

Roj: SAP S 1267/2023 - **ECLI:**ES:APS:2023:1267
Órgano: Audiencia Provincial
Sede: Santander
Sección: 2
Nº de Recurso: 58/2022
Nº de Resolución: 500/2023
Fecha de Resolución: 10/10/2023
Procedimiento: Recurso de apelación. Juicio ordinario
Ponente: LAURA CUEVAS RAMOS
Tipo de Resolución: Sentencia

Encabezamiento

SENTENCIA nº 000500/2023

Ilmo. Sr. Presidente.

D. José Arsuaga Cortázar.

Ilmos. Srs. Magistrados.

D. Miguel Fernández Díez..

D^a. Laura Cuevas Ramos.

=====

En la Ciudad de Santander, a diez de octubre de dos mil veintitrés.

Esta *Sección Segunda de la Ilma. Audiencia Provincial de Cantabria ha visto en grado de apelación los presentes Autos de juicio ordinario, núm. 16 de 2021 , Rollo de Sala núm. 58 de 2022, procedentes del Juzgado de Primera Instancia e Instrucción núm. 4 de Torrelavega, seguidos a instancia de Eugenia y de Fátima contra Unicaja Banco S.A.*

En esta segunda instancia ha sido parte apelante Unicaja Banco S.A, representado por la Procuradora Sra. Quirós Martínez y defendido por el Letrado Sr.; García López y apelada Eugenia y Fátima, representadas por la Procuradora Sra. Saez Bereciartu y defendidas por el Letrado Sr. Sainz de la Maza

Es ponente de esta resolución la Ilma. Sra. Magistrada Dña. Laura Cuevas Ramos.

ANTECEDENTES DE HECHO

PRIMERO: Por el Ilmo. Sr. Magistrado-Juez del Juzgado de Primera Instancia e Instrucción núm. 4 de Torrelavega, y en los autos ya referenciados, se dictó en fecha Sentencia cuya parte dispositiva es del tenor literal siguiente: *"FALLO: Que estimando íntegramente la demanda, debo declarar y declaro el incumplimiento por parte de LIBERBANK, S.A. de las obligaciones legales impuestas tanto por la relación contractual como por las exigencias del Real decreto-Ley 19/2018, de 23 de*

noviembre, de Servicios de Pago. Y debo condenar y condeno a LIBERBANK, S.A. a abonar:

1.º A D. ª Eugenia la cantidad de 23.240 euros más

intereses legales desde la interposición de la demanda.

2.º A D. ª Fátima la cantidad de

2.000 euros más intereses legales desde la interposición de la demanda. Se imponen las costas a la parte demandada."

SEGUNDO: Contra dicha Sentencia la representación de la parte interpuso recurso de apelación, que se tuvo por interpuesto en tiempo y forma, y dado traslado del mismo a la contraparte, que se opuso al recurso, se elevaron las actuaciones a esta Ilma. Audiencia Provincial, en que se ha deliberado y fallado el recurso en el día señalado.

TERCERO: En la tramitación del recurso se han observado las prescripciones legales salvo el plazo de resolución en razón al número de recursos pendientes y su orden.

FUNDAMENTOS DE DERECHO

Se admiten los de la Sentencia de instancia, en tanto no sean contradictorios con los que a continuación se establecen; y

PRIMERO. Resumen de antecedentes y planteamiento del recurso.

1. Por Dña. Eugenia y Dña. Fátima se presentó demanda de juicio ordinario contra LIBERBANK (hoy UNICAJA), al amparo del Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, exigiéndole responsabilidad por las distintas operaciones realizadas sin su autorización - reintegros en cajero con tarjetas de crédito, traspaso entre cuentas, trasferencias, descarga de saldo de tarjeta prepago y aumento de límite disponible en dos tarjetas de crédito - después de que recibir un mensaje en su móvil, aparentemente de LIBERBANK, que le solicitaba pinchar un enlace para confirmar una trasferencia a favor de Dña. Eugenia en agosto de 2020. Cifra el perjuicio sufrido en 23.240 €; en el caso de Dña. Eugenia y 2.000 €; en el caso de Dña. Fátima.

2. La demandada contesta a la demanda reconociendo que las demandantes han sido víctima de un fraude, y oponiéndose con solicitud de desestimación de la demanda, con el de que todas las operaciones fueron debidamente autenticadas con PIN o clave OTP, imputando el fraude sufrido a la propia actuación de Dña. Eugenia que pinchó el enlace recibido sin pensar, a pesar de que en el contrato digital firmado en el año 2004 se le advertía expresamente de que LIBERBANK no solicitaría código de usuario, PIN, tarjeta de coordenadas por ninguna vía, pinchó el primer enlace y autenticó las operaciones a que se referían otros tres mensajes recibidos el día 27 de agosto de 2020, en el cual se le pedía introdujese una clave que se le enviaba para confirmar operaciones que estaba realizando.

3. La *sentencia del juzgado de primera instancia nº 4 de Torrelavega de fecha 29 de octubre de 2021* estima la demanda, condenando a la entidad a abonar a Dña. Eugenia la suma de 23.240 €; y a Dña. Fátima la suma de 2.000 €, más

los intereses legales, con imposición de costas a la demandada.

Razona la juez de instancia sus conclusiones y decisión en que (i), en el supuesto del uso de medios de pago en línea son las entidades bancarias las que ha de asumir el riesgo en caso de que no pueda determinarse qué ha ocurrido exactamente, y que basta que un usuario informe que él no ha realizado la operación para que la entidad tenga que demostrar que sí la ha realizado; (ii) no debe entrarse a valorar en este caso si hubo fraude o negligencia por parte de Dña. Eugenia, que no consta realizase las operaciones ni que incurriera en negligencia, siendo víctima de " phishing " que es engaño suficiente para provocar una transferencia de dinero; (iii) según la directiva de Servicios de Pago DSP2, las órdenes de pago deben realizarse mediante una autenticación reforzada, además de la clave personal que autoriza la operación, y además, conforme al Reglamento Delegado (UE) 2018/389, los bancos deben disponer de mecanismos de supervisión que les permitan detectar operaciones que por su cuantía o por ser varias en un periodo breve, obedecen a phishing, pudiendo bloquear la operación u ponerse en contacto con el usuario para verificar que sea él quien realmente está realizando la operación y (iv) en este caso no las operaciones realizadas no pueden entenderse autorizadas ya que la ordenante no ha prestado su consentimiento.

4. La demandada interpone recurso de apelación alegando error en la valoración de la prueba e infracción de los *arts. 41.1 , 44.1 y 44.3 del RD 19/2018, de 23 de noviembre* , que concreta en que fue la propia actora quien, tras recibir un mensaje fraudulento, aparentemente enviado por LIBERBANK, pinchó el enlace que se le facilitaba para recibir una transferencia, actuando así de modo negligente, puesto que, no recibió un solo mensaje sino cuatro claramente burdos porque la dirección del remitente que figuraba no se parece nada a la de LIBERBANK, y cuyo contenido no podría hacer caer en un error a cualquier persona que obrase con una mínima precaución y diligencia, propiciando así el fraude.

5. La actora formula expresa oposición al recurso de la comunidad, interesando su íntegra desestimación con imposición de costas a la apelante.

SEGUNDO. - Phising. Modalidad de fraude informático.

Se centra el presente procedimiento en un supuesto de fraude informático conocido como " phishing ", denominación que proviene del inglés "fishing" (pesca) y que es resultado de la contracción de la frase "password harvesting fishing" (cosecha y pesca de contraseñas).

De acuerdo con la definición dada por la Agencia Española de Protección de Datos, en resolución de fecha 24 de mayo d 2006 "el objetivo de los ataques de " phishing " es la obtención de forma engañosa y fraudulenta de los códigos de usuarios y 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."

Habitualmente se hace efectiva a través del envío de correos electrónicos o SMS engañosos, en los que se imita el lenguaje, formato e imagen de las entidades bancarias o financieras suplantando su identidad y, solicitando los datos personales de las víctimas alegando diferentes motivos. Los métodos empleados para este tipo fraude son diversos (clonación de tarjetas, skimming o carcasa superpuesta, el pharming o introducirse en un servidor a través de hackers, capturando claves, contraseñas, etc.) y no necesariamente llega a descubrirse en todos los supuestos el concreto método empleado; si bien es evidente, en cualquier caso, que se trata de una operación no autorizada por el titular de la cuenta corriente, el cual ve sustraído sus datos y claves de una manera fraudulenta, a través de medios técnicos.

TERCERO. -Hechos y circunstancias relevantes para la decisión del Tribunal.

1. En el mes de agosto de 2020 la actora Dña. Eugenia, recibió en su teléfono móvil un mensaje, aparentemente de la entidad LIBERBANK, en el que se le requería pulsar un enlace para recibir una transferencia a su favor. Dña. Eugenia, distraída por estar ocupada en su negocio, pinchó el enlace.

2.- En la tarde del 27 de agosto, tras experimentar un problema en la tarjeta de su teléfono móvil, que hubo de ser sustituida, recibió en 6 minutos tres mensajes que le requerían la introducción de un código para las operaciones que, según se le informaba, estaba realizando. La actora se puso en contacto telefónico con la demandada tras recibir los mensajes.

3.- Entre los días 27 y 28 de agosto de 2020, con las credenciales, claves y OTPs que el Banco enviaba, en las cuentas de las que es titular Dña. Eugenia se realizaron 25 reintegros, aumento de disponible a favor de su tarjeta VISA y una orden de traspaso, en su tarjeta VISA se realizó un traspaso de crédito y desde su tarjeta prepago una descarga de saldo a una de sus cuentas, ascendiendo el importe total de lo dispuesto a 25.740 €;. Desde la cuenta de que es titular Dña. Fátima, se realizó una orden de transferencia por importe de 2.000 €;.

4.- En fecha 30 de septiembre de 2020 LIBERBANK contestó a la reclamación de las actoras informándoles de que todas las operaciones realizadas habían sido autenticadas con las correspondientes claves y credenciales, siendo registradas y contabilizadas sin dar ningún tipo de fallo técnico, y le adjuntaban los comprobantes. Igualmente, rechazaban atender su reclamación. La comunicación decía lo siguiente: "no se discute que el origen de las operaciones se encuentre en una actuación fraudulenta" y "que parece acreditado que el defraudador obtuvo previamente los datos necesarios para la comisión de fraude a través de " phishing ", una técnica que consiste en el envío de un correo electrónico o un SMS por parte del Ciberdelincuente, a un usuario simulando ser una entidad legítima, con el objetivo de robarle información privada, realizarle un cargo económico o infectar su dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico,

consiguiendo de este modo el control de las OTP' s, enviadas al teléfono y dejándole sin servicio telefónico". Y, a continuación, trasladaba a las usuarias la recomendación de una serie de medidas de seguridad que debían adoptar para evitar este tipo de fraudes.

CUARTO. - Marco normativo y jurisprudencial.

Las obligaciones exigibles a las entidades bancarias como proveedoras de pago, en relación con los instrumentos de y sistemas de pago que ponen a disposición de sus clientes en cuanto a la garantía del buen funcionamiento de los mismos preservándolos frente al fraude, se recoge, en el ámbito de la legislación nacional, en el Real Decreto Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en adelante, LSP), aprobado para transponer, entre otras, la *directiva UE 2015/2366* en materia de servicios de - la denominada "PSD2" -, complementada por el Reglamento Delegado (UE) 2018/396 de la Comisión de 27 de noviembre de 2017, con el objetivo de mejorar la protección de los usuarios de los servicios de pago, obligando a las entidades a usar la autenticación reforzada incrementando la protección de los clientes frente a sus pagos.

La norma contiene la siguiente regulación:

Artículo 41. Obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas. 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.

Artículo 42. Obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago. 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.

Artículo 43. Notificación y rectificación de operaciones de pago no autorizadas o ejecutadas incorrectamente. 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.

Artículo 44. Prueba de la autenticación y ejecución de las operaciones de pago. 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.

Artículo 45. Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas. 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.

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. 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".

En cuanto a la más reciente jurisprudencia en la materia, señala la **SAP de Madrid, Sec. 10ª, de 13 de enero de 2023**

"Sobre la jurisprudencia aplicable, la sentencia de la Audiencia Provincial de Madrid, sección 11ª, de fecha 28 de febrero de 2022 , hace un compendio de la misma y se menciona la sentencia de la Audiencia Provincial de Madrid (Sección 9ª) núm. 178/2015 de 4 mayo de 2015 (JUR 201551311), que se pronuncia en el sentido siguiente: ..." Salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante (Art. 32), la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la carga de la prueba de que la orden de pago " no se vio afectada por un fallo técnico o cualquier otra deficiencia" (art 30).

La responsabilidad contemplada en esta Ley es cuasi-objetiva, es decir, se trata de una responsabilidad de la entidad que presta servicios de pago que sólo permite exonerarse mediante la prueba de la culpa grave del ordenante.

Esta interpretación efectuada de la Ley 16/2009, de 13 de noviembre, de servicios de pago, es absolutamente acorde no sólo con la literalidad de la norma, sino con el espíritu y finalidad de la misma (ex. art. 3 CC), en función de lo previsto, por tanto, en los artículos 30 y 32 de la mentada Ley 16/2009, de 13 de noviembre , de servicios de pago.

En base a todos estos criterios la sentencia de la Audiencia Provincial de Madrid Sección 9ª 178/2015 de 4 mayo de 2015 (JUR 201551311), condena a la entidad al reembolso de las cantidades, señalando que la Ley de los Servicios de Pago establece un sistema de responsabilidad cuasi objetiva para la entidad financiera, previendo que en caso de disposiciones fraudulentas el proveedor de servicios de pago deberá devolver de inmediato el importe de la operación no autorizada, (art. 31), quedando exento de esta obligación solo en el caso de que la operación no autorizada sea fruto de la actuación fraudulenta del cliente o del incumplimiento, deliberado o por negligencia grave, de una o varias de sus obligaciones (art. 32). Además, la Ley prevé una inversión de la carga de la prueba en tanto es el proveedor de los servicios, quien debe probar que la operación fue debidamente autenticada, cuando el usuario de los servicios lo niegue (art. 30)" .

El carácter de cuasiobjetiva de la responsabilidad de la entidad bancaria, que sólo puede exonerarse si acredita la concurrencia de actividad fraudulenta o culpa grave del cliente, ha sido indicado también, entre otras, por las sentencias de las AAPP de Badajoz, de 7 de febrero de 2023 de la Rioja , de 17 de febrero de 2023 y Alicante, de 12 de marzo de 2018 .

Especial mención merece la última sentencia citada, de la **Audiencia Provincial de Alicante (632/2018, de 12 de marzo** , como referencia por su claridad y extensión sobre la cuestión de la carga de la prueba, señalando:

"..... es que no es cierto que la carga de la prueba sobre la implementación de medidas de seguridad adecuadas, suficientes, eficientes y actuales al nivel de riesgo

modalidades de ataques informáticos en la red bancaria de banca online lo sea a cargo del usuario del sistema, pues el marco de responsabilidad establecido para el caso de operaciones de pagos hechos por proveedores de servicios no autorizadas o ejecutadas incorrectamente, es el de la cuasi-objetividad tal cual se desprende de la regulación específica sobre la materia -a la que seguidamente aludiremos-, sin perjuicio del régimen general de la carga de la prueba. Tres son las razones que abogan la contrariedad del argumento del recurrente, a saber, el contenido del precepto que se dice infringido - art 217 LEC - y, por llamada del mismo, la legislación de consumo y la legislación específica de servicios de pago... 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 la culpa al demandado del 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 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". (...) En este caso, la disposición expresa existe, tanto en el ámbito de consumo, como en la regulación de los servicios de pago".

Señala la configuración de la específica modalidad de responsabilidad que asume el prestador y, con ello, la variación del régimen legal del sistema del gravamen probatorio y, concluye, en relación con la carga de la prueba, que la responsabilidad del proveedor de los servicios de banca online 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. Y recuerda que, siendo Internet una red pública de comunicaciones, la seguridad de las operaciones bancarias precisa de soluciones tecnológicas avanzadas a los efectos de garantizar tanto la autenticidad como la integridad y la confidencialidad de los datos motivo por el que las entidades prestadoras del servicio de banca online deben dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones, siendo consecuencia de dicha omisión, deficiencia o defectuoso funcionamiento que deban asumir la responsabilidad por los fallos de seguridad del sistema.

Según lo expuesto, salvo la actuación fraudulenta, incumplimiento deliberado o negligencia grave del usuario, la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la carga de la prueba de que la orden de pago " no se vio afectada por un fallo técnico o cualquier otra deficiencia". La interpretación efectuada por la Juzgadora ad quem de la Ley 16/2009, de 13 de noviembre, de servicios de pago, es acorde no sólo con la literalidad de la norma, sino con el espíritu y finalidad de la misma (ex. *art. 3 CC*), lo que obligó a la determinación de la responsabilidad de la entidad bancaria a pesar de sus afirmaciones sobre la implementación de un modelo seguro de banca online, lo que no implica que el sistema fuera genéricamente seguro, pero como es evidente no lo fue en el presente caso. Tampoco sirve de excusa a la entidad apelada la inclusión de avisos en web y otros medios de la entidad sobre el comportamiento seguro que en el uso de la plataforma había de tener el cliente, sino que la entidad bancaria debe dotar a la banca electrónica de las medidas de seguridad necesarias para prevenir unos tipos de fraude ya muy extendidos y que, como lo prueba el supuesto que nos ocupa, siguen produciéndose por falta de una medida adecuadas por la entidades bancarias, que ponen a disposición de sus clientes la banca online y la contratación electrónica como dotados de una seguridad que no garantizan.

Y la **SAP de Madrid, Sec. 20ª de 20 de mayo de 2022** , argumenta sobre este mecanismo de fraude informático.

*" TERCERO.- La aplicación de la normativa anteriormente indicada al caso presente, nos lleva a estimar la impugnación formulada por el demandante en cuanto, no discutiéndose la forma en que se llegaron a materializar las 6 retiradas de efectivo por un importe total de 6.000 € ; , iniciadas por una actuación fraudulenta de tercero, no cabe apreciar en el demandante un comportamiento negligente de la gravedad y entidad para con base en el mismo hacerle responsable, ni siquiera de la primera disposición de efectivo realizada con la tarjeta usada de manera fraudulenta por un tercero. Como se indica en la Directiva 2015/2036 la negligencia que le hace responder al cliente, es la que se deriva de una conducta caracterizada por un grado significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que ha sido inducido por un delincuente profesional. Tampoco puede calificarse como grave dicho comportamiento conforme a la normativa del código civil, pues siendo exigible al demandante la diligencia que exija la naturaleza de la obligación y correspondan a las circunstancias de las personas, tiempo y lugar (art. 1.104 del cc), el método fraudulento empleado - **phishing** - es de una complejidad y grado de perfección, difícilmente detectable por un cliente de las características del demandante, sin que la forma en que se denominaba al Banco en el SMS recibido o el error gramatical al emplear la palabra "lo" en lugar de "le", sean errores de entidad suficiente para detectar con base en ellos el fraude de que estaba siendo objeto. En esas circunstancias, era preciso ser un experto en la materia para poder detectar que la comunicación obedecía a una estafa o fraude. Es cierto que dicho comportamiento no puede considerarse diligente, pero para hacer soportar al cliente las consecuencias,*

aún parciales como se concluye en la sentencia apelada, es preciso apreciar en él una negligencia y que además sea grave, que en la normativa europea antes referida se equipara a la comisión de un fraude, actuación en la que no se ha acreditado incurriese el demandante, por el hecho de haber pinchado el link que se le ofrecía y facilitar los datos y clave de la tarjeta

*CUARTO .- Por el contrario, la responsabilidad exigida a la entidad demandada, como proveedora del servicio, es la que se deriva de la naturaleza de tal prestación y de la posición contractual en la que se encuentran las partes, lo que le obliga a adoptar una serie de medidas de seguridad y dotarse de mecanismos de supervisión que permitieran detectar operaciones fraudulentas en la prestación de servicios de pago, tal como señala el artículo 2 del Reglamento Delegado 2018/389 , pues como se indica también en la sentencia citada de la Audiencia de Pontevedra, incluyendo la técnica del **phishing**, la creación y puesta en la red de páginas que clonan las del sitio oficial de las entidades emisoras de instrumentos de pago, el deber de diligencia de la entidad demandada exigía dotarse de la tecnología antiphishing precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas, lo que, de producirse, impediría que el defraudador pudiera hacerse con las credenciales del usuario del instrumento de pago por ella emitido, pues la rotura del enlace del correo electrónico haría ya ineficaz cualquier conducta que frente al mismo pudiera observar el usuario receptor. Dicha actuación diligente no puede considerarse acreditada por la información que se facilita a los clientes a través de su página web, en cuanto la efectividad de esas obligaciones preventivas, lo que requerían era implementar en el sistema informático el mecanismo tecnológico adecuado para evitarlo; es decir mediante una conducta activa y no simplemente informativa o divulgativa" .*

*Y en el mismo sentido en que lo hace la Audiencia Provincial de Madrid, de incidir en la insuficiencia de avisos o advertencias genéricas a través de la web, se pronuncian las SSAAPP La Rioja, de 17 de febrero de 2023 , que recuerda que" es el banco quien ofrece este producto, en principio seguro, y es cierto que remite avisos y advertencias genéricas sobre su utilización; pero conociendo los distintos riesgos de los que avisa, le corresponde adoptar las medidas de seguridad o control necesarias, que en este caso no consta que se adoptaran. Y no basta con medidas genéricas de protección o avisos estereotipados de cuidado, pues tales avisos ostentarían la calificación de "formulas predispuestas", vacías de contenido. No son los clientes los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, o estar al tanto de los mismos, ni prevenir con su asesoramiento experto dichos riesgos" ; la de Asturias, Sec. 7ª, de 30 de junio de 2023, que cita la anterior; y la de Pontevedra, Sec. 3ª de 23 de marzo de 2023, que, a propósito del estudio de la negligencia grave del usuario indica " partiendo del admitido criterio de responsabilidad cuasi-objetiva de la entidad en la prestación del servicio de banda virtual respecto a operaciones de pago como la transferencia, reiterada jurisprudencia considera que dicha negligencia debe ser grave en atención a las circunstancias demostradas del caso, atribuyéndose en todo caso la carga probatoria de la misma al proveedor del servicio con arreglo a art. 217 LEC . En interpretación de directiva 2015/2366 , la negligencia que hace responder al cliente es la que se deriva de una conducta caracterizada por un grado significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que haya podido ser inducido por un delincuente profesional. Como parámetro del actuar negligente también cabrá acudir al art. 1.104 CC , que exige la diligencia asociada a la naturaleza de la obligación y a las circunstancias personales, de tiempo y lugar. Ello destacándose la complejidad y grado de perfección que presenta en la actualidad el método de " **phishing** " de difícil*

detección por persona de formación media, así como el deber de la proveedora, del servicio de dotarse de tecnología suficiente y adecuada con exigencia de medidas implantadoras activas, sin entenderse suficientes avisos generales o en página web de mero carácter informativo o divulgativo".

De la legislación de protección de servicios de pago (RDL 19/2018, como de la jurisprudencia que lo aplica y lo interpreta pueden extraerse como conclusiones: (i) la ley establece un sistema de responsabilidad cuasiobjetiva de la entidad o proveedor de pagos, que deriva del incumplimiento por su parte de los deber de diligencia en la garantía de operaciones de pago, implementando todos los mecanismos y controles de autenticación necesarios, incluido dotarse de tecnología "antiphishing" para proteger al cliente de este tipo de ataques fraudulentos y (ii) la entidad solo puede liberarse de tal responsabilidad si prueba que la orden de pago no se vio afectada por "un fallo técnico u otra deficiencia del servicio prestado por dicho proveedor", que el cliente ha actuado fraudulentamente o con negligencia grave a la hora de aplicar los medios razonables de protección de que haya sido provisto o cuando no haya comunicado a la entidad el pago no autorizado en cuanto tenga conocimiento del mismo.

QUINTO. - Resolución del litigio.

En el contexto legal y jurisprudencial descrito, vista la prueba practicada, no cabe concluir que la actora, a pesar de haber pinchado el enlace recibido inicialmente e introducido los códigos solicitados posteriormente haya incurrido en negligencia grave.

La propia entidad, en la contestación que en envió a la reclamación de la actora rechazando su responsabilidad en fecha 30 de septiembre de 2020, afirma que "no se discute que el origen de las operaciones se encuentre en una actuación fraudulenta" y "que parece acreditado que el defraudador obtuvo previamente los datos necesarios para la comisión de fraude a través de " phishing ", una técnica que consiste en el envío de un correo electrónico o un SMS por parte del Ciberdelincuente, a un usuario simulando ser una entidad legítima, con el objetivo de robarle información privada, realizarle un cargo económico o infectar su dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico, consiguiendo de este modo el control de las OTP' s, enviadas al teléfono y dejándole sin servicio telefónico".

Los términos y manifestaciones de la dicha contestación a la reclamación de la usuaria, determinan a nuestro entender la responsabilidad establecida legalmente para la entidad y excluyen la negligencia grave - única exigida - de la actora. El propio Banco asume que Dña. Eugenia fue objeto de un fraude, así como que el mismo fue realizado mediante la modalidad de " phishing ", cuyo funcionamiento, finalidad y efectos describe perfectamente. La existencia del engaño, del fraude, reconocida por la entidad evidencia que esta no había implementado todas las medidas o mecanismos necesarios para proteger a su cliente de tales ataques por ciberdelincuentes, cada vez más frecuentes y por todas las entidades conocidos, lo cual les exige una respuesta de seguridad acorde con la proliferación de este tipo de fraudes informáticos, lo cual comporta el incumpliendo de su obligación de garantizar la seguridad de los servicios de pago efectuados a través de internet o dispositivos móviles. Según el funcionamiento de esta modalidad de estafa informática que la propia apelante describe, producido el ataque, el usuario pierde todo control de sus credenciales, claves o OTP' s que son recibidas por el ciberdelincuente, situación en la que no puede imputársele negligencia alguna, ni siquiera inicialmente, cuando tras recibir el primero de los mensajes con un enlace, pinchó el mismo sin prestar mucho cuidado. Precisamente, lo que caracteriza a esta técnica de captación de datos confidenciales

informáticos es su sofisticación y capacidad de imitar el lenguaje, formato e imagen de las entidades financieras a las que suplantan, de modo que inducen fácilmente a error a la víctima, que, acostumbrada a recibir mensajes de su entidad por este canal, confían en su autenticidad, siendo fácil que incurran en error en determinados momentos en que otras actividades exijan su atención, como parece ser que sucedió en este caso, en que el mensaje llegó a Dña. Eugenia un día del mes de agosto, época de mucha actividad en el negocio que regenta, una casa rural.

Es también relevante en este caso el hecho de que la entidad, a pesar de gran número de operaciones realizadas con las claves o credenciales de la actora en sólo dos días, consistentes en extracciones en cajeros, órdenes de traspaso, transferencias, descargas de saldo hasta la cuantía que se reclama, y la importancia de las cantidades dispuestas, no tuviese capacidad para detectar que su cliente podría estar siendo víctima de un fraude informático, arbitrando las medidas necesarias para cerciorarse de que era el cliente quien realmente las estaba realizando, o bloquearlas mismas.

En consecuencia, hemos de compartir el criterio de la juez de instancia de apreciar la responsabilidad de LIBERBANK por incumplir sus obligaciones en relación con las medidas de seguridad en los medios de pago, medidas que han de ser acordes con las exigencias de los fraudes informáticos cada vez más habituales, y que, está demostrado han de ir más allá de la autenticación reforzada y, desde luego, de las recomendaciones que hacen a los usuarios.

Por tanto, el recurso debe ser desestimado.

SEXTO. - Costas procesales.

Desestimado el recurso, en aplicación de los *arts. 393.1 y 394 LEC*, las costas de esta alzada se imponen a la recurrente.

Así, en ejercicio de la potestad jurisdiccional que nos ha conferido la Constitución Española, y en nombre de Su Majestad El Rey.

FALLAMOS

1. DESESTIMAMOS EL RECURSO DE APELACIÓN INTERPUESTO POR UNICAJA BANCO S.A CONTRA LA *SENTENCIA DEL JUZGADO DE PRIMERA INSTANCIA E INSTRUCCIÓN Nº 4, DE TORRELAVEGA, DE FECHA 29 DE OCTUBRE DE 2021*, QUE CONFIRMAMOS EN TODOS SUS TÉRMINOS.

2. Imponemos al recurrente las costas de esta alzada.

PUBLICACION: La precedente Sentencia ha sido leída y publicada por el Ilmo. Sr. Magistrado Ponente en el día de su fecha, de lo que doy fe. -

DILIGENCIA: Seguidamente se procede a cumplimentar la notificación de la anterior resolución. Doy fe.

De conformidad con lo dispuesto por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, las partes e intervinientes en el presente procedimiento judicial quedan informadas de la incorporación de sus datos personales a los ficheros jurisdiccionales de este órgano judicial, responsable de su tratamiento, con la exclusiva finalidad de llevar a cabo la tramitación del mismo y su

posterior ejecución. El Consejo General del Poder Judicial es la autoridad de control en materia de protección de datos de naturaleza personal contenidos en ficheros jurisdiccionales.