Roj: **SAP B 7288/2025** - **ECLI:ES:APB:2025:7288**

Id Cendoj: **08019370042025100526**
Órgano: **Audiencia Provincial**
Sede: **Barcelona**
Sección: **4**
Fecha: **26/06/2025**
Nº de Recurso: **695/2024**
Nº de Resolución: **515/2025**
Procedimiento: **Recurso de apelación**
Ponente: **FRANCISCO DE PAULA PUIG BLANES**
Tipo de Resolución: **Sentencia**

Resoluciones del caso: **SJPII, Gavà, núm. 4, 12-02-2024 (proc. 940/2023),**
SAP B 7288/2025

Sección nº 04 de la Audiencia Provincial de Barcelona. Civil

Calle Roger de Flor, 62-68, Quarta planta - Barcelona - C.P.: 08013

TEL.: 935672160

FAX: 935672169

EMAIL:aps4.barcelona@xij.gencat.cat

N.I.G.: 0808942120238179343

Recurso de apelación 695/2024 -E

Materia: Juicio verbal

Órgano de origen:Sección Civil. Juzgado de Primera Instancia e Instrucción nº 4 de Gavà

Procedimiento de origen:Juicio verbal (250.2) (VRB) 940/2023

Entidad bancaria BANCO SANTANDER:

Para ingresos en caja. Concepto: 0650000012069524

Pagos por transferencia bancaria: IBAN ES55 0049 3569 9200 0500 1274.

Beneficiario: Sección nº 04 de la Audiencia Provincial de Barcelona. Civil

Concepto: 0650000012069524

Parte recurrente/Solicitante: Carlos José

Procurador/a: Jorge Bartolome Dobarro

Abogado/a: IÑIGO SERRANO BLANCO

Parte recurrida: BANCO BILBAO VIZCAYA ARGENTARIA, S.A.

Procurador/a: Carles Badia Martinez

Abogado/a:

SENTENCIA Nº 515/2025

Magistrado: Francisco de Paula Puig Blanes

Barcelona, 26 de junio de 2025

ANTECEDENTES DE HECHO

PRIMERO.-Se han recibido los autos de juicio verbal nº 940/2023 remitidos por Juzgado de Primera Instancia e Instrucción nº 4 de Gavà a fin de resolver el recurso de apelación interpuesto por el procurador Jorge Bartolomé Dobarro, en nombre y representación de Carlos José contra la sentencia dictada el 12.02.2024 y en el que consta como parte apelada Banco Bilbao Vizcaya Argentaria SA, representada por el procurador Carles Badía Martínez.

SEGUNDO.-El contenido del fallo de la sentencia contra la que se ha interpuesto el recurso es el siguiente:

"FALLO: Desestimo la demanda interpuesta por Carlos José contra Banco Bilbao Vizcaya Argentaria, S.A., absolviendo a la parte demandada de las pretensiones ejercitadas en su contra, con expresa condena en costas al demandante".

TERCERO.-El recurso se admitió y se tramitó conforme a la normativa procesal para este tipo de recursos.

Se señaló fecha para dictar resolución el 26.06.2025.

CUARTO.-En la tramitación de este procedimiento se han observado las normas procesales esenciales aplicables al caso.

Se designó ponente al magistrado Francisco de Paula Puig Blanes.

FUNDAMENTOS DE DERECHO

PRIMERO.- *Antecedentes y objeto del recurso*

Por parte del demandante Carlos José , se interpone recurso de apelación contra la sentencia por la cual fue desestimada la demanda por él presentada frente a Banco Bilbao Vizcaya Argentaria SA.

En la demanda se expone que el actor es titular de la cuenta bancaria en BBVA *** NUM000 , vinculada a una tarjeta de crédito con número *** NUM001 .

El 17.02.2023 el actor indica haber sido víctima del fraude conocido como "**phishing**" produciéndose hasta cuatro compras por él no autorizadas verificadas el 25.02.2023 por un importe de 3.649,50 €.

Ese día indica que recibió varios SMS que aparecían dentro la cadena de mensajes que habitualmente utiliza BBVA para enviarle información alertándole de una limitación de su cuenta por razones de seguridad, con un enlace para, supuestamente, actualizar su información. Este SMS se destaca que incluía la palabra BBVA y la URL era una "https"

Tal mensaje indica no haberlo visto hasta el momento en que recibió una llamada en su teléfono móvil desde aparentemente un número real y oficial de BBVA (944 16 15 96), en la que una mujer se hizo pasar por una gestora de BBVA facilitando datos personales del demandante (DNI, número de cuenta, domicilio...) que indica que tal persona había obtenido previamente de la banca online del actor. La estafadora se expone que indicó al actor que la entidad, por motivos de seguridad rutinaria, debía verificar su identidad, razón por la que previamente le habían remitido un SMS y por la que estaban realizando ahora esta llamada. Con la excusa de verificar la identidad y el dispositivo móvil, la supuesta gestora le solicitó que le proporcionase dos códigos que le iban a llegar a su dispositivo: el primero para -supuestamente- confirmar su tarjeta, y el segundo para confirmar que su dispositivo estaba enlazado correctamente con los servicios de Google y enlazarlo en caso de que no lo estuviera.

Gracias a dichos códigos, se sigue indicando en la demanda que la estafadora logró obtener los datos de la tarjeta (número, fecha de caducidad y CVV), y posteriormente vincularla a un nuevo dispositivo que obraba en su poder a través de Google Pay. Esta estafa se expone que fue tan perfecta que las operaciones no autorizadas se produjeron días después, hasta el punto de que el actor ni siquiera advirtió que dicha "gestión" telefónica de unos días atrás pudiera estar relacionada con las operaciones no autorizadas.

El actor indica haber llamado tras la llamada antes mencionada a la línea de BBVA y debido a que no funcionaba la banca online pues en ese momento aún no se había dispuesto de monto alguno (en concreto el 20.02.2023 cuando las disposiciones fraudulentas tuvieron lugar el 25.02.2023 desde el aeropuerto de Orly en París cuando el actor estaba en Madrid). Respecto de esta llamada a BBVI se indica que quien la atendió dijo que lo que se le indicó había sucedido sonaba a estafa, si bien nada se hizo al respecto mas allá de solucionar el problema de acceso a la banca online (se mantuvo la tarjeta vinculada a Google Pay).

Ninguna negligencia grave entiende el actor que en él concurre ante la operativa antes mencionada que es la del SMS spoofing y Spoofing telefónico, destacando que este último hace que sea prácticamente imposible

para la víctima desconfiar de la llamada que recibe. En concreto se pone de manifiesto que una persona que recibe primero un SMS de alerta y luego una llamada desde un número oficial de la entidad (refrendado por un nuevo SMS de la gestora que te está atendiendo) piensa que quien está al otro lado es el banco y no un estafador. Además, si los mensajes alertan de problemas de seguridad en la cuenta, ello provoca en la persona una urgencia y necesidad imperiosas de solucionar la situación, haciendo clic en el enlace que el banco -supuestamente- le indica y siguiendo las instrucciones que recibe de su banco para solucionarlo. Esta conducta entiende el actor que nunca podrá ser considerada como negligente, menos aún como negligencia grave, tal y como exige la ley.

Los estafadores se sigue exponiendo que enrolaron (vincularon) la tarjeta de crédito del actor a los servicios de Google Pay en un dispositivo que obraba en su poder, ajeno a cualquiera del actor. Desde ese momento indica que se puede pagar en los establecimientos con tarjeta utilizando el móvil y no la tarjeta física, lo que supone que una vez enrolada una tarjeta, se pueden realizar compras sin que se recoja del cliente ninguna muestra de consentimiento dado que basta la verificación de la compra por medios biométricos (huella dactilar o reconocimiento facial) en el dispositivo donde se ha vinculado la tarjeta (es decir, en estos casos, el propio del estafador) no produciéndose una doble autenticación, lo que entiende es una brecha de seguridad del banco entendiendo el demandante que en este caso existe además una responsabilidad de la entidad financiera en segundo plano que debería haber impedido la culminación de la estafa. En concreto se destaca que hubiera sido necesaria la comprobación del dispositivo desde el que se estaban realizando las operaciones, que no era el habitual del actor. A ello se añade la localización de los comercios donde se estaba realizando la operación (Orly, Francia) y la alteración clara de la "pauta de gasto" seguida, pues el actor destaca que nunca realiza operaciones por esos importes.

Tras exponer la denuncia y reclamación previa, solicitó el dictado de una sentencia por la que se condenase a la demandada a abonar al demandante la suma de 3.649,50 € más los intereses legales desde que tuvo lugar la operación no autorizada. Todo ello con condena en costas a la demandada.

Banco Bilbao Vizcaya Argentaria SA contestó y se opuso, alegando haber cumplido con todas sus obligaciones habiendo incurrido el actor en negligencia pues proporcionó sus datos personales y bancarios a un tercero, incumpliendo el deber de custodia de éstos.

Las operaciones objeto de la demanda se destaca que fueron realizadas a través de comercio electrónico seguro, siendo necesario introducir los datos de la tarjeta de crédito mediante la que se realizó la compra (los 16 dígitos, fecha de caducidad y CVV) y la vinculación de la tarjeta al método de pago Google Pay, lo que se destaca en la contestación que se realizó mediante un segundo factor de seguridad a través de un código OTP-SMS remitido al teléfono móvil del demandante (como método de firma de operaciones). Ello supone que para que las operaciones se pudiesen realizar de manera fraudulenta, fue necesario que el demandante: (i) revelara el usuario y pin de acceso a su banca online; (ii) revelara el CVV de la tarjeta bancaria o código OTP facilitado por BBVA para revelar el CVV y (iii) revelara el código OTP remitido por BBVA para confirmar la vinculación de su tarjeta bancaria a la aplicación Google Pay.

Todo ello considera que es una actuación constitutiva de negligencia grave por la que debe responder el actor, destacando 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: los datos de la tarjeta del cliente y el código OTP SMS. Igualmente se destaca que BBVA ha realizado diversas campañas de concienciación de todos sus clientes para evitar que sean víctimas de ciberataques.

Se detalla que en lo que es el mensaje del 17 de febrero de 2023, su apariencia es altamente sospechosa, pues es el único mensaje que no empieza por las siglas "BBVA", por lo que el actor podría haber detectado fácilmente que se trataba de un enlace fraudulento. Además, BBVA nunca manda a sus clientes enlaces por SMS ni pide ningún tipo de dato personal por este canal.

En cuanto a la llamada de una persona haciéndose pasar por un empleado de BBVA, informando al actor que por motivos de seguridad rutinaria debía verificar su identidad, para lo que le solicitó que le facilitara dos códigos que iba a recibir en su dispositivo: (i) el primero, supuestamente, para confirmar su tarjeta; y (ii) el segundo, para confirmar que su dispositivo se estaba enlazando correctamente con los servicios de Google; se destaca que fue atendida por el actor quien reveló los datos que se le solicitaban, lo que entiende BBVA es una negligencia grave por su parte. En concreto se pone de manifiesto que para asociar una tarjeta bancaria a una aplicación de pago como es Google Pay, es necesario además de acceder a la banca online, también el introducir todos los datos de la tarjeta bancaria, incluido el CVV que solamente aparece en el plástico físico de la tarjeta y posteriormente, autorizar la vinculación con el código OTP remitido por BBVA. Tras ello se hace llegar un correo electrónico de la vinculación de la tarjeta a la aplicación Google Pay a la dirección proporcionada por el actor.

En base a ello interesa que la demanda se vea desestimada con condena en costas al actor.

Tras la celebración el juicio el día 7.02.2024, se dictó sentencia que es desestimatoria de la demanda con condena en costas al demandante por entender que en su obrar concurrió negligencia grave. La misma analiza la prueba practicada y destaca que es difícil comprender que si en un principio no hizo caso el actor al mensaje SMS, luego atendiera a una llamada y facilitara dos claves privadas, es decir, información muy sensible. Gracias a ello destaca la sentencia que se procedió a primero ampliar el límite de disposición de la tarjeta, y después dar de alta el servicio de "Google Pay" a través del cual el delincuente realizó las compras por haber vinculado su teléfono móvil a la cuenta de tarjeta del actor, pudiendo realizar las compras con el dispositivo, sin necesidad de tarjeta física. Para ello el estafador accedió a la banca on line del actor y a todos los datos de su tarjeta (dígitos, fecha de caducidad, número de seguridad...), de modo que así pudo vincular la tarjeta del demandante a su móvil.

Se destaca que al actor se le enviaron dos alertas de seguridad por correo electrónico (documento nº 7 de la contestación) en las que el banco le advirtió que se habían vinculado los servicios de "Google Pay" a su tarjeta, indicándole que si no había sido él quien lo había vinculado y creyera que alguien pudiera haber accedido a sus datos, avisara inmediatamente. Estas alertas se señala en la sentencia que fueron desatendidas por el actor, pese a las campañas de seguridad a que hace referencia la demandada que considera son de conocimiento general y la existencia de fraudes bancarios mediante "phising" que son de pública noticia al aparecer continuamente en los medios de comunicación.

Carlos José recurre en apelación. En el mismo expone lo ya indicado en la demanda, destacando la apariencia de ser de BBVA quien hizo llegar las comunicaciones recibidas. También destaca la llamada por él verificada a BBVA antes de las disposiciones que no motivó ninguna actuación respecto de un posible fraude, ya que lo único que se hizo fue desbloquear la banca online, siendo prácticamente indetectable para un usuario medio el fraude tal y como expuso la propia policía.

Banco Bilbao Vizcaya Argentaria SA se opone al recurso entendiendo que es correcto el razonamiento de la sentencia con una exposición semejante a la ya expuesta en la contestación a la demanda considerando que la sentencia acierta en la valoración de la prueba que lleva a cabo, destacando que el actor reconoció en su demanda y en el acto del juicio que facilitó el código de seguridad a un tercero, lo que permitió al defraudador vincular la tarjeta bancaria del demandante al sistema de pago de Google Pay, no atendiendo a las alertas de seguridad que se le enviaron en el momento en el que se inició el registro de la tarjeta bancaria en el sistema de pago Google Pay informándole sobre esta circunstancia, e instándole a ponerse en contacto con la entidad para comunicar que él no había sido el que había iniciado este registro, si este fuera el caso.

SEGUNDO.- *Marco normativo*

Antes de entrar en el análisis de las concretas circunstancias del caso y de la valoración de la prueba que es lo que constituye el objeto del recurso de apelación presentado, se estima necesario concretar el marco normativo en que la misma opera teniendo en cuenta que las operaciones fraudulentas fundamento de la reclamación se llevaron a cabo en febrero de 2023.

A tal efecto cabe indicar que se parte de la existencia de una obligación de la entidad bancaria de conservar los fondos depositados, proceder solo a su entrega cuando se cumplan los requisitos que se establecen en el propio contrato y a favor de la persona de su titular.

Ello aparece recogido en el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, cuya finalidad ha sido trasponer al derecho español la Directiva de la 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) n.º 1093/2010 y se deroga la Directiva 2007/64/CE (Directiva PSD2)

El mismo, en su art. 42 regula las obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago y en el art. 45 el régimen de responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas, en concreto todo lo referente a la prueba de la autenticación y ejecución de las operaciones de pago.

La Directiva PSD2 y el Real Decreto Ley 19/2018 el 23 de noviembre tienen como objetivo conseguir que la seguridad y la comodidad vayan de la mano a la hora de llevar a cabo compras en el comercio electrónico, generando una mayor certidumbre y reduciendo los fraudes online.

Por medio de ellas se ha puesto en marcha la doble autentificación o la Strong Costumer Authentication (SCA). Con ello se introduce la «autentificación reforzada» del cliente para realizar pagos o acceder a su cuenta. Esto implica que, para cualquier tipo de pago se debe utilizar un sistema de doble autentificación.

El art 41 del Real Decreto Ley 19/2018 regula las obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas al indicar que:

"El usuario de servicios de pago habilitado para utilizar un instrumento de pago:

a) utilizará el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del instrumento de pago que deberán ser objetivas, no discriminatorias y proporcionadas y, en particular, en cuanto reciba un instrumento de pago, tomará todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas;

b) en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, lo notificará al proveedor de servicios de pago o a la entidad que este designe, sin demora indebida en cuanto tenga conocimiento de ello".

Por su parte el art 42 establece las obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago disponiendo que:

"1. El proveedor de servicios de pago emisor de un instrumento de pago:

a) Se cerciorará de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento, sin perjuicio de las obligaciones que incumben al usuario de servicios de pago con arreglo al artículo 41.

b) Se abstendrá de enviar instrumentos de pago que no hayan sido solicitados, salvo en caso de que deba sustituirse un instrumento de pago ya entregado al usuario de servicios de pago.

Esta sustitución podrá venir motivada por la incorporación al instrumento de pago de nuevas funcionalidades, no expresamente solicitadas por el usuario, siempre que en el contrato marco se hubiera previsto tal posibilidad y la sustitución se realice con carácter gratuito para el cliente.

c) Garantizará que en todo momento estén disponibles medios adecuados y gratuitos que permitan al usuario de servicios de pago efectuar una notificación en virtud del artículo 41.b), o solicitar un desbloqueo con arreglo a lo dispuesto en el artículo 40.4. A este respecto, el proveedor de servicios de pago facilitará, también gratuitamente, al usuario de dichos servicios, cuando éste se lo requiera, medios tales que le permitan demostrar que ha efectuado dicha comunicación, durante los 18 meses siguientes a la misma.

d) Ofrecerá al usuario de servicios de pago la posibilidad de efectuar una notificación en virtud del artículo 41.b), gratuitamente y cobrar, si acaso, únicamente los costes de sustitución directamente imputables al instrumento de pago.

e) Impedirá cualquier utilización del instrumento de pago una vez efectuada la notificación en virtud del artículo 41.b).

2. El proveedor de servicios de pago soportará los riesgos derivados del envío de un instrumento de pago al usuario de servicios de pago o del envío de cualesquiera elementos de seguridad personalizados del mismo".

El art 43 se refiere a la notificación y rectificación de operaciones de pago no autorizadas o ejecutadas incorrectamente señalando:

"1. El usuario de servicios de pago obtendrá la rectificación por parte del proveedor de servicios de pago de una operación de pago no autorizada o ejecutada incorrectamente únicamente si el usuario de servicios de pago se lo comunica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación, incluso las cubiertas por el artículo 60, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo.

Los plazos para la notificación establecidos en el párrafo primero no se aplicarán cuando el proveedor de servicios de pago no le haya proporcionado ni puesto a su disposición la información sobre la operación de pago con arreglo a lo establecido en el título II.

2. Cuando intervenga un proveedor de servicios de iniciación de pagos, el usuario de servicios de pago deberá obtener la rectificación del proveedor de servicios de pago gestor de cuenta en virtud del apartado 1, sin perjuicio de lo dispuesto en el artículo 45.2, y el artículo 60.1".

Respecto de la prueba de la autenticación y ejecución de las operaciones de pago señala el art 44:

"1. Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago.

Si el usuario de servicios de pago inicia la operación de pago a través de un proveedor de servicios de iniciación de pagos, corresponderá a éste demostrar que, dentro de su ámbito de competencia, la operación de pago fue autenticada y registrada con exactitud y no se vio afectada por un fallo técnico u otras deficiencias vinculadas al servicio de pago del que es responsable.

2. A los efectos de lo establecido en el apartado anterior, el registro por el proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, de la utilización del instrumento de pago no bastará, necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que éste ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 41.

3. Corresponderá al proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, probar que el usuario del servicio de pago cometió fraude o negligencia grave.

4. El proveedor de servicios de pago conservará la documentación y los registros que le permitan acreditar el cumplimiento de las obligaciones establecidas en este Título y sus disposiciones de desarrollo y las facilitará al usuario en el caso de que así le sea solicitado, durante, al menos, seis años. No obstante, el proveedor de servicios de pago conservará la documentación relativa al nacimiento, modificación y extinción de la relación jurídica que le une con cada usuario de servicios de pago al menos durante el periodo en que, a tenor de las normas sobre prescripción puedan resultarles conveniente para promover el ejercicio de sus derechos contractuales o sea posible que les llegue a ser exigido el cumplimiento de sus obligaciones contractuales.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, así como en otras disposiciones nacionales o de la Unión Europea aplicables".

La responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas se detalla en el art 45 según el que:

"1. Sin perjuicio del artículo 43 de este real decreto-ley, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada.

La fecha de valor del abono en la cuenta de pago del ordenante no será posterior a la fecha de adeudo del importe devuelto.

2. Cuando la operación de pago se inicie a través de un proveedor de servicios de iniciación de pagos, el proveedor de servicios de pago gestor de cuenta devolverá inmediatamente y, en cualquier caso, a más tardar al final del día hábil siguiente, el importe de la operación de pago no autorizada y, en su caso, restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada.

Si el responsable de la operación de pago no autorizada es el proveedor de servicios de iniciación de pagos, deberá resarcir de inmediato al proveedor de servicios de pago gestor de cuenta, a petición de este, por las pérdidas sufridas o las sumas abonadas para efectuar la devolución al ordenante, incluido el importe de la operación de pago no autorizada. De conformidad con el artículo 44.1, corresponderá al proveedor de servicios de iniciación de pagos demostrar que, dentro de su ámbito de competencia, la operación de pago fue autenticada y registrada con exactitud y no se vio afectada por un fallo técnico u otras deficiencias vinculadas al servicio de pago del que es responsable.

3. Podrán determinarse otras indemnizaciones económicas de conformidad con la normativa aplicable al contrato celebrado entre el ordenante y el proveedor de servicios de pago o el contrato celebrado entre el ordenante y el proveedor de servicios de iniciación de pagos, en su caso".

Por su parte la responsabilidad del ordenante en caso de operaciones de pago no autorizadas se regula en el art 46 que establece:

"1. No obstante lo dispuesto en el artículo 45, el ordenante podrá quedar obligado a soportar, hasta un máximo de 50 euros, 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, salvo que:

a) al ordenante no le resultara posible detectar la pérdida, la sustracción o la apropiación indebida de un instrumento de pago antes de un pago, salvo cuando el propio ordenante haya actuado fraudulentamente, o

b) la pérdida se debiera a la acción o inacción de empleados o de cualquier agente, sucursal o entidad de un proveedor de servicios de pago al que se hayan externalizado actividades.

El ordenante soportará todas las pérdidas derivadas de operaciones de pago no autorizadas si el ordenante ha incurrido en tales pérdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 41. En esos casos, no será de aplicación el importe máximo contemplado en el párrafo primero.

En todo caso, el ordenante quedará exento de toda responsabilidad en caso de sustracción, extravío o apropiación indebida de un instrumento de pago cuando las operaciones se hayan efectuado de forma no presencial utilizando únicamente los datos de pago impresos en el propio instrumento, siempre que no se haya producido fraude o negligencia grave por su parte en el cumplimiento de sus obligaciones de custodia del instrumento de pago y las credenciales de seguridad y haya notificado dicha circunstancia sin demora.

2. Si el proveedor de servicios de pago del ordenante no exige autenticación reforzada de cliente, el ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta. En el supuesto de que el beneficiario o el proveedor de servicios de pago del beneficiario no acepten la autenticación reforzada del cliente, deberán reembolsar el importe del perjuicio financiero causado al proveedor de servicios de pago del ordenante.

3. Salvo en caso de actuación fraudulenta, el ordenante no soportará consecuencia económica alguna por la utilización, con posterioridad a la notificación a que se refiere el artículo 41.b), de un instrumento de pago extraviado o sustraído.

4. Si el proveedor de servicios de pago no tiene disponibles medios adecuados para que pueda notificarse en todo momento el extravío o la sustracción de un instrumento de pago, según lo dispuesto en el artículo 42.1.c), el ordenante no será responsable de las consecuencias económicas que se deriven de la utilización de dicho instrumento de pago, salvo en caso de que haya actuado de manera fraudulenta".

Este régimen, parte de la realidad conforme a la que la tradicional forma de acceder a los servicios online a través de unas credenciales basadas exclusivamente en usuario y contraseña se han mostrado insuficientes, de ahí que la seguridad que proporciona la utilización de un único factor de autenticación haya sido considerada como demasiado limitada y se haya establecido normativamente la necesidad de introducir una autenticación fuerte, es decir, una autenticación basada en al menos dos factores de los siguientes: algo que se sabe, algo que se tiene y algo que se es.

Con este objetivo la Directiva PSD2 introduce el requisito de implementar la autenticación reforzada de la clientela (SCA), basada en un segundo factor de autenticación que proporciona una manera robusta de identificación.

Este segundo sistema de autenticación puede ser un certificado digital, un dispositivo criptográfico que genera un número único (One-Time-Password u OTP) para cada persona usuaria del tamaño de un llavero, una línea de telefonía para recibir SMS o una app en un dispositivo móvil. La tarjeta de coordenadas no forma parte de este conjunto de opciones ya que la Autoridad Bancaria Europea en su Dictamen de Noviembre de 2019, donde se identifican los mecanismos que son válidos, las descartó, así como los detalles impresos en la propia tarjeta tipo CVV.

En el caso de las OTP, al realizar la operación financiera se envía al número de teléfono móvil, que previamente se ha dado de alta en la cuenta, un mensaje SMS con un código (OTP) que se debe introducir en la web o app donde se esté realizando la compra o en el servicio bancario en el que se esté efectuando una transacción. De esta manera, el doble factor se consigue al conocer los datos bancarios y disponer del número de teléfono móvil donde recibir la contraseña de un solo uso.

Respecto de la operativa de este régimen, la **STS 571/2025** de 9 de abril de 2025 (ECLI:ES:TS:2025:1671) establece:

"6.- Con arreglo a la normativa comunitaria y nacional aplicable y a la jurisprudencia comunitaria recaída en interpretación de la regulación de la que trae causa la primera, podemos concluir:

1.º El usuario de servicios de pago debe adoptar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas y, en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, ha de notificarlo al proveedor de servicios de pago de manera inmediata, tan pronto tenga conocimiento de ello.

2.º En caso de que se produzca una operación de pago no autorizada o ejecutada incorrectamente, si el usuario de servicios de pago se lo comunica sin demora injustificada, el proveedor debe proceder a su rectificación y reintegrar el importe de inmediato, salvo que tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España.

3.º Cuando un usuario niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, incumbe al proveedor la carga de demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago.

4.º El mero hecho del registro por el proveedor de la utilización del instrumento de pago no bastará, necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que éste ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones, correspondiendo al proveedor la prueba de que el usuario del servicio de pago cometió fraude o negligencia grave.

En suma, la responsabilidad del proveedor de los servicios de pago, en los casos de operaciones no autorizadas o ejecutadas incorrectamente, tiene carácter cuasi objetivo, en el doble sentido de que, primero, notificada la existencia de una operación no autorizada o ejecutada incorrectamente, el proveedor debe responder salvo que acredite la existencia de fraude; y, segundo, cuando el usuario niegue haber autorizado la operación o alegue que ésta se ejecutó incorrectamente, corresponde al proveedor acreditar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio, sin que el simple registro de la operación baste para demostrar que fue autorizada ni que el usuario ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave.

Profundizando en este último punto, la expresión «operaciones no autorizadas» incluye aquellas que se han iniciado con las claves de usuario y contraseña del usuario -necesarias para acceder al sistema de banca digital- y confirmado mediante la inserción del SMS enviado por el propio sistema al dispositivo móvil facilitado por el usuario, siempre que éste niegue haberlas autorizado, en cuyo caso el banco deberá acreditar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio que presta.

A este respecto, la mención «deficiencia del servicio» no significa error o fallo del sistema informático o electrónico -posibilidad que estaría prevista en el concepto de «fallo técnico»-, sino que abarca cualquier falta de diligencia o mala praxis en la prestación del servicio, en el entendimiento de que el grado de diligencia exigible al proveedor de los servicios de pago no es el propio del buen padre de familia, sino que la naturaleza de la actividad y los riesgos que entraña el servicio que se presta, sobre todo en una relación empresario/consumidor, obliga a elevar el nivel de diligencia a un plano superior, como es el del ordenado y experto comerciante.

Lógicamente, las buenas prácticas pasan por adoptar las medidas de seguridad necesarias para garantizar el correcto funcionamiento del sistema de servicios de pago, entre las cuales destacan las orientadas a detectar de forma automática la concurrencia de indicios de que puede tratarse de una operación anómala y generar una alerta o un bloqueo temporal (v.gr. reiteración de transferencias sin solución de continuidad, horario en que se producen, importe de las mismas, destinatarios, antecedentes en el uso de la cuenta...), o las dirigidas a incrementar el control y vigilancia cuando se han recibido noticias o alertas de un posible aumento del riesgo".

De lo que se acaba de exponer (y a los efectos de las presentes actuaciones), cabe indicar que, para excluir la responsabilidad de la entidad financiera, es necesario que se acredite la existencia de negligencia grave por parte del cliente, respecto de la que el Considerando 72 de la Directiva (UE) 2015/2366 (es la que se traspone por medio del Real Decreto-ley 19/2018 a que se viene haciendo referencia) indica:

"(72) A la hora de evaluar la posible negligencia o la negligencia grave del usuario de servicios de pago, deben tomarse en consideración todas las circunstancias. Las pruebas de una presunta negligencia, y el grado de esta, deben evaluarse con arreglo a la normativa nacional. No obstante, si el concepto de negligencia supone un incumplimiento del deber de diligencia, la negligencia grave tiene que significar algo más que la mera negligencia, lo que entraña una conducta caracterizada por un grado significativo de falta de diligencia (...)"

La carga de la prueba de concurrir negligencia grave por parte del usuario incumbe a la entidad financiera tal y como se declara en la antes referida **STS 571/2025** de 9 de abril de 2025 (ECLI:ES:TS:2025:1671) que indica al efecto:

" (...) en el marco de esta regulación, el consentimiento no se entiende prestado por el solo hecho de que la operación de pago se haya realizado mediante la utilización de las claves personales, sino que es necesario que provenga del usuario o, en caso de que éste niegue su intervención, que se acredite fraude, incumplimiento deliberado o, al menos, negligencia grave por parte del usuario, cuya prueba recae sobre la entidad bancaria ...

... En otras palabras, el que la entidad bancaria acredite que la operación fue autenticada, registrada con exactitud y contabilizada, no es suficiente para eximirle de responsabilidad. Ha de probar que la operación no resultó afectada por un fallo técnico u otra deficiencia del servicio prestado, y, dado que el cliente niega que la operación fuera consentida, que no hubo por parte de este último fraude, incumplimiento deliberado o negligencia grave (...)"

Tras esta exposición ya es procedente analizar las concretas circunstancias del caso, lo que se verifica en el siguiente fundamento de esta sentencia.

TERCERO.- *Concurrencia o no de negligencia grave por parte del cliente.*

La sentencia de primera instancia la entiende concurrente, valoración con la que difiere el apelante (y con la que está conforme la apelada) en base a los términos que se han expuesto en el primer fundamento de derecho de esta sentencia que no se reproducen de nuevo a fin de evitar reiteraciones.

Para dar respuesta a lo planteado se deben analizar las concretas circunstancias del caso que vienen referidas a una actuación por parte de terceros que por lo que obra en autos parece que intentaron acceder sin éxito a la banca electrónica del demandante/apelante, si bien en paralelo verificaron toda una operativa para dar de alta el servicio de pago Google Pay a cargo de una tarjeta del actor/apelante que lograron emparejar/enrolar a un dispositivo que ellos controlaban y desde que el que hicieron las compras físicas en el aeropuerto de Orly (París) el 25.02.2023. Los justificantes de estas operaciones obran en autos siendo su importe de 3.649,50 € que es el aquí reclamado.

En cuanto a como se pudo ello verificar y si en el obrar del Sr. Carlos José pudo concurrir negligencia grave (que es lo que excluiría la responsabilidad de la demandada/apelada como se viene indicando), cabe señalar que el actor/apelante indicó ser un usuario frecuente de la banca electrónica (a diario dijo hacer uso de la misma).

A tal efecto se han aportado unos mensajes SMS, siendo el primero de ellos de 17.02.2023 a las 17:15 horas y recibido de una fuente que el Sr. Carlos José tenía en su teléfono móvil como BBVA. En este mensaje se hace referencia a una limitación temporal por razones de seguridad de la tarjeta indicándose un enlace para reactivarla señalando la necesidad de actualizar la información en un enlace identificado como https://bilbao-login.digital/BBVA0217/test. El Sr Carlos José señaló no haber recibido con anterioridad ningún mensaje parecido, llamándole el mismo la atención, lo que justificó que no pulsara/no entrase en el enlace.

No obstante lo anterior, un tiempo después (a las 17:52 horas) dijo que se produjo una comunicación con una operadora denominada Josefina enviándose un mensaje con un código para visualizar la tarjeta (en este caso y a diferencia del anterior el mensaje comenzaba con las siglas BBVA). Ello mismo sucedió con otros dos mensajes. El primero era referido a la clave para el registro en Google Pay de la tarjeta * NUM001 en un dispositivo-tableta (se indicaba que se podía obtener más información en un número de teléfono). El segundo (que también comenzaba con las siglas BBVA) indicaba que la tarjeta había sido activada en Google Pay en un dispositivo Smartphone-tableta.

Estos datos reconoció en el acto del juicio el demandante que los proporcionó, señalando que la llamada de la que se identificó como Josefina tenía por objeto un bloqueo de cuenta que ésta le indicó haberse producido si bien el Sr. Carlos José no comprobó la existencia de este bloqueo de cuenta.

En cuanto al número desde el que se hacía la llamada indicó que no sabía que era de BBVA (previamente había dicho que sí seguramente por las averiguaciones posteriores).

También dijo no haber leído los SMS referentes a la activación del Google Pay (dijo no saber lo que era), si bien las claves - códigos OTP (y todos los datos referentes a su tarjeta) señaló haberlos proporcionado a la persona de quien recibió la llamada.

Igualmente consta que se le hizo llegar en ese momento un correo electrónico (documento nº 7 de la contestación) en el que se indicaba que había iniciado el registro de la tarjeta * NUM001 en Google Pay señalándose de forma expresa lo siguiente: "Si no has sido tú y crees que alguien puede haber accedido a tu cuenta o a los datos de tu tarjeta, es importante que nos lo notifiques a través del 900 10 28 01".

Tras ello consta una comunicación el 20.02.2023 que mantuvo el Sr. Carlos José con un gestor de BBVA a quien expuso la llamada anterior y que desde ese momento no podía entrar en la aplicación de banca electrónica. El gestor indicó que no le constaba tal llamada indicando a ello el demandante/apelante que tenía los mensajes señalando el gestor de BBVA que le daba la sensación de que era un fraude. Tras exponer el contenido de los mensajes (con mención de la tarjeta) el gestor explicó la forma como proceder para reactivar la banca electrónica constatando que no le habían quitado nada (así lo destacó el Sr. Carlos José ya que pudo acceder a la banca electrónica empleando las claves de su mujer).

Hasta ese momento no se había producido ninguna operativa fraudulenta que tuvo lugar el 25.02.2023.

Todas estas operaciones fueron objeto de análisis en el informe de trazabilidad elaborado por BBVA. En el acto del juicio se tomó declaración como testigo perito a Gervasio , responsable del servicio de gestión de fraude de BBVA quien destacó que el cliente proporcionó a los terceros los datos de su tarjeta, incluyendo el CVV que solamente está en el soporte físico de la misma y que de cara a la consulta electrónica requiere de una primera validación con firma OTP (se trataría del primer SMS) siendo necesario además para emparejar la tarjeta a un dispositivo (móvil-tableta) otra firma OTP (sería el segundo SMS). Una vez producido ello señaló que la compra se puede hacer en la tienda física simplemente acercando el dispositivo con el que está emparejada al lector. En el informe se detalla todo ello.

De lo que se acaba de exponer se constata que el demandante/apelante verificó toda una actuación inadecuada, pues pese a sospechar de un primer SMS no habitual, dio los datos de su tarjeta a una persona que le llamó por teléfono (con un número que en ese momento desconocía de quien fuere) y permitió mediante dos firmas OTP que su tarjeta se vinculara por el sistema Google Pay a un dispositivo que le era ajeno, no leyendo ni el proceso de vinculación que expresamente mencionaba a esta pasarela de pagos, como tampoco el correo electrónico a ello referente en que se le advertía de que de no haber sido él lo comunicare.

No obstante lo anterior, y este es el aspecto que debe ser destacado y que viene referido a las concretas circunstancias del caso aquí analizado, ya que no todos los supuestos son iguales, antes de que se verificare el uso fraudulento (ello se produjo el 25.02.2023), en concreto el 20.02.2023, el Sr. Carlos José mantuvo una conversación con un gestor de BBVA con ocasión de habérsele bloqueado la banca electrónica, exponiendo lo sucedido. Este gestor comprobó que la llamada que dijo haber recibido el 17.02.2023 desde BBVA no era tal, pues no constaba en sus registros, indicando que le daba la sensación de que era un fraude. Lo que no hizo este gestor, pese a la advertencia del Sr. Carlos José y la consideración del propio gestor de poderse tratar de un fraude, es comprobar las operaciones llevadas a cabo el 17.02.2017 y en especial en referencia a la tarjeta que expresamente había sido mencionadas por el Sr. Carlos José , que la misma se vinculó en esa fecha a un dispositivo y a la plataforma de pagos Google Pay.

Esta actuación se estima que debió haberla verificado el gestor con quien contactó el Sr. Carlos José dados los términos de lo por él expuesto. De así haberse procedido, habría sido posible deshacer la vinculación de la tarjeta a un dispositivo y su alta en la plataforma de pagos Google Pay. Ello hubiera permitido que las operaciones fraudulentas no se habrían producido.

Esta situación constata que, si bien por una parte la actuación del Sr. Carlos José no fue la idónea dados los datos por él proporcionados y la no verificación de los mensajes que recibía de BBVA y su contenido; ello no obstante antes de producirse la sustracción contactó con BBVA y el gestor que le atendió no procedió en la forma que cabe entender habría sido la idónea cual era la de repasar todo lo llevado a cabo el 17.02.2023 respecto de la tarjeta (y en concreto lo referente a la vinculación de la misma con un dispositivo móvil).

Este obrar incorrecto de la demandada/apelada (por medio de su gestor), se considera que desactivó la actuación incorrecta del demandante/apelante (diferente hubiera sido el caso de haberse hecho las disposiciones antes de esta llamada ya que en tal caso nada podría haber hecho BBVA que ofreció los mecanismos de autenticación legalmente previstos).

Ante esta realidad y las concretas circunstancias que concurren en este caso que se acaban de exponer, se considera que la causa de exclusión de responsabilidad de BBVA referente a la negligencia grave del cliente, quedó desvirtuada a resultas de la llamada del 20.02.2023 hecha por el cliente a BBVA, lo que supone que los presupuestos de la acción ejercitada se estimen concurrentes.

Ello comporta que se deba estimar el recurso de apelación y con ello la demanda (incluidos intereses con fundamento en el art. 1.108 CC) condenando en costas a la demandada (art. 394 LEC), dado que desde un primer momento era conocedora de la conversación a que se viene haciendo referencia de 20.02.2023 que es la que determina que no concurran dudas de hecho o derecho en este caso.

CUARTO.-Por imperativo del art.398 LEC, al verse estimado el presente recurso de apelación no procede la condena en las costas del mismo a ninguno de los litigantes.

Vistos los preceptos legales citados y demás de general aplicación

FALLO

Con **estimación del recurso de apelación**interpuesto por el procurador Jorge Bartolomé Dobarro, en nombre y representación de Carlos José contra la sentencia dictada en fecha 12.02.2024 por el/la Magistrado/a-Juez/a del Juzgado de Primera Instancia e Instrucción nº 4 de Gavà en los autos de juicio verbal nº 940/2023 debo

REVOCAR Y REVOCO dicha resolución y en su virtud se estima la demanda presentada por el procurador Jorge Bartolomé Dobarro, en nombre y representación de Carlos José frente a Banco Bilbao Vizcaya Argentaria SA y en su virtud se condena a la demandada a abonar al demandante la suma de 3.649,50 € más los intereses legales desde que tuvieron lugar las operaciones no autorizadas. Todo ello con condena en las costas de primera instancia a la parte demandada.

En cuanto a las costas del presente recurso no procede su condena a ninguna de las partes.

Devuélvase al apelante, en su caso, el depósito que pudiera haber constituido de conformidad con lo establecido en la Disposición Adicional 15ª de la LOPJ.

Contra esta sentencia no procede recurso alguno.

Notifíquese la presente sentencia y remítase testimonio de la misma, junto con los autos principales al Juzgado de procedencia, para su ejecución y cumplimiento.

Así por ésta mi sentencia, lo acuerdo, mando y firmo.

El Magistrado:

Puede consultar el estado de su expediente en el área privada de seujudicial.gencat.cat

Los interesados quedan informados de que sus datos personales han sido incorporados al fichero de asuntos de esta Oficina Judicial, donde se conservarán con carácter de confidencial, bajo la salvaguarda y responsabilidad de la misma, dónde serán tratados con la máxima diligencia.

Quedan informados de que los datos contenidos en estos documentos son reservados o confidenciales y que el tratamiento que pueda hacerse de los mismos, queda sometido a la legalidad vigente.

Los datos personales que las partes conozcan a través del proceso deberán ser tratados por éstas de conformidad con la normativa general de protección de datos. Esta obligación incumbe a los profesionales que representan y asisten a las partes, así como a cualquier otro que intervenga en el procedimiento.

El uso ilegítimo de los mismos, podrá dar lugar a las responsabilidades establecidas legalmente.

En relación con el tratamiento de datos con fines jurisdiccionales, los derechos de información, acceso, rectificación, supresión, oposición y limitación se tramitarán conforme a las normas que resulten de aplicación en el proceso en que los datos fueron recabados. Estos derechos deberán ejercitarse ante el órgano judicial u oficina judicial en el que se tramita el procedimiento, y las peticiones deberán resolverse por quien tenga la competencia atribuida en la normativa orgánica y procesal.

Todo ello conforme a lo previsto en el Reglamento EU 2016/679 del Parlamento Europeo y del Consejo, en la Ley Orgánica 3/2018, de 6 de diciembre, de protección de datos personales y garantía de los derechos digitales y en el Capítulo I Bis, del Título III del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.