



ESTER ROQUETA MAURI
Procuradora de los Tribunales

N/ Ref.: 8991
S/Ref. [REDACTED] Ref. Tercer:

Autos [REDACTED] Jdo: PRIMERA INSTANCIA E
INSTRUCCIÓN (CIVIL) nº 4
Client: [REDACTED]
Advocat OSCAR SERRANO CASTELLS
Sentencia S'estima la demanda interposada contra BBVA i es
condemna a aquesta última a abonar a la Sra. [REDACTED] la
quantitat de 5.371,89 € juntament amb els interessos legals i
amb especial condemna en costes a la demandada.
Notificat: 10/03/2025

Sección Civil. Juzgado de Primera Instancia de Vic

Calle Bisbe Morgades (cantonada Dr.Junyent), 2 - Vic - C.P.: 08500

TEL.: 938834552
FAX: 938833149
EMAIL:mixt4.vic@xij.gencat.cat

N.I.G.: 0829842120238347125

Juicio verbal (250.2) (VRB) [REDACTED] 3

Materia: Juicio verbal (resto de casos)

Entidad bancaria BANCO SANTANDER:
Para ingresos en caja. Concepto: [REDACTED]
Pagos por transferencia bancaria: IBAN ES55 0049 3569 9200 0500 1274.
Beneficiario: Sección Civil. Juzgado de Primera Instancia e Instrucción nº 4 de Vic
Concepto: [REDACTED]

Parte demandante/ejecutante: [REDACTED]
Procurador/a: Ester Roqueta Mauri
Abogado/a: Óscar Serrano Castells

Parte demandada/ejecutada: BANCO BILBAO
VIZCAYA ARGENTARIA, S.A.
Procurador/a: Ignacio Lopez Chocarro
Abogado/a: [REDACTED]

SENTENCIA Nº 52/2025

Jueza: María Jesús Fernández González

Vic, 27 de febrero de 2025

Vistos por mí, Doña María Jesús Fernández González, juez titular del Juzgado de Primera Instancia e Instrucción número 4 de Vic y los de su partido, los autos de juicio verbal [REDACTED] promovidos a instancia de Doña Ester Roqueta Mauri Procuradora de los Tribunales y actuando en nombre y representación de DOÑA [REDACTED] contra la entidad BANCO BILBAO VIZCAYA ARGENTARIA S.A (en adelante BBVA), representada por el Procurador de los Tribunales Don Ignacio López Chocarro, sobre reclamación de cantidad y en base a los siguientes

ANTECEDENTES DE HECHO

PRIMERO. – Por la Procuradora la Procuradora Doña Ester Roqueta Mauri en nombre y representación DOÑA [REDACTED] se formuló demanda de juicio verbal que fue turnada a este Juzgado contra la entidad BANCO BILBAO VIZCAYA ARGENTARIA S.A (en adelante BBVA) en la que tras exponer los hechos y fundamentos de derecho que entendía de aplicación, suplicaba del Juzgado la admisión del escrito y documentos, y previos los trámites legales, se dictase sentencia por la que se



Data i hora 06/03/2025 13:13		Signat per Fernández González, María Jesús;	
------------------------------------	--	---	--



condene a la demandada a pagar a la actora la cantidad de 5.371,89 euros en concepto de principal más intereses legales devengados desde la primera reclamación extrajudicial, todo ello con la condena en costas.

SEGUNDO.- Con fecha 3 de noviembre de 2023 se dictó decreto admitiendo la demanda, acordando dar traslado a la demandada, emplazándola para que la contestase en el plazo de veinte días con los apercibimientos legales, presentándose por el Procurador de los Tribunales Don Ignacio López Chocarro en la ya indicada representación procesal escrito de contestación a la demanda en la que tras exponer los hechos y fundamentos de derecho que entendía de aplicación, suplicaba del Juzgado la admisión del escrito y documentos y tras los trámites legales se dictase sentencia en virtud de la cual, se desestime la demanda absolviendo a su representada de los pedimentos ejercitados en su contra, con la imposición de costas del procedimiento a la parte actora.

TERCERO. - Por diligencia de ordenación convocando a las partes para la celebración de vista, la cual tuvo lugar el día 29 de octubre de 2024 a las 11:30 horas ratificándose ambas partes en sus respectivos escritos de demanda y escrito de contestación. Recibido el procedimiento a prueba, por ambas partes se propuso prueba documental y testifical habiendo sido practicadas las propuestas, admitidas y declaradas pertinentes con el resultado que obra en autos. Quedando como diligencia final un oficio interesado por la parte actora, una vez recibido el mismo, se dio traslado a las partes trámite de conclusiones, quedando los autos pendientes para dictar sentencia por diligencia de ordenación en fecha 26 de febrero de 2025.

CUARTO. - En la tramitación del presente procedimiento se han observado las prescripciones legales.

FUNDAMENTOS DE DERECHO

PRIMERO. – Pretensiones de las partes

Se ejercita por la parte actora una acción de reclamación de cantidad por ejecución de transferencias no autorizadas, alegando que, con fecha 27 de septiembre de 2022 recibió en su dispositivo móvil un mensaje SMS de su entidad bancaria BBVA que debía acceder a un enlace de acceso para confirmar sus datos de identificación porque de lo contrario



Data i hora 06/03/2025 13:13	Signat per Fernández González, María Jesús;



procederían a suspender su cuenta corriente. Si bien, accediendo al mismo, resultó que el enlace no era legalmente de su entidad bancaria BBVA sino que se trataba de un mensaje tipo phishing con el objetivo de captar sus claves bancarias. A consecuencia de ello, y sin su consentimiento ni autorización, desde otro dispositivo se realizó un pago con su tarjeta vía Google Pay por importe de 5.371,89 euros en un establecimiento en la localidad de Rumanía.

La parte demandada se opone a las pretensiones de la actora por cuanto dicha transferencia se realizó por la actuación negligente de la Sra. [REDACTED] al haber facilitado sus datos personales y bancarios a tercero. Así, para para autorizar la compra objeto de reclamación -que se realizaron mediante el sistema GOOGLE PAY-, fue necesario que la demandante: (i) revelara los datos de la tarjeta (16 dígitos, fecha de caducidad y CVV) y; (ii) revelara el código OTP facilitado por BBVA mediante SMS para completar el proceso de enrolamiento de la tarjeta al sistema GOOGLE PAY. Asimismo, para aumentar el límite de la tarjeta fue necesario que la demandante: (i) revelara sus claves de acceso personales e intransferibles de la Banca a Distancia de BBVA y; (ii) el código OTP remitido vía SMS. En consecuencia, la revelación de las claves bancarias y los códigos OTP constituye una actuación de negligencia grave por la que debe responder la Sra. [REDACTED] y no BBVA.

Sin perjuicio de lo anterior, entiende que BBVA ha actuado con la diligencia debida y ha solicitado correctamente la autorización de las operaciones a través de un doble factor de seguridad: las claves de la banca online de BBVA y el código OTP, para autorizar el aumento del límite de la tarjeta. Además de los datos de la tarjeta y el código OTP para autorizar el enrolamiento.

SEGUNDO. - Normativa aplicable

Para una mejor respuesta al motivo, y dado que la responsabilidad que se imputa a la entidad, derivada de la ejecución de una transferencia no autorizada por el titular de la cuenta del cliente demandante realizada a través del sistema de banca online, vía SMS, lo es en tanto prestadora de servicios de pago a través del modelo de banca virtual puesta a disposición de su cliente, concretaremos el régimen legal y contractual en el que se desenvuelve la banca electrónica, cuáles son las obligaciones el prestador y del usuario conforme a la legislación aplicable, el significado jurídico de las órdenes de pago y el marco de responsabilidades que del mismo resulta y la jurisprudencia más señalada al



Data i hora 06/03/2025 13:13	Signat per Fernández González, María Jesús;



respecto.

Pues bien, tales aspectos pueden concretarse en los puntos que seguidamente numeramos.

1.- La transferencia bancaria es un servicio que forma parte del contrato de servicio de caja entre un proveedor de servicios de pago (el banco) y sus clientes y sirve de medio de pago mediante el débito en la cuenta del ordenante y abono en la del beneficiario, tratándose en suma de un procedimiento financiero de movimiento de la moneda. Se trata de un medio de pago consistente en una orden dada al banco (banco emisor) por parte de un cliente (ordenante) a fin de que, con cargo a su cuenta, abone un determinado importe en otra cuenta del mismo o distinto banco (banco destinatario) abierta a nombre de un tercero (beneficiario) o del propio ordenante.

2.- Las transferencias se regulan, trasponiendo la Directiva 2007/64/CE del Parlamento Europeo y del Consejo Europeo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2005/65/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE, en la Ley 16/2009, de 13 de noviembre, de Servicios de Pago (LSP). La Directiva 2007/64/CE ha sido derogada por la Directiva UE 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento UE nº 1093/2010 y se deroga la Directiva 2007/64/CE.

3.- La LSP define la orden de pago como " toda instrucción cursada por un ordenante o beneficiario a su proveedor de servicios de pago por la que se solicite la ejecución de una operación de pago " (art. 2.16 LSP).

4.- Desde un punto de vista contractual toda transferencia constituye una forma de ejecución de obligaciones contractuales previamente asumidas, ejecución obligada cuando se dan las condiciones pactadas, de ordinario, que haya provisión de fondos. Es por ello que se entiende que la orden de transferencia constituye una declaración de voluntad o mandato (en el sentido del art. 254 CCo) en virtud del cual el banco asume la realización de transferencias por cuenta del cliente como parte del contrato de servicio de caja.



Data i hora 06/03/2025 13:13		Signat per Fernández González, María Jesús;	



5.- Dado el carácter negocial de la orden de pago, ésta puede pactarse que tenga lugar en cualquier forma, incluida la electrónica. En particular, el consentimiento a operaciones de pago por el usuario en el ámbito de la banca electrónica suponen que el cliente deba haber firmado un contrato de adhesión a los servicios de banca electrónica.

El art. 25.1 II LSP establece al respecto que "el ordenante y su proveedor de servicios de pago acordarán la forma en que se dará el consentimiento así como el procedimiento de notificación del mismo", negocio jurídico que determina que la transferencia se entienda autorizada por el ordenante de acuerdo con el mismo precepto de la LSP.

El consentimiento del ordenante se prestará, según el medio utilizado para prestar dicho consentimiento, mediante, o la firma de la autorización y orden de transferencia correspondiente, o verbalmente a través de la vía telefónica o a través de banca por internet o electrónica.

6.- Tanto en la banca telefónica como por internet, el proveedor de servicios de pago, o lo que es lo mismo, el banco emisor, debe implementar las medidas necesarias para asegurar la autenticación e identidad del ordenante a la hora de prestar su consentimiento.

Por ello y para su ejecución, el banco debe comprobar en todo caso la autenticidad de la orden y, salvo pacto en contrario, que existe saldo suficiente.

7.- De ordinario, para la realización de transferencias ordinarias con cargo a una cuenta vinculada es preciso que el cliente haya de autenticar la operación mediante la introducción de las claves previamente facilitadas por la entidad de crédito con la que contrata, con respecto a las cuales tendrá unos deberes de custodia.

8.- La falsedad de la transferencia (es decir, que el ordenante no sea el titular de la cuenta) es un riesgo a cargo del banco porque, en principio, el deudor sólo se libera pagando al verdadero acreedor por lo que si el banco cumple una orden falsa, habrá de reintegrar en la cuenta correspondientes las cantidades cargadas. Una excepción a esta distribución de riesgos se produce en el caso de que el titular haya creado o elevado el riesgo de falsificación de forma imputable en el caso concreto (STS 15 de julio de 1988).

9.- El art. 30 LSP que " cuando un usuario de servicios de pago niegue haber autorizado



Data i hora 06/03/2025 13:13		Signat per Fernández González, María Jesús;	



una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá a su proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud, y que no se vio afectada por un fallo técnico o cualquier otra deficiencia. 2. A los efectos de lo establecido en el apartado anterior, el registro por el proveedor de servicios de la utilización del instrumento de pago no bastará necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que este actuó de manera fraudulenta o incumplió deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 27".

Y en el art. 31 se dice que "en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante le devolverá de inmediato el importe de la operación no autorizada y, en su caso, restablecerá en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada. "

10.- Siendo Internet una red pública de comunicaciones, la seguridad de las operaciones bancarias precisa de soluciones tecnologías avanzadas a los efectos de garantizar tanto la autenticidad como la integridad y la confidencialidad de los datos.

Por estos motivos las entidades prestadoras del servicio de banca online deben dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones.

Consecuencia derivada de la omisión, insuficiencia o defectuoso funcionamiento de las adoptadas es que han de ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema.

11.- La banca electrónica está siendo objeto de transferencias no autorizadas por el cliente y que vienen anteceditas por el método delictivo conocido como phishing que constituye una modalidad específica de fraude informático que visualiza las deficiencias de seguridad del sistema informático de una entidad y que trae causa en el uso de las redes telemáticas.

De acuerdo con la Agencia Española de Protección de Datos (Resolución del Expediente Nº: E/00762/2004, DE 24 DE MAYO DE 2006): " el objetivo de los ataques de "phishing" es la obtención de forma engañosa y fraudulenta de los códigos de usuarios y



Data i hora 06/03/2025 13:13		Signat per Fernández González, María Jesús;	



contraseñas de clientes de Banca Electrónica, al objeto de realizar transferencias no autorizadas...Su operatoria comienza con la adquisición en internet de un "paquete de herramientas", que incluyen programas informáticos e información necesaria para realizar los ataques. Esta información incluye "listas de equipos comprometidos" que pueden ser utilizados bien para mandar correos electrónicos, bien para alojar páginas web falsificadas. Incluyen además "bases de datos de direcciones de correo electrónico". Una vez en posesión del paquete, se remiten los correos electrónicos con carácter indiscriminado (buscando contactar con clientes de la entidad financiera) informando de la necesidad de conectarse a una página web que parece pertenecer a la citada entidad y portar los códigos de acceso y contraseñas de clientes. Dicha página web se suele alojar en un equipo conectado a Internet cuya seguridad se haya [visto] comprometida", sin conocimiento de su usuario, y que se encuentra normalmente en un país distinto al de los destinatarios del ataque. De esta forma se constituye un "fichero de datos personales con códigos de usuarios y contraseñas de clientes" recabados de forma engañosa y fraudulenta, que se ubica normalmente en el mismo "equipo remoto comprometido" en el que se aloja la página web falsificada. Con los datos obtenidos se realizan transferencias a cuentas de colaboradores situados en España los cuales a su vez retiran el dinero en efectivo y tras descontar una comisión realizan transferencias monetarias internacionales mediante entidades especializadas ".

12.-La responsabilidad en estos supuestos no puede atribuirse directamente al supuesto ordenante de la transferencia por entenderse ésta autorizada al haberse realizado de acuerdo con los sistemas de autenticación del banco.

Los sistemas de autenticación se establecen por los proveedores de servicios de pago y si un banco no ha sido capaz de limitar el acceso al canal de banca electrónica no puede pretender que el presunto ordenante víctima de esta práctica fraudulenta sea el único responsable, pues es el banco quien tiene responsabilidad respecto del buen funcionamiento y la seguridad del mismo.

Dispone a tal efecto el art. 25,1º LSP que " 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".



Data i hora 06/03/2025 13:13	Signat per Fernández González, María Jesús;



Por tanto, en el caso de ordenes de pago y transferencias fraudulentas esta disposición supone que si la orden de pago o transferencia emitida por el cliente contiene una manifestación voluntad que actúa como causa del pago al tercero o la remisión de fondos al beneficiario, a "sensu contrario" puede afirmarse que sin dicha declaración de voluntad la operación de pago o transferencia de fondos se considerará no autorizada.

13.- Las medidas de seguridad no solamente están destinadas a proteger la seguridad de las órdenes de pago emitidas por los clientes sino que su eficacia exonera a las entidades de crédito de sus responsabilidades frente a las órdenes de pago no emitidas por sus clientes de tal forma que el incumplimiento de este específico deber de vigilancia da lugar a una responsabilidad por " culpa in vigilando" o responsabilidad objetiva por el mal funcionamiento de los servicios de banca electrónica.

En base a este fundamento la Sentencia de la Audiencia Provincial de Barcelona, Sección 11, de fecha 23 de julio 2015, declaró la responsabilidad de Barclays Bank, S.A. a pagar a una clienta la cantidad de 9.979 € por cargos y extracciones de efectivo no autorizados que tuvieron su origen en la introducción por los delincuentes de un mensaje fraudulento en la página oficial del banco a través del cual se canalizó la operación. Este mismo hecho, considerado una infracción de los deberes de vigilancia del banco, fue la causa por la que el Banco de Santander fue condenado por sentencia dictada por la Audiencia Provincial de Valencia, Sección 9 de fecha 23 de abril de 2013 a restituir a su cliente la cantidad de 42.500 €.

La Sentencia de la Audiencia Provincial de Barcelona (Sección Decimocuarta) de fecha 7 de marzo de 2013 condenó a la CAIXA DE ESTALVIS DE CATALUNYA (actualmente CATALUNYA BANK,S.A.) a devolver a una empresa víctima de " phishing" la cantidad de 32.099 € por cuanto la entidad bancaria no adoptó las medidas de seguridad adicionales previstas en las Condiciones Generales del contrato al haberse producido movimientos inusuales de fondos de la cuenta corriente y ser transferidos a cuentas sospechosas de su control por " muleros" que la entidad debió detectar. Asimismo la entidad bancaria permitió que se sobrepasara el limite de disposición diario de las cuentas pactado en el contrato.

La Sentencia de la Audiencia Provincial de Zaragoza de fecha 14 de mayo de 2013



Data i hora 06/03/2025 13:13	Signat per Fernández González, María Jesús;



condenó a BARCLAYS BANK a reintegrar 20.947 € al cliente víctima de phishing. La Sentencia señala que la Ley de Servicios de Pago expresa con claridad que, salvo una tardanza injustificada del usuario del servicio de banca electrónica en comunicar la irregularidad de las operaciones, será el banco quien deberá devolverle de inmediato el importe de la operación no autorizada y, en su caso, restablecerá la cuenta de pago en que haya adeudado dicho importe al estado que habría existido de no haberse efectuado la operación de pago no autorizada. Por ello y salvo actuación fraudulenta o negligencia grave del titular de la cuenta, la responsabilidad de la operación es del banco al que corresponde además probar el correcto funcionamiento del sistema informático.

La Sentencia de la Audiencia Provincial de Madrid de 4 de mayo de 2015 condenó a CAJAMAR a abonar a la víctima la cantidad de 17.390'35 €. En este caso la víctima facilitó sus claves y contraseñas a una página web clonada que simulaba ser la del banco. La sentencia razona que el artículo 31 de la Ley 16/09 de 13 de noviembre de Servicios de Pago establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago con inversión de la carga probatoria al presumirse la falta de autorización de la orden de pago o transferencia si el cliente lo niega.

En consecuencia, 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.

Dice al respecto el art. 32.2 LSP que " El ordenante soportará el total de las pérdidas que afronte como consecuencia de operaciones de pago no autorizadas que sean fruto de su actuación fraudulenta o del incumplimiento, deliberado o por negligencia grave, de una o varias de sus obligaciones con arreglo al artículo 27. "

CUARTO. - Valoración de la prueba

Según la regla general en materia probatoria que se contienen en el artículo 217 de la LEC es al demandante en los procesos civiles al que corresponde probar los hechos constitutivos de su demanda de los que se desprendan las consecuencias jurídicas que solicita, y al demandado aquellos otros que extingan, impidan o enerven los anteriores, teniendo en cuenta los principios de facilidad y disponibilidad probatoria con arreglo a los cuales y con independencia de cuál haya sido la parte que haya introducido un hecho como objeto de debate será la que más próxima se encuentre a un medio de conocimiento



Data i hora 06/03/2025 13:13	Signat per Fernández González, María Jesús;



de los hechos la que debe aportarla al proceso y en caso contrario correr con la falta de prueba que se pueda producir si terminado el juicio el hecho en cuestión quedara como dudoso.

Por lo que hace al contenido del art. 217 LEC, hemos de recordar que párrafo séptimo establece que "para la aplicación de lo dispuesto en los apartados anteriores de este artículo el Tribunal deberá tener presente la disponibilidad y facilidad probatoria que corresponde a cada una de las partes del litigio". Para valorar el alcance de esta norma al caso hemos de entender que la regla general aplicable a la prestación de servicios que no tenga adjetivada una especial peligrosidad o requiera de un particular cuidado ha de ser la regla general del art. 217 LEC, de manera que cuando se trata de prestaciones contractuales o no contractuales, del tenor del art. 1101 y 1902 Cc en relación al art. 217.2 LEC se desprenderá que corresponde al perjudicado demandante la carga de la prueba de la culpa del causante del daño demandado.

Ahora bien, no es así cuando " una disposición legal expresa" -art 217.6- imponga al demandado la carga de probar que hizo cuanto le era exigible para prevenir el daño; o cuando tal inversión de la carga de la prueba venga reclamada por los principios de " disponibilidad y facilidad probatoria " a los que se refiere el artículo 217.7 LEC, y ello sin perjuicio de que en aplicación de lo dispuesto en el artículo 386 LEC el tribunal pueda imputar a culpa del demandado el resultado dañoso acaecido cuando, por las especiales características de éste y conforme a una máxima de la experiencia, pertenezca a una categoría de resultados que típicamente se produzcan (sean realización de un riesgo creado) por impericia o negligencia, y no proporcione el demandado al tribunal una explicación causal de ese resultado dañoso que, como excepción a aquella máxima, excluya la culpa por su parte.

La lógica de la norma de acceso a la fuente de la prueba y facilidad probatoria en lo que hace a la implementación de medidas de seguridad en la prestación de un servicio que se da por las entidades de crédito a sus clientes a través de una oficina virtual que se desenvuelve en redes bien de internet, bien de comunicaciones móviles, se presenta como criterio más que de razonable atención al caso en el que la propia seguridad y debida reserva de la red se contraponen al acceso por parte de un tercero distinto al titular de la misma que asume poner en la red pública un conjunto de comunicaciones para permitir



Data i hora 06/03/2025 13:13	Signat per Fernández González, María Jesús;



operaciones bancarias que requiere de soluciones tecnológicas muy avanzadas que minimicen las amenazas contra la autenticidad, integridad y la confidencialidad de los datos que circulan a través de la red.

Por otro lado, el apartado 6 del artículo 217 LEC dispone que las normas contenidas en los apartados precedentes "se aplicarán siempre que una disposición legal expresa no distribuya con criterios especiales la carga de probar los hechos relevantes".

QUINTO. Decisión

Por todo ello, y en virtud de la prueba practicada, queda probado por la documental aportada que la Sra. [REDACTED] fue víctima de una estafa informática consistente en acceder a un enlace vía SMS con la apariencia de su entidad bancaria BBVA. Así la misma en sede judicial manifestó que cuando recibió el SMS vino en la misma línea de mensajes que cuando los recibe de su cuenta bancaria BBVA de modo que dio por hecho que era de la misma, atribuyéndole credibilidad a dicho mensaje, siendo por ello, el motivo por el que accedió a ese enlace. Tras ello, accedió directamente en la página oficial de BBVA, poniendo su código con DNI y clave de acceso como ha hecho siempre. Por su parte BBVA recibió un correo de que había existido un acceso de un dispositivo nuevo a su banca.

Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ejecutada, como sucede en el presente caso, la utilización del instrumento de pago registrada por el proveedor de servicios de pago no bastará necesariamente para demostrar que la operación de pago fue autorizada por el ordenante, ni que este actuó de manera fraudulenta o incumplió deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 56.

Para una mejor respuesta al motivo, y dado que la responsabilidad que se imputa a la entidad, derivada de la ejecución de una transferencia no autorizada por la titular de la cuenta de la cliente demandante realizada a través del sistema de banca online, lo es en tanto prestadora de servicios de pago a través del modelo de banca virtual puesta a disposición de su cliente, concretaremos el régimen legal y contractual en el que se desenvuelve la banca electrónica, cuáles son las obligaciones el prestador y del usuario conforme a la legislación aplicable, el significado jurídico de las órdenes de pago y el marco de responsabilidades que del mismo resulta y la jurisprudencia más señalada al respecto.



Data i hora 06/03/2025 13:13	Signat per Fernández González, María Jesús;



En conclusión, a juicio de este juzgador, queda probado la existencia de unas transferencias fraudulentas y que la responsabilidad del proveedor de los servicios de banca online, en este caso a BBVA, es de riesgo y consecuentemente, es por ley que a la entidad corresponde acreditar que la operación ordenada sí fue auténtica y que no estuvo afectada por un fallo técnico o por otra deficiencia como, por ejemplo, por un ataque informático de naturaleza fraudulenta al sistema bancario que hubiera permitido el acceso a las cuentas de sus clientes y disponer ilícitamente, de las mismas ordenando operaciones en detrimento de aquellos, prueba que no ha sido aportada por la demandada. 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, prueba que no ha sido aportada.

Por tanto, a falta de prueba hemos de afirmar que la entidad financiera no cumplió con los deberes de seguridad frente a los riesgos concretos que podrían derivarse del funcionamiento de su plataforma de banca digital, deberes que no se cumplen con la mera literalidad genérica de los contratos suscritos, ni con la firma o suscripción de los mismos, pues son de índole material y técnico que han de fluir a través de diversos niveles de seguridad que pueden constituir opciones de la entidad pero no frente a sus clientes usuarios del sistema en caso de fallo del mismo pues, en tales casos, constituye objetivamente la omisión de una medida esencial en tanto tienen por objeto garantizar la autenticación de la orden de pago como, por lo demás, se desprende del propio tener del contrato de banca próxima.

En consecuencia, es la prestadora de los servicios de pago quien tiene la obligación de facilitar un sistema de banca telemática segura, y no son sus clientes- usuarios los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, ni prevenir con un asesoramiento experto los mismos, no pudiendo en suma la parte obligada legalmente a ofrecer un modelo de servicio de caja que requiere de un especial nivel de seguridad, objetar que el usuario debía conocer aspectos técnicos tales como identificar una web como falsa -cuando no consta que fuera burda y por tanto, evidente de toda falsedad-.

Ninguna constancia tenemos, por lo demás, de que hubiera un uso indebido del sistema



Data i hora 06/03/2025 13:13		Signat per Fernández González, María Jesús;	



por parte del cliente ni que incumpliera con sus obligaciones básicas.

Si con carácter general el banco tiene la obligación, dice la STS 311/16, de 12 de mayo, de comprobar la veracidad de la firma del ordenante -lo que no deja de ser una obviedad-, tanto más relevante lo es el ámbito de la banca electrónica a través de cualquiera de los sistemas ya existentes y que prestan un elevado nivel de garantía como son las claves aleatorias remitidas por la entidad directamente al usuario para cada operación y la firma electrónica.

En conclusión, resulta evidente que en el caso hubo un incumplimiento contractual del banco al ejecutar una orden de pago sin comprobar su legitimidad, es decir, que provenía efectivamente del titular (o autorizado) de la cuenta, al no disponer de un sistema adecuado de seguridad que previniera tal tipo de órdenes fraudulentas ni adoptar medidas concretas y específicas en el caso cuando toma conocimiento de una situación operativa anormal que debió, cuando menos de forma puntual y excepcional, a verificar cualquiera orden que se diera en relación a las cuentas de la demandante.

De modo que se estima la demanda interpuesta.

TERCERO. – En cuanto a los intereses solicitados, procede conceder de conformidad con los artículos 1100, 1108 del Código Civil y 576 de la LEC, los intereses legales desde la fecha de reclamación extrajudicial.

CUARTO.- En cuanto a las costas, en virtud de lo dispuesto en el artículo 394 de la Ley de Enjuiciamiento Civil, al ser una resolución estimatoria se imponen a la parte demandada.

Vistos los preceptos legales citados y demás de general y pertinente aplicación al caso

FALLO

Que estimando la demanda interpuesta por Doña Ester Roqueta Mauri Procuradora de los Tribunales y actuando en nombre y representación de DOÑA [REDACTED] contra la entidad BANCO BILBAO VIZCAYA



Data i hora 06/03/2025 13:13		Signat per Fernández González, María Jesús;	
------------------------------------	--	---	--



ARGENTARIA S.A (en adelante BBVA), representada por el Procurador de los Tribunales Don Ignacio López Chocarro, y en consecuencia declaro el incumplimiento de las obligaciones de seguridad contenidas en el contrato de cuenta bancaria de la Sra. [REDACTED] junto con sus anexos de servicios de pago y contrato de Banca a Distancia, declarando la responsabilidad de la entidad BBVA en la incorrecta ejecución de las operaciones realizadas contra la cuenta del demandante y que se corresponden por importe total de CINCO MIL TRESCIENTOS SETENTA Y UN EURO CON OCHENTA Y NUEVE CÉNTIMOS (5.371,89.-€). Se condena a la entidad BBVA a abonar al actor la cantidad de 5.371,89.-€. junto con los intereses legales desde su reclamación extrajudicial; todo ello con especial condena en costas a la demandada.

Notifíquese la presente resolución a las partes, haciéndoles saber que contra la misma cabe recurso de APELACIÓN ante la Audiencia Provincial de Barcelona (artículo 455 L.E.C.). El recurso se interpondrá por medio de escrito presentado en este Juzgado en el plazo de VEINTE DÍAS hábiles contados desde el día siguiente de la notificación, limitado a citar la resolución apelada, con expresión de los pronunciamientos que impugna (artículo 458 L.E.C.).

Para la admisión a trámite del recurso previamente deberá efectuarse constitución de depósito en cuantía de 50 euros, debiendo ingresarlo en la cuenta de este Juzgado de Banco Santander nº 1761, indicando en las Observaciones del documento de ingreso que se trata de un recurso de apelación seguido del código '02', de conformidad en lo establecido en la Disposición adicional Decimoquinta de la L.O 6/1985 del Poder Judicial, salvo concurrencia de los supuestos de exclusión previstos en la misma (Ministerio Fiscal, Estado, Comunidades Autónomas, Entidades Locales y organismos autónomos dependientes de todos ellos) o beneficiarios de asistencia jurídica gratuita.

Así por ésta mi sentencia de la que se unirá testimonio literal para su unión a los presentes autos, juzgando en primera instancia la pronuncio, mando y firmo

E.-



Data i hora 06/03/2025 13:13	Signat per Fernández González, María Jesús;