[redacted]

JUZGADO DE PRIMERA INSTANCIA Nº 2
Campo internacional de Maspalomas, Parcela 33
San Bartolomé de Tirajana
Teléfono: 928 72 46 41
Fax.: 928 72 46 52
Email.: instancia2.sbar@justiciaencanarias.org

Procedimiento: Juicio verbal (250.2)
Nº Procedimiento: [redacted]
NIG: [redacted]
Materia: Sin especificar
Resolución: Sentencia [redacted]
IUP: [redacted]

Intervención:	Interviniente:	Abogado:	Procurador:
Demandante	[redacted]	Raul Garcia Gamez	[redacted]
Demandado	BANCO SANTANDER S.A.	[redacted]	

SENTENCIA

En la villa de San Bartolomé de Tirajana, a VEINTITRÉS de noviembre de dos mil veintitrés.

Vistos por mí, D. [redacted], Juez sustituto del Juzgado de Primera Instancia n.º 2 de San Bartolomé de Tirajana, los autos de **JUICIO VERBAL** registrados con el nº [redacted] promovidos por **DON/DOÑA** [redacted] frente a **BANCO SANTANDER S.A. (A-39000013)**, sobre reclamación de cantidad derivada de fraude**.**

ANTECEDENTES DE HECHO

PRIMERO.- La representación procesal de la parte demandante formuló demanda frente a la demandada que por turno de reparto correspondió a este Juzgado, en la que, con fundamento en los hechos y consideraciones legales que cita, se concluía suplicando que se dictase sentencia por la que, estimando la demanda, *"1. DECLARE que la entidad bancaria BANCO SANTANDER ha incumplido el contrato de cuenta bancaria n.º [redacted] y tarjeta de crédito, así como el contrato de servicios de pago y banca electrónica, por haber permitido la ejecución de operaciones por tercero no autorizado de forma fraudulenta con suplantación de las credenciales de mi representado.*

2. DECLARE que las cantidades dispuestas y no autorizadas por mi representada suman la cantidad de DOS MIL TRESCIENTOS CUARENTA Y SEIS EUROS (2346 €), correspondientes a las operaciones realizadas los días 9 de noviembre de 2022.

3. DECLARE RESPONSABLE de las citadas disposiciones no autorizadas a la entidad demandada.

4. CONDENE a la entidad BANCO SANTANDER a indemnizar a mi representado en la suma de DOS MIL TRESCIENTOS CUARENTA Y SEIS EUROS (2346 €), dispuesta fraudulentamente, junto con los intereses legales desde la fecha de su anotación en cuenta.

5. CONDENE al demandado al pago de las costas causadas en la instancia".

SEGUNDO.- Admitida a trámite la demanda, se emplazó a la parte demandada para que se personara en los autos y la contestase.

TERCERO- Por escrito de fecha 14/03/2023 la demandada contestó a la demanda, oponiéndose a la misma interesando su desestimación y la condena en costas de la demandante.

CUARTO.- Habiendo interesado las partes la celebración de la vista, ésta tuvo lugar el 09/11/2023 con el resultado que obra en las actuaciones, quedando el procedimiento pendiente de dictar sentencia.

QUINTO.- Durante la tramitación de este proceso se han observado y cumplido las prescripciones legales.

FUNDAMENTOS DE DERECHO

PRIMERO.- La demandante [redacted], interpone demanda contra la demandada por la que reclama la cantidad de DOS MIL TRESCIENTOS CUARENTA Y SEIS EUROS (2.346,00 €), como consecuencia del presunto fraude sufrido, a través de la técnica conocida como “Phishing bancario”.

La parte actora solicita en este procedimiento que se declare la responsabilidad de la mercantil demandada por incumplimiento del contrato de cuenta bancaria, así como que abone a la actora la cuantía reclamada por los daños y perjuicios sufridos. La demanda se basa esencialmente en la alegación de que fue víctima del fraude conocido como phishing, lo cual llevó a que fueran cargados pagos sin su autorización en su cuenta bancaria, por la cuantía que se reclama.

La parte actora ejercita en el presente procedimiento la acción de reclamación de cantidad por incumplimiento por parte de la entidad bancaria de sus obligaciones como proveedor de servicios de pago, invocando la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior, el Reglamento Delegado (UE) 2018/389, 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, y el Real Decreto ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (artículos 36.1 y 41 y siguientes).

La demandante denunció los hechos el día 04/12/2022 y formuló reclamación frente a la entidad, solicitando la restitución de las cantidades defraudadas. Sin embargo, la entidad remitió contestación en fecha 24/11/2022 (previa a la denuncia) y en fecha 27/12/2022, desestimando la reclamación y argumentando que la demandante no había protegido debidamente sus elementos de seguridad, lo que constituía una negligencia grave por su parte.

La mercantil demandada formula oposición y alega esencialmente que los cargos fraudulentos en la cuenta bancaria se habrían realizado por responsabilidad exclusiva de la actora, al no haber actuado con la diligencia adecuada. La parte demandada se opone a las pretensiones de la actora, alegando que no se le puede exigir responsabilidad alguna a la entidad por cuanto la actora incurrió en negligencia o imprudencia, revestida de la suficiente gravedad, al facilitar, por acción u omisión, voluntaria o inconsciente, a través de algún sistema de ingeniería social de

los utilizados habitualmente para ello, sus propios datos de acceso a servicios de la banca digital. Así, las operaciones controvertidas fueron realizadas a través de un comercio electrónico seguro, siendo necesario para la emisión de las mismas introducir los datos de las tarjetas (16 dígitos, fecha de caducidad y CVV) y la autenticación mediante segundo factor que, en este caso, fue a través de OTP-SMS enviados por BANCO SANTANDER al móvil validado de la cliente, cumpliéndose, por tanto, todos los protocolos de seguridad para la operativa online de tarjetas. Dichas operaciones controvertidas fueron debidamente autorizadas, registradas con exactitud y contabilizadas, sin que se vieran afectadas por un fallo técnico u otras deficiencias, habiéndose procedido a la autenticación reforzada del cliente autorizante de la operación de pago. Por tanto, ninguna responsabilidad puede predicarse de la entidad BANCO SANTANDER en el fraude que pudiera haber padecido la actora, pues tales hechos son totalmente ajenos a la demandada.

En este sentido, si bien la actora niega la realización de las operaciones controvertidas, sin embargo ella misma reconoce, en la denuncia presentada, haber sido víctima de un engaño o fraude, que conllevó que incumpliese las medidas de diligencia debida en el uso de las tarjetas de crédito, facilitando así la suplantación de su identidad a través del método "smishing", método mediante el cual accedió a un enlace de un SMS que recibió en su teléfono móvil, facilitando así, necesariamente, las credenciales de acceso a su banca online (usuario y contraseña), con lo que el tercero (delincuente) ya tiene acceso a la banca digital del cliente y a los datos visibles de su tarjeta. Manifiesta la Entidad que a las 18:01 horas, la demandante recibió en su línea móvil un SMS por parte de BANCO SANTANDER con un código OTP (v.gr. N013N463) para autorizar el acceso a su banca digital; siendo que el ciber-delincuente remitió un nuevo SMS con el mismo enlace malicioso, a través del cual, probablemente se solicitó a la parte demandante para que introdujera el código remitido por Banco Santander para autorizar el acceso a la banca digital.

La segunda negligencia la cometió en un ataque de "vishing", facilitando a través de este enlace malicioso a un tercero las OTP-SMS necesarias para ver los datos de seguridad de las tarjetas (CVV) y autenticar las operaciones de comercio electrónico. Si la cliente hubiese aplicado la diligencia debida en su responsabilidad de custodia tanto de sus credenciales de acceso a su banca online como de las claves de autorización de operaciones, las operaciones no reconocidas se habrían evitado, siendo estas circunstancias totalmente ajenas a la demandada y por las que no se le puede exigir responsabilidad por cuanto no fue ella quien propició tal situación, sino la propia actora, quien, con sus acciones, facilitó sus claves de acceso, respecto de las cuales tiene el deber de custodia, a un tercero, facilitándole así el acceso y la utilización de la tarjeta objeto de controversia. Una vez que el tercero accede a los servicios de banca digital y al apartado correspondiente a las condiciones de seguridad relativas a la utilización de los mismos, queda facultada la modificación del teléfono móvil y/o dirección de correo electrónico facilitados como datos de contacto para el intercambio de comunicaciones, para lo que se exige la introducción de una clave remitida en forma de OTP (One Time Password), o contraseña de un solo uso, enviada al nuevo dispositivo móvil.

SEGUNDO.- No existe controversia entre las partes en que los cargos fraudulentos en la cuenta bancaria fueron realizados tras recibir la actora un mensaje de texto en su teléfono

móvil, que era en apariencia procedente del Banco Santander, y en el que se advertía que su cuenta corriente había sido suspendida por razones de seguridad y que debía reactivarla accediendo a la misma mediante un enlace web inserto en el mensaje. Este mensaje que estaba incluido dentro de la línea de conversación que mantiene con BANCO SANTANDER, hizo que no sospechara inicialmente del fraude que estaba sufriendo. Una vez en dicha web, y creyendo, dado su origen, que era un enlace de fiar de la Entidad demandada, la demandante introdujo su usuario y contraseña.

Tras aportar la demandante dichos datos, se habrían producido los cargos fraudulentos a través de tres compras, que fueron cargadas en la tarjeta de débito las siguientes cantidades: 918 euros a las 18:04 horas, 929 euros a las 18:09 horas, y 899 euros a las 18:12 horas, todos los cargos por compras en la entidad Media Markt Online. La demandante, una vez tuvo conocimiento de los cargos, efectuó a las 18:10 horas una llamada al teléfono de atención al cliente de la entidad (915 123 123), y comunicó al departamento habilitado para denunciar este tipo de actuación fraudulenta lo sucedido, procediendo a dar de baja la tarjeta inmediatamente.

Conviene indicar, lo cual resulta relevante al caso de Autos, que **en el oficio remitido por la compañía de teléfonos DIGI SPAIN TELECOM, no aparecen reflejados los mensajes que la demandante debió recibir,** tal como manifiesta la demandada, **al objeto de autorizar las compras por internet efectuadas por el defraudador**. De hecho en dicho oficio se evidencia que el día 09/11/2022 recibió un mensaje a las 10:16:17 y el siguiente lo recibió a las 18:56:17, por lo que tampoco queda acreditado que se utilizara el doble factor de identificación para autorizar las compras fraudulentas.

TERCERO.- Sobre el contrato de cuenta corriente, señala la STS de 19 de diciembre de 1995 que *"es en el Derecho español una figura atípica que encuentra su singularidad o elemento causal, desde el punto de vista de los titulares de la cuenta, en el llamado "Servicio de Caja", encuadrable en nuestro Derecho dentro del marco general del contrato de comisión; el Banco en cuanto mandatario ejecuta las instrucciones del cliente (abonos, cargos...) y como contraprestación recibe unas determinadas comisiones, asumiendo la responsabilidad propia de un comisionista"*. La STS de 15 de julio de 1993 establece: *"Ha de hacerse constar que la cuenta corriente bancaria va adquiriendo cada vez más autonomía contractual, despegándose del depósito bancario que le servía de base y sólo actúa como soporte contable. En todo caso la cuenta corriente bancaria expresa siempre una disponibilidad de fondos a favor de los titulares de la misma contra el Banco que los retiene..."*, y añade: *"el Banco en cuanto mandatario, ejecuta las instrucciones del cliente, con sus abonos y cargos"*.

Por su parte, la STS de 25 de julio de 1991 recoge como una obligación esencial de la entidad bancaria la de conservar y devolver el dinero depositado, respondiendo de los menoscabos, datos y perjuicios que este haya sufrido por su negligencia.

En el mismo sentido, la STS de 12 de mayo de 2016 establece: *"con carácter general debe señalarse que, conforme a la naturaleza y función del contrato de cuenta corriente bancaria, el cercioramiento o comprobación de la veracidad de la firma del ordenante constituye un presupuesto de la diligencia profesional exigible a la entidad bancaria con relación a sus*

obligaciones esenciales de gestión y custodia de los fondos depositados por el titular de la cuenta, cuyo incumplimiento da lugar a la indemnización de daños y perjuicios, conforme a lo dispuesto en los artículos 1101 y 1106 del Código Civil".

La STS de 16 de diciembre de 2011 ya señalaba que *"[l]a disposición de fondos en una cuenta corriente o de depósito bancaria por parte de una persona que no podía hacerlo por no ser la titular ni estar autorizada por ésta supone un incumplimiento contractual (SS., entre otras, 23 de noviembre de 2000, 26 de noviembre de 2003, 9 de marzo de 2006) dada la obligación esencial del Banco de conservar y devolver los fondos depositados como se haya previsto en el contrato y se haya ordenado por las personas autorizadas para disponer de ellos, que, caso de incumplirse, da lugar a la indemnización de daños y perjuicios conforme a los arts. 1101 y 1106 del Código Civil "*.

A nivel legislativo, esa obligación de la entidad bancaria de conservación de los fondos depositados y de proceder sólo a su entrega cuando se cumplan los requisitos que se establecen en el propio contrato, y a favor de la persona de su titular, aparece recogida actualmente en el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, cuya finalidad ha sido transponer al Derecho español la Directiva 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) nº 1093/2010 y se deroga la Directiva 2007/64/CE .

El **artículo 41** del citado Real Decreto-ley 19/2018 establece: *"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".

El **artículo 42** del mismo texto legal establece: *"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 [...]".

El **artículo 43,** relativo a *"Notificación y rectificación de operaciones de pago no autorizadas o ejecutadas incorrectamente"*, señala : *"1. El usuario de servicios de pago obtendrá la rectificación por parte del proveedor de servicios de pago de una operación de pago no*

autorizada o ejecutada incorrectamente únicamente si el usuario de servicios de pago se lo comunica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación, incluso las cubiertas por el artículo 60, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo.

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

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

En el presente supuesto, no cabe duda (cuestión no controvertida) de que la demandante contactó con la demandada a través del teléfono de servicio al cliente, incluso antes de que se efectuara el último cargo en la tarjeta.

El **artículo 44,** que se refiere a la *"Prueba de la autenticación y ejecución de las operaciones de pago"*, establece: *"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 [...]".

El **artículo 45**, *"Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas"*, dispone lo siguiente: *"1. Sin perjuicio del artículo 43 de este real decreto- ley, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine. En su caso, el proveedor de servicios de pago del ordenante*

restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada.

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

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

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

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

Por último, el **artículo 46**, sobre *"Responsabilidad del ordenante en caso de operaciones de pago no autorizadas"*, establece: *"1. No obstante lo dispuesto en el artículo 45, el ordenante podrá quedar obligado a soportar, hasta un máximo de 50 euros, las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado, sustraído o apropiado indebidamente por un tercero, salvo que:*

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

b) la pérdida se debiera a la acción o inacción de empleados o de cualquier agente, sucursal o entidad de un proveedor de servicios de pago al que se hayan externalizado actividades. El ordenante soportará todas las pérdidas derivadas de operaciones de pago no autorizadas si el ordenante ha incurrido en tales pérdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el articulo 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".

CUARTO.- En el presente supuesto, la parte demandada ha aportado con su contestación a la demanda sendas certificaciones expedidas por la entidad "Redsys Servicios de Procesamiento, S.L." que, según se indica en la contestación a la demanda, es la procesadora de pagos en la industria de pagos en España y, en consecuencia, un tercero imparcial en las que se hace constar que las operaciones que son objeto de controversia fueron autorizadas, registradas con exactitud y contabilizadas y no se vieron afectadas por un fallo técnico o cualquier otra deficiencia. Se certifica igualmente que dichas operaciones fueron de comercio electrónico y el cliente fue autenticado mediante el método "3D Secure" en comercio electrónico La parte demandada explica en su contestación a la demanda que dicho método requiere, además de los datos de la tarjeta, la introducción de una clave numérica o contraseña de un solo uso (OTP: One Time Password), que BANCO SANTANDER remite al terminal móvil del cliente, el cual tiene que estar previamente validado frente a la entidad, y que permite confirmar la operación bancaria de que se trate.

Sentado lo anterior, la controversia se centra en determinar si la demandante incurrió o no en negligencia grave en el cumplimiento de sus obligaciones de custodia de las credenciales de seguridad, pues en tal caso vendría obligada a soportar todas las consecuencias económicas derivadas de las operaciones de pago realizadas por un tercero sin su autorización.

Pues bien, como se recoge en los fundamentos jurídicos precedentes, teniendo en cuenta las alegaciones efectuadas por las partes y la documental aportada, se considera acreditado que el día 9 de noviembre de 2022, la demandante recibió en su teléfono móvil un mensaje de texto, en el mismo hilo en el que había recibido con anterioridad otros mensajes procedentes de la entidad BANCO SANTANDER, en el que se le indicaba que su cuenta había sido suspendida temporalmente por razones de seguridad instándola a reactivarla actualizando sus datos en el enlace https://santander.soporte-Inicio.com. Confiando en que el mensaje había sido enviado por su banco, la actora pulsó en el enlace y se abrió lo que aparentemente era la aplicación de

banca electrónica de BANCO SANTANDER, donde introdujo su usuario y contraseña. Horas más tarde, a las 18:01 horas, obra en Autos documental que acredita que recibió un mensaje en su dispositivo móvil que decía literalmente *"Santander: NO COMPARTA ESTE CÓDIGO CON NADIE: el código para el registro del dispositivo seguro es N013N463"*, y seguidamente recibió otro mensaje en el mismo hilo, lo que provoca sin género de dudas creer que se trata del mismo remitente, que indicaba *"Finalice la configuración para el correcto funcionamiento de su cuenta: https://santander.soporte-Inicio.com".* Es evidente que la demandante pinchó nuevamente en el enlace e introdujo el código facilitado en el mensaje anterior, pero ello no puede ser considerado negligente, toda vez que los mensajes se recibían en el mismo hilo que los mensajes remitidos verdaderamente por la Entidad demandada.

Señala la SAP de Valladolid de 19 de octubre de 2022 que *"La realidad de prácticas delictivas como el referido "phising", hace exigible aumentar las medidas de seguridad específicas, como recuerda la SAP de Barcelona, 7 de marzo de 2013, pues el banco no puede ofrecer un sistema online sin adoptar las medidas de seguridad necesarias, en el mismo sentido que hizo la ya citada sentencia de la Audiencia Provincial de Alicante, de 12 de marzo, aplicando los criterios que expresaba la STS de 18 de marzo de 2016, que imponía ponderar, en este tipo de supuestos, factores tales como la causa del evento dañoso, la concurrencia de un déficit de la seguridad que legítimamente cabía esperar y la facilidad probatoria correspondiente a cada una de las partes.*

Como se afirma en dicha sentencia, no basta con medidas genéricas de protección o avisos estereotipados de cuidado, sino que "la seguridad de las operaciones bancarias precisa de soluciones tecnológicas avanzadas a los efectos de garantizar tanto la autenticidad como la integridad y confidencialidad de los datos", sin que se repute suficiente los avisos genéricos de los bancos, a través de su web, que ostentarían la calificación de "fórmulas predispuestas ", vacías de contenido".

La SAP de Madrid de 13 de enero de 2023, por su parte, establece que *"... la entidad que presta el servicio de pago solo puede exonerarse de responsabilidad, mediante la prueba de culpa grave del usuario que emite la orden de pago. En el supuesto objeto de recurso, estamos ante un fraude llamado "phishing", por el que se suplanta la identidad de la entidad bancaria para obtener información sobre las claves o credenciales de las cuentas bancarias o tarjetas de crédito/débito. Se envía un correo electrónico con la apariencia de ser remitido por la entidad bancaria, que contiene un enlace a una pagina que aparenta ser sitio oficial de ésta, pero que en realidad pertenece a un dominio bajo control del phiser.*

Se reconoce por la propia demandada, que la demandante fue víctima de una estafa, que la llevó a creer que estaba operando en la WEB del Banco de Santander, pero necesariamente era una WEB distinta y, como consecuencia del engaño, en ella facilitó todas sus claves personales de acceso a la banca online o introdujo los códigos SMS/OPT remitidos para cada operación o se instaló desde dicha WEB algún troyano en el dispositivo móvil de la demandante. Se aduce que, los certificados de REDSYS y SMS/OTP, acreditan que las compras se autorizaron mediante un OTP previo y los SMS se remitieron al teléfono del que la actora era titular por lo que, o la actora introdujo los códigos recibidos o el dispositivo móvil sufrió una infección/hackeo a través de un malware.

Sobre la jurisprudencia aplicable, la sentencia de la Audiencia Provincial de Madrid, sección 11a I 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".

Por último, la reciente SAP de Pontevedra de 23 de marzo de 2023 señala que *"A la hora de estudiar la concurrencia de negligencia grave del usuario del servicio de pago online, 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 -por todas, SS. AP Pontevedra (Secc. 6ª) 21.12.21 y Madrid (20ª) 20.5.2022 , en la línea de lo razonado en SS. AP Valencia (6ª) 13.6.2022 , Granada (5ª) 20.6.2022 y Badajoz (3ª) 21.6.2022"*.

Así las cosas, valorando las circunstancias concurrentes en el presente caso, no cabe apreciar negligencia grave por parte de la demandante en el cumplimiento de su obligación de proteger sus credenciales de seguridad. No puede tacharse de gravemente negligente la conducta de quien, tras recibir en el mismo canal en el que recibe habitualmente las comunicaciones procedentes de su banco un mensaje de texto en el que se le informa de la suspensión de su cuenta por razones de seguridad, facilitándole un enlace para poder reactivarla, decide pulsar en ese enlace e introducir su usuario y contraseña, dado que, para una persona no experta, no es fácil detectar que el mensaje recibido es fraudulento o que la

web a la que ha accedido a través del enlace facilitado es falsa. Como señala la SAP de Madrid de 20 de mayo de 2022 , *"...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 "phising" es de una complejidad y grado de perfección, difícilmente detectable por un cliente de las características del demandante. 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, 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 la demandante, por el hecho de haber pinchado el link que se le ofrecía y facilitar los datos y clave de la tarjeta.

QUINTO.- 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 phising, 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 antiphising 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.

Por todo lo expuesto, al no resultar acreditado que la actora incurriera en negligencia grave en el deber de custodia de sus credenciales, siendo la parte demandada la que debería haber implementado un mecanismo antiphishing de protección de los usuarios frente al uso fraudulento por parte de terceros de páginas que imitan a las oficiales para hacerse con las credenciales de los clientes, procede estimar en lo sustancial las pretensiones de la parte actora, condenando a la entidad BANCO SANTANDER a pagar a la demandante la suma de

2.346 euros, más los intereses legales desde la fecha de presentación de la primera reclamación extrajudicial frente al banco, hasta la de esta sentencia (artículos 1.100, 1.101 y 1.108 del Código Civil), devengándose a partir de esta fecha los intereses procesales del artículo 576 de la Ley de Enjuiciamiento Civil hasta el completo pago.

SEXTO.- Al haber sido estimada en lo sustancial la demanda interpuesta, procede imponer las costas del presente procedimiento a la parte demandada (artículo 394.1 de la Ley de Enjuiciamiento Civil).

Vistos los artículos citados y demás de general y pertinente aplicación,

FALLO

Que **ESTIMANDO** o la demanda formulada por DON/DOÑA ADUA EL-MAKHTARI AMAR (42204894-D), contra la entidad BANCO SANTANDER S.A. (A-39000013):

- Declaro la responsabilidad de la mercantil demandada en las operaciones objeto de este procedimiento, que fueron realizadas con la tarjeta de la actora.

- Condeno a la mercantil demandada a abonar a la actora la cantidad de DOS MIL TRESCIENTOS CUARENTA Y SEIS EUROS (2346 €), en concepto de daños y perjuicios, más los intereses legales desde la primera reclamación judicial.

- Se impone las costas del procedimiento a la mercantil demandada.

Llévese certificación de la presente resolución a los autos de su razón, uniéndose el original al libro de sentencias de éste Juzgado.

Notifíquese la presente resolución a las partes conforme lo establecido en el Art. 248-4º de la Ley Orgánica del Poder Judicial. con indicación de que contra esta sentencia NO cabe recurso de Apelación.

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

Así lo acuerda, manda y firma, [redacted] Juez sustituto del Juzgado de 1ª Instancia n.º 2 de San Bartolomé de Tirajana y su Partido.- Doy fe.

EL/LA JUEZ