ADMINISTRACIÓN DE JUSTICIA

JUZGADO DE PRIMERA INSTANCIA Nº 3
Avenida Pedro San Martin S/N
Santander
Teléfono: 942357022
Fax.: 942357023
Modelo: TX901

Puede relacionarse telemáticamente con esta Admón. a través de la sede electrónica.
(Acceso Vereda para personas jurídicas)
https://sedejudicial.cantabria.es/

Proc.: **JUICIO VERBAL (250.2)**
Nº.: **0000452/2022**
NIG: 3907542120220006375
Materia: Obligaciones
Resolución: Sentencia 000555/2022

Intervención:	Interviniente:	Procurador:
Demandante		JOSÉ MIGUEL ARAUJO SIERRA
Demandado	BANCO SANTANDER SA	ISIDRO MATEO PEREZ

SENTENCIA

En Santander, a trece de diciembre de dos mil veintidós.

Vistos por la Ilma. Sra. Dª María Rosa Martínez López, Magistrada-Juez titular del Juzgado de Primera Instancia número 3 de Santander, los presentes autos de **JUICIO VERBAL sobre reclamación de cantidad**, seguidos ante este Juzgado bajo el número **452/2022**, a instancia de D. representado por el Procurador, D. José Miguel Araujo Sierra y asistida por el Letrado D. Emilio San Miguel Laso contra BANCO SANTANDER, S.A representada por el Procurador, D. Isidro Mateo Pérez y asistida por los Letrados, D. Gascón Durand Baquerizo y D. Juan Tomás Bilbao Goikoetxea.

ANTECEDENTES DE HECHO

PRIMERO. El Procurador, D. José Miguel Araujo Sierra, en la representación indicada, mediante escrito que por turno de reparto correspondió a este Juzgado, presentó demanda de juicio verbal en la que, tras alegar los hechos y fundamentos de derecho que estimaba de aplicación, terminaba solicitando se dictara una sentencia por la que, estimando de forma íntegra la demanda, se condene a BANCO SANTANDER, S.A a que reintegre al actor la cantidad de 5.870 euros que fueron trasferidos a otra cuenta bancaria sin su consentimiento, más el interés legal correspondiente desde el 27 de diciembre de 2020, con expresa condena en costas a la parte demandada.

SEGUNDO. Admitida a trámite la demanda por decreto de 2 de junio de 2022, se emplazó a la demandada para que en el plazo de veinte días presentase escrito de contestación a la demanda.

El Procurador, D. Isidro Mateo Pérez, en nombre y representación de BANCO SANTANDER, S.A, presentó escrito de contestación en el que, tras

alegar los hechos y fundamentos de derecho que estimaba de aplicación, terminaba solicitando se dicte sentencia por la que se desestime íntegramente la demanda, con imposición de las costas procesales.

TERCERO. Por diligencia de ordenación de 5 de julio de 2022 las partes, peritos y testigos fueron citados al acto de la vista para el día 24 de noviembre de 2022 a las 10.30 horas.

Llegado el día y la hora se celebró el acto de la vista con la comparecencia de ambas partes. La parte actora propuso, como medios de prueba, la documental por reproducida y más documental. La demandada, documental obrante en autos, e interrogatorio de parte. Todos los medios probatorios fueron admitidos. Tras su práctica, las partes formularon de forma oral sus conclusiones, quedando las actuaciones pendientes del dictado de la presente resolución.

FUNDAMENTOS DE DERECHO

PRIMERO. La parte actora, , interesa en esta litis que la entidad bancaria, BANCO SANTADER, S.A, sea condenada al pago de la cantidad de 5.870 euros, al entender que la demandada actuó en contra de las previsiones legales del artículo 44 y 45 del Real Decreto-Ley 19/2018, de 23 de noviembre de servicios de pago y otras medidas urgentes en materia financiera, al no devolver al actor, como usuario del oportuno servicio de pago, tras dar a conocer a la entidad bancaria que se había llevado a cabo una operación de pago no autorizada, en concreto, una trasferencia por importe de 5.870 euros, el importe así indicado, sin que el Sr. incurriera en negligencia grave desde el momento en que el SMS que da origen a la operación fraudulenta objeto de litis se recibió dentro del canal de mensajería que el actor mantenía abierto con tal entidad financiera, presentando de inmediato la oportuna reclamación ante el BANCO SANTANDER, S.A.

La demandada, BANCO SANTANDER, S.A, se opone a tal pretensión. Reconociendo de la parte actora fue víctima de un caso de "phising", niega cualquier tipo de responsabilidad en el resultado final al entender que fue el propio usuario quien incumplió las instrucciones y consejos implementados por la entidad bancaria para evitar este tipo de fraudes, incumpliendo con ello todas las obligaciones contractuales suscritas y asumidas dirigidas a ello, siendo ciertamente ilustrativa, completa, extensa y exhaustiva la información que proporciona al propia entidad bancaria en las dos cláusulas, claras y fáciles de comprender, que se hallan en el contrato "Multicanal" suscrito entre las partes. Mantiene que la demandada que la operación fraudulenta objeto de litis se llevó a efecto como consecuencia de un actuar negligente del actor (accede a un link que no proviene del BANCO SANTANDER, S.A, cede sus credenciales en lugar de comunicar tal incidencia a la entidad e introduce el código de registro seguro del dispositivo) haciendo caso omiso a las

advertencias que constaban en el contrato Multicanal suscrito entre las partes, cediendo sus credenciales a un tercero quien posteriormente realizó la trasferencia fraudulenta. Argumenta BANCO SANTANDER, S.A que fue el actor quien incumplió las obligaciones contractuales asumidas al efecto y las disposiciones del Real Decreto 19/2018 de 23 de noviembre de servicios de pago, entre ellas, el deber de custodiar las claves y adoptar todas las medidas que estén a su alcance para proteger los elementos de seguridad de que vayan provistos, sin que en momento alguno se haya puesto en entredicho el sistema de seguridad del BANCO SANTANDER ni su correcto funcionamiento, habiendo actuado la entidad bancaria respetando de forma escrupulosa los protocolos existentes en materia de prevención de fraudes. Consecuencia de lo así expuesto, entiende la entidad bancaria ahora demandada, que el perjuicio sufrido por el actor no trae como causa la acción o inacción de BANCO SANTANDER, S.A quien no pudo evitar la operación fraudulenta al provenir de una actividad delictiva cometida por un tercero, provocando el correspondiente quebrante económico, mediando en todo caso una palmaria negligencia del propio Sr.

SEGUNDO. De la documental obrante en las actuaciones se colige que el actor, , sobre las 17:07 horas del día 24 de diciembre de 2020 recibió un SMS en su teléfono personal dentro del mismo hilo de mensajes recibidos hasta la fecha a través del canal de mensajería que mantenía abierto con el BANCO SANTANDER, S.A, informando de lo siguiente, "*Acceso desconocido detectado en su cuenta. Su cuenta ha sido bloqueada temporalmente. Puede obtener acceso de forma segura desde: https://rb.gy/doxs4v*". D. [redacted] accede al citado link, entrando en una página web que, siendo falsa, resultaba muy parecida o similar a la del BANCO SANTANDER, S.A, facilitando su DNI, clave de acceso y firma electrónica, permitiendo al "phiser" instalar en su teléfono móvil la APP del BANCO SANTANDER, entrando con el usuario del , recibiendo este último un SMS un código de registro seguro del dispositivo seguro, siendo introducido por el actor. El día 26 de diciembre de 2020 el actor se percata que se había llevado a efecto una transferencia bancaria por él no autorizada desde su cuenta bancaria a otra cuenta abierta en Francia a nombre de un tercero por él desconocido y que responde al nombre de "Marie Berengere" por importe de 5.870 euros. El 20 de enero de 2021 BANCO SANTANDER, S.A remitió una comunicación a PFS Card Servises Ireland Limited solicitando la retrocesión de tal trasferencia, siendo tal petición rechazada al no hallarse el dinero trasferido en la cuenta bancaria del defraudador.

Como nos recuerda la Sentencia número 689/2022 de 19 octubre, de la Sección Tercera de la Audiencia Provincial de Valladolid, JUR\2022\368081, "*La cuestión enjuiciada se enmarca en el ámbito de la contratación electrónica, que es aquella en que la oferta y la aceptación se tramita por medios electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones. La normativa aplicable en este ámbito, como condensa la SAP de Zaragoza de 1 de julio de 2022 (PROV 2022, 278257) , se recoge en la ley 34/02, de 11 julio de "Servicios de la Sociedad de la Información" en cuyos artículos 27 y 28 establece la obligación del prestador de servicios de una información al destinatario que sea clara, comprensible e inequívoca; el Art 46 de la ley 7/96, de 15 de enero (RCL 1996, 148, 554) de*

Ordenamiento del Comercio Minorista (transposición de la Directiva 97/7 CE) (LCEur 1997, 1493); y la ley 22/07 de 11 julio (RCL 2007, 1356) (art. 12) de Comercialización a Distancia de Servicios Financieros destinados a Consumidores (transposición de Directiva 2002/65/CE) (LCEur 2002, 2613), que establecen una protección especial al consumidor frente a la incertidumbre jurídica que produce el desarrollo de Internet y las nuevas tecnologías, que se materializa en la inmediata reposición o anulación de los cargos indebidos al titular del elemento o medio de pago utilizado indebida o fraudulentamente. Por último, la Ley 16/09, de 13 de noviembre (RCL 2009, 2193y RCL 2010, 1119), de Servicios de Pago, cuya finalidad es el reforzamiento y protección de los usuarios de los servicios de pago, cuyo artº 31 establece que ... " en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante le devolverá de inmediato el importe de la operación no autorizada y, en su caso, restablecerá la cuenta de pago en que haya adeudado dicho importe al estado que habría existido de no haberse efectuado la operación de pago no autorizada". Salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante (art 32 LSP (LEG 1922, 70)), 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). Estas prevenciones se implementan en el citado R.D.- ley 19/2018 (LCV 2018, 283), respecto a lo dispuesto en la ley 16/2009, de 13 de noviembre, en cuyo art. 44.2 se establece que 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. Y en su numeral tercero se impone al proveedor de servicios de pago, y, en su caso, al proveedor de servicios de iniciación de pagos, acreditar que el usuario del servicio de pago cometió fraude o negligencia grave. En cuanto a la diligencia exigible a la entidad bancaria, que de manera incuestionable se beneficia de la extensión generalizada de este tipo de servicios de banca on line evitando los costes asociados a la atención de sus clientes en la red comercial mediante oficinas y personal, el art. 12 bis de la ley 34/02, de Servicios de la Sociedad de la información y de Comercio Electrónico obliga al proveedor de dichos servicios a realizar una información a sus clientes permanente, fácil, directa y gratuita sobre niveles de seguridad, restricción de correos no solicitados, y filtrado de servicios de Internet no deseados". Continúa indicando la referida Sentencia, "*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 (PROV 2013, 171665) , pues el banco no puede ofrecer un sistema on line 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 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 " formulas predispuestas", vacías de contenido.

En el supuesto de autos, el actor recibió el SMS fraudulento en el mismo hilo de mensajes dentro del canal de mensajería utilizado hasta ese momento con la entidad bancaria, siendo remitido seguidamente a una página web que, si bien resultaba ser falsa, lo cierto es que tenía la misma apariencia que la web oficial de la entidad bancaria, hallándonos por ello ante "*actos de emulación con apariencia de autenticidad reproduciendo las fórmulas que suelen utilizarse en las comunicaciones con los clientes a través de la banca on line. Precisamente la facilidad y sencillez en el manejo de este tipo de datos conlleva el riesgo del fraude electrónico, sin que sea exigible al cliente medio un conocimiento informático sobre las eventuales técnicas de apropiación de sus datos personales, expuestos en la red en aras de posibilitar la agilidad y tratamiento masivo de transacciones electrónicas. Comparte esta sala el criterio que expresan las sentencias citadas en cuanto a que la mera advertencia protocolaria o estereotipada acerca del riesgo del fraude pueda servir para excluir la responsabilidad de la entidad bancaria, conforme a la normativa incoada*"

Tratándose, como en el supuesto de autos, de una trasferencia no autorizada, traemos a colación la Sentencia número 107/2018 de 12 marzo, de la Sección 8ª de la Audiencia Provincial de Alicante:

"*Para una mejor respuesta al motivo, y dado que la responsabilidad que se imputa a la entidad, derivada de la ejecución de una transferencia no autorizada por la titular de la cuenta de la cliente demandante realizada a través del sistema de banca online, lo es en tanto prestadora de servicios de pago a través del modelo de banca virtual puesta a disposición de su cliente, concretaremos el régimen legal y contractual en el que se desenvuelve la banca electrónica, cuáles son las obligaciones el prestador y del usuario conforme a la legislación aplicable, el significado jurídico de las órdenes de pago y el marco de responsabilidades que del mismo resulta y la jurisprudencia más señalada al respecto.*

Pues bien, tales aspectos pueden concretarse en los puntos que seguidamente numeramos.

1.- La transferencia bancaria es un servicio que forma parte del contrato de servicio de caja entre un proveedor de servicios de pago (el banco) y sus clientes y sirve de medio de pago mediante el débito en la cuenta del ordenante y abono en la del beneficiario, tratándose en suma de un procedimiento financiero de movimiento de la moneda.

Se trata de un medio de pago consistente en una orden dada al banco (banco emisor) por parte de un cliente (ordenante) a fin de que, con cargo a su cuenta, abone un determinado importe en otra cuenta del mismo o distinto banco (banco destinatario) abierta a nombre de un tercero (beneficiario) o del propio ordenante.

2.- Las transferencias se regulan, trasponiendo la Directiva 2007/64/CE (LCEur 2007, 2042) del Parlamento Europeo y del Consejo Europeo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE (LCEur 1997, 1493) , 2005/65/CE (LCEur 2005, 2672) y 2006/48/CE (LCEur 2006, 1495) y por la que se deroga la Directiva 97/5/CE (LCEur 1997, 338) , en la Ley 16/2009, de 13 de noviembre (RCL 2009, 2193y RCL 2010, 1119) , de Servicios de Pago (LSP).

La Directiva 2007/64/CE (LCEur 2007, 2042) ha sido derogada por la Directiva UE 2015/2366 (LCEur 2015, 2231) 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 (LCEur 2002, 2613), 2009/110/CE (LCEur 2009, 1494) y 2013/36/UE (LCEur 2013, 928) y el Reglamento UE nº 1093/2010 (LCEur 2010, 1748) y se deroga la Directiva 2007/64/CE.

3.- La LSP define la orden de pago como toda instrucción cursada por un ordenante o beneficiario a su proveedor de servicios de pago por la que se solicite la ejecución de una operación de pago" (art. 2.16 LSP).

4.- Desde un punto de vista contractual toda transferencia constituye una forma de ejecución de obligaciones contractuales previamente asumidas, ejecución obligada cuando se dan las condiciones pactadas, de ordinario, que haya provisión de fondos.

Es por ello que se entiende que la orden de transferencia constituye una declaración de voluntad o mandato (en el sentido del art. 254 CCo (leg 1885, 21)) en virtud del cual el banco asume la realización de transferencias por cuenta del cliente como parte del contrato de servicio de caja.

5.- Dado el carácter negocial de la orden de pago, ésta puede pactarse que tenga lugar en cualquier forma, incluida la electrónica.

En particular, el consentimiento a operaciones de pago por el usuario en el ámbito de la banca electrónica supone que el cliente deba haber firmado un contrato de adhesión a los servicios de banca electrónica.

El art. 25.1IILSP establece al respecto que "el ordenante y su proveedor de servicios de pago acordarán la forma en que se dará el consentimiento así como el procedimiento de notificación del mismo", negocio jurídico que determina que la transferencia se entienda autorizada por el ordenante de acuerdo con el mismo precepto de la LSP.

El consentimiento del ordenante se prestará, según el medio utilizado para prestar dicho consentimiento, mediante, o la firma de la autorización y orden de transferencia correspondiente, o verbalmente a través de la vía telefónica o a través de banca por internet o electrónica.

6.- Tanto en la banca telefónica como por internet, el proveedor de servicios de pago, o lo que es lo mismo, el banco emisor, debe implementar las medidas necesarias para asegurar la autenticación e identidad del ordenante a la hora de prestar su consentimiento.

Por ello y para su ejecución, el banco debe comprobar en todo caso la autenticidad de la orden y, salvo pacto en contrario, que existe saldo suficiente. 7.- De ordinario, para la realización de transferencias ordinarias con cargo a una cuenta vinculada es preciso que el cliente haya de autenticar la operación mediante la introducción de las claves previamente facilitadas por la entidad de crédito con la que contrata, con respecto a las cuales tendrá unos deberes de custodia.

8.- La falsedad de la transferencia (es decir, que el ordenante no sea el titular de la cuenta) es un riesgo a cargo del banco porque, en principio, el deudor sólo se libera pagando al verdadero acreedor por lo que, si el banco cumple una orden falsa, habrá de reintegrar en la cuenta correspondientes las cantidades cargadas. Una excepción a esta distribución de riesgos se produce en el caso de que el titular haya creado o elevado el riesgo de falsificación de forma imputable en el caso concreto (STS 15 de julio de 1988 (RJ 1988, 5717)).

9.- La doctrina había abogado con anterioridad a la Ley de Servicios de Pago a favor de aplicar en el caso de la falsificación de una orden de transferencia, la solución que para la falsificación de un cheque establece el art. 156 de la Ley Cambiaria y del Cheque (RCL 1985, 1776, 2483) que establece que el daño que resulte del pago de un cheque falso o falsificado será imputado al librado, a no ser que el librador haya sido negligente en la custodia del talonario de cheques, o hubiere procedido con culpa.

Este es el principio se recoge hoy en el art. 30, 31 y 32 LSP. En concreto, dispone el art. 30 LSP que " 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 a su proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud, y que no se vio afectada por un fallo técnico o cualquier otra deficiencia. 2. A los efectos de lo establecido en el apartado anterior, el registro por el proveedor de servicios de la utilización del instrumento de pago no bastará necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que este actuó de manera fraudulenta o incumplió deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 27". Y en el art. 31 se dice que " en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante le devolverá de inmediato el importe de la operación no autorizada y, en su caso, restablecerá en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada. "

10.- Los servicios que prestan las entidades de crédito a sus clientes a través de su oficina virtual se desenvuelven en redes TCP/IP (Internet) o WAP (comunicaciones móviles).

11.- Siendo Internet una red pública de comunicaciones, la seguridad de las operaciones bancarias precisa de soluciones tecnologías avanzadas a los efectos de garantizar tanto la autenticidad como la integridad y la confidencialidad de los datos.

Por estos motivos las entidades prestadoras del servicio de banca online deben dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones.

Consecuencia derivada de la omisión, insuficiencia o defectuoso funcionamiento de las adoptadas es que han de ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema.

12.- La banca electrónica está siendo objeto de transferencias no autorizadas por el cliente y que vienen antecedidas por el método delictivo conocido como phishing que constituye una modalidad específica de fraude informático que visualiza las deficiencias de seguridad del sistema informático de una entidad y que trae causa en el uso de las redes telemáticas.

De acuerdo con la Agencia Española de Protección de Datos (Resolución del Expediente Nº: E/00762/2004, DE 24 DE MAYO DE 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 ".

13. -La responsabilidad en estos supuestos no puede atribuirse directamente al supuesto ordenante de la transferencia por entenderse ésta autorizada al haberse realizado de acuerdo con los sistemas de autenticación del banco.

Los sistemas de autenticación se establecen por los proveedores de servicios de pago y si un banco no ha sido capaz de limitar el acceso al canal de banca electrónica no puede pretender que el presunto ordenante víctima de esta práctica fraudulenta sea el único responsable, pues es el banco quien tiene responsabilidad respecto del buen funcionamiento y la seguridad del mismo.

Dispone a tal efecto el art. 25.1º LSP que " Las operaciones de pago se considerarán autorizadas cuando el ordenante haya dado el consentimiento para su ejecución. A falta de tal consentimiento la operación de pago se considerará no autorizada".

Por tanto, en el caso de órdenes de pago y transferencias fraudulentas esta disposición supone que si la orden de pago o transferencia emitida por el cliente contiene una manifestación voluntad que actúa como causa del pago al tercero o la remisión de fondos al beneficiario, a "sensu contrario" puede afirmarse que sin dicha declaración de voluntad la operación de pago o transferencia de fondos se considerará no autorizada.

14.- Las medidas de seguridad no solamente están destinadas a proteger la seguridad de las órdenes de pago emitidas por los clientes, sino que su eficacia exonera a las entidades de crédito de sus responsabilidades frente a las órdenes de pago no emitidas por sus clientes de tal forma que el incumplimiento de este específico deber de vigilancia da lugar a una responsabilidad por "culpa in vigilando" o responsabilidad objetiva por el mal funcionamiento de los servicios de banca electrónica.

En base a este fundamento la Sentencia de la Audiencia Provincial de Barcelona, Sección 11, de fecha 23 de julio 2015, declaró la responsabilidad de Barclays Bank, S.A. a pagar a una clienta la cantidad de 9.979 € por cargos y extracciones de efectivo no autorizados que tuvieron su origen en la introducción por los delincuentes de un mensaje fraudulento en la página oficial del banco a través del cual se canalizó la operación.

Este mismo hecho, considerado una infracción de los deberes de vigilancia del banco, fue la causa por la que el Banco de Santander fue condenado por sentencia dictada por la Audiencia Provincial de Valencia, Sección 9 de fecha 23 de abril de 2013 (PROV 2013, 254877) a restituir a su cliente la cantidad de 42.500 €.

La Sentencia de la Audiencia Provincial de Barcelona (Sección Decimocuarta) de fecha 7 de marzo de 2013 (PROV 2013, 171665) condenó a la CAIXA DE ESTALVIS DE CATALUNYA (actualmente CATALUNYA BANK,S.A.) a devolver a una empresa víctima de "phising" la cantidad de 32.099 € por cuanto la entidad bancaria no adoptó las medidas de seguridad adicionales previstas en las Condiciones Generales del contrato al haberse producido movimientos inusuales de fondos de la cuenta corriente y ser transferidos a cuentas sospechosas de su control por " muleros" que la entidad debió detectar. Asimismo, la entidad bancaria permitió que se sobrepasara el límite de disposición diario de las cuentas pactado en el contrato.

La Sentencia de la Audiencia Provincial de Zaragoza de fecha 14 de mayo de 2013 (PROV 2013, 197766) condenó a BARCLAYS BANK a reintegrar 20.947 € al cliente víctima de phising. La Sentencia señala que la Ley de Servicios de Pago expresa con claridad que, salvo una tardanza injustificada del usuario del servicio de banca electrónica en comunicar la irregularidad de las operaciones, será el banco quien deberá devolverle de

inmediato el importe de la operación no autorizada y, en su caso, restablecerá la cuenta de pago en que haya adeudado dicho importe al estado que habría existido de no haberse efectuado la operación de pago no autorizada. Por ello y salvo actuación fraudulenta o negligencia grave del titular de la cuenta, la responsabilidad de la operación es del banco al que corresponde además probar el correcto funcionamiento del sistema informático.

La Sentencia de la Audiencia Provincial de Madrid de 4 de mayo de 2015 (PROV 2015, 151311) condenó a CAJAMAR a abonar a la víctima la cantidad de 17.390'35 €. En este caso la víctima facilitó sus claves y contraseñas a una página web clonada que simulaba ser la del banco. La sentencia razona que el artículo 31 de la Ley 16/09 de 13 de noviembre de Servicios de Pago establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago con inversión de la carga probatoria al presumirse la falta de autorización de la orden de pago o transferencia si el cliente lo niega.

15.- Por su parte los clientes tienen un deber de custodia respecto de sus claves de acceso a la banca electrónica similares al que tienen los titulares de tarjetas de crédito respecto de su correspondiente número secreto.

En este sentido la Sentencia de la Audiencia Provincial de Sevilla, Sección Quinta, de fecha 26 de mayo de 2014 (PROV 2014, 221495) desestimó la demanda formulada contra BARCLAYS BANK en reclamación de la cantidad de 11.703'05 €. El fundamento de dicha desestimación fue la imputación de responsabilidad al cliente por imprudencia o" negligencia grave" al haber hecho caso omiso de las advertencias y avisos de seguridad del banco, en particular de aquel que rezaba " Barclays nunca le pedirá más de una coordenada de seguridad, ni por correo ni en la web". A pesar de esta advertencia los clientes introdujeron la totalidad de las claves de su tarjeta de coordenadas en una ventana emergente que inmediatamente se abrió en la página web de la entidad bancaria.

Por su parte la Sentencia de la Audiencia Provincial de Las Palmas de Gran Canaria de fecha 20 de diciembre de 2012 (AC 2013, 1010) también desestimó la reclamación frente al Banco Santander Central Hispano S.A., y lo hace con un argumento alejado de las previsiones analizadas de la Ley de Servicios de Pago que ni tan siquiera cita. Para esta sentencia el banco se limitó a ejecutar una orden de pago ordenada por quien al parecer era su cliente y por ello no incurrió en responsabilidad alguna que le obligase a reintegrar las cantidades transferidas.

16.- En consecuencia, hay responsabilidad bancaria por los defectos de seguridad del sistema que determina la ejecución de órdenes de pago no autorizadas por su cliente, con la única excepción de que el banco acredite la culpa o negligencia de la víctima.

Dice al respecto el art. 32.2 LSP que " El ordenante soportará el total de las pérdidas que afronte como consecuencia de operaciones de pago no autorizadas que sean fruto de su actuación fraudulenta o del incumplimiento, deliberado o por negligencia grave, de una o varias de sus obligaciones con arreglo al artículo 27. "

Estas obligaciones a cargo del usuario respecto a las entidades de crédito se concretan - art 27LSP – en tomar las medidas razonables a fin de proteger los elementos de seguridad personalizados y en caso de extravío, sustracción o utilización no autorizada del instrumento de pago, notificarlo sin demoras indebidas al proveedor de servicios de pago o a la entidad que este designe en cuanto tenga conocimiento de ello.

17.- Constituye por tanto obligación esencial de las entidades prestadoras del servicio de banca online el dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones por lo que, en el supuesto de insuficiencia o mal funcionamiento de las adoptadas, deben ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema.

18.- A tal efecto, aparte el uso de protocolos seguros de cifrado de información que permite establecer una conexión cifrada entre el usuario y la entidad de crédito impidiendo con ello el que terceras personas no autorizadas puedan acceder a la información confidencial que viaja a través de la Red, los sistemas de seguridad empleados por las entidades de crédito en sus operaciones electrónicas deben estar basados en última instancia en infraestructuras de claves públicas que garantizan la autentificación del usuario mediante el uso de claves de firma digital.

19.- Normalmente las medidas establecidas por los bancos se articulan en varios niveles de seguridad complementarios y compatibles entre sí.

El primer nivel consiste en un código de usuario y contraseña o clave secreta privada que cada cliente podrá configurar para acceder a la oficina virtual.

En otro nivel de seguridad se sitúa la denominada tarjeta de coordenadas proporcionada por la entidad bancaria a cada usuario que consiste en un código de autorización de las operaciones, único y personal para cada una de ellas. Estas claves se exigen al cliente para realizar cualquier operación que no sea una mera consulta de saldos como puede ser el movimiento de dinero entre cuentas, compras o transferencias.

Un tercer nivel lo constituye las comunicaciones con el cliente de las operaciones que se ejecutan en la red, advirtiéndole de las mismas a fin de tomar conocimiento inmediato y eficaz caso de fraude.

20.- Otra medida distinta de la tarjeta de coordenadas lo constituye el empleo de claves aleatorias perecederas de un solo uso ("One time password") que evitan el riesgo de copia, pérdida o robo de las claves de seguridad, sistema de seguridad que cuenta además con el refrendo de la European Banking Authority (Autoridad Bancaria Europea). Estas claves aleatorias se remiten por la entidad de crédito al teléfono móvil del cliente mediante SMS con la finalidad de autorizar la operación.

21.- El uso de la firma digital permite a la entidad de crédito imputar la autoría de la orden de pago al cliente presumiéndose por ello que ha sido

válidamente emitida por éste. Sobre este particular debe recordarse que la firma electrónica avanzada o reconocida respecto de los datos consignados en forma electrónica tiene el mismo valor que la firma manuscrita en relación con los consignados en papel (artículo 3 apartados 2 y 4 de la Ley 59/2003, de 19 de diciembre (RCL 2003, 2975) de Firma Electrónica).

22.- Aparte de estas medidas, las entidades de crédito introducen advertencias de seguridad -recomendaciones- en sus páginas web oficiales, entre otras y como más habitual, que en ningún caso la entidad solicitará al cliente sus claves confidenciales previniéndoles del riesgo de facilitar sus datos confidenciales a terceros.

En cuanto a la pretendida información facilitada por la entidad bancaria al actor sobre las medidas de seguridad a adoptar expuestas en el clausulado del contrato suscrito entre las partes, la referida Sentencia afirma lo siguiente:

"Pues bien, y a pesar de las afirmaciones del recurrente sobre la implementación de un modelo seguro de banca online, es lo cierto que ninguna prueba objetiva se aporta, lo que no implica que el Tribunal niegue que el sistema fuera genéricamente seguro, porque es consustancial al propio sistema, sino porque no consta qué medidas en particular constituían el modelo de actuación progresivo y de respuesta ante las distintas formas o riesgos de acceso ilegítimo a la plataforma por parte de terceros no autorizados, siempre en progreso y evolutivas, y de protección de los productos de los clientes accesibles a través de dicha plataforma telemática. Desde luego, en caso alguno bastaban los avisos y advertencias a los clientes. En efecto, tampoco sirve de excusa 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 -que por lo demás, conforma una concreta obligación contractualmente asumida, tal cual ya hemos apuntado- en tanto no es sino una fórmula predispuesta por el profesional, vacía de contenido al resultar contradicha por los hechos que no son otros que las barreras informáticas efectivas que deben estar implementando el sistema. Por tanto, a falta de prueba hemos de afirmar que la entidad financiera no cumplió con los deberes de seguridad frente a los riesgos concretos que podrían derivarse del funcionamiento de su plataforma de banca digital, deberes que no se cumplen con la mera literalidad genérica de los contratos suscritos, ni con la firma o suscripción de los mismos, pues son de índole material y técnico que han de fluir a través de diversos niveles de seguridad que pueden constituir opciones de la entidad pero no frente a sus clientes usuarios del sistema en caso de fallo del mismo pues, en tales casos, constituye objetivamente la omisión de una medida esencial en tanto tienen por objeto garantizar la autenticación de la orden de pago como, por lo demás, se desprende del propio tener del contrato de banca próxima. En consecuencia, es la prestadora de los servicios de pago quien tiene la obligación de facilitar un sistema de banca telemática segura, y no son sus clientes- usuarios los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, ni prevenir con un asesoramiento experto los mismos, no pudiendo en suma la parte obligada legalmente a ofrecer un modelo de servicio de caja que requiere de un especial nivel de seguridad, objetar que el usuario debía conocer aspectos técnicos tales como identificar una web como falsa -cuando no consta que fuera burda y por tanto, evidente

de toda falsedad-, ni que no eran fallos técnicos sino riesgos fraudulentos, determinados comportamientos de la plataforma que, no se olvide, son tan factibles que incluso el contrato de banca directa alude -para eludir responsabilidades el prestador- al riesgo de fallos técnicos, errores, interrupciones, desconexiones, sobrecargas y otras formas de defectos en la conexión, identificando precisamente como tales la empleada de la entidad, Sra. Joaquina, el relato que en su día ofrece el marido de la actora".

En conclusión, resulta evidente que en el caso hubo un incumplimiento contractual del banco al ejecutar una orden de pago sin comprobar su legitimidad, es decir, que provenía efectivamente del titular (o autorizado) de la cuenta, al no disponer de un sistema adecuado de seguridad que previniera tal tipo de órdenes fraudulentas ni adoptar medidas concretas y específicas en el caso cuando toma conocimiento de una situación operativa anormal que debió, cuando menos de forma puntual y excepcional, verificar cualquiera orden que se diera en relación a las cuentas del demandante. La responsabilidad en estos supuestos no puede atribuirse directamente al supuesto ordenante de la transferencia por entenderse ésta autorizada al haberse realizado de acuerdo con los sistemas de autenticación del banco. Los sistemas de autenticación se establecen por los proveedores de servicios de pago y si un banco no ha sido capaz de limitar el acceso al canal de banca electrónica no puede pretender que el presunto ordenante, víctima de esta práctica fraudulenta, sea el único responsable, pues es el banco quien tiene responsabilidad respecto del buen funcionamiento y la seguridad del mismo.

Todo lo así argumentado conlleva que, de conformidad con la previsión legal contenida en el artículo 45, "Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas", la entidad bancaria ahora demandada satisfaga al actor la cantidad de 5.870 euros, más los intereses legales del artículo 1.108 del Código Civil devengados desde 28 de diciembre de 2020, fecha de la reclamación efectuada de forma extraprocesal por la parte actora, Documento número 5 de la demanda, al entender que desde ese momento la demandada incurrió en mora en el pago de tal importe, artículo 1.100 CC.

TERCERO. En cuanto a las costas del presente procedimiento, la estimación íntegra de la demanda conlleva que, de conformidad con la previsión legal contenida en el artículo 394.1 LEC, las mismas han de ser satisfechas por la parte demandada.

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

FALLO

Que **ESTIMANDO ÍNTEGRAMENTE** la demanda interpuesta por el Procurador, D. José Miguel Araujo Sierra, en nombre y representación de D. [redacted], contra BANCO SANTANDER, S.A representada por el Procurador, D. Isidro Mateo Pérez, **DEBO CONDENAR y CONDENO** a la referida demandada a satisfacer al actor la cantidad de 5.870 euros, más los intereses legales devengados desde el 28 de diciembre de 2020; todo ello, con expresa imposición de las costas procesales a la parte demandada.

Notifíquese esta sentencia a las partes, haciéndoles saber que contra la misma cabe **RECURSO DE APELACIÓN** que, en su caso, deberá interponerse ante este mismo Juzgado dentro de los veinte días siguientes al en que se notifique esta resolución. De conformidad con lo establecido en la disposición adicional decimoquinta de Ley Orgánica 1/2009, de 3 de noviembre, complementaria de la Ley de reforma de la legislación procesal para la implantación de la nueva Oficina judicial, por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, se hace saber a las partes la necesidad de acreditar documentalmente, en el momento de anunciar o preparar el referido Recurso de Apelación, la previa constitución de un **depósito** por valor de 50 euros en la oportuna entidad de crédito y en la "Cuenta de Depósitos y Consignaciones" abierta a nombre de este Juzgado.

Llévese el original al libro de sentencias.

Por esta mi sentencia, de la que se expedirá testimonio para incorporarlo a las actuaciones, lo pronuncio, mando y firmo.