ADMINISTRACION DE JUSTICIA

AUD.PROVINCIAL SECCION CUARTA
OVIEDO

SENTENCIA: 00166/2024

Modelo: NI0250
C/ CONCEPCION ARENAL **N°** 3 - 3

Telefono: 985968737 **Fax:** 985968740
Correo electr6nico:

Equipo/usuario: **ARM**

N.I.G. 33033 41 1 2022 0000940
ROLLO: RPL RECURSO DE APELACION (LECN) 0000084 /2024
Juzgado de procedencia: JOO.lA.INST.E INSTRUCCION N.2 de LENA
Procedimiento de origen: ORD PROCEDIMIENTO ORDINARIO 0000517 /2022

Recurrente: UNICAJA, S.A.
Procuradora: MARIA CONSUELO MORALES SUAREZ
Abogada: ALEJANDRA SEVARES CARAS
Recur.idos:
Procurador: TOMAS GARCIA-COSTO ALVAREZ
Abogado: JOSE ANTONIO BALLESTEROS GARRIDO

NUMERO 166

En Oviedo, a diez de abril de dos mil veinticuatro, la Secci6n Cuarta de la Ilma. Audiencia Provincial de Oviedo, compuesta por Don Francisco Tuero Aller, Presidente, Don Javier Alonso Alonso y Dona Raquel Blazquez Martin, Magistrados, ha pronunciado la siguiente:

S E N T E N C I A

PRINCIPADO DE ASTURIAS

En el recurso de apelaci6n numero **84/2024**, procedente del juicio ordinario numero 517/2022 del Juzgado de Primera Instancia numero 2 de Lena, interpuesto por **UNICAJA BANCO**

ADMINISTRACION DE JUSTICIA

S.A., demandado en primera instancia, contra [redacted] demandantes en primera instancia, ha sido ponente la Ilma. Sra. Magistrada oa RAQUEL BLAZQUEZ MARTIN.

ANTECEDENTES DE HECHO

PRIMERO.- El Juzgado de Primera Instancia n° 2 de Lena dict6 sentencia el veinte de noviembre de dos mil veinti tres en el juicio ordinario n° 517/2022 cuya parte dispositiva es del tenor literal siguiente:

> *"**ESTIMANDO iNTEGRAMENTE** la demanda formulada por el Procurador de los Tribunales, Don Tomas Garcia-Cosio Alvarez, en nombre y representaci6n de [redacted] frente a la entidad **UNICAJA BANCO S.A., SE DEBE CONDENAR Y SE CONDENA** a la demandada a reembolsar a los demandantes los 19. 999 euros que le fueron defraudados, con sus intereses legales desde su primera reclamaci6n, el 10 de junio de 2.022 (documento 9). Conimposici6n de costas a la parte demandada.n*

SEGUNDO.- Contra la expresada resoluci6n la parte demandada interpuso recurse de apelaci6n, del que se dio el preceptive traslado. Se remitieron los autos a esta Audiencia Provincial y se sustanci6 el recurse, sefialandose para deliberaci6n y fallo el dia 9 de abril de dos mil veinticuatro.

TERCERO.- Enla tramitaci6n del presente recurso se han observado las prescripciones legales.

FUNDAMENTOS DE DERECHO

PRIMERO.- Resumen del litigio. Planteam.iento del recurso.

1. La sentencia de primera instancia estim6 la demanda formulada por [redacted]

PRINCIP,_00 D[
AsTURIAS

ADMINISTRACION DE JUSTICIA

y conden6 a Unicaja Banco al pago de 19.999 € mas los intereses legales devengados desde la reclamaci6n extrajudicial, asi como al abono de las costas procesales. La sentencia consider6 probado que los demandantes habian sido victimas de una estafa cometida bajo la modalidad conocida *coma smishing par* el importe objeto de condena y que no concurria negligencia grave en su actuaci6n, apreciando por el contrario que el banco demandado no habia acreditado el cumplirniento de las deberes de diligencia que le son exigibles en la gesti6n de las operaciones de pago.

2. La dernandada ha formulado recurso de apelaci6n en el que alega error en la valoraci6n de las pruebas y, en particular, que la sentencia recurrida no ha tenido en cuenta que los dernandantes primero facilitaron las datos de su tarjeta de credito, sin raz6n alguna, en el enlace remitido a traves del SMS fraudulento y, segundo, que recibieron un mensaje de Unicaja Banco con una clave para autorizar una vinculaci6n de un nuevo dispositivo e introdujeron dicha clave sin mediar engano alguno, lo que permiti6 la consumaci6n de la estafa, puesto que el delincuente ya recibi6 en su dispositivo las claves para autorizar las dos transferencias controvertidas. En sintesis, sostiene la recurrente, la disposici6n patrimonial fue posible por el incumplimiento de los dernandantes del deber de custodia de sus claves bancarias.

3. Los demandantes se han opuesto al recurso de apelaci6n.

SEGUNDO.- Circunstancias de hecho relevantes para la resoluci6n del recurso de apelaci6n

1. Se expondran a continuaci6n las hechos que se consideran mas relevantes para la resoluci6n del recurso, que han quedado acreditados a traves de los documentos y pruebas que se especificaran en cada caso y/o de la admisi6n las partes litigantes.

2. Es un hecho no controvertido que el 8 de junio de 2022 a las 20:35 h, recibi6 en su telefono m6vil un SMS procedente, en apariencia, de Liberbank, entidad que par esas fechas estaba en pleno proceso de integraci6n tecnol6gica con Unicaja Banco S.A. El SMS se agrup6 con el hilo de otros SMS enviados par la entidad y contenia el siguiente texto:

ADMINISTRACION DE JUSTICIA

"Hemos detectado un inicio de sesi6n inusual, su cuenta va a ser bloqueada por motivos de seguridad. Puede evitarlo aquí: https://app.liberbank.-es.me"

[redacted] clic6 el enlace que aparecia en el SMS y accedi6 a lo que parecia el entorno web del banco demandado y que, en realidad, era una replica fraudulenta de la aplicaci6n. Para ello introdujo en las espacios destinadas a tal fin su identificaci6n de usuaria y su cantrasena.

3. Aunque en la denuncia yen la reclamaci6n a las que se hara referencia a cantinuaci6n manifesto que una vez dentra de la aplicaci6n fraudulenta introduja las datas que le fueron requeridas para restablecer la aperativa de la cuenta, y concretamente el numero de tarjeta de credito, la fecha de caducidad y el c6diga eve, no esta acreditado que asi fuera. Los dacumentas 2 y 3 de la contestaci6n a la demanda recogen las trazas de operaciones y navegaci6n realizadas por [redacted] el 8 de junio de 2022 (su numera de usuaria es [redacted] y en ellas no aparece la introducci6n de estos datos. Como luego se razonara, este extrema no es especialmente relevante, ya que no se realiz6 ninguna operaci6n fraudulenta a traves de la tarjeta de credito.

4. Es un hecho no controvertido que la demandante recibi6 a continuaci6n (20:37 h) otro SMS con el siguiente texto ***"Unicaja Banco: Introduce la clave de seguridad 363375 para finalizar conla vinculaci6n de disposi ti vo de Banca Digital",*** lo que efectivamente hizo. Aunque este dato no ha sido tenido en cuenta par la sentencia recurrida, se trata de un hecha un relevante que, ademas de ser reconocido de contrario en el escrito de oposici6n al recurso, esta probado a traves de los dacumentos 2 y 3 de la contestaci6n a la demanda. Este SMS, que procedia del canal legitimo del banco demandado, se genera par la operativa del delincuente, que vincul6 otra dispasitiva m6vil a los productos bancarios de los demand.antes, de modo que a traves de el puda realizar las aperacianes fraudulentas, coma ahora se vera.

5. A partir de ahi, el usuario ilicito contaba con las claves de acceso a los servicios de banea digital y con un dispositivo m6vil en el que recibir las contrasenas OTP (one *password time,* de un solo uso) necesarias para ejecutar operaciones, y realiz6 las dos transferencias controvertidas.

PRINCIP,_00 D[
AsTURIAS

ADMINISTRACION DE JUSTICIA

La primera de ellas se ejecut6 a las 20:42 h del 8 de junio de 2022, por importe de 10.000, a una cuenta de destino finalizada en 9197 con el concepto *"Rebellionn "*. Para la ejecuci6n de esta transferencia, que fue ordenada corno transferencia inrnediata, los servicios del banco enviaron una clave OTP al dispositivo vinculado ilicitarnente, que aparece identificado corno dispositivo rn6vil de la dernandante era rnediante el sisterna de notificaciones, no a través del canal SMS.

6. Esta operaci6n fue comunicada a_,. traves del sisterna de rnensajeria SMS autentico de Unicaja, y fue este rnensaje el que sirvi6 de alerta para que los demandantes intentaran cornunicar con el telefono de atenci6n al cliente y se dirigieran seguidarnente al cuartel de la Guardia Civil de Pola de Lena para denunciar lo ocurrido. La diligencia de inicio de la denuncia penal esta datada a las 21:52 horas del 8 de junio. Poco antes habian logrado contactar, despues de varies intentos fallidos, con el Servicio de Atenci6n al Cliente, desde donde se les indic6 que debian denunciar los hechos y acudir a su sucursal al dia siguiente. Pese a ello, la entidad bancaria no procedi6 al bloqueo de la cuenta. Del docurnento 3 de la contestaci6n a la demanda se desprende que antes de ejecutar esta transferencia se habia intentado realizar otra u otras (constan tres registros par igual importe en la hoja Excel) por importe de 12.000 €, que no llegaron a consurnarse posiblernente porque el lirnite de disposici6n asociado por defecto a la cuenta de los demandantes era de 10.000 €.

7. La segunda transferencia fue realizada a las 00:26 horas del 9 de junio de 2022. Su importe fue de 9.999 €, la cuenta de destino una cuenta finalizada en 7045 y el concepto *"numero del diablo"*. La entidad destinataria de estas transferencias fue, segun se explica en la contestaci6n a la dernanda, PFS Card Ireland Limited Sucursal en Espana, que no ha dado ninguna respuesta al intento de retrocesi6n de las mismas.

Tras recibir la comunicaci6n de esta segunda transferencia por el sistema de mensajeria autentico de Unicaja, los demandantes ampliaron la denuncia a las 11:49 h del 9 de junio ante el mismo puesto de la Guardia Civil.

ADMINISTRACION DE JUSTICIA

8. Como ya se ha apuntado, los demandantes habian intentado hablar con el Servicio de Atenci6n al Cliente de Unicaja antes de la presentaci6n de la denuncia. El documento 6 de la demanda acredita seis llamadas realizadas desde el nurnero [redacted] al numero 91 0150100 a partir de las 21:17 h del 8 de junio y hasta las 8:48 h del dia siguiente, asi como otras 10 llamadas desde el telefono , entre las 20:51 y las 23:06 horas del 8 de junio. No se discute que el numero 910150100 es el telefono de atenci6n al cliente de la demandada y que los otros dos telefonos corresponden a los m6viles de los demandantes. La repetici6n de las llamadas da cuenta de la dificultad de establecer contacto real con el mencionado servicio.

9. La reclamaci6n presentada por los demandantes el 10 de junio de 2022 fue rechazada par la demandada, que aleg6 en su contestaci6n (documento 11 de la demanda) que aunque no se discutia que en el origen de las operaciones pudiera encontrarse una actuaci6n fraudulenta ejecutada mediante la tecnica del *smishing*, las operaciones habian sido autenticadas mediante sistema de autenticaci6n reforzado con claves OTP enviadas a traves de SMS de un solo uso al numero de telefono de la demandante y que fueron debidamente contabilizadas sin error tecnico alguno conforme a la normativa de servicios de pago. Sin embargo, no fue asi: coma ya se ha apuntado, de las documentos 2 y 3 de la contestaci6n y del inforrne pericial aportado par las demandantes se desprende que las claves OTP no fueron enviadas al m6vil de la demandante par SMS, sino al nuevo dispositivo fraudulentamente vinculado a traves del canal de notificaciones de la entidad bancaria, que es distinto del canal SMS.

10. La entidad demandada se vio afectada par multiples operaciones fraudulentas similares a la descrita en el mes de junio de 2022. Nose discute la creaci6n de una plataforma de afectados, segun resulta del documenta 14 de la demanda. El proceso de integraci6n tecnol6gica entre Liberbank y Unicaja se habia iniciado el 20 de mayo de 2022 (documento 15 de la demanda}.

SEGUNDO.- El marco normativo aplicable a los hechos controvertidos

PRINCIP,_00 D[
AsTURIAS

ADMINISTRACION DE JUSTICIA

1. Esta sala ha tenido ocasi6n de analizar el rnarco normativo aplicable a hechos similares a los descritos en el fundamento de derecho anterior en las sentencias 624/2023, de 13 de diciembre, 142/2024, de 21 de marzo y 154/2024, de 3 de abril, en procedimientos en que la demanda se dirigia tambien contra Unicaja, por lo que hemos de estar al contenido de dichas resoluciones.

2. Se trataban en estas sentencias los fraudes informaticos cometidos mediante la captaci6n de datos bancarios, induciendo a error a la victima tras hacerse pasar por la propia entidad bancaria, a la que suplantan a traves de correos electr6nicos ("phishing"), llamadas telef6nicas ("vishing") o bien a traves de SMS fraudulentos corno en este caso ("srnishing"), con el objetivo final de que los clientes proporcionen sus datos y claves bancarias para acceder asi a sus cuentas de forrna fraudulenta. En particular, en el caso de la sentencia 142/2024, de 21 de marzo apuntabamos que ***"[l]a excusa frecuentemente utilizada [...] es la de informar sabre un acceso no autorizado a las cuentas online, de tal modo que los clientes alertados ante esa circunstancia, intentan comunicar con el banco cuando en realidad lo que hacen es facili*** tar ***sus datos bancarios al defraudador".***

3. El marco normativo aplicable este tipo de operaciones fraudulentas se encuentra en el RDL 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que sustituy6 a la precedente Ley 16/2009, de 13 de noviembre, de servicios de pago, y que incorpor6 parcialmente a nuestro derecho las instrumentos europeos que se aprobaron a partir de 2015 para dar respuesta a la necesidad de generar un entorno mas seguro y fiable para el desarrollo de unos servicios de pago sometidos a constantes innovaciones, tanto licitas como ilicitas. La Directiva (UE) 2015/2366 sabre servicios de pago en el mercado interior y el Reglamento (UE) 2015/751 sobre las tasas de intercambio aplicadas a las operaciones de pago con tarjeta, respondian a ese designio y su aprobaci6n motiv6 la necesidad de incorporar al derecho espanol el nuevo marco regulatorio, lo que se verific6 a traves del citado RDL 19/2018.

(i) En dicha norma se regulan las obligaciones esenciales tanto del usuario de servicios de pago como de las entidades

ADMINISTRACION DE JUSTICIA

que los pres tan. Desde el primer punto de vista, el usuario esta obligado (art. 41 a]) a utilizar el instrumento de pago de conformidad con las condiciones que regulen la emisi6n y utilizaci6n del misrno, y, en particular, a tornar "*todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas*".

Par su parte, el proveedor de esos servicios esta obligado (art. 42 .1 a]) a cerciorarse que de que "*las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento* [..].".

(ii) En las casos de operaciones no autorizadas o ejecutadas incorrectamente, el usuario esta obligado (art. 43.1) a cornunicar su existencia "*sin demora injustificada, en cuanto tenqa conocimiento de cualquiera de dichas operaciones [...]*" y debe soportar (art. 46.1.3°) "*todas las perdidas derivadas de operaciones de pago no autorizadas si [...] ha incurrido en tales perdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el articulo 41*".

(iii) Fuera de esos tres supuestos -ausencia de comunicaci6n en tiempo de las operaciones, actuaci6n fraudulenta del usuario y negligencia grave- la proveedora del servicio esta obligada a realizar la rectificaci6n del cargo (art. 43.1) y devoluci6n del importe (art. 45.1). Por un lado, ante la negaci6n por el usuario de haber autorizado la operaci6n o la afirmaci6n de que la misma fue realizada de manera incorrecta, corresponde a la proveedora del servicio (art. 44.1°) "*demostrar que la operaci6n de pago fue autenticada, registrada con exactitud y contabilizada, y que nose vio afectada por un fallo tecnico u otra deficiencia del servicio prestado...*". Por otro lado, la proveedorea del servicio tambien tiene la carga de acreditar (art. 44.3°) "que *el usuario del servicio de pago cometi6 fraude o negligencia grave*". Y, por ultimo, el registro de la utilizaci6n del instrumento por el proveedor no basta por si solo y necesariamente para demostrar que "*la operacion de pago fue autorizada por el ordenante, ni que este ha actuado de manera*

fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus *obligaciones [...}"* (art. 44.2º).

(iv) La responsabilidad de la entidad proveedora del servicio de pago se acentua aun mas cuando el proveedor no exige "autenticaci6n reforzada" del cliente, supuesto en que este ultimo unicamente responde de haber actuado de forma fraudulenta (art. 46.2°). La autenticaci6n reforzada se define en el art. 2.5 coma *"la autenticaci6n basada en la utilizaci6n de dos o mas elementos categorizados coma conocimiento (algo que solo conoce el usuario), posesi6n (algo que solo posee el usuario) e inherencia (algo que es el usuario), que* son *independientes -es decir, que la vulneraci6n de uno no compromete la fiabilidad de los demas-, y concebida de manera que se proteja la confidencialidad de los datos de identificaci6n".* No se discute que, en el caso que nos ocupa, las operaciones controvertidas se ejecutaron con el sistema de autenticaci6n reforzada.

3. Del analisis de la normativa expuesta resulta el establecimiento a cargo de la proveedora de los servicios de pago de un riguroso regimen de responsabilidad ante disposiciones no autorizadas, que solo cede con la demostraci6n de la actuaci6n fraudulenta o gravemente negligente del usuario, y que no solo conlleva una inversion de la carga de la prueba, sino que apunta tambien hacer las mecanismos de responsabilidad cuasi objetiva a los que se refiere la sentencia recurrida. Como apuntabamos en las sentencias precedentes de esta sala dicho regimen esta *"sin duda inspirado en la idea de que las beneficios que comporta (tanto para el trafico econ6mico, coma para la actividad del proveedor de los servicios) el avance tecnol6gico en los instrumentos de pago, debe estar justamente compensado con la protecci6n reforzada de quien los emplea y se ve expuesto a actuaciones fraudulentas* [...]"

4. La negligencia grave del usuario coma causa de exoneraci6n de la entidad bancaria es tratada par la Directiva (UE) 2015/2366 en un sentido restrictivo. Segun su considerando 72 *"[a) la hora de evaluar la posible negligencia o la negligencia grave del usuario de servicios de pago, deben tomarse en consideraci6n todas las circunstancias. Las pruebas de una presunta negligencia, y el grado de esta, deben*

ADMINISTRACION DE JUSTICIA

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 mas que la* mera *negligencia, lo que entrana una conducta caracterizada por un grado significati vo de fal ta de diligencia. Un ejemplo seria el guardar las credenciales usadas para la autorizaci6n de una operaci6n de pago junta al instrumento de pago, en un formato abierto y facilmente detectable para terceros".*

Como complemento a esta cualificaci6n de la negligencia del usuario, el considerando 71 de la Directiva establece que *"una vez que el usuario de servicios de pago haya comunicado al proveedor de servicios de pago que su instrumento de pago puede haber sido objeto de* uso *fraudulento, no deben exigirsele responsabilidades por las ul teriores perdidasque pueda ocasionar el uso no autorizado del instrumento".*

Debe tenerse en cuenta, ademas, que la diligencia o negligencia del usuario no pueden ser confrontadas con el sesgo retrospectivo que da el conocimiento final de que las operaciones bancarias se cometieron con fraude. En otras palabras, el patron de referencia debe ser el de quien toma decisiones en la confianza de que el entorno informatico en el que se mueve es el propio de su entidad bancaria. Si nose ha incurrido en una negligencia grave en el primer paso, las decisiones ul teriores deben ser valoradas desde la 6ptica de quien se cree en un entorno **lici** to y seguro, y no desde el conocimiento final de que ese entorno result6 ser fraudulento.

5. Esta misrna configuraci6n de la responsabilidad de la entidad proveedora de servicios de pago ha sido considerada por otras Audiencias Provinciales, corno las que hemos citado en nuestras tres sentencias precedentes (sentencias de las Audiencias Provinciales de Lleida, Sec. 2a, de 29 de junio de 2023; La Rioja, Sec. ia, de 17 de febrero de 2023; Almeria, Sec. la, de 31 de enero de 2023; Madrid, Sec. 10a, de 13 de enero de 2023; Asturias, Sec. 5a, de 22 de junio de 2023, y las queen ellas se citan).

TERCERO.- Desestimaci6n del recurso

1. La aplicaci6n de este sistema normativo a los hechos que se han considerado probados conduce a la desestimaci6n del

ADMINISTRACION DE JUSTICIA

recurso de apelaci6n, porque no se aprecia el error en la valoraci6n de la prueba queen else denuncia.

2. En efecto, ninguna de las actuaciones que el banco apelante califica de gravemente negligentes pueden tener ese calificativo.

(i) El hecho de clicar en el enlace que contenia el SMS fraudulento ni siquiera es calificado por el apelante como una actuaci6n gravemente negligente, sino solo negligente, con la afirmaci6n de que este tipo de enlaces no son entornos seguros. En todo caso, no podemos compartir esta opinion por varias razones. En primer lugar, la distinci6n entre entornos seguros y no seguros requiere de ciertos conocimientos que no todos los usuarios poseen. Como resul ta del informe pericial aportado por los demandantes y de las explicaciones de su autor en el acto del juicio, lo que distingue el protocolo seguro es que la URL contiene los caracteres HTTPS (frente a los no seguros: HTTP), asi coma la aparici6n del simbolo de un candado cerrado cuando la URL completa nose ve en la barra de direcciones del navegador, y no todos los usuarios tienen la formaci6n o la experiencia suficientes como para distinguir una y otra situaci6n. En segundo lugar, se trata de una alegaci6n un tanto ociosa, porque en este caso el enlace que contenia el SMS fraudulento estaba configurado con las caracteristicas de un entorno seguro (https://app.liberbank.-es.me).

(ii) El hecho de que el primer SMS fraudulento ofrezca una completa apariencia de lici tud, por la forma en la que esta redactado, y porque utiliza el identificador (ID) del propio banco para agruparse con el resto de los mensajes legitimos, justifica la actuaci6n del usuario, de modo que el hecho de clicar en el enlace no constituye en modo alguno una negligencia grave. Como apuntabamos en la sentencia 142/2024, de 21 de marzo, se aprecia *"la imposibilidad para el cliente, o para su terminal telef6nico, de percibir que se estaba ante un SMS fraudulento, dada la tecnica utilizada de SPOOFING, pues el estafador utilizaba el propio ID de la entidad bancaria. Actuaci6n la del cliente, por lo demas 16gica ante la alerta, que se suponia enviada por el Banco, de que alguien no autorizado habia entrado en su cuenta onlinell.*

PRINCIP,_00 D[
AsTURIAS

(iii) Sobre la posible introducci6n de los datos de la tarjeta de credito de la demandante, ya se ha explicado que no existe traza de tal actuaci6n en la hoja Excel que recoge toda la operativa vinculada a su usuario el 8 de junio de 2022. Ciertamente, [redacted] mencion6 tanto en la denuncia penal como en la reclamaci6n presentada ante el Servicio de Atenci6n al Cliente que habia facilitado estos datos tras acceder a la aplicaci6n fraudulenta, lo que luego ha explicado en el interrogatorio de parte como fruto de un error achacable al nerviosismo que la situaci6n le produjo. Como quiera que fuera, ya hemos dicho que esta cuesti6n no es especialmente relevante, primero porque no se realiz6 ninguna operaci6n de tarjeta de credito, y, segundo, porque tampoco incurriria en el concepto de negligencia grave el hecho de facilitar los datos que pide la aplicaci6n que el usuario considera que es la autentica aplicaci6n de su banco para evitar el bloqueo de la cuenta, precisamente porque de lo que se trata es de evitar ese bloqueo y de restablecer la operativa normal de dicha cuenta.

(iv) Sobre la autorizaci6n por la demandante de la vinculaci6n de otro dispositivo m6vil, se trata de una conducta que ya ha sido analizada en la sentencia 142/2024, de 21 de marzo, en estos terminos:

> *"Nose advertia entonces, como pretende la apelante, de que se trataba de vincular otro dispositivo distinto, circunstancia que podria haber generado desconfianza en el cliente, sino que se hablaba solo de dispositivo, sin indicar cual fuera, de tal modo que lo que hubo de presumir este es que se trataba del propio, que habia que vincular de nuevo dado el acceso no autorizado del que habia sido informado. No es cierto, en consecuencia, que el demandante hubiera introducido la clave OTP necesaria para llevar a cabo la concreta operaci6n, la transferencia indicada, sino que, una vez vinculado el dispositivo que utilizaba el ciberdelincuente, a este le serian remitidas las claves necesarias para las nuevas operaciones que deseara realizar, y no a quien aqui acciona.*
>
> *En definitiva, este segundo paso venia precedido y motivado por el engaiio ya consumado con el primer SMS, y estaba sin duda guiado por el animo de evitar lo que,*

desgraciadamente, se perseguia con el, por lo que esa actuaci6n no puede calificarse de temeraria ni gravemente negligente, sin que, coma deciamos en la sentencia citada de 13 de diciembre de 2023, "pueda exigirse a quien resul t6 enganada mayor precauci6n que a quien debia poner las medias necesarios para evitar el engaiio".

(v) Es evidente que la actuaci6n de la demandante estuvo enteramente condicionada par el engan.o ya consumado con el SMS, y, coma hemos advertido en casos similares, estuvo ademas guiada par el anirno de evitar lo que, desgraciadamente, se perseguia con ella. Por ello, esa actuaci6n no puede calificarse coma gravemente negligente en el contexto de engano consumado, sin que pueda exigirse al usuario que resulta engan.ado mayor precauci6n que a la entidad bancaria que debe poner las medics necesarios para evitar el engano.

3. En efecto, concurren datos plurales que apuntan a la responsabilidad del banco apelante. Es muy significativo que el conjunto de las operaciones trazadas en el documento Excel aportado con la contestaci6n a la demanda no hiciera saltar alguna alerta 0 aviso que llarnara a corroborar su autenticidad.

(i) Asi, las transferencias fraudulentas fueron ejecutadas utilizando una operativa singular y completamente ajena a la que era propia de las demandantes.

(ii) Fueron realizadas par importes elevados, hasta el limite de lo permitido en un caso y por 1 € menos en el otro, como transferencias de ejecuci6n inmediata, que no suelen ser las habituales en la operativa de un usuario media, par el importe de las comisiones que conllevan.

(iii) Se realizaron ademas inmediatamente despues de un cambio en el dispositivo m6vil vinculado a la aplicaci6n.

(iv) La vinculaci6n de un nuevo dispositivo m6vil fue posible porque el sistema empleado par la entidad bancaria no era especialmente seguro, por el texto equivoco del SMS enviado a tal fin y por la facilidad de que un SMS de este tipo no despierte las sospechas de los usuarios previamente alertados por un mensaje fraudulento de accesos indebidos a su cuenta online.

ADMINISTRACION DE JUSTICIA

(v) La primera transferencia se realize despues de uno o varios intentos de ejecutar otra u otras operaciones por un importe superior, 12.000 €, intento que result6 frustrado por los limites de disposici6n de la cuenta.

(vi) La segunda transferencia se llev6 a cabo a los pocos minutes del cambio de fecha, cuando ya no estaba operative el limite diario de disposici6n de la cuenta. Esa segunda transferencia fue posible ademas porque el Servicio de Atenci6n al Cliente del banco demandado no bloque6 la cuenta, pese a tener ya conocimiento de la prirnera operaci6n, cuando ademas podia haber cornprobado los intentos fallidos de realizar otras transferencias por un irnporte superior al autorizado diario. Ademas, las transferencias iban dirigidas a una cuenta de la entidad PFS Card Ireland Limited Sucursal en Espana, una entidad inusual en el trafico bancario, con conceptos tan llarnativos coma *"Rebellion"* [rebeli6n] y *"Numero del diablo"*.

4. Este conjunto de circunstancias evidencia la falta de medidas de seguridad de los sisternas de detecci6n de fraude en la fecha en la que sucedieron los hechos o, coma minima, el fallo de las rnedidas irnplernentadas a tal fin, lo que queda ratificado por el elevado nurnero de operaciones fraudulentas concentradas en las mismas fechas, pues, como hemos apuntado en otras resoluciones, dificilmente puede sostenerse que un gran numero de usuarios hubiera incidido casi simultaneamente en una conducta gravemente negligente en sus interacciones con el banco.

CUARTO.- Costas

Las costas del recurso se imponen a la apelante (art. 398.1° LEC).

En atenci6n a lo expuesto, esta Sala pronuncia el siguiente

FALLO

1. Desestirnamos el recurso de apelaci6n interpuesto por Unicaja Banco S.A. frente a la sentencia dictada por el Juzgado de Primera Instancia 2 de Lena el 20 de noviembre de 2023 en el juicio ordinario 517/2022.

ADMINISTRACION DE JUSTICIA

2. Imponemos a la parte apelante las costas de esta segunda instancia.

3. Acordamos la perdida del dep6sito constituido para SU interposici6n, al que se dara el destino legal.

Contra esta sentencia podra interponerse recurso de casaci6n, en los casos, par los motivos y con los requisitos prevenidos en los arts. 477 y ss. L.E.C., debiendo interponerse en el plaza de veinte dias ante este Tribunal, con constituci6n del dep6sito previsto en la D.A. 15 LOPJ.

Asi, por esta sentencia, lo pronunciamos, mandamos y firmamos.