

**JUZGADO DE 1ª INSTANCIA Nº 96 DE MADRID**

Calle Rosario Pino 5 , Planta 10 - 28020

Tfno: 914936408,6409

Fax: 915351357

juzpriminstancia096madrid@madrid.org

42020306

NIG: 28.079.00.2-2024/0216121

Procedimiento: Juicio Verbal [REDACTED]/2024

Materia: Acción declarativa

2 MAR

Demandante: D./Dña. [REDACTED]

PROCURADOR D./Dña. [REDACTED]

Demandado: [REDACTED]

PROCURADOR D./Dña. [REDACTED]

SENTENCIA Nº [REDACTED]/2025**JUEZ/MAGISTRADO- JUEZ:** D./Dña. ELISA MARTI VILACHE**Lugar:** Madrid**Fecha:** dieciocho de noviembre de dos mil veinticinco

Vistos por mí, Elisa Marti Vilache, Magistrada-juez titular del Juzgado de 1ª instancia nº 96 de Madrid, los presentes autos de procedimiento verbal nº [REDACTED]/24, seguidos ante este Juzgado a instancia de Dª [REDACTED], representada por la Procuradora Sra. [REDACTED], y defendida por la Letrada Sra. Martínez Fernández, contra [REDACTED], representados por la Procuradora Sra. [REDACTED], y defendidos por el Letrado Sr. [REDACTED], en reclamación de 2.786 €.

ANTECEDENTES DE HECHO

PRIMERO.- Procedente del turno de reparto fue incoada en este Juzgado demanda de Juicio verbal sobre reclamación de cantidad, promovida por Dª [REDACTED], contra [REDACTED], alegando los hechos y fundamentos de derecho que estimó aplicables al caso, y terminó suplicando al Juzgado se dictara sentencia conforme a sus pedimentos.

SEGUNDO. - Admitida a trámite la demanda, se dio traslado a las demandadas para su contestación, lo que verificó [REDACTED] SA, siendo declarado [REDACTED] en rebeldía procesal.

Habiéndose solicitado celebración de vista, tuvo lugar el día señalado, quedando a continuación los autos conclusos para sentencia. En la vista, la actora manifestó que las diligencias penales están archivadas, por lo que no hay motivo para suspender el procedimiento por prejudicialidad penal.

TERCERO.- En la tramitación del presente procedimiento se han observado las prescripciones legales, incluido el plazo para dictar sentencia.



FUNDAMENTOS DE DERECHO

PRIMERO.- Pretensión de la demanda

Se ejercita por la actora acción de reclamación de la cantidad de 2.786 €, basando su demanda en los hechos siguientes: la demandante es cliente de la entidad demandada desde el año 2001, habiendo operado siempre con normalidad. El día 20 de julio de 2023, [REDACTED] sufrió una caída en sus servicios de banca online de forma generalizada y que imposibilitó que la demandante realizara una transferencia a través de Bizum esa mañana, pudiendo realizar la transferencia a través de Bizum ya durante la tarde, cuando los servicios bancarios online se habían recuperado.

El día 21 de julio, a las 13 horas, la demandante recibió diversos SMS o mensajes de texto bajo un identificador de [REDACTED] y de los que, por la app de Mensajes del teléfono móvil no permitía la identificación del número, con un identificador de enlace bajo especial seguridad https que dirigían a una web que redirecciona a un enlace fraudulento, indicando que se había registrado un nuevo dispositivo móvil y la necesidad de verificar las credenciales. La demandante intentó realizar la identificación en la web fraudulenta (https://[REDACTED]) con un aspecto externo absolutamente igual al de la web real de [REDACTED]. A las 13:04 la demandante recibió una llamada fraudulenta del número [REDACTED], identificándose el interlocutor como personal de Banca Electrónica de [REDACTED] e indicándole que se habían realizado una serie de cargos y compras en Marsella. La demandante indicó a su vez que no había ordenado dichos cargos y que no sabía quién los estaba realizando. La demandante facilitó todos los códigos que le iban enviando por SMS desde otro número de teléfono a partir de las 13:09, con el objetivo de, siempre según el interlocutor fraudulento, revertir los cargos que se estaban haciendo en su cuenta.

Por primera vez a las 13:31, llamó al número que figura como de Banca Telefónica de [REDACTED] en la que tras comprobar su identidad le indicaron que habían sustraído de su cuenta a través de transferencias a través de Bizum y pagos con tarjeta de crédito una cantidad que posteriormente se supo que alcanzó los 2.806 € en menos de media hora, además de realizar un Smart Cash (un instrumento comercial de [REDACTED] del que la demandante nunca había hecho uso), de forma fraudulenta por 500 €.

Posteriormente (a las 14:42), recibió una llamada de María, gestora de su oficina de [REDACTED], desde el teléfono [REDACTED], para preguntarle si estaba realizando una transferencia bancaria a través de Bizum por importe de 1000 €, indicando la demandante que no los había hecho ella en ningún caso.

La actora interpuso denuncia ante la Policía por estos hechos, y también reclamó extrajudicialmente a [REDACTED] quien se negó a indemnizar a la demandante, devolviéndole solo 20 €.

SEGUNDO.- Contestación de [REDACTED]

La demandada se opone a la demanda, alegando, en primer lugar, falta de legitimación pasiva de [REDACTED], por no haber intervenido en los hechos. En



segundo lugar, no existe negligencia de la demandada, por haber accedido la actora a una app de [REDACTED] claramente fraudulenta, y autorizó los pagos. En tercer lugar, [REDACTED] ha actuado de conformidad con la normativa vigente al respecto, advirtiendo periódicamente de las ciberestafas.

TERCERO.- Rebeldía de [REDACTED] y legitimación pasiva

Es doctrina procesal consolidada la de que la rebeldía del demandado no implica allanamiento ni "ficta confessio", solución que encuentra cobertura legal en el artículo 496 de la vigente Ley de Enjuiciamiento Civil, por lo que la parte actora debe probar la realidad de los hechos conforme al artículo 217 de la Ley de Enjuiciamiento Civil, pero sí le impide oponer excepciones, procesales o de fondo, derivadas de hechos impositivos o extintivos, limitando la cuestión litigiosa a lo que resulte de la pretensión formulada en la demanda, cuya eficacia, total o parcial, está condicionada a la prueba de los hechos que le sirven de fundamento.

En cuanto a la alegación de falta de legitimación pasiva de [REDACTED] alegada por la codemandada, hay que partir de que la legitimación "ad causam" (STS de 28 de febrero de 2002 ó 31 de mayo de 2006) consiste en una posición o condición objetiva con la relación material objeto del pleito que determina una aptitud para actuar en el mismo como parte; se trata de una cualidad de la persona para hallarse en la posición que fundamenta jurídicamente el reconocimiento de la pretensión que se trata de ejercitar, teniendo, por tanto, legitimación a los efectos del art. 10 de la LEC, quien afirme hallarse en dicha relación con el objeto del proceso, lo que obliga al Tribunal a entrar en el conocimiento del litigio y a dictar una sentencia de fondo, sea ésta favorable o desfavorable al sujeto legitimado.

De la documental obrante en autos ha quedado acreditado que la actora es cliente de [REDACTED] (doc. 6 de la demanda), que hizo su reclamación a [REDACTED] y fue contestada por ésta (docs. 5 y 8 de la demanda), y que la actora no tiene por qué conocer la relación interna en cuanto al contrato de tarjeta, que hay entre [REDACTED] y [REDACTED], pues la demandante contrata con [REDACTED] y es ésta quien, en su caso, debe responder de una mala praxis por parte de sus filiales, tengan la denominación que tengan, porque lo cierto es que forman parte del mismo grupo empresarial, y no pueden desvincularse a la hora de responder frente a terceros. Por ello se rechaza la falta de legitimación pasiva de [REDACTED]

CUARTO.- Resultado de la prueba

En primer lugar, respecto a la prejudicialidad penal que se alegó en su día, no consta la existencia de procedimiento penal abierto, por lo que no procede acceder a la suspensión del presente procedimiento.

En cuanto al fondo del asunto, la normativa al respecto viene constituida por el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que, en su art. 46.1, señala que: *"Artículo 46. Responsabilidad del ordenante en caso de operaciones de pago no autorizadas. 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.”

Por su parte, el art. 41 de dicha norma establece 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”.

El art. 43 del RD Ley de Servicios de pago dispone que “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”.

El art. 44 del mismo cuerpo legal señala que “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.”*

La sentencia de la Audiencia Provincial de Cáceres, de 18 de diciembre de 2023, en un supuesto similar, señala que “no cabe apreciar en el comportamiento seguido por el demandante conducta alguna que pueda ser calificada como negligente, de gravedad y entidad suficiente para hacerle responsable del quebranto sufrido, pese a haber facilitado sus datos personales y/o claves de seguridad a un supuesto empleado de la entidad tras recibir un falso SMS del banco”.

Como destaca la sentencia, “aun cuando pudiera calificarse el comportamiento del actor como no diligente, para que sea él quien soporte las consecuencias del fraude o de la estafa sufrida es preciso apreciar negligencia, y además que dicha negligencia sea grave, lo que no es el caso, pues el método fraudulento empleado es de una complejidad y grado de perfección difícilmente detectable por un cliente de sus características”.

Considera que “es preciso ser un experto en la materia para poder detectar que la comunicación obedecía a una estafa o fraude”. Recuerda que “la llamada telefónica que recibió del supuesto empleado del banco (alertándole de un “movimiento sospechoso” en su cuenta por haberse realizado una transferencia de 4.999 euros negada por el cliente y que el interlocutor se ofreció a “anular”), no proviene de un teléfono oficial de comunicación del banco, sino de un tercero que, a través de una aplicación móvil o desde una web, logra ficcionar tal acción, cambiando el número del remitente a la hora de verlo reflejado en la pantalla del cliente que recibe la llamada, a lo que se suma el posterior SMS recibido, que imita tanto el diseño como la terminología utilizada por su entidad bancaria, por lo que generada la confianza en el usuario de que se trata de su entidad bancaria, no hay capacidad real para detectar el engaño o fraude”.

Por último, explica la Sala que “a lo expuesto no es obstáculo lo que afirma el banco sobre la inexistencia de brechas de seguridad, pues, aunque el sistema del banco pueda ser genéricamente seguro, no lo fue en este caso concreto”. Subraya en este punto que “al asumir el banco que el actor fue objeto de un fraude mediante la modalidad conocida como “Caller ID Spoofing”, evidencia que no había implementado todos las medidas o mecanismos necesarios para proteger a su cliente de ataques realizados por ciberdelincuentes, lo que comporta un incumplimiento de su obligación de garantizar la seguridad de los servicios de pago efectuados a través de internet o dispositivos móviles”.

Pese a lo manifestado por dicho testigo, lógicamente exculpatario del Banco, el Tribunal Supremo, en la reciente sentencia de 9 de abril de 2025, señala que “los operadores de servicio de pago, como son las entidades, tienen la obligación de elevar su nivel de diligencia y buenas prácticas, lo que pasa por incrementar la seguridad y el control para detectar estas operaciones fraudulentas. Y les insta a desarrollar herramientas que detecten operaciones anómalas, como de altos importes



o realizadas de madrugada, para poder bloquear los fraudes. Dice dicha sentencia que "Los avances de la tecnología actual hacen relativamente sencillo diseñar sistemas o aplicaciones informáticas idóneas para detectar ciertas anomalías en la prestación de los servicios de pago. [...] A este respecto, sería suficiente un control automático de determinados factores, como el número y sucesión de operaciones, el intervalo en que se ejecutan, la hora del día, su importe o entidades de destino, para generar un aviso que reforzara los requisitos de confirmación y minimizara los posibles riesgos", indica la sentencia. Según el fallo, "no puede considerarse como normal e irrelevante que una persona que jamás efectúa operaciones de madrugada, de repente, proceda a llevar a cabo hasta diecisiete operaciones seguidas y por un importe tan elevado".

A este respecto, el Supremo concluye que "el hecho de que un tercero accediera a las claves del cliente no supone una negligencia grave por su parte y que la filtración o el conocimiento de las claves no sea imputable a la entidad bancaria "tampoco la libera de obligación de responder ni traslada al usuario la obligación de soportar las pérdidas, ya que el proveedor de servicios de pago, además de demostrar que el servicio se prestó correctamente (lo que no sucedió), debía acreditar la concurrencia de fraude o incumplimiento deliberado o gravemente negligente por parte del usuario...De conformidad con el art. 44 RDL, en caso de que el usuario niegue haber autorizado una operación de pago ya autorizada, el cumplimiento de las obligaciones relativas a la autenticación, registro y contabilización de la operación de pago fue autenticada, no exime de responsabilidad al proveedor de servicio, sino que deberá acreditar además que la operación no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado, sin que mero registro de la utilización del instrumento de pago baste 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.

En el supuesto enjuiciado fallan ambos presupuestos. En primer lugar, la entidad demandada debía probar, no solo que la operación no se vio afectada por un fallo técnico, sino que no se ha producido una prestación defectuosa del servicio, cuestión que ya ha sido objeto de análisis con ocasión de examinar el anterior motivo, concluyendo que el servicio no se prestó correctamente.

Asimismo, el hecho de que la filtración o el conocimiento de las claves por el tercero no sea imputable a la entidad bancaria tampoco la libera de obligación de responder ni traslada al usuario la obligación de soportar las pérdidas, ya que el proveedor de servicios de pago, además de demostrar que el servicio se prestó correctamente -lo que no sucedió-, debía acreditar la concurrencia de fraude o incumplimiento deliberado o gravemente negligente por parte del usuario, y, en relación con este extremo, las sentencias de instancia y de apelación coinciden en que no se ha probado fraude ni incumplimiento doloso o por negligencia grave de las obligaciones que correspondían al demandante, y, en concreto, las de tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas y de notificar al proveedor de servicios de pago la utilización no autorizada del instrumento de pago, tan pronto tuvo conocimiento de ello, lo que así hizo, participando las tentativas de acceso a su cuenta con una antelación de tres semanas.

Obsérvese que, contra lo que mantiene por la recurrente, el que un tercero hubiera podido acceder a las claves de acceso a la banca digital del demandante no supone per se que haya incurrido en negligencia alguna, pudiendo existir múltiples explicaciones,



muchas de las cuales resultan difícilmente atribuibles a título de negligencia, y menos aún, de negligencia grave”.

Aplicando dicha doctrina al supuesto de autos, se llega a la conclusión de que en modo alguno puede hablarse de negligencia grave de la actora en este caso concreto, cuando confió en que tanto el SMS como la llamada telefónica que recibió, y que se relatan en la denuncia interpuesta ante la Policía (doc. 4 de la demanda) procedían de los canales habituales del Banco, por lo que no puede decirse que incurriera en la negligencia grave que exige la jurisprudencia, pues tal como se produjo el engaño, el cliente no pudo imaginar que quien estaba al otro lado de la línea no fuera un empleado del banco.

Las anteriores consideraciones conducen a la estimación íntegra de la demanda.

QUINTO.- Solidaridad

La solidaridad de las obligaciones, interpretando el art. 1137 del Código Civil a sensu contrario, implica, en el caso de solidaridad de deudores, como el presente, que frente al acreedor cada uno de los deudores debe prestar, íntegramente, las cosas objeto de la obligación, dado que las cantidades impuestas en sentencia generan la llamada por la jurisprudencia solidaridad impropia, por lo que procede la condena solidaria a ambos demandados.

SEXTO.- Intereses

En materia de intereses, son de aplicación los arts. 1.100, 1.108 del Código Civil, 576 de la LEC, y concordantes, desde la fecha de la interpelación judicial.

SÉPTIMO.- Costas

Las costas de este juicio deberán ser soportadas por la parte demandada, según se desprende de la aplicación del artículo 394.1 de la Ley de Enjuiciamiento Civil para los supuestos de estimación íntegra de la demanda.

Vistos los artículos citados y demás de general y pertinente aplicación, en nombre de S.M. el Rey,

FALLO

Que **ESTIMANDO ÍNTEGRAMENTE** la demanda interpuesta por la Procuradora Sra. [REDACTED], en nombre y representación de D^a [REDACTED] frente a [REDACTED], representados por la Procuradora Sra. [REDACTED], condeno a las demandadas a abonar a la actora la suma de 2.786 €, más intereses legales desde de la fecha de la interpelación judicial, imponiendo a la parte demandada las costas causadas en este juicio.

Así por esta mi Sentencia, lo pronuncio, mando y firmo.





Regístrese la presente sentencia mediante certificación literal en el sistema procesal electrónico por inserción de la misma con firma electrónica avanzada, y quede la misma depositada en el Libro que a tal efecto se genera automáticamente por el sistema de gestión procesal electrónico.

Esta sentencia es firme.

El/la Juez/Magistrado/a Juez

La difusión del texto de esta resolución a partes no interesadas en el proceso en el que ha sido dictada sólo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contuvieran y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda.

Los datos personales incluidos en esta resolución no podrán ser cedidos, ni comunicados con fines contrarios a las leyes.



La autenticidad de este documento se puede comprobar en www.madrid.org/cove mediante el siguiente código seguro de verificación: **130301252460001003047**



Este documento es una copia auténtica del documento Sentencia Juicio Verbal firmado electrónicamente por ELISA MARTI VILACHE