3.- LA LEY DE SERVICIOS DE PAGO: ASPECTOS GENERALES

Dr. Pascual Martínez Espín
Catedrático de Derecho Civil
UCLM

Phishing smishing unicaja banco

- Los clientes de Unicaja sufren una ciberestafa masiva: a través de SMS con phishing o llamadas de teléfono falsas
- Solo entre Cantabria y Málaga las víctimas ascienden a 700 y a 4 millones de euros, mientras que las primeras demandas, en Asturias, les dan la razón frente al banco.
- Ha habido dos grandes oleadas. Una, en primavera, tras la fusión de Unicaja con Liberbank, que tuvo lugar el 23 de mayo.
- Ha habido dos grandes oleadas. Una, en primavera, tras la fusión de Unicaja con Liberbank, que tuvo lugar el 23 de mayo.
- La segunda tuvo lugar en enero de 2023
- Hay casos en Andalucía, en Castilla-La Mancha, en Asturias, en Madrid, muchos también en Toledo..."

Mezcla de *pshishig* (obtención de datos personales a través de internet, fundamentalmente bancarios) que se han subastado y usado posteriormente, y *smishing* (el fraude por mensajes sms).

- **Un sistema de ataque combinado**, que comienza por un clásico **envío de SMS de phishing** con un enlace que se tratará por todos los medios que pulse el usuario. Se trata de conseguir que se pulse en el enlace a través de un mensaje de alerta en el que se recomienda pulsar para **dar solución a un problema técnico**. Al momento se abrirá una página que es exactamente igual a la de Unicaja donde **se solicitará la firma digital.** De esta manera se estarán dando los permisos necesarios para que se hagan transferencias sin control.
- Pero además de estos mensajes de texto, también se hace uso de ingeniería social a través de llamadas de teléfono por parte de supuestos gestores que se ponen en contacto con los clientes. Al hacerse pasar por un gestor del banco, se trata de dar la máxima confianza y conseguir todos los datos para entrar en la banca online. Para esto se trata de mostrar un problema en la banca y se requieren las claves para mitigarlo.
- **Se utilizan programas que están especializados, llamados "call spooofind"** que hace cuando se realice una llamada aparezca un prefijo malagueño.

- Hay un aspecto fundamental: que por lo menos, ha habido una fuga de datos segura: **los números de teléfono** asociados a la cuenta on line" de los clientes.
- Según la **Ley de Servicios de Pago**, el banco debe hacer frente a esos pagos fraudulentos a excepción de si demuestra que el cliente cometió una negligencia grave, algo que debe demostrar la entidad bancaria, en todo caso.
- En los casos de fraude mediante sms, la entidad debe demostrar que la operación fue autenticada, registrada y contabilizada, algo que es obvio, pero con un matiz: que el cliente tiene un cargo en la cuenta que no ha autorizado y que fueron ejecutadas por un tercero mediante engaño.
- En agosto de 2022 existía **"una campaña subasta y venta de bases de datos de clientes de Unicaja"**, realizada mediante canales de *Telegram*.
- "aparte de bases de datos de clientes, se vendían los procedimientos de phishing y de robo de contraseñas", y se encontraron "varios **vídeos demostrativos",**

Estimación integra Phishing UNICAJA

- El supuesto de hecho radica en la reclamación de las cantidades sustraídas por un tercero phisher mediante 23 operaciones de bizun no autorizadas en una cuenta corriente de Unicaja. Se reclama incumplimiento contractual en el deber de guarda y custodia del dinero por parte de Unicaja para con su cliente.
- Hay responsabilidad bancaria por los defectos de seguridad del sistema que determina la ejecución de órdenes de pago no autorizadas por su cliente, con la única excepción de que el banco acredite la culpa o negligencia de la víctima. Constituye por tanto obligación esencial de las entidades prestadoras del servicio de banca online el dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones por lo que, en el supuesto de insuficiencia o mal funcionamiento de las adoptadas, deben ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema.

La entidad bancaria aporta como documental (documento no7) una serie de SMS que, según la entidad demandada, fueron enviados a la parte actora con la clave de seguridad necesaria para realizar las operaciones, lo que acreditaría que el señor Montes, conocía las claves de seguridad y las introdujo voluntariamente, por lo que no habría un negligente funcionamiento de los medios de seguridad en el pago. Sin embargo, no ha quedado acreditado que dichos mensajes fueran recibidos, y aun cuando se hubiera admitido la solicitud extemporánea realizada por la parte demandada de oficio a la compañía telefónica, ello únicamente habría permitido probar el envío y en su caso recepción de los mensajes en el teléfono móvil de la parte demandante, no su validación o introducción por el señor Montes, teniendo la carga de probar este hecho la parte demandada por cuanto es la entidad bancaria la que se entiende que posee los documentos y registros necesarios para ello.

Lo cierto es, además, que la parte demandada aporta una serie de mensajes enviados a la parte demandante (documento no 7) pero solo 9 de ellos corresponden a los días 19 y 20 de junio, y de esos 9, solo 7 contienen claves de seguridad para operaciones realizadas el día 19 de junio. Además, los extractos bancarios que constan en el documento no 4 aportado por la parte, no nos permiten comprobar las horas de los bizums, por lo que no se pueden comparar con los SMS aportados. Por otra parte, los SMS contienen cantidades diferentes a los bizums enviados pues dos de ellos comunican que se va a realizar un bizum de 500 euros cuando de dichos extractos bancarios se constata que las operaciones de transferencia no superaron los 200 euros, por lo que las cantidades no cuadran.

Por todo ello, teniendo en cuenta que se realizaron hasta 25 operaciones de bizum no autorizadas, como se acredita del documento no 4 aportado por la parte demandada, y que solo se aportan por la parte demandada 7 mensajes con claves de seguridad, **ES CLARO QUE EXISTIÓ UN DEFICIENTE FUNCIONAMIENTO DE LA NORMATIVA SOBRE SEGURIDAD EN EL PAGO Y, POR LO TANTO, LE CORRESPONDE AL BANCO LA RESPONSABILIDAD DE ABONO DE LA CANTIDAD DEFRAUDADA.**

Por consiguiente, acreditado el incumplimiento por la entidad bancaria demandada de sus obligaciones en los sistemas de pago online o a distancia, la demanda debe ser estimada.

Contextualización

Revolución digital: comercio y a los servicios de pago

Transacciones online, con alternativas variadas a las ofrecidas por la Banca tradicional

Regulación uniforme de los servicios de pago

Estos engloban numerosas transacciones (v. gr., ingreso y retirada de efectivo en cuentas de pago, ejecución de adeudos domiciliados; operaciones mediante tarjeta de pago o dispositivo similar; transferencias; envío de dinero; operaciones a través de dispositivos de telecomunicación, digitales o informáticos; etc.), en las que intervienen varios sujetos: ordenante, proveedores de servicios de pago y beneficiario.

Pagos flexibles

- Métodos de pago más flexibles, entre los que ahora predominan la tarjeta bancaria (92 %), las transferencias (75 %) y la pasarela de pago PayPal (68 %), aunque Bizum (14 %) y la facturación a través de dispositivos móviles (37 %) van ganando posiciones.

ANTECEDENTES

Directiva europea 2007/64/CE, sobre servicios de pago en el mercado interior (en adelante DSP1),

y su transposición al ordenamiento jurídico español a través de la Ley 16/2009, de 13 de noviembre, de Servicios de Pago,

sistematizaban de manera novedosa este entorno,

la realidad práctica de las citadas operaciones generó paulatinamente la necesidad de una regulación revisada

La DSP1

- Tenía como objetivo principal "garantizar que los pagos realizados en el **ámbito de la Unión Europea** –en concreto, las transferencias, los adeudos directos y las operaciones de **pago directo efectuadas mediante tarjeta-** puedan realizarse con la **misma facilidad, eficiencia y seguridad** que los pagos nacionales internos de los Estados miembros.
- Contribuye al reforzamiento y **protección de los derechos de los usuarios de los servicios de pago** y facilita la aplicación operativa de los instrumentos de la zona única de pagos en euros (SEPA)".

Ley de Servicios de Pago de 2009

- Finalidad de contribuir a “una mayor eficiencia, un nivel más elevado de automatización y un procedimiento común sujeto a la legislación comunitaria”.

Directiva Europea 2015/2366 sobre servicios de pago en el mercado interior conocida como PSD2.

- CARENCIAS DE LA PRIMERA DIRECTIVA
- Desde la DSP1 "el mercado de pagos minoristas ha experimentado notables **innovaciones técnicas**, que han dado lugar a un rápido **incremento del número de pagos electrónicos y pagos móviles,** y a la aparición de **nuevos tipos de servicios de pago en el mercado,** y que han puesto en entredicho la validez del marco actual" (Considerando 3).
- 2) "Muchos **productos o servicios de pago innovadores** no entran, en su totalidad o en gran parte, en el ámbito de aplicación de la Directiva 2007/64".
- "Además, la Directiva (…) ha demostrado ser en algunos casos, en su ámbito de aplicación y, en particular, en los elementos excluidos del mismo, como determinadas actividades conexas a los pagos, demasiado **ambigua o general, o simplemente obsoleta**, vista la evolución del mercado.

- Se ha constatado la dificultad que tienen los proveedores de servicios de pago para lanzar **servicios de pago digitales innovadores**, seguros y de fácil uso, de modo que los consumidores y los minoristas puedan disfrutar de métodos de pago eficaces, cómodos y seguros a escala de la Unión" (Considerando 4).

- "En los últimos años, han aumentado los **riesgos de seguridad** de los pagos electrónicos, debido a la mayor complejidad técnica de estos, el **incesante incremento del volumen de pagos electrónicos** en todo el mundo y los **nuevos tipos de servicios de pago**. Disponer de servicios de pago **fiables y seguros** es condición esencial para el buen funcionamiento del mercado de servicios de pago, por lo que los usuarios de esos servicios deben gozar de la debida protección frente a tales riesgos" (Considerando 7).

Directiva 2015/23662, sobre servicios de pago en el mercado interior (PSD2)

PSD2. ¿PSD2? ¿Sabes de qué estamos hablando? No es un robot de Star Wars y, aunque no lo hayas oído nunca, pronto lo harás, porque **va a afectar a tu bolsillo** y porque muy pronto comenzarás a recibir invitaciones de empresas no bancarias que te pedirán acceso a tus datos financieros.

¿Qué es la PSD2?

El **PSD2** (Payment Service Directive 2) es una **directiva europea que tiene como objetivo mejorar la seguridad y reforzar la protección contra fraudes en las operaciones bancarias hechas a través de internet.**

Además, también regula el acceso, con consentimiento, de los datos de tus cuentas bancarias a terceros (Facebook, Amazon, etc.)

DPS2

- Facilitar que los nuevos medios de pago lleguen a un mayor número de consumidores y asegurar una elevada protección del consumidor en el uso de esos servicios de pago
- 1) Definición neutra del **concepto de operaciones de pago** para englobar no solo los modelos habituales, estructurados en torno a la utilización de tarjetas de pago, sino también **otros modelos de negocio**, incluidos aquellos en los que intervienen varios adquirentes.
- 2) Autorización de la figura de **prestatarios de servicios** (v. gr., operadores de telecomunicaciones, proveedores de acceso a Internet, portales, motores de búsqueda), muy activos en aplicaciones para móviles y otros canales electrónicos, lo que conlleva un desafío para los Bancos.
- 3) Requisitos de **seguridad más estrictos** (**autenticación reforzada**) para la tramitación de los pagos electrónicos y la protección de los datos financieros de los clientes.

- 4) **Protección a los consumidores** frente a prácticas comerciales engañosas y desleales, en particular reforzando los requisitos de **información precontractual**.
- 5) Derecho del consumidor a recibir la **información pertinente de forma gratuita** antes de quedar vinculado por un contrato de servicios de pago. Dicha información se realizará con elevado nivel de **claridad**, teniéndose en cuenta las necesidades del consumidor, así como los aspectos técnicos de carácter práctico y la relación coste-eficacia.
- 6) **Prohibición** de métodos de fijación de **precios no transparentes** ya que dificultan extremadamente al usuario la determinación del precio real del servicio de pago.
- 7) **Prohibición de cargos adicionales** por el uso de determinado **instrumento de pago**.

- 8) Racionalización y armonización de las normas en materia de **responsabilidad en las operaciones no autorizadas**, ofreciendo una protección reforzada de los intereses legítimos de los usuarios de servicios de pago. Salvo en caso de fraude o negligencia grave, **el importe máximo** que, en cualquier circunstancia, un usuario de servicios de pago podría verse obligado a desembolsar de realizarse una operación de pago no autorizada **desciende del originario importe de 150 euros a 50 euros**.
- 9) Creación a nivel nacional de una **figura competente** para manejar las **quejas de los servicios de pagos** de particulares y de las asociaciones de consumidores.
- 10) Continua actividad de la Entidad Bancaria Europea (EBA) para la elaboración de **directrices**.

LEY DE SERVICIOS DE PAGO

- La nueva Ley de Servicios de Pago y otras medidas urgentes en materia financiera (en adelante LSP), aprobada por Real Decreto-Ley 19/2018, de 23 de noviembre y publicada en el BOE el 24 de noviembre, en sustitución de la Ley 16/2009, de 13 de noviembre, de Servicios de Pago, **entró en vigor el día 25 de noviembre de 2018** y transpone al ordenamiento jurídico español la nueva Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo sobre servicios de pago en el mercado interior.
- No obstante, los Títulos II (Transparencia de las condiciones y requisitos de información aplicables a los servicios de pago, resolución y modificación del contrato marco) y III (Derechos y obligaciones en relación con la prestación y utilización de servicios de pago) fueron de aplicación a los 3 meses de su publicación en el BOE, el 25 de febrero de 2019.

Glosario de términos

Usuario de servicios de pago: la persona física o jurídica que hace uso de un servicio de pago, ya sea como ordenante, beneficiario o ambos.

- **Ordenante**: la persona física o jurídica titular de una cuenta de pago que autoriza una orden de pago a partir de dicha cuenta o, en el caso de que no exista una cuenta de pago, la persona física o jurídica que dicta una orden de pago.

- **Beneficiario**: la persona física o jurídica que sea el destinatario previsto de los fondos objeto de una operación de pago.

- **Proveedor de servicios de pago**: las entidades y organismos contemplados en los apartados 1 y 2 del artículo 5, y las personas físicas o jurídicas que se acojan a las exenciones previstas en los artículos 14 y 15.

- **Proveedor de servicios de iniciación de pagos**: el proveedor de servicios de pago que ejerce a título profesional las actividades a que se refiere el artículo 1.2.g) (servicios de iniciación de pagos).

- **Proveedor de servicios de pago gestor de cuenta**: un proveedor de servicios de pago que facilita a un ordenante una o varias cuentas de pago y se encarga de su mantenimiento.

- Microempresa: una empresa, considerando como tal tanto a las personas físicas que realizan una actividad profesional o empresarial como a las personas jurídicas, que, en la fecha de celebración del contrato de servicios de pago ocupa a menos de diez personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los dos millones de euros.

- • Servicio de iniciación del pago: servicio que permite iniciar una orden de pago, a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago.

- • Servicio de información sobre cuentas: servicio en línea cuya finalidad consiste en facilitar información agregada sobre una o varias cuentas de pago de las que es titular el usuario del servicio de pago bien en otro proveedor de servicios de pago, bien en varios proveedores de servicios de pago.

- **• Autenticación reforzada de cliente: la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario), que son independientes –es decir, que la vulneración de uno no compromete la fiabilidad de los demás–, y concebida de manera que se proteja la confidencialidad de los datos de identificación.**

¿Cuál es su objetivo?

- El objetivo principal de la LSP y de la Directiva es avanzar en la adaptación de la regulación a los **nuevos cambios tecnológicos** que permiten a los usuarios disponer de forma **más fiable de nuevos servicios de pago y nuevos agentes** que van implantándose de forma cada vez más intensa, especialmente en el contexto de un mercado más amplio que el nacional.
- Los objetivos de la LSP son:
- • Facilitar y mejorar la **seguridad** en el uso de sistemas de pago a través de internet.
- • Reforzar el **nivel de protección** al usuario contra fraudes y abusos potenciales.
- • Promover la **innovación** en los servicios de pago a través del móvil y de internet.
- La LSP regula **tres aspectos** básicos: los **servicios a prestar, la transparencia frente al usuario y las obligaciones de las partes** intervinientes.

¿Cuál es su ámbito de aplicación?

- Afecta a todos los servicios de pago prestados en España, cualquiera que sea el origen o el destino final de las operaciones, tanto en euros, en monedas nacionales de los estados miembros o en otras monedas:
- • Servicios de pago prestados dentro de España.
- • Operaciones de pago efectuadas en una moneda de un Estado miembro de la Unión Europea cuando tanto el proveedor de servicios de pago del ordenante como el del beneficiario, o el único proveedor de servicios de pago que intervenga en la operación de pago, estén situados en España.
- • Operaciones de pago efectuadas en una moneda que no sea la de un Estado miembro que se lleven a cabo en España, cuando al menos uno de los proveedores de servicios de pago que intervengan en la operación de pago esté situado en España y el otro esté situado en la Unión Europea.
- • Aquellas partes de la operación de pago, cualquiera que sea la moneda en la que se efectúe, que se lleven a cabo en España, en las que alguno de los proveedores de servicios de pago esté situado fuera de la Unión Europea.

¿A qué tipos de operaciones aplica?

La LSP contempla los siguientes servicios de pago:

- Transferencias, incluidas las órdenes permanentes.
- Adeudos domiciliados, incluidos los no recurrentes.
- Operaciones con tarjetas de débito o de crédito.
- Ingresos y retiradas de efectivo en cuenta.
- Emisión de instrumentos de pago o adquisición de operaciones de pago.

Aspectos comunes

- La LSP incrementa el nivel de protección a los usuarios y la seguridad de los pagos, disminuyendo el volumen de fraude y el abuso a los consumidores.
- Protección del consumidor restringiendo comisiones, provenientes de comercios que cobren recargos en función del medio que hayan utilizado y regula la actividad de los cajeros independientes limitando el cobro de las dobles comisiones.
- Para lograr esta mayor protección, la LSP:

1. Transparencia e información

- El acceso a la información no tendrá coste alguno para los usuarios que deberán conocer **gratuitamente los gastos asociados a cada operación, las condiciones de la misma y el plazo de ejecuci**ón en que se llevará a cabo.

2. Facultad de rescisión

En todo momento, salvo que se pacte lo contrario, el usuario de los servicios PSD2 podrá rescindir su contrato marco sin aviso previo.

En caso de existir pacto en contra, este no podrá superar el mes.

La rescisión de un contrato, será gratuita. Es más, la rescisión sólo pierde su carácter gratuito si el contrato ha tenido una duración inferior a seis meses.

3. MICROEMPRESAS COMO CONSUMIDORES

- • Las Microempresas pasan a tener la misma consideración que los consumidores en cuanto al régimen de protección otorgado en derechos y obligaciones relacionados con la prestación y utilización de servicios de pago, así como con la transparencia de las condiciones y requisitos de información, resolución y modificación del contrato marco.

4. Rectificación de operaciones no autorizadas

Ante el uso fraudulento de un instrumento de pago extraviado o sustraído, el ordenante soportará hasta un máximo de 50€ por las pérdidas derivadas de operaciones de pago no autorizadas, salvo fraude o negligencia por parte del usuario.

RESPONSABILIDAD DEL PROVEEDOR

- El proveedor es responsable de devolver el importe del servicio cuando:
- • La operación no haya sido autorizada por el ordenante.
- • El ordenante no le fuera posible detectar la pérdida, extravío o apropiación.
- • El proveedor del servicio no tenga medios adecuados para que pueda notificarse el extravío o sustracción del instrumento de pago.
- • El proveedor del servicio de pago no exige autenticación reforzada, deberá soportar las consecuencias económicas si el ordenante no actúa de forma fraudulenta.

El consumidor será responsable:

- • De las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado, sustraído o apropiado indebidamente por un tercero. Con límite de hasta 50 euros.
- • De las pérdidas derivadas de operaciones de pago no autorizadas si el ordenante ha incurrido en tales perdidas por actuar de forma fraudulenta.
- • Quedando exento de toda responsabilidad en el caso de sustracción, extravío o apropiación indebida del instrumento de pago, siempre y cuando, las operaciones de pago se hayan efectuado de forma no presencial y utilizando datos de pago impresos en el mismo instrumento.

5. PLAZO RESOLUCIÓN RECLAMACIONES

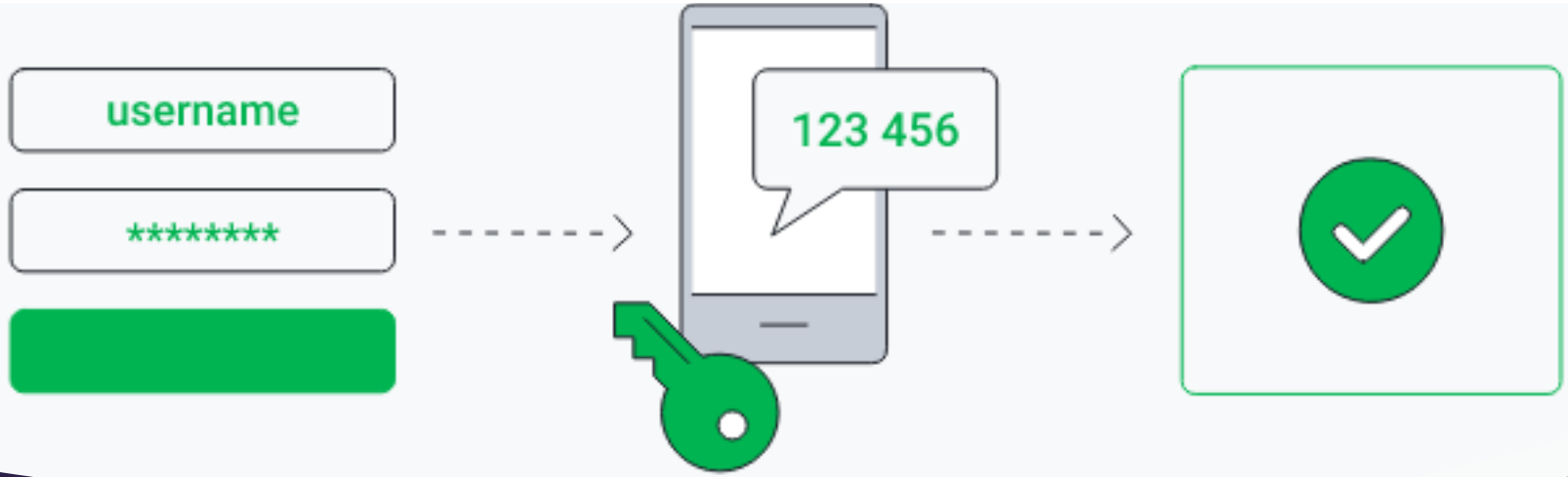
Reduce el plazo de respuesta para la resolución de las reclamaciones de los usuarios de servicios de pago, pasando de los dos meses que preveía la normativa anterior, a quince días hábiles.

Cómo reclamar los abusos en medios de pago

- Las vías que existen son tres:
- Servicio de atención al cliente,
- Sistema arbitral de consumo
- y Organismos de supervisión.
- Los proveedores del servicio tienen que dar respuesta a las cuestiones que se plantean en la reclamación en un plazo de 15 días hábiles.
- Cuando no pueda ofrecerse una respuesta en ese plazo por razones ajenas del proveedor, deberá enviar una respuesta provisional, especificando el plazo que recibirá la contestación.
- Si tenemos una respuesta insatisfactoria podemos dirigirnos al organismo supervisor, que en este caso, es el Banco de España según la normativa de medios de pago. Cabe destacar que tiene un periodo de 3 meses para contestar y su resolución no es vinculante para el proveedor del servicio de pago.

6. AUTENTICACIÓN REFORZADA

- Medidas de autenticación reforzada o doble autenticación. Uno de los objetivos es reducir el fraude y aumentar la seguridad. Esto significa que para autorizar una operación será necesario emplear al **menos dos de estos métodos**:
- **Elemento inherente: huella dactilar, iris o reconocimiento facial, sistemas habituales en los dispositivos móviles.**
- **Elemento poseído: algo físico como una tarjeta, un certificado digital o un teléfono móvil.**
- **Elemento conocido: un número PIN o contraseña.**
- Como estas medidas de control son **independientes entre sí**, en el caso de que una de ellas esté comprometida a efectos de ciberseguridad, el riesgo de amenaza disminuye dado que va a ser necesario pasar un doble filtro de control.

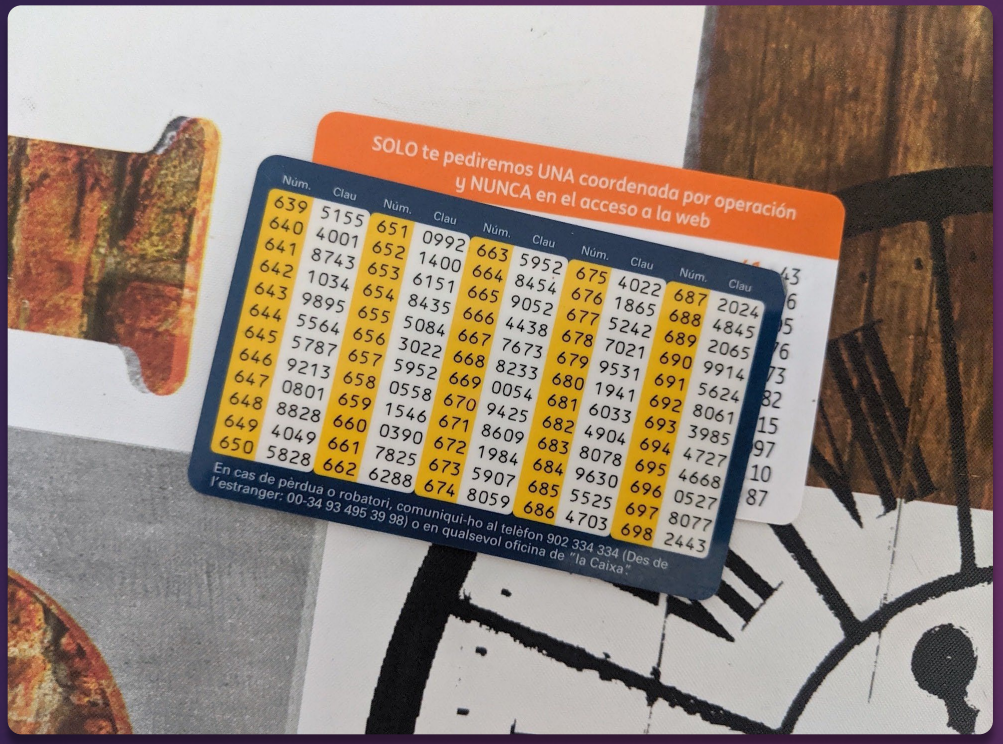


Así es como funciona la 2FA cuando quiere acceder a su cuenta:

- Usted escribe el nombre de usuario y la contraseña, y luego hace clic en enviar. Luego, el servicio en línea envía una solicitud automática para el segundo dato: un SMS con un código de verificación, un mensaje de Google de autenticación u otra opción que haya establecido. Hasta que no confirme su identidad con este segundo dato, no podrá acceder a su cuenta en línea.

¿POR QUÉ NO ES SUFICIENTE CON UNA CONTRASEÑA?

- Aunque tenga una contraseña muy compleja, los hackers más habilidosos son capaces de averiguarla de varias maneras:
- Filtraciones de datos: cuando una organización de gran tamaño sufre un ataque de ciberseguridad, los nombres de usuario y las contraseñas (así como otros datos confidenciales) de millones de personas pueden terminar vendiéndose en la web oscura. Los ciberdelincuentes pueden comprar listas de nombres de usuario y contraseñas, e intentar reciclar las credenciales, es decir, probarlas en toda la red para ver si con ellas pueden acceder a alguna cuenta. Por eso nunca se deben reutilizar las contraseñas para varias cuentas.
- Spyware: este tipo de software malicioso tan insidioso es capaz de espiar a los usuarios. En concreto, existe un software que registra las pulsaciones de las teclas capaz de guardar discretamente todo lo que usted escribe, nombres de usuario y contraseñas incluidos, y de enviar esta información a los hackers que instalaron el malware en su dispositivo de forma subrepticia.
- Phishing: el phishing es un tipo de estafa basado en la ingeniería social por la que los ciberdelincuentes suplantan un negocio o a una persona de confianza para, así, conseguir que revele su información personal. En este caso, podría recibir un correo electrónico falso donde se le pidiera confirmar su nombre de usuario y contraseña de algún servicio en línea que utilice; al escribirlas, las credenciales se enviarían directamente al estafador.



Adiós a las tarjetas de coordenadas: así afecta a nuestro banco la normativa PSD2 y qué cambios llegan al pagar por internet

Excepciones a la doble autenticación

- El acceso a las cuentas de pago y a la consulta de movimientos, **salvo que se acceda por primera vez o no se haya accedido en los últimos 90 días**
- En los **PAGOS CONTACTLESS**, siempre que el importe sea **inferior a 50 euros**, que el **saldo acumulado** de compras desde la última vez que se solicitó la autenticación reforzada **no pase de 150 euros** o que no se **hayan producido más de 5 compras contactless** desde la última operación con autenticación reforzada.
- En **pagos de escasa cuantía a distancia si el importe es inferior a 30 euro**s, el **saldo acumulado** de compras desde la última vez que se solicitó la autenticación reforzada **no supere los 100 euros** o **se hayan producido más de 5 compras** desde ese momento.
- En **máquinas automáticas de parkings y peajes**.
- En pagos a tus "**beneficiarios de confianza**", siempre que estén incluidos en una **lista que hayas creado**. Tampoco es preciso cuando el **ordenante y el beneficiario sean la misma persona**,
- En el caso de **pagos frecuentes** por el **mismo importe y al mismo beneficiario, a partir de la segunda operación no es necesario la autenticación reforzada**.

7. Transferencias

- Los gastos en transferencias intracomunitarias en cualquier divisa serán **compartidos**, lo que significa que **el beneficiario pagará los gastos cobrados por su proveedor de servicios de pago y el ordenante abonará los gastos cobrados por su proveedor de servicios de pago**.

8. Ingresos en Efectivo

- En caso de ingresos de efectivo, la fecha valor será la de del día en que se realice el mismo.

9. Compras online más rápidas

- Con la nueva Directiva el intercambio monetario se hace de **forma instantánea**, al estilo de una transferencia.
- Una vez que se ha autorizado la operación, **no existirán retrasos motivados por procesos de confirmación de pago** que alarguen la disponibilidad de los fondos implicados en la operación.
- Se apuesta por la **agilidad** de las operaciones y por la rapidez sí, pero respaldada por una **mayor seguridad**.

10. Nuevos Derechos

- Derecho de **devolución incondicional de recibos durante las primeras 8 semanas** desde su adeudo en cuentas.
- Derecho a obtener una respuesta a las reclamaciones que puedas plantear ante el Servicio de Atención al Cliente en **un plazo máximo de 15 días hábiles**, prorrogable hasta un mes en casos excepcionales y siempre que comuniquen el motivo de la prórroga

CASO PRÁCTICO: VENTAS ONLINE CON PAGO CON TARJETA: ¿EN CASO DE NO ENTREGA DEL PRODUCTO PUEDE ANULARSE EL CARGO?

Se trata de un supuesto de compra online y pago con tarjeta. **El producto comprado nunca llega al cliente**, por alguno de estos motivos:

1.- La página web ha desaparecido. En algunas ocasiones se ignora el motivo y en otras como en el caso de la empresa costomovil.com, cerrada por orden judicial.

2.- La página web sigue existiendo, pero no se envía el producto al cliente, a veces se explica que es por falta de existencias, en otras ocasiones la empresa online no contesta al cliente.

EN NINGUN CASO SE DEVUELVE EL IMPORTE DE LA COMPRA AL CLIENTE

1.- ¿En estos supuestos se puede reclamar a la entidad bancaria emisora de la tarjeta de crédito o débito con la que se ha pagado, la devolución del importe de la compra a distancia aplicando por analogía el art. 112 del TRLGDCU y el art. 31 de la Ley de Servicios de Pago (compras fraudulentas o no autorizadas por no haber recibido el bien o servicio comprado)?

- El artículo 112 TRLGDCU contempla el pago del contrato a distancia mediante tarjeta. Dicho precepto dispone:
- "1. Cuando el importe de una compra o de un servicio hubiese sido cargado fraudulenta o indebidamente utilizando el número de una tarjeta de pago, el consumidor y usuario titular de ella podrá exigir la inmediata anulación del cargo. En tal caso, las correspondientes anotaciones de adeudo y reabono en las cuentas del empresario y del consumidor y usuario titular de la tarjeta se efectuarán a la mayor brevedad.
- 2. Sin embargo, si la compra hubiese sido efectivamente realizada por el consumidor y usuario titular de la tarjeta y la exigencia de devolución no fuera consecuencia de haberse ejercido el derecho de desistimiento o de resolución, aquél quedará obligado frente al empresario al resarcimiento de los daños y perjuicios ocasionados como consecuencia de dicha anulación."

- 1.- El ámbito objetivo de aplicación son los "cargos fraudulentos o indebidos" utilizando el número de la tarjeta. Sólo en ese caso podrá el consumidor exigir la anulación del cargo. Y solo en ese caso surge la obligación de devolver a la mayor brevedad.

- 2.- Dicha interpretación es confirmada por el número 2 del citado precepto que contempla la obligación del consumidor de resarcir daños y perjuicios cuando el reembolso no tenga su origen en los supuestos contemplados en el mismo. Es decir, el derecho de devolución sólo procede en los siguientes casos:

- - En caso de cargo fraudulento, lo que no se produce cuando hay consentimiento para la compra. En efecto, el artículo **36 Real Decreto-ley 19/2018, de 23 de noviembre,** de servicios de pago y otras medidas urgentes en materia financiera (en adelante LSP), relativo al consentimiento y retirada del consentimiento, prevé que

- **"1. Las operaciones de pago se considerarán autorizadas cuando el ordenante haya dado el consentimiento para su ejecución. A falta de tal consentimiento la operación de pago se considerará no autorizada. 2. Sin embargo, si la compra hubiese sido efectivamente realizada por el consumidor y usuario titular de la tarjeta y la exigencia de devolución no fuera consecuencia de haberse ejercido el derecho de desistimiento o de resolución, aquél quedará obligado frente al empresario al resarcimiento de los daños y perjuicios ocasionados como consecuencia de dicha anulación".**

- - En caso de haber prestado un **consentimiento válido, el precepto solo permite la anulación del cargo en caso de haber ejercitado el derecho de desistimiento** (arts. 74 y 106 TRLGDCU).

- Lo contrario nos llevaría a hacer responder al Banco por **los incumplimientos o imposibilidades de cumplimiento del vendedor**, lo cual no responde a la intención del legislador, sin que exista una norma que establezca el **carácter vinculado de los contratos** y la consiguiente responsabilidad de los bancos por el incumplimiento del vendedor al modo de los arts. 26 y 29 de la LCC.

Entonces, si el consumidor no puede anular el cargo, ¿qué opciones tiene?

- La única opción será los **remedios de que goza frente al vendedor**.
- En este sentido, el art. 66 bis TRLGDCU dispone que, salvo en pacto en contrario, la entrega del bien deberá producirse sin demora indebida y en un plazo máximo de 30 días desde la celebración del contrato.
- Si el empresario no cumple su obligación de entrega, el consumidor deberá emplazarlo en un plazo adicional adecuado a las circunstancias. Si el empresario no cumple su obligación de entrega de los bienes en el plazo acordado con el consumidor y usuario, o en el plazo fijado de nuevo, el consumidor y usuario tendrá derecho a resolver el contrato de inmediato. También tendrá derecho a resolver en el momento en que se den cualquiera de estas circunstancias (por tanto, sin necesidad de un nuevo requerimiento):
- a) si el empresario ha rechazado entregar los bienes o se desprende de las circunstancias que no lo entregará;
- b) en caso de término esencial (expreso o tácito).

- Pero **esta resolución no es oponible al proveedor de servicios de pago, sino únicamente al vendedor**. Aquí pueden darse distintas **situaciones**.

- - **Que el empresario siga existiendo y no entregue por falta de existencias o que no conteste**. En este sentido, **el artículo 110** TRLGDCU, sobre la falta de ejecución del contrato a distancia, dispone: "En caso de no ejecución del contrato por parte del empresario por no encontrarse disponible el bien o servicio contratado, el consumidor y usuario deberá ser informado de esta falta de disponibilidad y deberá poder recuperar sin ninguna demora indebida las sumas que haya abonado en virtud del mismo. En caso de retraso injustificado por parte del empresario respecto a la devolución de las sumas abonadas, el consumidor y usuario podrá reclamar que se le pague el doble del importe adeudado, sin perjuicio a su derecho de ser indemnizado por los daños y perjuicios sufridos en lo que excedan de dicha cantidad". Y a **tenor del art. 111**: "De no hallarse disponible el bien o servicio contratado, cuando el consumidor y usuario hubiera sido informado expresamente de tal posibilidad, el empresario podrá suministrar sin aumento de precio un bien o servicio de características similares que tenga la misma o superior calidad. En este caso, el consumidor y usuario podrá ejercer sus derechos de desistimiento y resolución en los mismos términos que si se tratara del bien o servicio inicialmente requerido".

- - **Que el empresario haya desaparecido**. El consumidor tendrá pocas opciones para recuperar su dinero, salvo la de concurrir al concurso de acreedores, en su caso.

INFRACCIÓN DE CONSUMO

- El incumplimiento de estas normas es calificado como **infracción de consumo** (art. 47.1) y, en consecuencia, la Administración competente (art. 49) podría iniciar el correspondiente expediente administrativo sancionador.
- En efecto, el art. 47) prevé como infracción (calificadas como grave por el art. 50) "el incumplimiento de las obligaciones que la regulación de contratos celebrados a distancia impone en materia de información y documentación que se debe suministrar al consumidor y usuario, de los plazos de ejecución y de devolución de cantidades abonadas".
- En el procedimiento sancionador podrá exigirse al infractor la reposición de la situación alterada por la infracción a su estado original y, en su caso, la indemnización de daños y perjuicios probados causados al consumidor que serán determinados por el órgano competente para imponer la sanción (art. 48).

2.- PLAZOS: en el caso de que se pudieran aplicar estos artículos y reclamar al banco, ¿qué plazo habría para ejercitar esta acción?

- RESPUESTA:
- Negada la aplicación del art. 112 al supuesto que nos ocupa, no procede la aplicación de plazo alguno para exigir el reembolso del cargo realizado en supuestos de incumplimiento del vendedor.

3.- La respuesta ofrecida a la consulta se podría aplicar a la compra de billetes de avión cancelados por la pandemia y pagados con tarjeta de crédito?

- RESPUESTA:
- Negada la aplicación del art. 11 TRLGDCU, no procede la anulación del cargo en caso de cancelación de vuelos a causa del Covid.

¿Y si interviene una plataforma intermediaria? Lo anterior es válido si el vendedor utiliza su propia web para la venta on line. Pero ¿y si actúa a través de una plataforma en línea?

- El **art. 95.2 TRLGDCU**, relativo a los servicios de intermediación en los contratos a distancia, dispone que no será exigible a los prestadores de servicios de intermediación de la sociedad de la información el respeto a los derechos de los consumidores previsto en el art. 95.1, que se regirán por lo previsto en la normativa específica sobre servicios de la sociedad de la información y el comercio electrónico.
- En las plataformas de venta de bienes, es difícil encontrar un fundamento de la responsabilidad de la plataforma por el correcto cumplimiento del contrato de venta del bien, salvo que la plataforma actúe como importadora del bien en el territorio del mercado interior de bienes procedentes de vendedores profesionales con domicilio fuera del espacio comunitario. Por tanto, las plataformas suelen estar **exoneradas de responsabilidad** en el contrato de consumo celebrado entre comerciante y consumidor.

CONCLUSIÓN

- PRIMERA.- El proveedor del servicio de pago (en general) responde de las compraventas falsificadas pero no de las compraventas incumplidas por el vendedor on line.
- SEGUNDA.- El proveedor de servicio de pago no realiza con el comprador un contrato vinculado de los arts. 26 y 29 LCCC, por lo que el comprador no podrá ejercitar los derechos frente al proveedor de servicios de pago que le correspondan frente al vendedor.

¿En qué casos el banco me devolverá el dinero robado de mi tarjeta?

- La Memoria anual sobre la vigilancia de los sistemas de pago del Banco de España de 2021, ese año en nuestro país se produjeron más de un millón de operaciones fraudulentas con tarjetas bancarias por un valor de 88 millones de euros.
- Esto supone 1,4 operaciones fraudulentas por cada 100 tarjetas con un valor medio de 74 euros.
- Entre los fraudes con tarjeta más comunes encontramos las compras online (77%) y las compras físicas (20%).
- En caso de robo o uso fraudulento de las tarjetas, el banco es quien debe hacerse cargo de las pérdidas, pero ¿nos devolverá siempre el dinero al cancelar la tarjeta?

¿Qué dice la ley?

- La regla general es que todos los bancos deben devolvernos el dinero ante un robo o uso fraudulento con tarjeta, aunque con algunas excepciones.
- En el caso del robo de una tarjeta, el banco nos devolverá el 100% de lo robado una vez cancelada la tarjeta.
- En cambio, hasta haberla cancelado, nuestra responsabilidad serán los primeros 50 euros, de acuerdo con la Directiva (UR) 2015/2366 del Parlamento Europeo.
- Por ejemplo, si nos roban 200 euros antes de cancelar la tarjeta, el banco debería devolvernos 150 euros.
- En cambio, si hemos notificado al banco el incidente y nos roban 200 euros tras el aviso, la entidad nos debería devolver el dinero total,

- En el caso de los **duplicados de tarjeta** (crear una copia de nuestra tarjeta sin que perdamos la nuestra y sin darnos cuenta), la regla es distinta.
- La normativa considera que es muy difícil que una persona sea consciente de que le han duplicado la tarjeta hasta que vea un cargo indebido en el extracto. Por esta razón, en estos casos **la entidad devolverá el importe íntegro siempre.**
- Hay que tener en cuenta que no siempre el banco nos devolverá el dinero robado.
- El Parlamento Europeo considera que el banco no será responsable cuando el usuario ha realizado alguna negligencia por su parte. Por ejemplo, tenemos apuntado el pin sobre nuestra tarjeta o hemos dado los datos de nuestra tarjeta a un tercero.
- Además, si todos los pasos de seguridad en la transacción se han seguido (introducir el pin y el código de confirmación), la entidad no devolverá el dinero robado, ya que la doble autenticación se ha llevado a cabo.

¿Cómo pedir al banco que nos devuelva el dinero robado?

- Lo primero que debemos hacer cuando notamos que no tenemos nuestra tarjeta con nosotros o vemos un movimiento extraño en el extracto es cancelarla.
- Una vez cancelada, debemos notificar al banco el problema y solicitar la devolución mediante el "Formulario de Cargos No Reconocidos". Muchas entidades permiten tramitarlo telemáticamente simplemente llamando a atención al cliente.
- En la gran mayoría de las entidades nos devolverán el dinero robado de manera automática y en un plazo de 24 horas o menos, aunque esto no implica que ya se haya solucionado.
- El banco investigará el robo o el duplicado de la tarjeta para saber si hubo negligencia o no por nuestra parte y así tomar la decisión definitiva. Así, una vez termine la investigación, si la resolución es positiva, podremos quedarnos con el dinero. En cambio, si la resolución es negativa, deberemos devolver el dinero y, si queremos recuperarlo, deberemos reclamar de manera formal al banco.

Thanks!

- Any questions?
- You can find me at:
  - Pascual.martinez@uclm.es