Roj: **SAP M 7327/2022** - **ECLI:ES:APM:2022:7327**

Id Cendoj: **28079370202022100180**
Órgano: **Audiencia Provincial**
Sede: **Madrid**
Sección: **20**
Fecha: **20/05/2022**
Nº de Recurso: **945/2021**
Nº de Resolución: **184/2022**
Procedimiento: **Recurso de apelación**
Ponente: [redacted]
Tipo de Resolución: **Sentencia**

Audiencia Provincial Civil de Madrid

Sección Vigésima

[redacted]

Recurso de Apelación 945/2021

O. Judicial Origen: Juzgado de 1ª Instancia nº 02 de Madrid

Autos de Procedimiento Ordinario 551/2020

APELANTE: BANCO SANTANDER S.A.

PROCURADOR D./Dña. [redacted]

APELADO: D./Dña. [redacted]

PROCURADOR D./Dña. [redacted]

SENTENCIA Nº 184/2022

TRIBUNAL QUE LO DICTA:

ILMOS. SRES. MAGISTRADOS:

D. [redacted]

D. [redacted]

Dña. [redacted]

En Madrid, a veinte de mayo de dos mil veintidós.

La Sección Vigésima de la Ilma. Audiencia Provincial de esta Capital, constituida por los Sres. que al margen se expresan, ha visto en trámite de apelación los presentes autos civiles Procedimiento Ordinario 551/2020 seguidos en el Juzgado de 1ª Instancia nº 02 de Madrid a instancia de BANCO SANTANDER S.A. apelante - demandado, representado por el Procurador D. [redacted] contra D. [redacted] apelado - demandante - impugnante, representado por la Procuradora Dña. [redacted]; todo ello en virtud del recurso de apelación interpuesto contra Sentencia dictada por el mencionado Juzgado, de fecha 27/04/2021.

VISTO, Siendo Magistrado Ponente **D.** [redacted]

ANTECEDENTES DE HECHO

PRIMERO.- Por Juzgado de 1ª Instancia nº 02 de Madrid se dictó Sentencia de fecha 27/04/2021, cuyo fallo es el tenor siguiente: Que estimando parcialmente la demanda promovida por D. [redacted] representado por el procurador Dª. [redacted] y asistido por el letrado D. [redacted] contra BANCO SANTANDER S.A., representado por el procurador D. [redacted] y asistido por el letrado D. [redacted] debo condenar y condeno a la parte demandada a que abone al actor la cantidad de 5.000 euros, más intereses legales desde la reclamación extrajudicial, sin hacer expresa imposición de costas.

SEGUNDO.- Contra la anterior resolución se interpuso recurso de apelación por la parte demandada, exponiendo las alegaciones en que basa su impugnación. Admitido el recurso en ambos efectos, se dio traslado del mismo a la apelada, que presentó escrito oponiéndose al recurso formulado de contrario e impugnando la sentencia. Elevados los autos ante esta Sección, fueron turnados de ponencia, y quedando pendientes de resolución, se señaló fecha para la deliberación y votación, que se ha llevado a cabo por los Magistrados de esta Sección.

TERCERO.- En la tramitación del presente procedimiento han sido observadas las prescripciones legales.

FUNDAMENTOS JURIDICOS

Se aceptan los de la resolución apelada en los términos de la presente, debiendo sustituirse en lo necesario.

PRIMERO.- En la demanda que dio inicio a las presentes actuaciones, el demandante titular de una tarjeta de débito asociada a una cuenta corriente que tiene abierta en el BANCO DE SANTANDER, ejercita una acción en reclamación de 6.090 € en que cuantifica los daños y perjuicios que se le causaron como consecuencia de las 6 disposiciones que por un tercero desconocido, se hicieron con cargo a la cuenta de la que era titular al haber sido víctima de un uso fraudulento de la tarjeta, mediante la actuación fraudulenta denominada "phising" de la que fue víctima, cuando el recibió un SMS en móvil asociado a la tarjeta y contrato de cuenta corriente, en el que se le invitaba a hacer un clic en un enlace clonado de la página web del Banco demandado, realizando las operaciones que se le requirieron, sin que por el Banco se le hubiera advertido previamente sobre posibles fraudes o incidencias de suplantación de identidad, procediendo a continuación a descargar la aplicación que se le ofrecía en su móvil, comprobando al día siguiente que entre los días 12 y 13 de julio se habían realizado 6 reintegros consecutivos de efectivo con su tarjeta de débito por importes de 1.000 € cada uno de ellos. Atribuye a la demandada haber incurrido en el incumplimiento que contractual y legalmente le corresponden, al no haberle alertado cuando se efectuó la primera extracción, enviándole un aviso vía SMS al teléfono móvil adherido a la tarjeta, lo que le hubiera permitido bloquearla cuando se efectuó la primera extracción y podido bloquear la tarjeta.

Invoca al respecto las obligaciones que imponen a la entidad bancaria el Real Decreto Ley 19/2018 de 23 de noviembre de Servicios de Pago, la Directiva (UE) 2915/2366 del Parlamento y del Consejo, de 25 de noviembre sobre servicios de pago en el mercado interior y el Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017.

La entidad demandada se opuso a las pretensiones formuladas en su contra. Sostiene que la pérdida patrimonial sufrida por el demandante se debe a la actuación delictiva de un tercero y niega haber incurrido en los incumplimientos que se le atribuyen, en cuanto en su página web da continuas instrucciones sobre cómo prevenir el fraude e identificar el phishing, no obstante lo cual y a pesar de que del texto del correo recibido por el demandante se podía cuando menos, sospechar de que el mismo no era remitido por la entidad bancaria, el demandante, voluntariamente cliqueó el enlace y facilitó los datos que permitieron efectuar las disposiciones, que se encontraban dentro del límite autorizado y por tanto no le imponían avisar al cliente, negando que éste tuviera concertado el servicio de alerta para la tarjeta a través de la que se hicieron las disposiciones.

Frente a dicha resolución interpuso recurso de apelación la entidad demandada articulando el mismo en un único motivo de impugnación, mediante el que sostiene haberse efectuado una incorrecta valoración probatoria e incurrido en infracción de los artículos 41 y 46 del RDL 19/2018.

El demandante se opuso al recurso e impugnó la sentencia en los pronunciamientos que le resultan desfavorable, centrando su discrepancia en la negligencia que se le atribuye en la sentencia, en cuanto insiste que conforme a la normativa nacional y comunitaria aplicable, para que el usuario quede obligado a soportar las pérdidas ha de acreditarse por la entidad demandada que el cliente actuó con negligencia grave y ésta no se puede apreciar al haber sido víctima de un delito de estafa y haber facilitado los datos personales motivado por el error a que se le indujo. Niega por otro lado, que el Banco adoptara las medidas de seguridad que le eran exigibles.

SEGUNDO.- Centrada la discrepancia en si el comportamiento adoptado por las partes aquí enfrentadas debe ser calificado como negligente, en el cumplimiento de las obligaciones que para cada uno de ellos se deriva del contrato de tarjeta de débito que les vincula y las consecuencias a extraer de todo ello, para el análisis del cumplimiento que cada una de las partes ha hecho de las obligaciones que les corresponde como titular y usuario de la tarjeta el demandante y como prestadora del servicio de pago la demandada, el marco normativo de que debe partirse viene constituido por el RDL 19/2018, que derogó la Ley 16/2009 a la que se remite la sentencia de primera instancia. La Directiva 2015/2366 y el Reglamento delegado 2018/389 de la Comisión, interpretado todo ello conforme a las reglas y principios básicos establecidos en el cc, respecto de las obligaciones y contratos y ello a la vista de todas las circunstancias concurrentes en el supuesto de hecho enjuiciado. Como se indica en la sentencia nº 539/2021 de 21 de diciembre de la Sec. 6ª (Sede Vigo) de la Audiencia provincial de Pontevedra,(ponente el Ilmo Sr. [redacted]), en la que se analiza un supuesto de hecho similar al presente, el marco nopr,matrivo del que debe partirse es el siguiente:

" Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015 , sobre servicios de pago en el mercado interior

Considerando:

(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. Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros. Se deben considerar nulas las cláusulas contractuales y las condiciones de prestación y utilización de instrumentos de pago mediante las cuales aumente la carga de la prueba sobre el consumidor o se reduzca la carga de la prueba sobre el emisor. Además, en situaciones específicas y, más concretamente, cuando el instrumento de pago no esté presente en el punto de venta, como en el caso de los pagos en línea, resulta oportuno que el proveedor de servicios aporte pruebas de la presunta negligencia, puesto que los medios a disposición del ordenante son limitados en esos casos.

Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros . En vigor desde el 14 de septiembre de 2019 (artículo 38)

Artículo 1 Objeto

El presente Reglamento establece los requisitos que deben cumplir los proveedores de servicios de pago a efectos de la aplicación de medidas de seguridad que les permitan hacer lo siguiente:

a) aplicar el procedimiento de autenticación reforzada de clientes, de conformidad con el artículo 97 de la Directiva (UE) 2015/2366 ;

b) eximir de la aplicación de los requisitos de seguridad de la autenticación reforzada de clientes, bajo determinadas condiciones limitadas y basadas en el nivel de riesgo, el importe de la operación de pago y la frecuencia con que se repite, y el canal de pago empleado para la ejecución de dicha operación;

c) proteger la confidencialidad y la integridad de las credenciales de seguridad personalizadas del usuario de servicios de pago;

d) establecer estándares abiertos comunes y seguros para la comunicación entre los proveedores de servicios de pago gestores de cuenta, los proveedores de servicios de iniciación de pagos, los proveedores de servicios de información sobre cuentas, los ordenantes, los beneficiarios y otros proveedores de servicios de pago en relación con la provisión y la utilización de servicios de pago en aplicación del título IV de la Directiva (UE) 2015/2366 .

Artículo 2 Requisitos generales de autenticación .

1. Los proveedores de servicios de pago dispondrán de mecanismos de supervisión de las operaciones que les permitan detectar operaciones de pago no autorizadas o fraudulentas a efectos de la aplicación de las medidas de seguridad a que se hace referencia en el artículo 1, letras a) y b).

Dichos mecanismos se basarán en el análisis de las operaciones de pago teniendo en cuenta los elementos que caractericen al usuario de servicios de pago en el contexto de un uso normal de las credenciales de seguridad personalizadas .

2.Los proveedores de servicios de pago garantizarán que los mecanismos de supervisión de las operaciones tengan en cuenta, como mínimo, todos los factores basados en el riesgo siguientes: a) listas de elementos de autenticación comprometidos o sustraídos; b) el importe de cada operación de pago; c) supuestos de fraude conocidos en la prestación de servicios de pago; d) señales de infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación; e) en caso de que el dispositivo o el programa informático de acceso sea facilitado por el proveedor de servicios de pago, un registro de la utilización del dispositivo o el programa informático de acceso facilitado al usuario de los servicios de pago y de su uso anormal.

Artículo 3 Revisión de las medidas de seguridad

1.La aplicación de las medidas de seguridad a que se refiere el artículo 1 deberá documentarse, probarse periódicamente, evaluarse y auditarse de conformidad con el marco jurídico aplicable al proveedor de servicios de pago por auditores con experiencia en el ámbito de la seguridad y los pagos informáticos y funcionalmente independientes, ya pertenezcan al organigrama del propio proveedor de servicios de pago o sean externos a él.

.....

12. El RDL 19/2018 derogó la ley 16/2009 de 13 de noviembre de servicios de pago (disposición derogatoria única) y dispuso, en cuanto al régimen transitorio, que los contratos de servicios de pago suscritos con anterioridad a su entrada en vigor seguirían siendo válidos pero en todo caso habría de aplicarse las disposiciones de carácter imperativo que resulte más favorables para los consumidores y microempresas (Disposición Transitoria quinta). La Disposición Final 13ª estableció un régimen de entrada en vigor de la norma de manera escalonada que, partiendo de la general vigencia desde el día 25 de noviembre de 2018 (el siguiente a la fecha de publicación de la norma en el BOE, DF 13ª.1) culminó el 14 de septiembre de 2019 (18 meses desde la entrada en vigor del Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017, DF 131ª2.b) fecha desde la que habrían de aplicarse los artículos 37, 38, 39 y 68.

13. De las normas que en la legislación vigente regulan las obligaciones del proveedor y del usuario de los servicios de pago y el régimen de responsabilidad importa a efectos de este proceso considerar:

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;

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.

.....

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 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.

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.

.....

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.

Artículo 64. Ausencia de responsabilidad cuando concurran circunstancias excepcionales e imprevisibles.

La responsabilidad establecida con arreglo a los Capítulos II y III de este Título no se aplicará en caso de circunstancias excepcionales e imprevisibles fuera del control de la parte que invoca acogerse a estas circunstancias, cuyas consecuencias hubieran sido inevitables a pesar de todos los esfuerzos en sentido contrario, o en caso de que a un proveedor de servicios de pago se le apliquen otras obligaciones legales.

Artículo 68. Autenticación.

1. Los proveedores de servicios de pago aplicarán la autenticación reforzada de clientes, en la forma, con el contenido y con las excepciones previstas en la correspondiente norma técnica aprobada por la Comisión Europea, cuando el ordenante:

a) acceda a su cuenta de pago en línea;

b) inicie una operación de pago electrónico;

c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos.

.....

6. No obstante, no será preciso aplicar la autenticación reforzada de clientes a la que se refiere el apartado 1 a los supuestos indicados en el artículo 98.1.b) de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 .

***TERCERO** . Responsabilidad por operaciones de pago fraudulentas.*

14. El proveedor de servicios de pago se encuentra sujeto al cumplimiento de específicas obligaciones de protección en la emisión de los instrumentos de pago y en los procesos de autenticación de las operaciones de pago cuya finalidad es minimizar la probabilidad de ejecución de operaciones no autorizadas.

15. En relación con los instrumentos de pago ha de cumplir con las obligaciones sobre emisión y uso seguro que se establecen en el artículo 42.1 RDL 19/2018 .

16. Los procesos o mecanismos de autenticación de las operaciones de pago deben cumplir con los requisitos que establece el Reglamento Delegado 2018/389 , lo que exige:

- a) Implementar las medidas de seguridad previstas en el artículo 1, que han de incluir el procedimiento de autenticación reforzada de clientes, con las salvedades específicamente señaladas.

- b)Incluir mecanismos de supervisión de las operaciones que permitan al proveedor de servicios de pago detectar operaciones de pago no autorizadas o fraudulentas. A tal efecto el proveedor de servicios de pago ha de tener en cuenta la totalidad de los factores de riesgo enumerados en el artículo 2, y, entre ellos, los supuestos de fraude conocidos en la prestación de servicios de pago.

- c) Auditar las medidas, en las condiciones del artículo 3.

17. El usuario de los servicios de pago deberá cumplir con las obligaciones que se establecen en el artículo 41 RDL 19/2010 : a) Usar del instrumento de pago conforme a lo pactado y tomar las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas; b) En cuanto tenga conocimiento de haber perdido la posesión del instrumento de pago o de haber sido este utilizado sin su autorización, lo notificará sin demora indebida al proveedor de servicios de pago.

18. El régimen de la responsabilidad por las pérdidas derivadas de operaciones de pago por uso fraudulento de un instrumento de pago por un tercero se determina interpretando de manera integrada las previsiones del

artículo 46 con la regulación general de las pérdidas por operaciones de pago no autorizadas del artículo 45 y con el régimen de la carga probatoria que se establece en el artículo 44 (todos del RDL 19/2018).

19. Será el proveedor de los servicios de pago quien habrá de responder de las pérdidas de importe superior a 50 euros por las operaciones de pago resultantes del uso fraudulento del instrumento de pago por un tercero; responderá de la totalidad de la pérdida cuando al ordenante no le hubiera sido posible detectar el posible uso fraudulento antes de que éste se hubiese materializado o cuando la pérdida se debiera a la acción u omisión de cualquier persona de la que el proveedor de servicios hubiera de responder.

20. El ordenante será quien soporte la totalidad de las pérdidas cuando concurran dos requisitos: a) La operación de pago fue autenticada y registrada con exactitud y no se vio afectada por ninguna deficiencia del servicio prestado por el proveedor de servicios de pago; b) El ordenante actuó de manera fraudulenta, o incumpliendo deliberadamente o por negligencia grave alguna de las obligaciones recogidas en el artículo 41 RDL 19/2018 .

21. Al proveedor de servicios de pago le corresponde la carga procesal de acreditar tanto su propio comportamiento diligente en la autenticación de la operación de pago como el fraude o la negligencia grave del ordenante. La prueba de la diligencia en el procedimiento de autenticación deberá realizarse en relación a las exigencias del Reglamento Delegado 2018/389 . La prueba del fraude del ordenante requerirá de la acreditación de hechos de los que pudiera llegar a inferirse que aquel actuó con engaño para beneficiarse de la operación de pago. La prueba de la negligencia grave del ordenante requerirá de la acreditación de las circunstancias concurrentes en la operación de pago de las que quepa inferir que la misma pudo realizarse porque aquel obró con una significativa falta de diligencia al usar del instrumento de pago o al proteger sus credenciales.

22. Cuando el proveedor de servicios de pago no acredite el cumplimiento de los deberes de diligencia propios en la autenticación habrá de responder de la pérdida resultante del uso fraudulento del instrumento de pago por un tercero salvo que concurra el fraude del ordenante."

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 palabro "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 las 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 con una conducta activa y no simplemente informativa o divulgativa.

De dicha omisión, no puede quedar exonerada por el hecho de que el cliente no tuviera activado el sistema de alarma en la tarjeta utilizada fraudulentamente, pues siendo obligación suya adoptar las medidas de seguridad adecuadas, esa obligación no puede entenderse cumplida con la simple puesta a disposición del cliente, sino que es ella quien debe adoptar una actitud activa para su implantación, no solo ponerla a disposición del cliente.

En consecuencia, la demandada incurrió en un incumplimiento de los deberes de diligencia en la prevención del fraude mediante phising, que le hace ser responsable del perjuicio total sufrido por el demandante, pues no podía la entidad desconocer que frecuentemente mediante esa técnica el tercero defraudador utiliza los datos de la tarjeta para activarla en una aplicación de pago de la que tiene dominio, por lo que debiendo conocer que el teléfono desde el que se le había solicitado la activación no se encontraría entre los que hubiera registrado su nombre el demandante en su ficha de cliente, la comunicación del número de terminal telefónico devenía exigible para que aquélla pudiera conocer que era un tercero quien podría disponer de los datos de la tarjeta mediante la aplicación de pago que se activaría.

No habiendo quedado acreditado que la entidad demandada cumplió en la forma que le es exigible los deberes de diligencia en la autenticación de las operaciones de pago, pues ni habría probado haber implementado un mecanismo antiphising de protección de los usuarios de los instrumentos de pago por ella emitidos frente al uso fraudulento por un tercero de páginas imitativas de las propias para hacerse con las credenciales del instrumento, ni habría puesto en conocimiento del usuario los datos necesarios para que este conociera que se trataba de instalar su tarjeta en una aplicación de pago de un terminal de un tercero y no apreciándose que el demandante incurrió en negligencia grave en el cumplimiento de sus deberes de custodia y uso de la tarjeta, ha de declararse la responsabilidad de la entidad demandada como proveedora de los servicios de pago usados de manera fraudulenta por un tercero y por tanto es quien debe responder de las pérdidas sufridas por el demandante con tales operaciones, responsabilidad que se hace extensible a la totalidad de la pérdida, pues en momento alguno anterior a que se realizase la última de las operaciones fraudulentas de pago, la entidad demandada había informado a la demandante del número del terminal telefónico desde el que se estaban realizando las órdenes de pago fraudulentas, ni de circunstancia alguna que hubiera permitido conocer al demandante tal uso fraudulento.

QUINTO.- Lo indicado comporta la desestimación del recurso de apelación interpuesto por le entidad demandada y la estimación de la impugnación formulada por el demandante, con la consecuencia derivada de ello de imponer las costas causadas en primera instancia a la entidad demandada, así como las causadas en esta alzada como consecuencia del recurso de apelación por ella interpuesto, en aplicación de lo establecido en los artículos 394.1 y 398.1 de la Ley de Enjuiciamiento Civil. L desestimarse el recurso se acuerda la pérdida del depósito constituido para recurrir.

En cuanto a las costas causadas por la impugnación formulada por el demandante, al estimarse la misma no procede formular pronunciamiento de condena, tal como establece el art. 398.2 de la LEC. Procede igualmente devolver a la demandante el depósito constituido ara recurrir.

Vistos los artículos citados y demás de pertinente aplicación.

FALLAMOS

SE DESESTIMA el recurso de Apelación interpuesto por la representación procesal de la entidad "BANCO DE SANTANDER S.A" y

SE ESTIMA la impugnación formulada por la representación procesal de D. [redacted], ambos contra la sentencia dictada por el Juzgado de Primera Instancia nº 2 de los de Madrid de fecha 27 de abril de 2021, en los autos de Procedimiento Ordinario, seguido bajo el nº 55129/2020, la cual **SE REVOCA PARCIALMENTE EN EL SIGUIENTE SENTIDO**

SE ESTIMA ÍNTEGRAMENTE LA DEMANDA INTERPUESTA POR LA REPRESENTACIÓN PROCESAL DE DON [redacted] CONTRA "BANCO DE SANTANDER S.A." A LA QUE SE CONDENA A QUE ABONE AL DEMANDANTE LA CANTIDAD DE SEIS MIL NOVENTA EUROS,(6.090 €) INCREMENTADA CON LOS INTERESES LEGALES DESDE LA RECLAMACIÓN EXTRAJUDICIAL.

SE IMPONEN LAS COSTAS DE PRIMERA INSTANCIA A LA PARTE DEMANDADA

Todo ello con imposición a BANCO DE SANTANDER las costas procesales causadas en esta alzada, como consecuencia del recurso por ella interpuesto y con pérdida de depósito constituido por su parte para recurrir.

Y sin imposición de las costas causadas en esta alzada como consecuencia de la impugnación formulada por D. [redacted], a quien se devolverá el depósito constituido en primera instancia

MODO DE IMPUGNACION: Se hace saber a las partes que frente a la presente resolución cabe interponer **Recurso de Casación y/o Extraordinario por Infracción Procesal**, en los supuestos previstos en los artículos 477 y 468 respectivamente de la LEC en relación con la Disposición Final 16ª de la misma Ley, a interponer en el plazo de VEINTE DÍAS ante este mismo órgano jurisdiccional. Haciéndose saber a las partes que al tiempo de la interposición de los mismos, deberán acreditar haber constituido el depósito que, por importe de 50 euros, previene la Disposición Adicional Decimoquinta de la L.O.P.J., establecida por la Ley Orgánica 1/09, de 3 de noviembre, sin cuyo requisito el recurso de que se trate no será admitido a trámite, excepto en los supuestos de reconocimiento expreso de exención por tener reconocido el derecho de asistencia jurídica gratuita. (Caso de interponerse ambos recursos deberá efectuarse un depósito de 50 euros por cada uno de ellos).

Dicho depósito habrá de constituirse en la Cuenta de Depósitos y Consignaciones de esta Sección abierta con el nº [redacted] en la sucursal 6114 del Banco de Santander sita en la calle Ferraz nº 43 de Madrid.

Así, por esta nuestra Sentencia, lo pronunciamos, mandamos y firmamos.

PUBLICACION.- Firmada la anterior resolución es entregada en esta Secretaría para su notificación, dándosele publicidad en legal forma y expidiéndose certificación literal de la misma para su unión al rollo. Doy fe.

NOTA: De conformidad con el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se informa que 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.