ADMINISTRACION DE JUSTICIA

JUZGADO DE PRIMERA INSTANCIA
NÚMERO QUINCE
ALICANTE

SENTENCIA Nº 15/2023

En la ciudad de Alicante, a 13 de enero de 2023.

Vistos por mí, José Antonio Pérez Nevot, magistrado titular del Juzgado de Primera Instancia número Quince de los de esta ciudad y su partido judicial, los autos de **juicio verbal** sobre acción de indemnización de daños y perjuicios que, bajo **número 852 de 2022**, se han seguido ante este Juzgado a instancia de don [redacted], representado por la procuradora doña [redacted] y asistido del letrado don Juan Pablo Palomar Pérez, contra BANCO SANTANDER, S. A., representada por la procuradora doña [redacted] y asistida del letrado don [redacted]; y atendidos los siguientes

ANTECEDENTES DE HECHO

PRIMERO.- Resumen de la demanda.

Con fecha de 9 de junio de 2022 se registró escrito de demanda presentado por la procuradora doña [redacted], en la representación arriba indicada. En dicho escrito, tras exponer los hechos y fundamentos de derecho, terminaba solicitando la condena de la parte demandada al pago de la suma de 5.101,39.- €, más los intereses legales desde la fecha de la reclamación extrajudicial, los intereses del art. 576 LEC desde la fecha de la sentencia y las costas.

La anterior petición se fundaba, esencialmente, en los hechos que se pasan a resumir a continuación:

1º El demandante era cliente de BANCO POPULAR ESPAÑOL, S.A. desde el año 2011, año en el cual abrió su cuenta de ahorro en la referida entidad. Su relación con la entidad bancaria, en tanto que cliente de la misma, lo fue en su condición de consumidor.

2º En fecha 4 de febrero de 2019 suscribió un contrato de tarjeta de débito con BANCO SANTANDER, con número inicial [redacted], siendo éste posteriormente sustituido por el número [redacted], y siendo éste a su vez finalmente sustituido por el número [redacted]

ADMINISTRACION DE JUSTICIA

JUZGADO DE PRIMERA INSTANCIA
NÚMERO QUINCE
ALICANTE

3º La tarjeta de débito vinculada a dicho contrato, con número [redacted], fue utilizada por mi mandante conforme efectuaba compras domésticas. Dicha tarjeta ha estado en todo momento, mientras estuvo activada, en posesión de mi mandante.

4º También suscribió, de otro lado, el día 25 de septiembre de 2019, un contrato de tarjeta de crédito con BANCO SANTANDER, con número [redacted], el cual por cierre de oficina paso a tener el número [redacted], estableciéndose en el mismo un límite de crédito de 1.000.- €. Esta tarjeta también ha estado en todo momento bajo la custodia del demandante.

5º En la fecha 31 de enero de 2022 (domingo), a las 20:18 horas, se inició un ciberataque, con aplicación de una técnica de ingeniería social, sobre la plataforma de banca *on line* del demandante, a través del envío a su dispositivo móvil de un mensaje SMS al que se dio la apariencia de haber sido remitido por BANCO SANTANDER, entremezclándolo dentro del hilo de mensajes SMS auténticos provenientes de la referida entidad bancaria.

6º El referido mensaje manifestaba lo siguiente:

"INFO: Estimado cliente, se ha detectado actividad en su cuenta online, le rogamos acceda a nuestra web: http://verificación-cuenta.online."

7º El referido enlace provino de un ciberdelincuente, tal y como queda acreditado en la página web analizadora de enlaces sospechosos "Virus Total", recomendada por la "Oficina de Seguridad del Internauta" del Instituto Nacional de Ciberseguridad de España.

8º Del potencial riesgo de ataque por parte de tal dominio u otros no recibió el actor la menor advertencia o aviso, aun cuando la entidad bancaria venía experimentando durante el último año continuados ataques de *phishing*.

9º El actor, creyendo que tal mensaje provenía realmente de su entidad bancaria, en la confianza de que se le pretendía proteger frente a un acceso no autorizado a su cuenta, pulsó dicho enlace, que le redirigió a través de la web internet a un dominio de internet que a su vez aparentaba la página web de BANCO SANTANDER (lo que en el argot del "phishing bancario" se denomina "página espejo").

10º La página web fraudulenta le solicitó toda una serie de datos bajo el pretexto de solventar la incidencia de seguridad, los cuales fueron suministrados de buena fe por el Sr. [redacted]. Tales datos, entregados a petición del requirente, fueron éstos: el número de usuario, y la contraseña o clave de acceso.

11º Pocos segundos después de introducir tales datos, el demandante recibió en su móvil comunicaciones instantáneas de que se habían realizado transacciones con sus tarjetas de crédito y débito, lo que hizo que accediera rápidamente a la plataforma *on line* y constatara que se había efectuado una operación de pago no autorizada con su tarjeta de crédito por importe de 600.- € al comercio de Barcelona "TIENDA DEL VI", y las siguientes tres operaciones de pago no autorizadas con su tarjeta de débito: una por importe de 1.000.- € al comercio de Barcelona "TIENDA DEL VI", otra por importe de

3.501,39.- € al comercio "Marketplace PCC" de Alhama de Murcia, y otra por importe de 1.000.- € al comercio de Barcelona "TIENDA DEL VI".

12º Conmocionado y alertado por la situación, el Sr. [redacted] desactivó desde la plataforma *on line* tanto la tarjeta de crédito como la de débito y trató en sucesivas ocasiones, sin resultado, de contactar telefónicamente con el servicio de atención telefónica de BANCO SANTANDER.

13º Al día siguiente, 1 de febrero de 2022, acudió a su oficina bancaria con el fin de denunciar presencialmente los hechos. El empleado que le atendió le indicó que, aun cuando procedería a dar inmediato traslado del incidente al Departamento correspondiente del Banco, por el momento tan solo era preciso que se limitara a formalizar un documento de reclamación únicamente respecto a una de las operaciones.

14º Produciéndole no obstante una cierta reserva o desconfianza la explicación recibida respecto a la operación de pago no autorizada con tarjeta de débito por importe de 3.501,39.- € al comercio "Marketplace PCC", el Sr. [redacted] adoptó la cautela de remitir en fecha 1 de febrero de 2022 un e-mail al empleado de BANCO SANTANDER.

15º Asimismo, el día 3 de febrero de 2022 remitió un correo electrónico a la dirección de correo del denominado "servicio antiphishing" de Banco Santander, recibiendo una respuesta estereotipada.

16º En fecha 3 de febrero de 2022, conclusas todas las gestiones y trámites frente a la entidad bancaria, y tras hacer acopio en ésta de cuanta documentación pudo obtener, se personó a las 10:17 horas ante la Dirección General de la Policía, Dependencia Alicante (Inspección Central de Guardia) e interpuso ante dicho órgano la pertinente denuncia.

17º En fecha 9 de febrero de 2022 recibió un e-mail de respuesta a la reclamación interpuesta en el formulario de fecha 1 de febrero de 2022 (registrado con el nº [redacted]), comunicándole que no se procedería a la devolución del importe de 1.000.- €.

18º En fecha 11 de febrero de 2022 el actor recibió un e-mail de respuesta a la solicitud remitida por e-mail en fecha 1 de febrero de 2022 (registrado con el nº [redacted]), comunicándole que no se procedería a la devolución del importe de 3.501,39.- €.

19º Visto el desalentador resultado de sus gestiones, se remitió una reclamación extraprocesal por burofax con certificación de contenido a BANCO SANTANDER el 15 de marzo de 2022.

20º En fecha 20 de abril de 2022 BANCO SANTANDER remitió una carta de contestación a la referida reclamación extraprocesal por la que le comunicó la denegación de la reclamación.

21º Como consecuencia de los hechos descritos, el demandante ha sufrido una pérdida patrimonial por un importe total de 5.101,39.- €.

ADMINISTRACION DE JUSTICIA

JUZGADO DE PRIMERA INSTANCIA
NÚMERO QUINCE
ALICANTE

Al anterior escrito se adjuntaban diversos documentos.

SEGUNDO.- Admisión a trámite de la demanda.

Admitida a trámite la anterior demanda se acordó emplazar en legal forma a la parte demandada para que en diez días compareciera en legal forma y contestara a la demanda.

TERCERO.- Resumen de la contestación a la demanda.

Por el procurador don [redacted], se presentó escrito de contestación a la demanda en tiempo y forma. En dicho escrito se solicitaba el dictado de una sentencia absolutoria con imposición de las costas a la parte demandante por los siguientes motivos:

1º Tal y como se desprende de la documental aportada por la parte actora, ésta interpuso una denuncia en la comisaría de la Policía de la Policía Nacional de Alicante, el pasado 3 de febrero de 2022, con el fin de que se procediese a la investigación de hechos que indudablemente integran la causa de pedir de las acciones civiles que se están ejercitando en la presente demanda.

2º Nos encontramos ante una clara concurrencia de prejudicialidad penal, que determina que se tenga que acordar la suspensión del procedimiento civil.

3º La actora mantiene una relación contractual con BANCO SANTANDER S. A. según contrato de cuenta corriente y de tarjeta de crédito asociada, contrato sobre los que, hasta la fecha en la que se produjeron los hechos, no existió controversia alguna respecto a la prestación del servicio contratado por parte de BANCO SANTANDER S. A.

4º El objeto de la litis parte del daño sufrido por el demandante quien, a resultas de la documental obrante en las actuaciones y de lo que se probará en el momento oportuno, fue víctima de un caso de "phishing".

5º Ningún incumplimiento puede reputarse a BANCO SANTANDER sobre este supuesto, ya que media negligencia y/o incumplimiento de sus obligaciones por parte del actor.

6º El presente fraude trae causa de la recepción por parte del Sr. [redacted] de un SMS cuyo remitente era, a todas luces, fraudulento, y cuya única finalidad era crear alarma en el demandante. Ello, al objeto de conseguir sus credenciales de seguridad y consumar el fraude objeto de litis.

7º La actitud negligente del actor se circunscribe a la cesión de sus credenciales de seguridad a través del enlace contenido en el SMS malicioso. Así, del propio tenor literal del relato de hechos vertido ante la Policía Nacional, se desprende que el actor cedió sus claves al estafador.

8º Como consecuencia de esta cesión de claves de seguridad, y transcurrido un lapso temporal muy breve desde la misma, la actora sufrió los cargos objeto del proceso, lo que acredita la relación de causalidad entre la cesión de claves y la consumación del fraude descrito en la demanda.

9º Concurre negligencia grave, en tanto en cuanto el fraude no se habría producido si el ciberdelincuente no hubiera dispuesto de información tan sensible. Tal y como se acreditará, no nos encontramos ante un supuesto de quebrantamiento de los sistemas de seguridad de BANCO SANTANDER, sino ante un fraude consumado cuyo primer paso era conseguir las herramientas necesarias para burlar los estrictos controles de seguridad de la demandada.

10º BANCO SANTANDER lamenta lo acontecido, pero la parte actora necesariamente ha incumplido las obligaciones que le incumben en materia de custodia y uso de medios de pago, ya que ninguna injerencia en el sistema de la demandada se ha producido.

11º La actora omite un hecho muy relevante en su escrito de demanda, cual es que no sólo facilitó al estafador su firma electrónica -emitida por BANCO SANTANDER a cada uno de sus clientes-, sino que también remitió sus claves de acceso a la Banca Online.

12º BANCO SANTANDER ya avisa de este tipo de prácticas y enfatiza que jamás se solicitan accesos o claves por medios electrónicos.

13º Si el propio actor reconoce que ha incumplido los deberes de custodia (se entiende que, sin intención, lógicamente) ese comportamiento no es oponible a BANCO SANTANDER.

14º BANCO SANTANDER necesita de la colaboración de sus clientes en el cumplimiento de los deberes de custodia sobre las claves asociadas a medios de pago y banca electrónica ya que, si se quebrantan estos deberes por el cliente, difícilmente puede la entidad evitar supuestos como el aquí descrito.

15º BANCO SANTANDER S.A. emplea a una entidad de comercio electrónico, "REDSYS", que se asegura que las operaciones realizadas por clientes de la entidad sean siempre en comercios reconocidos como "seguros".

16º Para que un cliente realice un pago "on-line" con su tarjeta de crédito se requiere de unos pasos que permitan acreditar de manera reforzada las compras.

17º En el presente supuesto no se remite un SMS con OTP (*one time password*: código de un solo uso), sino un mensaje PUSH, es decir, una notificación enviada desde la APP de Banco Santander, que facilita al cliente un enlace que le lleva a su Banca por Internet, donde debe validar la operación. Es decir, tiene que introducir la clave de su Banca a Distancia, y una vez dentro de ésta, validar la compra mediante su firma electrónica, autenticando doblemente el proceso de pago.

18º Tal y como se certifica desde Redsys, el método de autenticación utilizado fue OoBA (*Out of Band*)

19º La autenticación fuera de banda es un tipo de autenticación de dos factores (2FA) que requiere un método de verificación secundario a través de un canal de comunicación independiente.

ADMINISTRACION DE JUSTICIA

JUZGADO DE PRIMERA INSTANCIA
NÚMERO QUINCE
ALICANTE

20º En un sistema de autenticación fuera de banda (OOBA), el canal que se utiliza para autenticar a un cliente está completamente separado del canal utilizado por el cliente para iniciar sesión o realizar una transacción. El uso de un canal separado disminuye la posibilidad de ataques *Man-in-the-Middle* y otros ataques por violación de datos.

21º Las notificaciones *push* proporcionan un código de autenticación o una contraseña de un solo uso (OTP) a través de una notificación que aparece en la pantalla de bloqueo del dispositivo móvil del cliente. Por tanto, en lugar de remitirse la clave de un solo uso (OTP) vía SMS, se remitió a través de la App de Banco Santander, controlando así la entidad todo el proceso de autenticación de la compra.

22º Previamente, para que el estafador pudiera recibir estas notificaciones, debió dar de alta el dispositivo seguro (esto es, vincular su terminal móvil concreto a la App de Banco Santander). Para ello, se remitieron unas claves por SMS al teléfono móvil del actor.

23º El límite de disposición de la tarjeta del actor fue modificado, aunque esta actuación vino precedida del consiguiente proceso de autenticación.

24º BANCO SANTANDER ha actuado en todo momento de manera diligente, respetando la normativa de aplicación y la *lex artis* del sector.

25º Se advierte expresamente a todos los clientes de la imposibilidad de que la entidad, a través de correo electrónico, pueda solicitar claves de acceso o similares, y que nunca se debe confiar en correos electrónicos o comunicaciones en las que se requiera el acceso con claves a la web de la entidad.

26º El delincuente y estafador consiguió realizar esos movimientos gracias a las facilidades que le dio el actor, que dejan a todas luces claro que el hecho de que pudieran realizar esas disposiciones se produjo, sólo y exclusivamente, por la negligencia del propio demandante.

27º La demandada hace ya muchos años que ofrece, en su propia página web www.bancosantander.es, instrucciones sobre cómo prevenir este tipo de delitos telemáticos, *phising* y *smishing*.

28º Los distintos entes públicos realizan también una constante campaña concienciando a la población sobre estas prácticas con el objetivo de prevenir a los/as ciudadanos/as de incurrir en comportamientos como el de la parte actora.

29º El demandante incumplió todas estas pautas y los deberes de custodia que le impone la Ley de Servicios de Pago.

30º No es posible la realización de las transferencias, pagos ni disposiciones en efectivo sin contar con el conocimiento del titular de la cuenta de la corriente y, lógicamente, la entidad bancaria entiende prestado este consentimiento a través de la firma electrónica y a través de los mecanismos de seguridad de doble autenticación que exige para dichas operaciones.

ADMINISTRACION DE JUSTICIA

JUZGADO DE PRIMERA INSTANCIA
NÚMERO QUINCE
ALICANTE

31º Queda sobradamente demostrado en el proceso, que el demandante incumplió con su deber de guarda y custodia al entregar sus claves a los delincuentes, aunque lo haya hecho engañado, y en consecuencia, no es exigible responsabilidad a la entidad bancaria. Ésta no puede ser responsable de que sus clientes faciliten las claves de seguridad de manera tan sencilla, ya que el daño no lo ha producido la entidad, sino el tercero que ya ha sido objeto de denuncia en vía penal.

32º Esta actuación, aunque fue absolutamente inintencionada, no solo provocó la pérdida patrimonial sufrida por la demandante, sino que privó de cualquier opción a la entidad de prevenir que ocurrieran los hechos.

33º Los sistemas de seguridad del BANCO SANTANDER funcionaron en todo momento y, prueba de ello, es que las operaciones se realizaron porque los delincuentes tuvieron en su poder el control absoluto del teléfono móvil, tras facilitar el demandante las claves de seguridad.

34º BANCO SANTANDER en todo momento ha cumplido con la normativa de aplicación en materia de servicios de pago.

35º El organismo regulador, en todos estos supuestos en los que la acción ilícita del estafador que ha empleado el mecanismo de "phishing", entiende que la entidad bancaria ha cumplido en todo momento con la normativa de aplicación.

Al anterior escrito se acompañaban varios documentos.

CUARTO.- Vista de juicio verbal.

Previa citación de las partes, se celebró juicio con la asistencia y resultado que constan en la grabación realizada bajo la fe pública judicial.

Constatada la subsistencia del litigio y fijados los hechos controvertidos se practicó la prueba admitida, previa declaración de su pertinencia, y se declararon los autos vistos para sentencia.

QUINTO.- Control de la actividad procedimental.

En la sustanciación de este proceso se han respetado todas las prescripciones legales, salvo algunos plazos procesales, debido a la acumulación de asuntos que soporta este órgano jurisdiccional, fruto de la sobrecarga estructural de trabajo que padecen los Juzgados de Primera Instancia de Alicante sin competencias en Derecho de Familia, cuya tasa de entrada de asuntos, en el año 2022, es de un 207,82 % (desviación de un 107,82 % sobre la carga máxima de trabajo aprobada por el Consejo General del Poder Judicial).

FUNDAMENTOS DE DERECHO

PRIMERO.- Delimitación de la controversia.

ADMINISTRACION DE JUSTICIA

JUZGADO DE PRIMERA INSTANCIA
NÚMERO QUINCE
ALICANTE

D. [redacted] solicita la condena de BANCO SANTANDER, S. A. al pago de 5.101,39.- €, más los intereses legales desde la reclamación extrajudicial, los del art. 576 LEC desde la fecha de la sentencia y las costas.

Alega, en resumidas cuentas, haber suscrito sendos contratos de tarjeta de débito y crédito con la demandada los días 4 de febrero y 25 de septiembre de 2019. En virtud de tales contratos, el Sr. [redacted] recibió dos tarjetas que ha venido empleando en la realización de compras domésticas y de las que nunca se ha separado. El día 31 de enero de 2022, sobre las 20:18 horas, el actor alega haber recibido en su teléfono móvil un mensaje SMS, aparentemente enviado por la demandada, en el que se le alertaba de la existencia de actividad en su cuenta *on line* y se le conminaba a acceder a la página web de la entidad en una dirección facilitada con un hipervínculo (http://verificación-cuenta.online). Como quiera que tal mensaje SMS aparecía dentro del hilo de mensajes auténticos previamente enviados por la entidad financiera, el Sr. [redacted] pulsó el hipervínculo, que lo redirigió a una página web falsa ("página espejo") que simulaba ser la propia del BANCO SANTANDER. Así las cosas, la persona o personas que habían orquestado este fraude solicitaron, a través de la referida página web, el número de usuario y la contraseña o clave de acceso propios del demandante, que este facilitó en la creencia de que su interlocutor era BANCO SANTANDER. De esta forma, se llevaron a cabo cuatro operaciones de pago no autorizadas por importes de 600, 1.000, 3.501,39 y 1.000.- € en un breve espacio de tiempo. Y ello, pese a que tales operaciones no habían sido autorizadas por el Sr. [redacted], titular de la cuenta corriente en que se cargaron, ya que no se cumplió, en este caso, con el doble factor de autenticación de la operación. Siendo así, la demandada debe responder del perjuicio sufrido por el actor, que asciende a la suma reclamada.

BANCO SANTANDER, S. A. se opone totalmente a la anterior reclamación por los motivos que se han consignado en el antecedente de hecho tercero, al que me remito en aras de la brevedad. Lo que se viene a argumentar es, en esencia, que la entidad financiera no tiene por qué responder de los perjuicios patrimoniales ocasionados por la actividad delictiva de un tercero cuando fue el propio demandante el que, de forma negligente, proporcionó sus datos personales, claves de acceso y firma electrónica al presunto delincuente. Además, la entidad financiera cumplió con todos los requisitos de seguridad exigibles en materia de comercio electrónico y por la normativa sobre servicios de pago, llevando a cabo campañas activas de información a sus clientes para evitar fraudes como el descrito en la demanda. Es por ello que considera que no ha de responder de los perjuicios ocasionados.

SEGUNDO.- Prejudicialidad penal.

Se alega por la demandada, en primer lugar, que ha de proveerse a la suspensión del proceso por prejudicialidad penal. Según BANCO SANTANDER, el propio actor admite en su demanda haber interpuesto una denuncia por los mismos hechos que sirven de fundamento a la acción entablada, razón por la cual habrá de aguardarse a la finalización del proceso penal antes de poder decidirse definitivamente el presente proceso civil.

El art. 40 LEC regula la prejudicialidad penal de la siguiente forma:

1. Cuando en un proceso civil se ponga de manifiesto un hecho que ofrezca apariencia de delito o falta perseguible de oficio, el tribunal civil, mediante providencia,

ADMINISTRACION DE JUSTICIA

JUZGADO DE PRIMERA INSTANCIA
NÚMERO QUINCE
ALICANTE

lo pondrá en conocimiento del Ministerio Fiscal, por si hubiere lugar al ejercicio de la acción penal.

2. En el caso a que se refiere el apartado anterior, no se ordenará la suspensión de las actuaciones del proceso civil sino cuando concurran las siguientes circunstancias:

1.ª Que se acredite la existencia de causa criminal en la que se estén investigando, como hechos de apariencia delictiva, alguno o algunos de los que fundamenten las pretensiones de las partes en el proceso civil.

2.ª Que la decisión del tribunal penal acerca del hecho por el que se procede en causa criminal pueda tener influencia decisiva en la resolución sobre el asunto civil.

3. La suspensión a que se refiere el apartado anterior se acordará, mediante auto, una vez que el proceso esté pendiente sólo de sentencia.

4. No obstante, la suspensión que venga motivada por la posible existencia de un delito de falsedad de alguno de los documentos aportados se acordará, sin esperar a la conclusión del procedimiento, tan pronto como se acredite que se sigue causa criminal sobre aquel delito, cuando, a juicio del tribunal, el documento pudiera ser decisivo para resolver sobre el fondo del asunto.

5. En el caso a que se refiere el apartado anterior no se acordará por el Tribunal la suspensión, o se alzará por el Letrado de la Administración de Justicia la que aquél hubiese acordado, si la parte a la que pudiere favorecer el documento renunciare a él. Hecha la renuncia, se ordenará por el Letrado de la Administración de Justicia que el documento sea separado de los autos.

6. Las suspensiones a que se refiere este artículo se alzarán por el Letrado de la Administración de Justicia cuando se acredite que el juicio criminal ha terminado o que se encuentra paralizado por motivo que haya impedido su normal continuación.

7. Si la causa penal sobre falsedad de un documento obedeciere a denuncia o querella de una de las partes y finalizare por resolución en que se declare ser auténtico el documento o no haberse probado su falsedad, la parte a quien hubiere perjudicado la suspensión del proceso civil podrá pedir en éste indemnización de daños y perjuicios, con arreglo a lo dispuesto en los artículos 712 y siguientes.

Para que pueda existir prejudicialidad penal es necesario -entre otras cosas- "que se acredite la existencia de una causa criminal", lo que no equivale a acreditar la presentación de una denuncia o la interposición de una querella criminal, pues tanto la una como la otra pueden ser inadmitidas a trámite y no provocar el inicio de ningún proceso penal.

En el caso de autos, dado que no se ha probado en el proceso que, sobre los hechos que están siendo objeto de enjuiciamiento, penda una causa criminal, no es posible atender a la solicitud de suspensión interesada por la parte demandada.

TERCERO.- Consideraciones previas sobre el régimen jurídico aplicable.

JUZGADO DE PRIMERA INSTANCIA
NÚMERO QUINCE
ALICANTE

Es un hecho pacífico en el proceso que los contratos de tarjeta de débito y crédito que motivaron la expedición de las tarjetas con cargo a las cuales se han llevado a cabo las operaciones no autorizadas por el actor se concertaron los días 4 de febrero y 25 de septiembre de 2019. Es por ello que están sujetos al Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en lo sucesivo, TRLSP). Este Real Decreto-ley vino a sustituir a la Ley 16/2009, de 13 de noviembre, de servicios de pago (LSP), que transpuso al ordenamiento interno la Directiva 2007/64/CE, con la finalidad de transponer 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. Es por ello que las posibles dudas interpretativas que puedan surgir en la aplicación del TRLSP deberán de resolverse a la luz de la indicada Directiva (UE) 2015/2366.

Los derechos y obligaciones que surgen en relación a la prestación y utilización de servicios de pago se regulan en el Título III TRLSP (arts. 34 y ss.). Por lo que interesa al caso que es objeto de enjuiciamiento, de dicha regulación debe destacarse que el art. 36.1 TRLSP dispone que una operación de pago se considerará autorizada "cuando el ordenante haya dado el consentimiento para su ejecución" y que, a falta de tal consentimiento, "la operación de pago se considerará no autorizada". La forma con arreglo a la cual deba prestarse el consentimiento será la pactada entre el ordenante y su proveedor de servicios de pago (art. 36.1.II TRLSP).

Cuando se habilita al usuario de servicios de pago para utilizar un "instrumento de pago" (como sucede en este caso, en el que se le dotó de dos tarjetas), el mismo ha de cumplir con las obligaciones que señala el art. 41 TRLSP:

> *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.*

Por otra parte, en el caso de que un usuario de servicios de pago considere que no ha autorizado una operación o que ésta ha sido ejecutada incorrectamente por el proveedor, sólo podrá obtener la rectificación si 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" (art. 43 TRLSP). Hasta tal punto es así, que el Tribunal de Justicia de la Unión Europea ha señalado que "el régimen de responsabilidad del proveedor de servicios de pago en caso de pago no autorizado está supeditado a la notificación por parte del usuario de esos servicios de cualquier operación no autorizada a dicho proveedor" (sentencia *DM y LR contra Caisse régionale de Crédit agricole mutuel (CRCAM) — Alpes-Provence*, de 2 de septiembre de 2021, asunto C-337/20, ap. 34). Es por ello que la obligación de notificación del usuario de servicios de pago en el indicado plazo de trece meses opera como condición para que el régimen de responsabilidad del

proveedor pueda aplicarse (ap. 39). Hasta tal punto es así, que los Estados miembros no están autorizados para ampliar el referido plazo sin quebrantar la Directiva (ap. 51).

Efectuada la notificación que ha quedado dicha en el referido plazo de trece meses contados desde la fecha del adeudo, el proveedor de servicios de pago ha de proceder a la rectificación (art. 43 TRLSP). Así, en el caso de que haya ejecutado una operación de pago no autorizada, procederá a devolver al ordenante el importe de dicha operación "de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquél en el que haya observado o se le haya notificado la operación, salvo cuando (...) 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" (art. 45.1 TRLSP).

Desde el momento en que un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada (o si alega que la ejecución ha sido 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" (art. 44.1 TRLSP). Ahora bien, para demostrar la existencia de autorización no puede bastar el registro, por el proveedor de servicios de pago, "de la utilización del instrumento de pago", que tampoco es suficiente para demostrar que el usuario "ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 41" (art. 44.2 TRLSP). La prueba de que el usuario "cometió fraude o negligencia grave" corresponde al proveedor de servicios de pago (art. 44.3 TRLSP), debiendo conservar "la documentación y los registros que le permitan acreditar el cumplimiento de [sus] obligaciones" durante, al menos, seis años (art. 44.4 TRLSP). De esta forma, el ordenante "soportará todas las pérdidas derivadas de operaciones de pago no autorizadas" si "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 cuyo caso no se aplica el límite de responsabilidad de cincuenta euros (art. 46 TRLSP).

A los efectos de determinar qué ha de entenderse por "negligencia grave" del usuario resulta de utilidad transcribir el considerando 72 de la Directiva (UE) 2015/2366:

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

ADMINISTRACION DE JUSTICIA

JUZGADO DE PRIMERA INSTANCIA
NÚMERO QUINCE
ALICANTE

servicios aporte pruebas de la presunta negligencia, puesto que los medios a disposición del ordenante son limitados en esos casos.

CUARTO.- Aplicación de las anteriores consideraciones al caso enjuiciado.

La aplicación de las anteriores consideraciones al caso enjuiciado determina la estimación de la demanda, por cuanto que:

1º Es un hecho pacífico en el proceso que los cargos sufridos por el Sr. [redacted] en su cuenta corriente no fueron por él autorizados, sino más bien por un tercero o terceros que se hicieron con sus datos personales tras enviarle un mensaje SMS, simulando haber sido remitido por BANCO SANTANDER. Dicho mensaje, que se insertó en el hilo de mensajes propios de esta entidad en el teléfono móvil del demandante, advertía a éste de la existencia de actividad en su cuenta *on line* y lo conminaba a acceder a la web de la demandada a través del hipervínculo http://verificación-cuenta.online.

2º Es igualmente incontrovertido en la litis que el Sr. [redacted], alertado por el contenido del mensaje recibido y creyendo en todo momento que provenía de su entidad financiera, pulsó el enlace web, que lo redirigió a una página falsa ("página espejo") que simulaba ser la propia de BANCO DE SANTANDER. Una vez allí, introdujo sus datos personales y, en particular, su nombre de usuario y clave o contraseña de acceso, que fueron empleados por el tercero o terceros que habían enviado el mensaje SMS y creado la "página espejo" para realizar, de inmediato, cuatro operaciones de comercio electrónico, con cargo a la cuenta corriente del demandante, por importes de 600.- €, 1000.- €, 3.501,39.- € y 1.000.- €.

3º Tampoco se discute que el demandante, en el momento en que tuvo conocimiento de tales cargos, procedió a bloquear de inmediato sus tarjetas de débito y crédito y a comunicar los hechos a BANCO DE SANTANDER (así se desprende, en todo caso, de la captura de pantalla de los mensajes SMS recibidos en el móvil del demandante: doc. nº 5 de la demanda, ac. 6 del visor Horus).

Sentado lo anterior, la cuestión a resolver se torna en esencialmente valorativa y consiste en determinar si el hecho de haber facilitado el Sr. [redacted] sus claves y datos personales al presunto ciberdelincuente que le envió el mensaje SMS podría considerarse como una conducta gravemente negligente. Como ya se ha explicado en el fundamento anterior, no basta con considerar que el demandante pudo incurrir en algún tipo de negligencia o falta de diligencia, sino que es necesario que ésta sea grave. Es decir, que hubiera desatendido deberes de cuidado que, incluso personas poco cuidadosas habrían observado. La respuesta a esta cuestión ha de ser obviamente, negativa. Cualquier persona medianamente diligente podría haber sido víctima de un fraude como el descrito en la demanda y admitido en la contestación (no es objeto de disputa que lo hubo): si se examina la forma y contenido del mensaje SMS recibido por el demandante (doc. nº 5, ac. 6), que aparecía clasificado, por el terminal de telefonía móvil del actor, dentro de la misma cadena o hilo de mensajes SMS propios del BANCO DE SANTANDER, lo normal era experimentar un sentimiento de peligro que -conocido es conforme a máximas de la experiencia- activa áreas cerebrales que nublan el juicio o raciocinio como consecuencia del proceso evolutivo sufrido por la especie humana. En tales circunstancias, el cerebro concede prioridad a respuestas más impulsivas, frente a las reflexivas, en aras de conjurar cuanto antes el

peligro percibido. Es por ello que no se puede considerar gravemente negligente la conducta de quien, guiado por tan humana sensación (especialmente, cuando había sido suscitada por un mensaje SMS aparentemente veraz), procede a pulsar de inmediato el hipervínculo para, a continuación, acceder a una página web que simula ser la de su entidad financiera en aras de comprobar si, realmente, se están produciendo cargos en su perjuicio. Es por ello que no se comparte la valoración que realiza la demandada en su escrito de contestación pues, de existir negligencia imputable al actor -cuestión en la que ni siquiera resulta necesario entrar-, ésta no sería grave y, al no ser grave, es la entidad financiera la que ha de responder de los daños y perjuicios ocasionados por las operaciones no autorizadas, que ascienden a 5.101,39.- € (art. 45 TRLSP). En este sentido, cabe citar igualmente la SAP de Castellón (Sección 3ª) nº 201/2020, de 21 de mayo (rollo nº 26/2019) y la SAP de Madrid (Sección 21ª) nº 293/2019, de 2 de julio (rollo nº 467/2018):

No se acredita en modo alguno que las operaciones de pago fueran autorizadas por la demandante, sino todo lo contrario, no demostrándose ni que ésta actuara fraudulentamente o con negligencia grave, por lo que aplicando la normativa expresada recogida en la Ley 16/2009 de servicios de pago corresponde a la entidad bancaria demandada asumir el perjuicio económico causado a la actora por la utilización indebida y no autorizada por tercero desconocido de la tarjeta de crédito y las ordenes ilícitas cursadas en la cuenta bancaria.

A ello no obsta que el responsable de las operaciones que motivaron los cargos fuera un tercero, pues siempre quedarán a salvo las acciones de la demandada para repetir frente al mismo. Tampoco, el hecho de que la entidad demandada incluyera recomendaciones genéricas de seguridad en su página web desde hacía tiempo, tal y como señala la SAP de Alicante (Sección 8ª) nº 107/2018, de 12 de marzo (rollo nº 622/2017):

(...) 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. [redacted] el relato que en su día ofrece el marido de la actora.

Ninguna constancia tenemos, por lo demás, de que hubiera un uso indebido del sistema por parte del cliente ni que incumpliera con sus obligaciones básicas.

Dado que en el caso de autos tampoco se ha probado la existencia de un uso indebido del sistema por parte del deudor que, simplemente, fue víctima de un fraude que podría haber sido evitado con el diseño de una plataforma web más segura, los argumentos de la demandada no pueden merecer acogida.

QUINTO.- Intereses de demora y procesales.

El principal devengará, en concepto de intereses de demora y procesales, el interés legal del dinero desde el día 1 de febrero de 2022, fecha de la primera reclamación extrajudicial (hecho que no ha sido objeto de específica controversia: art. 405.2 LEC), hasta la fecha de esta sentencia, en que se incrementará en dos puntos hasta su completo pago (arts. 1108 CC y 576 LEC).

SEXTO.- Costas de la primera instancia.

Dado que la demanda va a ser estimada íntegramente, procede imponer las costas a la parte demandada, con arreglo al criterio del vencimiento objetivo y habida cuenta de que el caso enjuiciado no presenta serias dudas de hecho ni de derecho (art. 394 LEC).

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

FALLO

Que estimando íntegramente la demanda interpuesta por don [redacted] Cuenca **debo condenar y CONDENO** a BANCO SANTANDER, S. A. a pagar a la primera la suma de CINCO MIL CIENTO UN EUROS CON TREINTA Y NUEVE CÉNTIMOS (5.101,39.- €), que devengará el interés legal del dinero desde el día 1 de febrero de 2022 hasta la fecha de esta sentencia, en que se incrementará en dos puntos hasta su completo pago, y con imposición de las costas de esta instancia a la parte demandada.

Notifíquese en legal forma a las partes haciéndoles saber que esta sentencia no es firme y que contra la misma se puede interponer recurso de apelación que, en su caso,