanto al uso en el ectranjero el uso de cajero automático resulta ser más limitado. El titular de la tarjeta de crédito, a su vez, la usa sólo en el extranjero si se siente suficientemente seguro

- Existe una temor generalizado a sufrir fraude y robos de identidad en tarjetas de crédito. De hecho, el 90% de las personas entrevistadas declaran tener "miedo de resultar víctimas de los fraudes en medios de pago"

- El 92,11% de los usuarios de cajero automático y el 91,91% de los titulares de tarjeta de crédito tienen miedo a convertirse en víctimas de fraude en medios de pago.

Estos temores, de hecho, se pueden considerar justificados ya que el 38% de los entrevistados ha tenido alguna experiencia como víctima indirecta o directa en el último año.

No obstante, es cierto que la mayor parte de los ciudadanos (61%) se declara atento respecto a la seguridad de sus datos personales, prestando atención a la hora de darlos hasta en los momentos más habituales. Las medidas más comunes son las que implican el menor esfuerzo posible y, a menudo se encuentran en línea con la información transmitida por los medios de comunicación genéricos: la firma de la tarjeta (65%), una advertencia genérica a la hora de pagar (61%), la destrucción de la tarjeta, una vez caducada (58%). El porcentaje empieza a reducirse sensiblemente cuando hablamos de activación del sistema de alertas por SMS (30%), verificación de la recepción de la tarjeta de crédito en el periodo de tiempo previsto (18%) y activación de diversos servicios anti-fraude para las compras por Internet -tales como Verified by Visa, MastercardSecureCode- (18%)

La citada encuesta se realizó a más de 400 personas, en las localidades italianas de Padua, Milán, Roma y Nápoles.

Existe, por tanto, un problema de sensibilización, atención y educación de los ciudadanos respecto al tema de la seguridad; también hay, sin embargo, un problema de excesivo alarmismo y de una representación no siempre correcta de la situación real.

Por todas las cuestiones antes expuestas, RISCC ha emprendido en ámbito nacional en colaboración con UCAMP (Oficina Central contra el Fraude en los Medios de Pago del Ministerio de Economía y Finanzas) el Proyecto ALIAS- Reforzamiento de la cooperación público-privada contra el robo de identidad y fraudes en tarjetas de pago. (http://www.rissc.it/alias) El principal problema que pretende abordar este Proyecto es la evolución y rápida difusión de los esquemas de fraude, un problema de importancia creciente en toda Italia además de Europa.

CONCLUSIONES

- Es necesario iniciar en Italia un debate real sobre la lucha contra este tipo de crímenes, los cuales son particularmente insidiosos ya que es relativamente fácil cometerlos y muy difícil detectarlos (al menos, en cuanto a tiempo se refiere).

- Se considera un aspecto bastante importante es la necesidad de mejorar la legislación y aumentar la cooperación interenacional, teniendo en cuenta que este tipo de crímenes ya no tiene fronteras ni separación entre países.

- El hecho de que los usuarios deberían tener a su disposición una serie de mecanismos fáciles en cuanto a su aplicación para protegerse es una medida muy necesaria de llevar a cabo.

- El problema de los fraudes en medios de pago debería ser permanentemente controlado y recordado a usuarios y consumidores mediante campañas publicitarias en los medios de comunicación y en propuestas legislativas de nueva elaboración.

SEMINARIO ITALIA (II) MDC

- Organizado por MDC, Movimiento para la Defensa del Consumidor.
- Roma, 13 de Febrero de 2009
- Universidad Roma III

Movimento Difesa del Cittadino (MDC): El Movimiento para la Defensa del Ciudadano se fundó en Roma el año 1987 con el objetivo de promover la defensa de los derechos de los ciudadanos, informándoles y dotándoles de instrumentos de autodefensa, prestándoles ayuda y asesoramiento por parte de expertos. Cuenta con una Oficina de Consulta Jurídica y una Oficina de Prensa, entre otros departamentos de temática más específica.

PROGRAMA:

14.00 APERTURA Y PREENTACIÓN DEL PROYECTO:
Antonio Longo, Presidente Movimiento Difesa dei Cittadino

PRESENTACIÓN DE LOS RESULTADOS DEL ESTUDIO SOBRE LA SITUACIÓN DE LOS FRAUDES EN MEDIOS DE PAGO EN ITALIA

MEDIOS DE PAGO ELECTRÓNICOS: ¿TUTELACIÓN O LIBERTAD DEL CONSUMIDOR?
Federico Regaldo, Abogado de MDC y Responsable del Estudio

EXPERIENCIA EN MATERIA DE FRAUDES EN MEDIOS DE PAGO EN LA ACTIVIDAD DE LAS ASOCIACIONES DE CONSUMIDORES
Mattia Cappello, Abogado de MDC

LA VISIÓN DE INSTITUCIONES Y FUERZAS DE SEGURIDAD
Antonio D'Onofrio, Director del departamento de Cibercrimen de la Unidad Especial de la Policía Financiera para el Fraude Telemático (G.A.T.);
Giovanni Pollastrini Director del Área de Pagos con Tarjeta y Crédito al Consumo, UCAMP (Oficina Central Antifraude de Medios de Pago del Ministerio de Finanzas y Economía)

LA VISIÓN DE INDUSTRIA Y ENTIDADES PRIVADAS
Alessandro Zollo, Director de ventas y medios de pago de la Asociación Bancaria Italiana (ABI)
Raffaele Panico, Representante del Servicio Nacional de Correos en Italia (Poste Italiane)
Luigi Altavilla, Banco Unicredit
Antonio Galiano, Banco ICCREA

LA VISIÓN DE LOS ACADÉMICOS: LA PROTECCIÓN DE LOS AHORRADORES EN LOS SERVICIOS FINANCIEROS ON-LINE
Ettore Battelli, Investigador de la Universidad Roma III.
Liliana Rossi Carleo, Coordinadora del Master "Globalización de los Mercados y Protección del Consumidor", Universidad Roma III

Datos estadísticos ITALIA

■ El número de hogares en Italia que dispone de conexión a Internet ha crecido en los últimos años; ha pasado del 40% en 2006 al 42% en 2008 (fuente: Eurostat) Sin embargo, a pesar del relativamente pequeño porcentaje de conexión a Internet (en Suecia, para el año 2008, el porcentaje de hogares con conexión es exactamente el doble) vemos que avanza muy lentamente, al contrario de lo que cabría esperar -es decir, rápidos aumentos a partir de los niveles de 2006, como lo que observamos en España, Portugal, Estonia o Letonia)que sólo un 5% de los usuarios checos utilizan este recurso.

PRESENTACIÓN DE LOS RESULTADOS DEL ESTUDIO SOBRE LA SITUACIÓN DE LOS FRAUDES EN MEDIOS DE PAGO EN ITALIA

El legislador italiano redactó la Ley 206 de 2005 (el llamado "Código del Consumidor) y estableció que, para los contratos on-line y otras modalidades de contrato no presencial "el emisor de la tarjeta deberá reembolsar al consumidor todos los pagos para los cuales los consumidores aporten evidencias de que se ha cometido un exceso en cuanto al precio, comparado con el precio previamente acordado o mediante un uso fraudulento de las tarjetas por parte de los dependientes de establecimientos comerciales o terceras personas"

El mismo principio se ha establecido también en solicitudes on-line de servicios financieros por parte de los consumidores, de acuerdo con la sección 67 del Código de Consumo, tal y como introdujo la sección 9 de la Ley nº221 del 23 de Octubre de 2007. Existen algunas lagunas o problamas en cuanto a la interpretación de la presente normativa; per, en virtud de esta Ley, la protección al usuario de este tipo de medios de pago (tarjetas) ha sido reforzada considerablemente.

Las instituciones bancarias y asociaciones de consumidores han sido testigos en los últimos tiempos de que los fraudes por Internet en medios de pago electrónicos son una cuestión de gran calado social.

LA VISIÓN DE INDUSTRIA Y ENTIDADES PRIVADAS

Opiniones sobre la relevancia y futuro de los medios de pago en Italia

La entidad financiera Unicredit, uno de los principales proveedores de servicios de Banca On-Line, expresó su preocupación por este fenómeno y explicó su compromiso con la erradicación de este tipo de crímenes, ya que el 40% de sus clientes realizan operaciones mediante Banca Electrónica.

La persecución criminal de los autores de cibercrímenes, aunque en teoría es posible, en la práctica no representa una solución viable. Como ejemplo, se puede citar un proceso judicial iniciado en Rusia contra los autores de uno de estos fraudes electrónicos al final no tuvo ningún resultado práctico para las víctimas del mismo.

Por tanto, también Unicredit insistió en la necesidad de centrarse en el aspecto de la prevención para erradicar los fraudes en medios de pago distintos al efectivo, y de aclarar que, para no dinamitar la confianza que los clientes poseen en estos mecanismos bancarios de contratación remota, Unicredit está preparado para asumir la responsabilidad y reembolsar la cantidad sustraída a las víctimas de los fraudes en la mayor parte de los casos.

ABI, la asociación que engloba a los bancos comerciales que operan en Italia, resaltó que la asunción de la responsabilidad es ya un hecho en el sector de los pagos mediante tarjeta de crédito; mientras que los propietarios de nuevas tarjetas (aquéllas que están dotadas tanto de banda magnética como microchip) deberían resultar exentos de responsabilidad en los casos en que se entrega la misma al dependiente del establecimiento comercial y se realiza el pago no mediante el chip de la tarjeta sino mediante la banda magnética.

ABI, asimismo, resaltó como principales razones de la predominancia del uso de efectivo en Italia las cuestiones siguientes:

- Barreras culturales para la utilización del dinero electrónico.
- Pequeño alcance de los Terminales Punto de Venta entre los pequeños comercios (sólo el 16,5% de los pequelos comercios ofrecen la posibilidad de pagar con tarjeta).
- Falta de instrumentos alternativos al efectivo para los pequeños pagos.
- Elevada fragmentación del tejido económico.

Se pueden destacar como características positivas para los consumidores en cuanto a la utilización del efectivo para sus pagos la total difusión de su uso, la mayor velocidad de las transacciones, la anonimidad, la ausencia de costes para el usuario y la sensación de un mayor control de los gastos. Por otra parte, cabe destacar como aspectos negativos de la utilización del efectivo, como el coste para el sistema en general (costes de producción de monedas y billetes, seguridad de los mismos), la imposibilidad de realización de compras por Internet, el límite físico a su capacidad de gasto -se limita a la cantidad de la que se dispone en ese momento- y la posibilidad de robos y fraudes asociada a su uso.

Asimismo, también se explicó el acuerdo al cual habían llegado ABI junto con el consorcio BANCOMAT (red de cajeros en Italia) , en colaboración con el Ministerio de Economía y Finanzas y la UCAMP (Oficina Central para la Lucha contra el Fraude en Medios de Pago). Este acuerdo se materializa en la creación del SIPAF, archivo informático que contiene información útil para la prevención del fraude con tarjetas de crédito y que fue creado el 1 de Diciembre de 2008. Esta iniciativa, en la cual participan 700 entidades financieras y

Algunas de estas cuestiones también fueron confirmado por la entidad financiera ICCREA: el fraude en medios de pago impide la generalización aún mayor de los medios de pago electrónicos entre los consumidores y, por tanto, dificulta el proceso de reducción de costes asociado al menor uso de monedas y billetes. Por tanto, los Bancos cuentan con incentivos reales y considerables para luchar contra esta problemática; la cual no sólo se basa en la necesidad de devolver la cantidad sustraída al consumidor que ha sido víctima del fraude. Analizando los mercados de servicios de medios de pago más desarrolados (por ejemplo, Reino Unido) ICCREA anticipa que, para el merdado italiano, habrá una reducción de los fraudes que utilizan el skimming; pero que sin embargo esa reducción contrastará con el sensible aumento en fraudes no presenciales y robo de identidad (en Reino Unido, los fraudes no presenciales suponen un 52% del total, comparado con el 29% en Italia)

El servicio público de correos en Italia, Poste Italiane S.p.A.,es en la actualidad uno de los principales proveedores a nivel mundial de servicios de banca electrónica, con más de 4 millones y medio de clientes, y que está dotada de varias unidades especiales dedicadas a la prevención del fraude en medios de pago.

De acuerdo con Poste Italiane, este fenómeno es bastante grave: por ejemplo, en Internet se ofrecen kits anti-phishing por 200-300€ para la protección de los usuarios ante este tipo de ataques; este tipo de crímenes no están penados con cárcel (si previamente no se han cometido otros crímenes) y además los ataques por phishing está aumentando dramáticamente: desde 67 en 2007 hasta 6700 en 2008.

Además de sugerir el uso con especial cuidado del servicio de banca por Internet (p.ej., comprobar que la página web es un dominio protegido -identificado por el "https" de la barra de direciones- y que, además, aparece el símbolo de un candado en la página web. También es importante tener el ordenador protegido con un antivitus y que no sean solicitados más de 4 caracteres para identificarse, etc.) Poste Italiane anunció la introducción de un nuevo mecanismo, una especie de lector de tarjetas personal, necesario para trasnferir dinero por Internet. De esta manera se establecerá una medida de seguridad adicional independiente de Internet, la cual se espera que aumente

LA VISIÓN DE LAS ASOCIACIONES DE CONSUMIDORES:

Principales barreras a la ejecución de los derechos de los consumidores

- Falta de información de los consumidores sobre sus derechos cuando, habiendo sido víctimas de uno de estos fraudes, acuden a las oficinas de las asociaciones. En este sentido, Movimento Difesa dei Cittadino, la organizadora del Seminario, ha colgado en su página web para que pueda ser accedido on-line la mayor parte del Seminario y entrevistas a participantes.
- Las iniciativas de mediación entre asociaciones y bancos u otras instituciones están excluidas del ámbito de los medios de pago electrónicos. Ésto representa una molestia más para las víctimas de los fraudes, la cual está particularmente injustificada, teniendo en cuenta que para otros sectores tecnológicos (por ejemplo, discrepancias en cuanto a programas que redirigen a líneas de tarificación adicional desde el PC del usuario) las empresas se han mostrado de acuerdo en cuanto a realizar la negociación directamente con las asociaciones de consumidores.

CONCLUSIONES

- Se considera que debería asumirse la responsabilidad, al menos en ciertos casos de fraude, no por parte de las víctimas sino por parte de las entidades financieras o emisores de tarjetas, siguiendo el camino ya marcado por la Directiva (CEE) 85/374 sobre responsabilidad ante daños producidos por productos defectuosos

- La escasez de información de los usuarios de medios de pago distintos al efectivo todavía es notable en cuanto sus derechos como consumidores, y las vías a las que se puede recurrir para restituir una situación injusta o conflicto con un proveedor de medios de pago o entidad financiera.

- Es necesario incrementar la cooperación internacional entre autoridades judiciales de distintos países, ya que la persecución criminal de los autores de cibercrímenes en la mayor parte de los casos presenta grandes dificultades prácticas. En muchos casos de fraude electrónico al final no se da ninguna solución práctica para las víctimas del mismo.

Fraude y desarrollo de nuevas tecnologías:

Una amenaza para los consumidores

Phishing, spoofing, pharming, vishing, scam, troyanos... **Los consumidores se enfrentan a miles de amenazas con tan sólo sentarse ante su ordenador y comprar cualquier tipo de bien o servicio, o incluso simplementepor consultar su saldo bancario através de la web.**

CONSIGA TODAS ESTAS INTERESANTES Y AMENAS PUBLICACIONES

Llámenos: ADICAE
C./ Gavín, 12 local. 50001 ZARAGOZA
Tfno.: 976 390060 ■ Fax: 976 390199
email **aicar.adicae@adicae.net**

SEMINARIO RUMANÍA

■ Organizado por ANPCPPSR, Asociación Nacional para la Protección del Consumidor y para la Promoción de Estrategias en Rumanía
■ Bucharest, 23 de Marzo de 2009
■ Anfiteatro Ion Heliade Radulescu de la Biblioteca de la Academia Rumana (Calea Victoriei, nº125, Sector 1, Bucharest)

Asociación para la Protección del Consumidor y la Promoción de Programas y Estrategias en Rumanía (ANPCPPS Romania): Fundada en Bucarest el año 2003, ANPCPPSR es una organización no gubernamental que pretende proteger los derechos legítimos e intereses de los consumidores rumanos, informarles de sus derechos e integrarlos en la vida social. Una de sus actividades es la creación de sellos de calidad que otorgan a las empresas respetuosas con los derechos de los consumidores.

INTERVENCIONES DE:

Sorin Mierlea,
Presidente de la Asociación Nacional para la Protección del Consumidor y la Promoción de Programas y Estrategias de Rumanía

Adrian Trandafir,
Inspector General de la Policía Rumana – Dirección General para la Cuantificación del Crimen Organizado

Răzvan Resmeriță,
Director del Centro Europeo del Consumidor (ECC-Net) en Rumanía

Alexandru Molodoi,
Oficial Técnico Director, Gecad-Net

Doctora Virgina Campeanu,
Directora del Insituto para la Economía Mundial (IEM) "Costin Murgescu"

Juanjo Machado,
Responsible de Relaciones Internacionales de la Asociación de Usuarios de Bancos, Cajas y Seguros (ADICAE)

Juan Manuel Viver,
Responsable de Proyectos Internacionales de la Asociación de Usuarios de Bancos, Cajas y Seguros (ADICAE)

Mugur Amariei,
Experto de la Asociación Nacional para la Protección del Consumidor y la Promoción de Programas y Estrategias de Rumanía

Datos estadísticos RUMANÍA

■ Se registraron 12 millones de usuarios de Internet en marzo del 2008, con un porcentaje del 53,9% de penetración, según datos de ITU (Unión Internacional de Telecomunicaciones). Ha habido un crecimiento en el uso desde 2000 a 2008 del 1.400%.
■ Se contabilizaron 1.769.300 conexiones a Internet por banda ancha en Septiembre del 2007 (según ITU), lo cual suponetasa de penetración del 7,9%. En cuanto a usuarios de Internet, en Agosto se registraron 5.062.500 en 2007, el 23,9% de la población.
■ Según el EuroStat, los países de la Unión Europea con menos compradores por Internet son Bulgaria y Rumanía (ambos con un 3%) Este porcentaje contrasta claramente con los siete países de la UE donde más se compra por Internet, en los que de la mitad de sus ciudadanos realizó alguna compra por internet en 2008. Se trata de Dinamarca, Reino Unido, Holanda, Alemania, Suecia y Finlandia.
■ En cuanto al porcentaje de pagos on-line para el mercado del comercio electrónica, fue del 15% ol 20% en el 2007. El crecimiento es considerable, ya que se estima que para el 2008 ya sea el 25%.

LEGISLACIÓN PARA LA PROTECCIÓN DEL USUARIO DE MEDIOS DE PAGO EN RUMANÍA.

Experiencia y opiniones del Cuerpo Nacional de Policía de Rumanía

La Dirección de Crímenes Cibernéticos, dentro de la Dirección General contra el Crimen Organizado, es el departamento del Cuerpo Nacional Policial de Rumanía encargado de la lucha contra el fraude en los medios de pago diferentes al efectivo en Rumanía

En cuanto a las competencias desarrolladas por la Dirección de Crimenes Cibernéticos de la Policía Nacional de Rumanía, cabe destacar, en primer lugar, la prevención y lucha contra los crímenes cibernéticos (subastas fraudulentas, acceso ilegal a sistemas informáticos) y crímenes cometidos con instrumentos de pago electrónicos. La cooperación interna e institucional a nivel internacional, y cooperación en general con sector público y privado se revelan como muy necesarias también para la lucha contra este tipo de crímenes.

Es bastante común que al hablar de los medios de pago electrónicos normalmente se asocie este concepto sólo a las tarjetas de crédito. De acuerdo con la legislación de Rumanía (Ley de Comercio Electrónico, no. 365/2002) un instrumento de pago electrónico es un sistema que permite al usuario realizar las siguientes operaciones:

■ Transferencia de fondos diferentes a aquéllas ejecutadas por instituciones financieras.

■ Extracción de dinero mediante cajero automático, además de poner en disposición de u obtener efectivo de instrumentos de dinero electrónico

También la Ley nº 365/2002 (Art.1, puntos 11 y 12) dispone dos tipos de instrumentos de pago electrónicos:

■ Instrumentos de pago de acceso remoto: Permite al usuario acceder a sus fondos, los cuales están en disposición de una institución financiera- y autorizar un pago utilizando un código de identificación personal o similar sistema de identificación. Ejemplo: Banca On-Line.

■ Instrumento de dinero electrónico: Es un instrumento de pago recargable, distinto a los instrumentos de pago de acceso remoto, en el cual las unidades de valor son almacenadas electrónicamente, y permiten a su propietario a ejecutar una de las operaciones descritas en la Ley (transferencias de fondos, obtención de efectivo).

PENAS

La falsificación de medios de pago electrónicos está castigada con penas de entre 3 y 12 años y la supresión de ciertos derechos

La fabricación o posesión de equipamiento, incluyendo hardware y software, para ser utilizado en la falsificación de medios de pago electrónicos, está penado con penas de cárcel desde 6 meses hasta 5 años.

La falsificación en declaraciones para la emisión o uso de medios de pago electrónicos está condenado con penas de entre 3 meses a 12 años

El uso de un instrumento de pago electrónico sin el consentimiento de su propietario, incluyendo las contraseñas identificativas que permiten su uso, está castigado con penas de prisión de 3 meses a 2 años.

La aceptación de operaciones financieras, aun sabiendo que quien las realiza está falsificando un medio de pago electrónico o utilizando un medio de pago electrónico sin el consentimiento de su dueño, está castigado con penas de prisión de 1 a 12 años.

La Policía Nacional de Rumanía ha realizado actuaciones policiales en casos de fraude con interconexiones no sólo en toda Europa (Rumanía a Italia, España, Irlanda, Reino Unido, Holanda, Suecia, Alemania y Chipre) sino también en todo el mundo (Europa a EEUU, Brasil, Australia, Thailandia, China, Túnez)

Para el desarrollo de actividades de educación e información para consumidores sobre los aspectos relacionados con el fraude en medios de pago, la asociación de consumidores A.N.P.C.P.P.S. Romania participa en un grupo de trabajo en este ámbito, con el objetivo de mantener un diálogo proactictivo entre las partes interesadas (autoridades, ONGs, bancos, consumidores, etc) y estableciendo una estrategia nacional en ese sentido, con el propósito de reducir el número de casos de fraudes en medios de pago.

CONCLUSIONES

- Necesidad de proveer a los consumidores de una mejor educación e información, además de medios prácticos para la lucha contra el fraude, sobre todo en los países donde los medios de pago están menos generalizados.
- Necesidad de contar con aplicacines web seguras que establezcan unos altos estándares de seguridad en las operaciones remotas de los usuarios de medios de pago, así como incrementar la seguridad de las operaciones de pago presenciales.
- La creación de grupos de seguimiento del fraude en medios de pago en cada país, con la colaboración de todos los agentes a nivel nacional vinculados a esta problemática asociada al uso de instrumentos de pago, es básica para luchar por la erradicación de este tipo de crímenes

ADICAE

al servicio de los usuarios en toda España y en Europa

SEDES DE ADICAE

Servicios Centrales ADICAE
C/ Gavín, 12 local 50001 **Zaragoza**
Tfno. 976 390060 - Fax 976 390199
aicar.adicae@adicae.net

Madrid
Embajadores, 135 1º C int.- 28045 **Madrid**
Tfno. 91 5400513 Fax 91 5390023

Catalunya
c/ Entença, 30 entlo. 1º - 08015 **Barcelona**
Tfno. 93 3425044 Fax 93 3425045

Comunidad Valenciana
Av. Pérez Galdós, 97 pta.1 - 46018 **Valencia**
Tfno. 96 3540101 Fax 96 3540106

c/ Aparicio, 5 entlo. 5 - 03003 **Alicante**
Tfno. 96 5926583

Galicia
Avda. Gral. Sanjurjo, 119 -1º dcha
15006 **A Coruña**
Tfno. 981 153969 Fax 881 927603

Castilla y León
c/ Caridad, 1 - 2ºC - 47001 **Valladolid**
Tfno/Fax. 983 373173

Extremadura
c/ Camilo José Cela, 1 3º - 06800 **Mérida**
Tfno/Fax. 924 387468

c/ Gómez Becerra, 25 3º - 10001 **Cáceres**
Tfno/Fax. 927 626336

Andalucía
Av. Eduardo Dato, 85 1ºB - 41005 **Sevilla**
Tfno/Fax. 954 652434

c/ Salvador Noriega, 7 entreplanta dcha
29006 **Málaga**
Tfno/Fax. 952 088955

... o pregunte por nuestras delegaciones en otras provincias

SEMINARIO REPÚBLICA ESLOVACA

- Organizado por ZSS, la Asociación Eslovaca de Consumidores.
- Bratislava, 7 de Abril de 2009
- Odborarske namestie, 3 (Sede del Instituto de Turismo, Oficina Nacional para la Protección de Datos, etc.)

"Združenie slovenských spotrebiteľov (ZSS): La Asociación Eslovaca de Consumidores se creó en 1990, es la única asociación de consumidores eslovaca que abarca todo el territorio nacional, con su oficina central en Bratislava. Sus principales tareas son el asesoramiento y educación de los consumidores, así que llevar iniciativas legales en procesos legislativos que involucren a los consumidores..

PROGRAMA:

LA VISIÓN DE ASOCIACIONES DE CONSUMIDORES. LA PROTECCIÓN DEL CONSUMIDOR ANTE LOS FRAUDES EN MEDIOS DE PAGO EN LA REPÚBLICA ESLOVACA

LA VISIÓN DE INDUSTRIA Y ENTIDADES PRIVADAS

LA VISIÓN DE LAS FUERZAS DE SEGURIDAD

INTERVENCIONES DE:

Miro Túlak,
Presidente de la Asociación Eslovaca de Consumidores

Juan Manuel Viver,
Coordinador del Proyecto y Responsable de Proyectos Internacionales de ADICAE

Gabriel Tocka,
representante de supermercados TESCO en República Eslovaca

Olga Petrovicova,
representante de la entidad financiera UNICREDIT

Roland Katona,
Director de la sección de tarjetas de créditodel Banco CSOB (Grupo KBC)

Robert Bohunicky,
representante del Departmento contra la Falsificación y Crímenes Informáticos de la sede central de la Policía Nacional

Datos estadísticos R. ESLOVACA

- Según Eurostat, los usuarios eslovacos cada vez más acceden en mayor número y más frecuentemente a Internet. Se pasó de un 27% de los hogares con conexión a Internet en 2006 a un porcentaje del 58% en 2008.
- Los usuarios eslovacos utilizan Internet, principalmente, para consultar periódicos y noticias on-line (34%), realizar trámites administrativos (30%), contratación y búsqueda de servicios de transporte y alojamiento (29%) y buscar información sanitaria (25%)
- El porcentaje de usuarios eslovacos que utilizan la banca electrónica es del 24%.

HISTORIA DE LOS MEDIOS DE PAGO EN REPÚBLICA ESLOVACA

El desarrollo a lo largo de la historia de las tarjetas de pago en República Eslovaca ha sido largo, contando con hitos como la primera tarjeta de pago (o sistema con la misma finalidad) por la Western Union Telegraph Company. Ya en 1950 se empezó a emitir Diners Club, una versión mucho más perfeccionada; además de la emitida en 1951 el Banco Nacional Franklin de Nueva York Podemos decir que es en 1958 cuando Bank of America empoeza a emitir tarjetas que seguirán un funcionamiento muy similar a las actuales.

Concretamente, en Rep. Eslovaca (antiguamente Checoslovaquia) fue en 1968 cuando la agencia de viajes Čedok empezó a aceptar tarjetas de crédito extranjeras como medio de pago. Las primeras tarjetas de crédito no se emiten en Checoslovaquia hasta 1988, por el Banco Živnostenská Banka; y en 1989 por la caja de ahorros, Česká štátna sporiteľňa .

No obstante, se puede decir que sólo en 1992 Checoslovaquia adopta los sistemas más modernos en cuanto a tarjetas de crédito, equiparándose a otros países con mayor tradición en estos medios de pago.

LA VISIÓN DE ASOCIACIONES DE CONSUMIDORES. LA PROTECCIÓN DE LAS VÍCTIMAS DE FRAUDE

Las asociaciones de consumidores de la República Eslovaca consideran que hay una insuficiente regulación en esta materia en República Eslovaca

La nueva Directiva sobre Servicios de Pago supone una buena ocasión para actualizar los derechos de los consumidores y usuarios eslovacos ante los problemas que pueden derivar del uso de medios de pago distintos del efectivo.

LA PROTECCIÓN DEL USUARIO DE MEDIOS DE PAGO EN LA LEGISLACIÓN ESLOVACA

Aunque se puede considerar que las leyes son tan claras y suficientes en la práctica, existen muchos problemas en caso de que una tarjeta o información de identificación de una tarjeta sea mal usada y un consumidor se viese perjudicado por una retirada ilegal de dinero de su cuenta bancaria. En la mayoría de los casos los bancos / emisores de tarjetas no están dispuestos a aceptar el punto de vista del consumidor o sus argumentos y normalmente declaran que el consumidor causó el problema y que el emisor de la tarjeta no cometió ningún fallo – sobre todo en casos en casos donde se desconoce al autor del fraude, lo que es muy común.

El mal uso de las tarjetas de crédito se regula mediante el decreto de Sistemas de pago número 510/2002, efectivo a partir del 31 de agosto del 2002. § 25 – obligaciones y reclamaciones del consumidor contra el banco / emisor de tarjetas en casos de mal uso de la tarjeta.

También se encuentran disposiciones relevantes en el Código Penal, Ley 300/2005, § 219 – sobre la falsificación y uso no autorizado de un medio de pago electrónico y tarjetas de pago de terceras personas (la pena básica es de 1 a 5 años de prisión y de 5 a 12 años en casos especiales, cuando se causa gran daño, como cuando se pertenece a un grupo organizado peligroso)

En cuanto a transferencias, encontraríamos sólo el decreto de Sistemas de pago número 510/2002, efectivo desde el 31 de agosto del 2002, §§ 3 – 11 para transferencias nacionales y §§ 12 -20 para transferencias internacionales. Sin embargo, no contiene ninguna provisión específica para los Consumidores.

Para los pagos on line, que son transferencias de dinero unidas a las tecnologías de la información (sistemas informáticos e Internet) encontramos el Decreto de Sistemas de pago número 510/2002, §§ 21–24, efectivo desde el 31 de agosto del 2002. No obstante, debido a la rápida evolución en este sector se puede considerar que la presente norma se encuentra poco actualizada y es necesario el establecimiento de nuevas leyes al respecto.

EXPERIENCIA DE LAS ENTIDADES FINANCIERAS EN LA LUCHA CONTRA EL FRAUDE

La cadena internacional de supermercados TESCO en Rep. Eslovaca baraja datos concretos sobre el fraude en medios de pago en la República Eslovaca, además de contar con experiencia práctica sobre los pagos con tarjetas de crédito en Eslovaquia desde la entrada de TESCO en el mercado eslovaco, en 1996.

Concretamente, 1'8 millones de clientes realizan sus pagos en los establecimientos de TESCO en la República Eslovaca mensualmente, con un total anual de 93 millones de operaciones en 2008. En total, los pagos con tarjeta suponen el 26% del

total de todos los pagos realizados por los clientes de TESCO. Desde el año 1996, el mismo momento en el que TESCO se estableció en República Eslovaca, es posible el pago con tarjeta de crédito en todos los hipermercados de TESCO.

Los principales problemas a los que se enfrenta TESCO en cuanto a los medios de pago diferentes del efectivo son:

El importe a cobrar es cargado más de una vez de la cuenta corriente del cliente

En caso de que el problema sea identificado inmediatamente por el cliente (por ejemplo, por un mecanismo de avisos por sms) los sistemas informáticos de TESCO devolverán inmediatamente (tras confirmar el error)el importe cargado incorrectamente a la cuenta del cliente.

En el caso de que el problema se descubra más tarde por el cliente, el sistema de control de pagos durante el cierre de cajas diario revelará el problema e iniciará por su propia cuenta el procedimiento para contactar noc la entidad financiera del cliente para resolver el problema.

El cobro del importe no es posible

Este problema puede venir motivado porque se haya utilizado 3 veces un código incorrecto; porque la firma del recibo es sospechosa o no coincide con la del titular de la tarjeta o cuando la identidad del cliente no coincide con la identidad del titular de la tarjeta (por ejemplo, cuando la esposa paga con la tarjeta del marido o viceversa)

La entidad financiera UNICREDIT opera en República Eslovaca además de otros 21 países del centro y este de Europa. Las principales actividades criminales que han detectado los servicios de seguridad en medios de pago de UNICREDIT son el uso indebido de tarjetas de pago por parte de una tercera persona que la ha sustraido al titular, uso indebido de tarjeta por parte de los familiares del titular, sistemas susceptibles de fraude por parte del emisor de la tarjeta, skimming y phishing.

En República Eslovaca, las tarjetas incorporan deiversos mecanismos de seguridad para dificultar la falsificación de las mismas, como el establecimiento de unos estándares en cuanto a tamaño, la intorducción de hologramas o kinegramas en la tarjeta, la utilización de materiales especiales en la parte donde el titular debe firmar la tarjeta, introducción de elementos que sólo pueden observarse con luz ultravioleta, utilización de elementos protectores varios además del establecimiento de un tiempo limitado en cuanto a la validez de la tarjeta.

La protección de los datos electrónicos también se da tanto en las tarjetas de banda magnética como de chip; y se quiere incluso incrementar para las tarjetas de pago sin contacto y tarjetas virtuales.

El skimming es un tipo de fraude en medios de pago especialmente común en la República Eslovaca, frente a otros tipos de fraudes mucho más sofisticados tecnológicamente que se dan en otros países donde el uso de tarjetas está mucho más extendido y que, por tanto, se encuentran en una fase más madura en el uso de medios de pago. El skimming consiste básicamente en un copiado ilegal de la banda magnética de las tarjatas, aunque pueden encontrarse variantes del mismo como el copiado de datos de la tarjeta en ordenadores, el copiado de datos ilegalmente desde el ordenador a una tarjeta virgen y el consiguiente uso de estas tarjetas creadas para realizar transacciones financieras ilegales.

La producción ilegal y utilización de medios de pago electrónicos u tarjetas está penado por el Código Penal, artículo 219, con penas de 1 a 5 años.

LA EXPERIENCIA DE LAS FUERZAS DE SEGURIDAD

La policía eslovaca destaca los siguientes fraudes como los más frecuentes en la República Eslovaca:

- Tarjetas robadas / transacciones fraudulentas en cajeros automáticos o en establecimientos comerciales.
- "skimming" o copiado de banda magnática de tarjetas en cajeros.
- "skimming" en establecimientos comerciales.
- Tarjetas no recibidas por el titular.
- Diversos tipos de fraudes electrónicos, como el pharming, phishing, etc. (sin presencia de la tarjeta).

En cuanto a la situación actual y tendencias en Rep. Eslovaca destacan las siguientes cuestiones:

- Se ha detectado un aumento continuado a lo largo del tiempo en este tipo de crímenes.
- El modus operandi se va especializando cada vez más, introduciéndose modificaciones en sus técnicas para que así sea a las autoridades policiales así como empresas de seguridad and modifications.
- Se dará una concentración de los criminales por países, o nacionalidades (especialización de las mafias).
- Es necesario monitorizar riesgos en tiempo real continuadamente (24 horas los 7días de la semana).
- Existen nuevos tipos de tarjetas que aumentan notablemente la seguridad de los sistemas ante ataques de terceras personas.

Las tarjetas híbridas son tarjetas que incorporan un chip para la utilización de las mismas sin contacto, además de un segundo chip para su utilización mediante tecnología chip-EMV. Ambos chips pueden ser o chips microprocesadores o simples chips de memoria. El chip sin contacto es generalmente usado en aplicaciones que requieren transacciones rápidas (por ejemplo, transporte) mientras que el chip de contacto es generalmente utilizado en aplicaciones que requieren de alta seguridad como las bancarias.

También encontramos tarjetas de interfaz dual, similares a las tarjetas híbridas (en que la tarjeta presenta ambas interfaces, con y sin contacto). La diferencia más importante es el hecho de que la tarjeta de interfaz dual tiene un solo circuito integrado.

Ha habido una serie de factores y cuestiones que han sido determinantes en cuanto a la situación de los fraudes en medios de pago distintos al efectivo en la República Eslovaca:

- Localización de Eslovaquia dentro del Espacio Europeo Schengen.
- Entrada de la República Eslovaca en la Unión Europea (aceleración del proceso de convergencia con los países europeos miembros de la UE).
- Estabilidad económica y mejora de la calidad de vida de los eslovacos.
- Aumento del turismo.
- Apertura del mercado eslovaco.
- Especificación del Código Penal.
- Cooperación entre las distintas entidades financieras (monitorización de las transferencias,aumento de la seguridad en terminales de ventay cajeros, cooperación entre bancos y policía, tarjetas híbridas, regulación bancaria, etc.)

CONCLUSIONES

- En necesario aumentar la concienciación de los ciudadanos, así como su participación en la lucha contra el fraude en medios de pago, tanto en países donde su uso está más avanzado como en otros donde en la actualidad se está generalizando su uso, como es el caso de la República Eslovaca
- La introducción de nuevos dispositivos de seguridad y comercialización de nuevos instrumentos de pago más sofisticados (por ejemplo, el caso de las tarjetas híbridas) puede ser beneficioso en cuanto a establecer una mayor dificultad para violar la protección que los diversos mecanismosde seguridad ejercen sobre los instrumentos de pago.
- Deberá incrementarse la seguridad de los cajeros automáticos, estableciendo algún tipo de normativa para las entidades financieras a este respecto, con estándares y requisitos mínimos de seguridadde los cajeros, y obligando a establecer el chequeo dual de las tarjetas de pago.

SEMINARIO DE CLAUSURA DEL CICLO Y CONCLUSIONES

LOS CONSUMIDORES ANTE EL FRAUDE EN LOS MEDIOS DE PAGO

- Organizado por ADICAE
- Fecha: 3 de Abril de 2009, 10:30
- Lugar: Parlacio Municipal del Congreso de Madrid

Ponentes:

D. Piet Lakeman,
Fraud Management Senior Manager (Visa Europa)

D. Emilio Castellote,
Director de Márketing de Producto, Panda Security

D. Miguel de Bas Sotelo,
asesor ejecutivo OPTIMAWEB, representante de ANEI (Asociación Nacional de Empresas en Internet)

Angel Barbero,
Consejero de SAFETYPAY

Gabriel Agatiello,
representante de Trend Micro.

LOS CONSUMIDORES ANTE EL FRAUDE EN MEDIOS DE PAGO

INICIATIVAS DEL SECTOR PRIVADO

El papel de VISA Europa en la lucha contra el fraude en medios de pago

Visa Europe forma parte de la red mundial de Visa. Es una asociación de 4.600 entidades financieras europeas que, conjuntamente, ejercen su influencia y supervisan la dirección de la compañía, sus sistemas y operaciones. Visa Europe es una sociedad de propiedad privada. La sede central de Visa Europe está en Londres, contando con oficinas locales en Atenas, Bucarest, Bruselas, Estambul, Estocolmo, Francfort, Lisboa, Madrid, Milán, Paris y Varsovia.

La estructura del mercado europeo de sistemas de pago está cambiando en la actualidad. Los bancos europeos han funcionado tradicionalmente como un mosaico de diferentes infraestructuras de pago nacionales. Sin embargo, se acepta universalmente que todos (entidades financieras, comercios minoristas, consumidores y la economía en general) se beneficiarían de un mercado europeo de pagos más abierto y coherente.

La Comisión Europea ha esbozado su visión de un mercado interior de pagos. Y hay otras dos iniciativas en marcha que están contribuyendo a convertir esta visión en realidad:

El Banco Central Europeo ha invitado a los bancos europeos a crear una Zona Única de Pagos en Euros (SEPA)

La industria de servicios financieros ha creado el Consejo Europeo de Pagos para acordar una respuesta común, que ya ha finalizado el marco de SEPA para las tarjetas (SEPA Cards Framework – SCF).

Medidas de seguridad en favor de los consumidores

Exigencia de stándares a sus miembros

Se creó un estándar establecido por la industria de medios de pago PCI DSS. Es un conjunto de requisitos exhaustivos destinado a mejorar la seguridad de los datos de la cuenta de pago establecida. PCI DSS, incluye 12 requisitos clave para aquellas organizaciones que aceptan o procesan pagos con tarjeta:

- Instalar y mantener una configuración firewall para proteger los datos

- No utilice contraseñas por defecto proporcionadas por el proveedor u otros parámetros de seguridad

- Proteja la información almacenada

- Encripte la transmisión de datos de titulares o información sensible

- Utilice y actualice regularmente un programa anti-virus

- Desarrolle y mantenga las aplicaciones y sistemas más seguros

- Restrinja el acceso a los datos únicamente a las personas imprescindibles

- Asigne una identificación única para cada persona con acceso informático a la misma

- Restrinja el acceso físico a los datos de los titulares

- Localice y realice un seguimiento de todos los accesos a los recursos de su red y a la información de los titulares
- Pruebe con regularidad sus sistemas y procesos de seguridad

- Mantenga una política específica para la seguridad de la información

La migración a la tecnología del Chip EMV ha sido encabezada por Visa Europe, añadiendo un nuevo elemento de protección contra el fraude.

Protección contra el fraude no presencial en tarjetas

Cuando una tarjeta Visa no está presente durante una transacción (el comercio electrónico, móvil, telefónico o por correo), se utiliza una gran variedad de servicios de verificación para autenticar y proteger la transacción.

Las tres principales soluciones propuestas para autenticar estas transacciones son:

Código de Seguridad (CVV)

Es el llamado código de seguridad de la tarjeta. Este es el código de seguridad de tres números que aparece en el reverso de cada tarjeta Visa sobre el panel de firma o a su derecha

Valoración ADICAE: Éste código puede volverse contra el usuario en caso de robo físico de la tarjeta ya que el delincuente tendría acceso a la numeración y códigos.

Verified by Visa

Solución de seguridad para el comercio electrónico. Es un sistema de autenticación de la identidad del titular protegido por contraseña que ha sido diseñado para contrarrestar el fraude online.

Valoración ADICAE: Vulnerable si el ordenador tiene troyanos, spy-ware o en definitiva ante la actuación de un hacker.

El sistema de verificación de la dirección (AVS)

Este sistema verifica la dirección de facturación del titular. Actualmente, es utilizado únicamente por comercios en el Reino Unido.

MEDIDAS EN LA LUCHA CONTRA LOS DELINCUENTES INFORMÁTICOS

La experiencia de PANDA y Trend Micro

La mayor problemática en cuanto a las transacciones on-line está asociada a 2 timos muy comunes el "Phising 2.0" (fraudes informáticos personalizados) y el "spam financiero" (fraude que nos intenta persuadir de que compremos un determinado tipo de acciones porque van a aumentar de valor muy rápidamente).

Se destacó como factores especialmete peligrosos:

-Inocencia y falta de información del consumidor ante estos fraudes vía Internet (estudio realizado por el FBI)

-Complejidad de los últimos virus que se están empleando para cometer fraudes, los cuales son aparentemente inofensivos; es decir, se instalan en el ordenador sin provocar ningún desperfecto; es más,para que no venga otro virus y le quite el sitio o destruya el sistema operativo (y a él) descarga automáticamente actualizaciones de Windows para proteger el sistema; por lo que es complicado que el usuario los detecte.

¿Autorregulación = Seguridad de los usuarios?

La creación de sellos de confianza

La ANEI (Asociación Nacional de Empresas en Internet) creó un sello confianza en línea, Optima Web. Éste es un sello de calidad (al igual que los conocidos ISO 9000 e ISO 14000), que asegura la protección del consumidor en todos los ámbitos de Internet, desde el comercio on-line hasta la protección de menores. Así, cuando el usuario vea que la página web que está consultando tiene el sello de óptima web, tiene la certeza de que la empresa que hay detrás de esa web cumple con las normas que el sello de calidad establece. También incluye vías de resolución de conflictos como el arbitraje on-line o que un tercero medie en la resolución. Explicó que para el año 2010 esperan que ya esté implantado.

Safetypay

Los principales problemas que los consumidores encuentran en sus compras por internet ha ido variando a lo largo de los años, ya queen el 2005 las mayores preocupaciones de los consumidores eran que los productos llegaban estropeados, problems logisticos ,sin embargo en el 2007 los problemas con los cuales se encuentra el consumidor ya no son problemas relacionados con la logística sino más bien, con problemas como que los productos adquiridos no se corresponden con los ofrecidos en la web, problemas en su devolución, y problemas a la hora de descargarlo.

A través de diversas estadísticas se pone de manifiesto que la demanda de compras por internet se verían incrementadas

La experiencia de ADICAE en la protección de los derechos de usuarios de medios de pago

ADICAE denuncia la falta de protección de los usuarios en sus transacciones a través de "banca por Internet". Las entidades de crédito prefieren ocultar estos graves problemas antes que invertir en sistemas de seguridad adecuados.

Una de las cuestiones generales planteadas es que actualmente son muchos los medios de pago al alcance de los usuarios: tarjetas de crédito, transferencias por banca electrónica, pago por móvil, dinero electrónico... pero, ¿Son realmente seguros? Desde ADICAE se manifiestan serias dudas al respecto.

Las entidades tan solo invierten en su propia seguridad informática y no en la de sus clientes a quienes pretenden imponer toda la responsabilidad en caso de fraude. En la mayoría de ocasiones, los consumidores no disponen ni tan siquiera de una copia del contrato firmado, lo cual genera multitud de problemas prácticos frente a los tribunales, porque se desconocen las cláusulas del contrato con carácter previo a la interposición de la demanda. La solución a este tipo de contenciosos debe ser extrajudicial, y necesariamente se debería articular un control más efectivo previo a la vía judicial

Los bancos y cajas de ahorros no sólo deberían proceder de inmediato a dotarse de mejoras en las medidas de seguridad, que hoy por hoy pasan por la implantación del chip, sino que pueden articular otros mecanismos menos costosos pero que pueden ser igualmente eficaces. Por ejemplo, enviar un mensaje de confirmación inmediata al teléfono móvil cada vez que se realiza una compra con la tarjeta, algo que ya han comenzado a hacer algunas entidades, lo que no exime evidentemente a los consumidores de comprobar los extractos del banco con mayor atención y asiduidad.

ADICAE insta a la erradicación inmediata de todos los contratos de las cláusulas por las que las entidades limitan su responsabilidad en estos supuestos, ya que muchas se sujetan a estas cláusulas, abusivas a todas luces, para evitar responder ante sus clientes. La despreocupación de nuestros servicios bancarios parece olvidar que los consumidores asumen en muchas ocasiones parte del fraude, respondiendo de los primeros 150 euros siempre y cuando las compras fraudulentas se hayan cargado antes de que el cliente lo notifique al servicio de atención al cliente pidiendo su cancelación, ya que una vez cancelada al cliente no se le debe cargar cantidad alguna. Pero lo más grave sin duda son las frecuentes ocasiones en que bancos y cajas desoyen las reclamaciones de los clientes afectados.

LOS PROBLEMAS DE LOS CONSUMIDORES ANTE LOS MEDIOS DE PAGO

Propuestas de ADICAE para su resolución

Problemas de los medios de pago

Problemas técnicos derivados del funcionamiento normal del medio de pago (fraude a las expectativas del Consumidor por el uso de medios de pago)

Solución propuesta por ADICAE:

- Inversiones continuas y controles adecuados por parte de las Entidades emisoras de medios de pago y entidades de crédito. Necesidad de establecer legalmente unos mínimos exigibles de inversión
- Controles de supervisión cautelar
- Sistema de Alerta: Comunicación continua y rápida entre Entidades emisoras, entidades de crédito y Asociaciones de Consumidores para comunicar los defectos detectados
- Regulación que establezca perfectamente los compromisos de las entidades emisoras evite las cláusulas exoneratorias de responsabilidad por parte delas entidades (Control de los contratos de las entidades financieras).
- Campañas de información a los consumidores
- Mecanismos de solución de litigios eficaces y con participación de las Asociaciones de Consumidores.

Problemas derivados de actividades delictivas (fraudes delictivos con medios de pago)

Solución propuesta ADICAE:

- inversiones continuas y controles adecuados por parte de las Entidades emisoras de medios de pago y entidades de crédito. Necesidad de establecer legalmente unos mínimos exigibles de inversión
- Controles de supervisión cautelar
- Sistema de Alerta: Comunicación continua y rápida entre Entidades emisoras, entidades de crédito, Policía y Asociaciones de Consumidores para comunicar losriesgos y actuaciones delictivas detectadas.
- Regulación que evite las cláusulas exoneratorias de responsabilidad por parte de las entidades.
- Mecanismos de solución de litigios eficaces y con participación de las Asociaciones de Consumidores

PARTE 3

Conclusiones y propuestas de ADICAE

Este Proyecto supone una novedad en cuanto a la lucha contra el fraude en los medios de pago y otros crímenes económicos en general que perjudican los intereses de los consumidores. Tradicionalmente, en las diversas iniciativas llevadas a cabo por las diversas instituciones (y especialmente por la Comisión Europea) se han dejado de lado a consumidores y usuarios, excluyendo de los procesos legislativos a sus representantes legítimos, que son las Asociaciones de Consumidores.

A pesar de ello, la Comisión Europea, consciente de los crecientes problemas asociados al uso de los medios de pago distintos al efectivo, ha admitido en diversas ocasiones que es necesario implicar a las asociaciones de consumidores en la lucha contra este tipo de delitos.

Por ejemplo, en la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y a Europol - Un nuevo Plan de Acción de la UE (2004 - 2007) para la prevención del fraude sobre los medios de pago distintos al efectivo {SEC(2004) 1264} se señala:

Que los ciudadanos de la Unión Europea deben de disponer de una información más abundante y más clara sobre la seguridad de los pagos.

Se deben de preparar iniciativas específicas dirigidas a prevenir las usurpaciones de identidad en la UE.

Que la difusión de información sobre el material pedagógico existente es todavía limitado entre las Asociaciones de Consumidores, en particular a nivel transfronterizo.

Todavía es necesario definir las mejores practicas a respetar en las guías destinadas a los consumidores resaltando los riesgos asociados a los pagos por medios distintos al efectivo e indicando los mejores medios para evitarlos.

Concretamente, la prevención del fraude y la falsificación de los medios de pago distintos del efectivo se ha venido delimitando como una medida prioritaria en el marco de los diversos Planes de Acción sobre Servicios Financieros realizados por la Comisión Europea; ello es así porque unos medios de pago distintos del efectivo eficientes y de fácil empleo, ampliamente aceptados, fiables y disponibles a un bajo coste relativo son esenciales para una economía moderna y un Mercado Unico integrado.

Dada la gravedad y el avance del fraude en medios de pago es necesario operar desde todos los sectores de modo coordinado. El nivel de fraude transfronterizo es superior al de fraude nacional, en el caso de las tarjetas de pago es varias veces superior a la tasa de fraude global de la UE. El fraude se ha venido incrementando en todas las modalidades, pero sobre todo en el caso de las transacciones con pago a distancia, especialmente a través de Internet. Mientras que las ventas del comercio electrónico en los últimos años han superado las previsiones más favorables, su potencial se esta viendo frenado por la falta de confianza de los consumidores en la seguridad de las operaciones de pago efectuadas a través de Internet. Por ello es necesario afrontar las medidas desde una perspectiva netamente europea.

adicae en internet

www.adicae.net

Información, artículos, consejos, actividades de ADICAE...
Una herramienta útil para los usuarios de medios de pago

Los consumidores y su papel en la erradicación del fraude en medios de pago

Los diversos Planes de Acción contra el fraude establecidos por la Comisión Europea señalan la necesidad de incrementar la atención sobre el fraude en medios de pago y en este sentido resultan de importancia fundamental, además de otras acciones, unas medidas preventivas para combatir el fraude y la falsificación de medios de pago distintos del efectivo. Además de utilizar un principio de prudencia y de especial protección a los consumidores, en el caso de nuevos medios de pago, más y más tecnológicos es necesario crear un elemento de contrapeso y diálogo con las empresas.

Las acciones que a continuación se van a señalar van dirigidas a afrontar el problema del fraude en medios de pago distintos al efectivo desde la perspectiva de las legítimas asociaciones representantes de los consumidores y a resaltar la importancia de la participación de los consumidores en la lucha contra el fraude, puesto que suponen el eslabón más débil de la cadena de fraude. Cualquier decisión que afecte a los consumidores debe ser consultada y consensuada con ellos.

Sin duda es en la Comisión Europea, y en particular en las Direcciones Generales de: Mercado Interior y SANCO donde ha de recaer en origen la coordinación de acciones de fomento de medidas preventivas, incluidas las iniciativas de promoción del grado de concienciación sobre el riesgo de fraude en los pagos y la recogida de información, y quien ha proponer alcanzar un elevado nivel de prevención del fraude mediante la aplicación homogénea de iniciativas en todos los Estados miembros de la Unión. En lo que a los consumidores, representados a través de sus legítimas organizaciones se refiere, se debe de fomentar la creación de un frente común de los consumidores en esta materia. ADICAE pretende continuar con los objetivos generales que motivaron la puesta en marcha de este proyecto, ya que como Asociación especializada en consumo financiero esta problemática es de su máximo interés.

Propuestas de ADICAE para la lucha contra el fraude en medios de pago

Creación del observatorio de fraude en medios de pago:

Sería útil el establecimiento de un convenio de colaboración entre las partes para crear un mecanismo que permitiese establecer un diálogo permanente entre todas las partes interesadas (sistemas de tarjetas de pago, bancos, sistemas nacionales de pago, asociaciones bancarias, fabricantes de equipo y de tarjetas de pago, Europol, Interpol, autoridades públicas, incluidos los organismos de aplicación de la reglamentación, sector minorista, consumidores, operadores de redes) con el fin de aplicar el enfoque de asociación propuesto y garantizar una eficacia máxima en la lucha contra el fraude y la falsificación en los pagos además de realizar nuevas acciones.

Funcionamiento del Observatorio:

- Participación de expertos de fraude de cada sector y país.

- Trabajo en sub–grupos, dirigidos por un Grupo Organizativo

- El Pleno del Observatorio se reunirá al menos dos veces por año.

Objetivos del Observatorio:

Colaborar con el sector de sistemas de pago para revisar sus prácticas y procedimientos de forma constante y modificar o interrumpir aquellos que puedan favorecer un comportamiento fraudulento.

Colaborar con el sector de pagos para establecer las mejores prácticas en lo que se refiere a material docente destinado a los minoristas y consumidores y preparar nuevo material conforme vaya siendo necesario.

Colaborar en informar a los minoristas a ser mejor informados sobre la situación de los instrumentos de pago presentados para su aceptación y recibir asesoramiento sobre la forma de tratar las transacciones sospechosas.

Colaborar con las Asociaciones de Consumidores en elaborar directrices sobre nuevos ámbitos de riesgo (por ejemplo, pagos en línea) y sobre comportamientos fraudulentos, alentando a los consumidores a adoptar las medidas razonables para evitar el fraude.

Colaborar en implementar un número de teléfono único para todos los consumidores de la UE que facilite la notificación de la pérdida o robo de un instrumento de pago, o al menos de un único número de teléfono para todos los emisores de cada Estado miembro.

Colaborar en el examen, implementación y propuesta de las garantías jurídicas y las obligaciones de las diferentes partes relacionadas con el fraude y la falsificación de los medios de pago distintos del efectivo.

La Comisión organizará una reunión con las organizaciones de consumidores y otras partes interesadas para examinar los modos de desarrollar y promover la formación de los consumidores acerca de los riesgos asociados a los diferentes mecanismos de pago y la mejor forma de evitar estos riesgos.

Creación de un logo de confianza europeo en materia de medios de pago

Este logo de confianza, en línea con otras iniciativas especialmente de carácter empresarial (aunque bastante infructuosas hasta el momento), se basaría en los siguientes elementos:

- Un conjunto de normas deontológicas recogidas en un Código Ético sobre Medios de pago debería recoer, en especial, el régimen de responsabilidad de los operadoras en relación con las diversas Recomendación Europea que, en general, no son respetadas por proveedores de medios de pago y entidades financieras.

- Un mecanismo de aplicación de esas reglas debería encargarse de resolver las controversias y reclamaciones que se presenten. Asimismo, debería crearse una Junta Arbitral de carácter especial para medios de pago, que actuaría previo intento de mediación por parte de las Asociaciones de Consumidores.

- Un órgano de AUTOCONTROL, encargado de los aspectos de tramitación y procedimientos así como de la gestión cotidiana del sistema de autorregulación y del sello de confianza, y a la que se dirigirán las reclamaciones presentadas por pretendidas infracciones de las normas de este Código.

- Y un sello de confianza que permita identificar a las compañías adheridas a este sistema de autorregulación, que podrían exhibir en sus elementos informativos y publicitarios las empresas que forman parte de este sistema de autorregulación como distintivo de su adhesión.

La cooperación internacional

La cooperación internacional entre los agentes involucrados, la mejor arma para combatir el fraude.

Ha quedado de manifiesto que para luchar contra casos delictivos que están formados por hechos delictivos en varios países los cuerpos policiales nacionales deben cooperar entre ellos, preferiblemente supervisados por un agente supranacional como en este caso podría ser Europol.

Pues bien, en otros ámbitos como los procesos legislativos o la creación de políticas de educación de los consumidores, que contribuyen a luchar contra este tipo de crímenes económicos, la cooperación entre los diversos agentes interesados debe darse de igual modo.

Para otras conclusiones y consejos técnicos revise el resto de publicaciones de ADICAE del proyecto.