JUZGADO DE PRIMERA INSTANCIA Nº 2
Alcoy (Alicante)
Plaza MARE DE DEU,2
TELÉFONO: 96.533.00.54
N.I.G.: **03009-41-1-2023-0001733**

Procedimiento: Juicio verbal (250.2) [VRB] - 000474/2023 -

Demandante: [redacted]
Procurador: [redacted]
Letrado: PALOMAR PEREZ, JUAN PABLO

Demandado: BANCO BILBAO VIZCAYA ARGENTARIA SA
Procurador: [redacted]

SENTENCIA
Nº26/24

En Alcoy, a veintede febrero de dos mil veinticuatro.

D. Carlos Gómez Tejada, Magistrado del Juzgado de Primera Instancia e Instrucción nº 2 de Alcoy, ha visto los presentes autos de Juicio Verbal nº 474/2023sobre reclamación de cantidad, promovidos por**Dª** [redacted] representada por la Procuradora Sra. [redacted] y asistida por el Letrado Sr.Palomar Pérez**frente a BANCO BILBAO VIZCAYA ARGENTARIA SA,** representada por la Procuradora [redacted] y asistida por el Letrado [redacted].

ANTECEDENTES DE HECHO

PRIMERO Por el demandante se interpuso, ante los Juzgados de Primera Instancia de Alcoy, con fecha 17/05/2023demanda de Juicio verbal contra la demandada solicitando que se le condene a indemnizar a la actora en DOS MIL SETECIENTOS NOVENTA Y CINCO EUROS CON NOVENTA Y UN CÉNTIMOS DE EURO (2.795,91.- €), más los intereses legales de esta cantidad desde la fecha de la reclamación extraprocesal hasta la fecha de la sentencia y los intereses judiciales del art. 576 de la LEC desde la fecha de la sentencia hasta su completo pago; con imposición de costas a la parte demandada.

SEGUNDO Que admitido a trámite el procedimiento, se dio traslado de la demanda a la demandada, quien contestó oponiéndose a la misma.

[redacted]

TERCEROEn la fecha fijada se celebró la vista, a la que comparecieron las partes, se admitió y practicó la prueba propuesta en el acto. Tras el trámite de conclusiones, los autos quedaron vistos para dictar sentencia.

CUARTO En el presente procedimiento se han cumplido las prescripciones legales.

FUNDAMENTOS JURÍDICOS

PRIMERO.- La demandante alegatener contratado con la demandada una tarjeta de crédito con el número [redacted], que estaba vinculado a la cuenta con IBAN [redacted], teniendo igualmente suscrito un contrato de servicios banca online. La demandante alega que durante los dos años anteriores a los hechos solo se conectaba desde los siguientes dispositivos:

- Ordenador fijo marca "AMD A10 7860K 3,6 Mhz/8GB/500GB".
- Dispositivo móvil modelo SAMSUNG GALAXY A71 6+128 GB.

Igualmente expresa que su ordenador portatil estaba dotado de antivirus "Microsoft Defender".
El 13 de junio de 2022, a las 19:15 horas, se alega que se inició sobre la plataforma de banco online de la actoraun ciberataque, con aplicación de una técnica de ingeniería social, a través del envío de un mensaje SMS a su dispositivo móvil, con la apariencia de haber sido remitido por BBVA, entremezclándolo dentro del hilo de mensajes SMS auténticos provenientes de tal entidad bancaria. El texto del mensaje sería el siguiente:

"Su cuenta ha sido suspendida. Por seguridad es obligatorio instalar BBVA Protect para prevenir mensajes fraudulentos. Descarga: https://bbva.movil#descarga.click"

Que la demandante, creyendo que tal mensaje provenía realmente de su entidad bancaria, al constatar que se entremezclaba dentro del hilo de mensajes de BBVA, junto a mensajes auténticos de tal entidad, al visualizar que mostraba un link encabezado por la extensión "https" (normalmente perteneciente a páginas web verdaderas), y que el mismo hacía constar la leyenda "BBVA", en la convicción de que se pretendía protegerle frente a una utilización fraudulenta de su tarjeta de pago, 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 BBVA, donde se le solicitó y facilitó el DNI y contraseña, creyendo estar al habla con un empleado de la entidad.

Se alega que ese mismo día 13 de junio de 2022, pocos minutos después, se produjeron 13 operaciones de pago no autorizadas con su tarjeta de crédito , cuyos beneficiarios fueron los proveedores "Quantfuri Tradi", "transak.com", "BitBase", "Moon Pay 3998" "Rebellion Pay" y "014 LOYALIA", ascendiendo la suma de tales operaciones a 2.795,91.-euros; no habiendo recibido SMS alguno de BBVA con clave de autenticación de doble factor, siendo cargada tal cantidad por la entidad bancaria en fecha 5 de julio de 2022.

La demandante lo habría detectado el 14 de junio de 2022 a raiz de una comprobación rutinaria de su cuenta, interponiendo denuncia policial ese mismo día, formulando reclamación a al entidad que fue desestimada; formulando petición de mediación a al a OCE que fue desestimada por la otra parte; así como otra reclamación ante el Banco de España; y otra reclamación mediante carta, dirigida a la demandada, de fecha 3 de marzo de 2023.

Se reclama pues la cuantía de los pagos que se dicen fraudulentos, dado que existiría responsabilidad de la entidad por haber podido disponer de trazabilidad de la aplicación, evidenciando que las conexiones se habrían efectuado desde un dispositivo distinto de los habituales; por no existirnegligencia de la demandante al ser que las claves se seguridad fueronconservadas diligentemente y no existir o sustracción de la tarjeta, la numeración identificativa de tal documento, nunca fue guardada junto a su instrumento de pago, ni en formato abierto alguno detectable por terceros; ypor no haber autenticado la operación adecuadamente.

La parte demandada se opone y solicita la desestimación de la demanda, alegando que no ha cumplido ninguna de sus obligaciones; que la responsabilidad sería de la demandante por haber revelado los datos de acceso a su banca electrónica y el número de la tarjeta y CVV de la misma; que las operaciones fueron autenticadas con los correspondientes códigos OTP remitidos a su teléfono móvil; yque la entidad lleva advirtiendo a sus clientes de que tomen medidas para evitar estos fraudes.

SEGUNDO.- ElReal Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, en su artícul0 41, respecto a las obligaciones a cargo del usuario establece:

"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."

En cuanto a la demandada en el caso que nos ocupa, sus obligaciones se reflejan en el Art.44 del mismo texto legal:

"1. Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago.

Si el usuario de servicios de pago inicia la operación de pago a través de un proveedor de servicios de iniciación de pagos, corresponderá a éste demostrar que, dentro de su ámbito de competencia, la operación de pago fue autenticada y registrada con exactitud y no se vio afectada por un fallo técnico u otras deficiencias vinculadas al servicio de pago del que es responsable.

2. A los efectos de lo establecido en el apartado anterior, el registro por el proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, de la utilización del instrumento de pago no bastará, necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que éste ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 41.

3. Corresponderá al proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, probar

que el usuario del servicio de pago cometió fraude o negligencia grave.

4. El proveedor de servicios de pago conservará la documentación y los registros que le permitan acreditar el cumplimiento de las obligaciones establecidas en este Título y sus disposiciones de desarrollo y las facilitará al usuario en el caso de que así le sea solicitado, durante, al menos, seis años. No obstante, el proveedor de servicios de pago conservará la documentación relativa al nacimiento, modificación y extinción de la relación jurídica que le une con cada usuario de servicios de pago al menos durante el periodo en que, a tenor de las normas sobre prescripción puedan resultarles conveniente para promover el ejercicio de sus derechos contractuales o sea posible que les llegue a ser exigido el cumplimiento de sus obligaciones contractuales.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, así como en otras disposiciones nacionales o de la Unión Europea aplicables."

Por lo tanto, si bien el usuario tiene la obligación de tomar las precauciones necesarias para evitar el uso indebido o fraudulento de su tarjeta, es el prestador quien tiene la obligación y carga de probar la negligencia del usuario.

No es controvertido la relación contractual ni el uso y titularidad de la tarjeta bancaria por la demandante.

La demandante ha relatado, tanto en el escrito de demanda como en el interrogatorio practicado, que en fecha 13 de junio de 2022, a las 19:15 horas, recibió un mensaje SMS a su dispositivo móvil, con la apariencia de haber sido remitido por BBVA, entremezclándolo dentro del hilo de mensajes SMS auténticos provenientes de tal entidad bancaria. El texto del mensaje erael siguiente:

"Su cuenta ha sido suspendida. Por seguridad es obligatorio instalar BBVA Protect para prevenir mensajes fraudulentos. Descarga: https://bbva.movil#descarga.click"

Así aparece en el documento n.º 7 de la demanda, no impugnado de contrario. En ese mismo documento se aprecia que el sms aparece en el hilo de conversación con BBVA, dejándose entrever parte de un mensaje anterior, y figurando a continuación otro posterior

solicitando confirmar un pago de 180 Euros de MOONPAY.IQ, con la tarjeta acabada en [redacted] con remisión del código de confirmación.

La demandante reconoce que pinchó en dicho enlace y expresa que el aparecía una web como la habitual de BBVA, por lo que no le resultósospechosa, donde le pedían, y así introdujo, el DNI y su contraseña.

No se acredita cómo se obtuvieron el número de tarjeta y el CVV de la misma. Según la máxima de la experiencia solo puede obtenerse o por un clonado de la tarjeta, o por acceso de la aplicación con los datos que la demandante facilitó, o por haberlo facilitado ella personalmente. Ninguna de las tres se acredita. De ser la segunda de ellas, habrá que valorar a continuación que grado de diligencia puso o no la demandante en facilitar los datos al pinchar en el enlace, cuestión esta que se valorará más adelante.

Con esos datos se efectuaron los pagos fraudulentos. Ahora bien, la demandada dice que esos trece pagos fueron confirmados por el sistema OTP-SMS. Dicho sistema consiste en que se envía un sms al móvil que figura en los datos de la aplicación de banca online, conteniendo un código numérico, que se ha de introducir para completar la operación.

La demandante niega haber recibido ninguno de los 13 sms's de confirmación, solo uno, el que figura en el documento n.º 7, percatándose del engaño.

La demandada afirma que sí que los envió. Si examinamos el resultado de sus medios de prueba, en cuanto al informe pericial, en este no figura en ningún momento a que terminal se enviaron dichos OTP-SMS. El perito en su declaración afirma que sí se enviaron. Hay que tener en cuenta que la declaración de este perito no puede ser valorada como prueba plena porque ha manifestado ser empleado de la entidad demandada, lo que supone concurrencia de causa de tacha.

No obstante, el documento n.º 1 de la contestación, no impugnado de contrario, es un pantallazoen el que en la primera de las líneas de color verde aparece el móvil de la demandante (tal y como ha confirmado en el interrogatorio en la vista) figurando a continuación el envío de sms's, para cada una de las operaciones que se han alegado fraudulentas, remitiendo código OTP. No obstante del mismo no se desprende la recepción sino el envío pues solo aparece el término "sent" (enviado).

Igualmente el documento ºn 2 corresponde a un pantallazo donde se confirma que dicho terminal móvil era de la demandante.

Del acta notarial aportada como documento n.º 5, consiste en una acta notarial, de fecha 29 de marzo de 2022, requiriendo, a petición de un representante de la entidad demandada, para que compruebe la ventana informativa en la web de la entidad, pantalla de splash en la app, artículos publicados en la partepública de la página web; vídeo de youtube sobre celebración de evento dirigido a clientes particulares; contenidos en redes sociales de la entidad; noticia que se publicará en la app entre los días 4 y 8 de abril sobre proteger la privacidad en redes sociales; celebración de webinar dirigido a clientes de Banca Empresa; puzzle publicado durante el mes de marzo en la Home de particulares de la página web; consejos de seguridad permanentes en el área de login de la página web.

Al respecto hay que decir que el hecho de que se hagan anuncios de cyberseguridad en artículos publicados, noticias, vídeos de youtube o en sedes sociales, o el enlace a "consejos de seguridad", no significa que la información necesaria para evitar un fraude estuviera al alcance de la demandante.

Cuestión distinta es si a cada vez que accediera a la web o al app de banca online, apareciese una ventana emergente avisando de que no facilite sus datos personales. Existen algunas capturas de pantalla que hacen expresa referencia a que nunca se entregue los datos mediante sms, enlaces ni llamadas. Sin embargo, el acta notarial, pese a expresar en cada diligencia que operación realiza y que efectúa captura de pantalla y/o impresión todas estas aparecen continuación seguida sin poder saberse cuáles de ellas corresponden a ventanas emergentes. No obstante, aunque así fuera, la fecha en que dichos avisos o pantallas emergentes aparecen es anterior a la fecha de los hechos que nos ocupan. Por otra parte, la demandante en el interrogatorio manifiesta que no vio nunca tales avisos.

Respecto al documento n.º 4 de la parte demandada, Redsys acredita que las operaciones fueron autorizadas, registradas y contabilizadas, sin que hubiera fallo informático. Sin embargo hay que ponerlo en relación con la contestación remitida a requerimiento judicial en donde expresa que la entidad bancaria es la responsable de su autenticación. Por lo tanto Redsys ni aclara ni oscurece ninguno de los puntos de controversia. Amén de que resulta contradictorio que en el documento n.º 24 de la demanda Redsys exprese que el dispositivo o entidad que autentifica al cliente es "no identificado".

Por otra parte, de las respuestas a los oficios remitidos a Telefónica y Orange se desprende que la demandante es cliente de aquella pero nunca lo ha sido de esta última.

Ello enlaza con el informe pericial que expresa que la IP de conexión para la verificación de las operaciones pertenecía al proveedor de servicios Orange.

A pesar de lo manifestado por el perito, respecto de que efectuó comprobaciones de las IP's de conexión en un periodo de 3o dáis anteriores, tal información no consta en el informe.

Hay que resaltar que de ninguno de los medios de prueba resulta que la aplicación bancaria emita aviso, bloqueando la operación, cuando la conexión se ha efectuado a través de una IP no habitual.

De todo lo anterior hay que concluir que no queda acreditado que la demandante hubiera sido advertida de que debía adoptar la precaución de no facilitar en ningún enlace o llamada sus datos de conexión a la aplicación de banca online.

En segundo lugar, no puede considerarse una actitud negligente de la demandante al introducirlos en el enlace al que se le remitía en el sms recibido. Se alega por la demandada que el posible mecanismo empleado por los defraudadores en cuanto a que dicho sms aparezca en el mismohilo de conversaciones que los sms remitidos por la entidad no es responsabilidad de esta. Nadie pone en duda en este aspecto, pero la recepción del sms en esas circunstancias no supone responsabilidad de la entidad sino que lo que determina es que no pueda apreciarse negligencia por la demandante dada la confianza que ello inspira. Como también lo inspira el hecho de que la web espejo empelada sea muy similar a la web habitual de la entidad.

En tercer lugar, de la documental aportada por la demandada, si bien se desprende el envío de sms al móvil de la actora con el código de confirmación desde las operaciones, no se acredita en ningún momento su recepción. Pero es que tampoco se acredita que dichos códigos hayan sido introducidos para finalizar la operación pues Redsys dice que tal autenticación corre a cargo de la entidad bancaria y esta no aporta documental en este sentido.

Así pues, con tales hechos probados, la demandada no ha probado ninguna causa legal de exención de responsabilidad a que viene obligada.

A ello hay que añadir que la IP de conexión expresada en el informe pericial no sería habitual, sin que la demandante hubiera sido advertida de ello.

Existe un incumplimiento contractual imputable a la parte demandada. Hay que recordar que conforme al Art.1258 CC se integran con arreglo a la ley, por lo las normas examinadasmás arriba, de carácter imperativo lo integran, habiendo incumplido con la obligación de atender la reclamación ante un cargo no autorizado por el titular, no existiendo ni fraude ni negligencia de su parte.

No acreditando pues fraude ni negligencia grave, existiendo un incumplimiento del contrato, con daños y perjuicios generados exArt.1101 CC, procede estimar la demanda, debiendo condenar al pago de los intereses legales desde la fecha de interpelación extrajudicial, ex Arts. 110 y 1108 CC, que este caso es desde que se formuló la reclamación, en fecha 16de juniode 2022, hecho que refleja el documento n.º 16de los aportados con la demanda.

TERCERO.- De acuerdo con el artículo 394.1 LEC, procede imponer las costas a la parte demandada. No siendo preceptiva la asistencia de abogado ni procurador, y no apreciándose temeridad, de acuerdo con el Art.32.5 LEC por remisión al Art.394.3 LEC, estando solo obligado a pagar, de la parte que corresponda a los abogados y demás profesionales que no estén sujetos a tarifa o arancel, una cantidad total que no exceda de la tercera parte de la cuantía del proceso.

CUARTO.- A tenor del Art.455 LEC, contra esta sentencia no cabe interponer recurso alguno.

FALLO

Debo estimar la demanda interpuesta por**Dª.** [redacted] representada por la Procuradora [redacted], y asistida por el Letrado Sr.Palomar Pérez**frente a BANCO BILBAO VIZCAYA**

[redacted]

ARGENTARIA SA, representada por la Procuradora Sra. [redacted], y asistida por el Letrado [redacted], **por lo que debo condenar y condeno a la demandada a pagar a la actora DOS MIL SETECIENTOS NOVENTA Y CINCO EUROS CON NOVENTA Y UN CÉNTIMOS DE EURO (2.795,91.- €), más los intereses legales desde el 16de juniode 2022, fecha de interpelación extrajudicial, hasta la fecha de la sentencia, y los intereses judiciales del art. 576 de la LEC desde la fecha de la sentencia hasta su completo pago,todo ello con imposición de costas a la demandada, limitadas respecto a la parte que corresponda a los abogados y demás profesionales que no estén sujetos a tarifa o arancel, a una cantidad total que no exceda de la tercera parte de la cuantía del proceso.**

Notifíquese esta resolución a las partes, haciéndoles saber que la misma es firme, y contra ella no cabe recurso interponer recurso alguno

Así lo acuerda, manda y firma, D.Carlos Gómez Tejada, titular del Juzgado de Primera Instancia Instrucción nº 2 de Alcoy. Doy fe.