ADMINISTRACION DE JUSTICIA

JDO. PRIMERA INSTANCIA N. 3
GIJON

SENTENCIA: 00161/2024

PLAZA DECANO EDUARDO IBASETA, S/N, 3 PLANTA
Teléfono: 985175673-2-4, Fax: 985175675
Modelo: 0030K0
N.I.G.: 33024 42 1 2023 0009305
JVB JUICIO VERBAL 0000873 /2023
Sobre OTRAS MATERIAS

SENTENCIA

En Gijón, a 11 de marzo de 2024.

Vistas por Coral Gutiérrez Presa, Magistrada-Juez del Juzgado de Primera Instancia nº 3 de esta ciudad, las presentes actuaciones de juicio verbal que, bajo el nº 873/23, se siguen en este Juzgado entre las siguientes partes, como demandante, don , representado por la Procuradora Sra. Revuelta Capellín y asistido técnicamente por el Abogado Sr. García López y como demandada, la entidad "UNICAJA BANCO, S.A", representada por el Procurador Sr. y defendida por la Abogada Sra. y que versan sobre reclamación de cantidad y, atendiendo a los siguientes,

ANTECEDENTES DE HECHO

PRIMERO. Por la Procuradora Sra. Revuelta Capellín, en representación de don , se formuló, en fecha 12 de julio de 2.023, demanda de juicio verbal contra Unicaja Banco, S.A, en reclamación de la cantidad de 5.000 euros.

La demanda se basa, en síntesis, en los siguientes hechos: el demandante, en su condición de cliente minorista-consumidor, es titular de una cuenta bancaria de la entidad demandada. El día 12 de julio de 2022 recibió un SMS de Unicaja a través del canal de comunicación por el que recibe todos los SMS de su entidad bancaria. En el mismo se le advierte que se ha vinculado un nuevo dispositivo y que si no reconoce esta actividad, pinche en un link de Unicaja. El actor, al pensar que se trataba de un mensaje de su entidad bancaria, pinchó en el enlace, siendo derivado a una página de Unicaja Banco. Una vez en la página web, le solicitan sus datos personales y contraseña. Al comprobar que se trataba de la página web de su entidad bancaria (mismos logotipo y apariencia), facilitó sus datos y su contraseña, siendo

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

informado de que un agente se pondrá en contacto telefónico con él en breves momentos. El actor recibió entonces una llamada telefónica de una persona que se identificó como agente de su entidad bancaria, le informó que habían realizado dos transferencias desde su cuenta. Al confirmarle el actor que no había realizado ni autorizado movimiento alguno, el agente le informa que para anularlas ha de facilitarle las claves que le iban a llegar por SMS. A través de la app de Unicaja recibe unos mensajes con un código, el cual facilita al agente en la convicción de que eran para anular las transferencias. Finalizada la llamada, comprobó en la banca digital que se habían realizado dos transferencias no consentidas ni autorizadas por importe total de 5.000 euros.

Alega el actor que no actuó de forma negligente y que, en cambio, los sistemas de seguridad del Banco han fallado.

Finalmente, alega que en el contrato de cuenta bancaria que tiene suscrito con la demandada, la entidad bancaria ha fijado una comisión por reclamación de posiciones deudoras que es abusiva y, por tanto, nula.

Por todo ello, concluye suplicando que se dicte sentencia por la que se condene a la demandada a abonar al actor la cantidad de 5.000 euros, más los intereses legales y se declare la nulidad por el carácter abusivo de la cláusula que establece la comisión por reclamación de posiciones deudoras, condenando, además, a la demandada a abonar a la demandante la cantidad total resultante que le hayan venido siendo impuesta en concepto de tal cláusula controvertida, según se determinará en ejecución de sentencia; que adecúe su actuar futuro a tal declaración; con intereses legales.

Y todo ello, con imposición de las costas a la parte demandada.

SEGUNDO. Admitida a trámite la demanda, se dio traslado de la misma a la parte demandada. Por escrito presentado el 3 de noviembre de 2.023, el Procurador Sr. , en representación de Unicaja Banco, S.A, se opuso a la demanda argumentando que fue la negligencia grave del actor la que propició que los defraudadores pudieran tener acceso a sus claves y así poder efectuar las operaciones con cargo a su cuenta corriente, habiendo actuado correctamente la entidad bancaria, ya que envió al teléfono móvil del actor los mensajes con la clave para autorizar las operaciones, y añade que la mera lectura de los mensajes le hubiera puesto de manifiesto que estaba autorizando las transferencias.

Por todo ello, suplica que se dicte sentencia por la que se desestime la demanda y se impongan las costas a la parte actora.

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

TERCERO. El día 6 de marzo de 2.024 se celebró la vista, a la que acudieron ambas partes. En primer lugar, la parte demandada se allanó a la pretensión de nulidad de la comisión de reclamación de posiciones deudoras. Subsistiendo el litigio en relación con la otra pretensión, se procedió a fijar el objeto del proceso y se continuó con la proposición de prueba; las partes propusieron los medios de prueba de que intentaban valerse, siendo admitidos los considerados útiles y pertinentes, los cuales se practicaron con el resultado obrante en autos, quedando, a continuación, el juicio visto para sentencia.

CUARTO. En la tramitación del presente juicio, se han observado las formalidades legales.

FUNDAMENTOS DE DERECHO

PRIMERO. A través de la demanda rectora del presente procedimiento, el demandante Sr. , titular de una cuenta corriente abierta en la entidad Unicaja Banco, S.A, ejercita una acción en reclamación de 5.000 euros en que cuantifica los daños y perjuicios que se le causaron como consecuencia de dos operaciones realizadas por un tercero desconocido con cargo a la cuenta de la que era titular, al haber sido víctima de un uso fraudulento de su cuenta, mediante la actuación fraudulenta denominada "phising" o "smishing" de la que fue víctima, cuando recibió un SMS en el que se le indicaba que se había vinculado un nuevo dispositivo en su cuenta y que si no reconocía esa actividad, pinchara en un link, lo que realizó el actor en la creencia de que se trataba de la página web de su Banco.

Sostiene el actor que la entidad bancaria demandada ha incumplido sus deberes contractuales y legales e invoca las obligaciones que imponen a la entidad bancaria el Real Decreto Ley 19/2018 de 23 de noviembre de Servicios de Pago, la Directiva (UE) 2915/2366 del Parlamento y del Consejo, de 25 de noviembre sobre servicios de pago en el mercado interior y el Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017.

Frente a ello, la entidad bancaria alega que la pérdida patrimonial sufrida por el demandante se debe a la actuación delictiva de un tercero y niega haber incurrido en los incumplimientos que se le atribuyen, añadiendo que ha sido la negligencia del propio actor la que ha permitido el acceso por los defraudadores a sus claves y así poder hacer las operaciones con cargo a su cuenta corriente, señalando que la entidad bancaria envió al teléfono del actor los mensajes con las claves necesarias para autorizar las operaciones y añade

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

que la mera lectura de los mensajes ya habría puesto al actor en aviso porque se le indicaba que iban a realizar dos transferencias.

Fijadas así las posiciones de las partes, para resolver sobre la pretensión ejercitada conviene fijar previamente los hechos que han quedado acreditados a lo largo del procedimiento.

Así, constituye un hecho no controvertido que el actor es titular de una cuenta corriente que tiene abierta en la entidad bancaria demandada (documento nº1 de la demanda).

De los documentos nº2 a 4 de la demanda y de las actuaciones realizadas por la Policía estimo acreditado que el día 12 de julio de 2.022 el demandante recibió un SMS a través del canal de comunicación por el que recibe todos los SMS de su entidad bancaria Unicaja, que decía: "Se ha vinculado un nuevo dispositivo (iPhone X, Ibiza) el 12/07 a las 14:43h. Si no reconoce verifique inmediatamente (enlace https://unicaja-movil.alerta.com/r/UNIVIA)."

Tal como reconoció el actor en la vista, pinchó en el enlace, en la creencia de que era de su entidad y le derivó a una página con la misma apariencia que la página en la que opera normalmente con Unicaja, introduciendo su usuario y clave apareciendo un mensaje que le indicaba que le iba a llamar personal del banco. En ese momento, recibió una llamada de teléfono identificada en el dispositivo como procedente de Málaga, de una persona que se identificó como empleado de Unicaja, que le indicó que para anular dos transferencias que acababan de efectuarse en su cuenta tenía que facilitarle las claves que le iban a llegar por SMS.

En ese momento Unicaja envió al teléfono móvil del actor el siguiente mensaje: "UNIVIA: Transferencia internacional, Cuenta de Abono: IE37 PFSR 9910 7013 5508 71, importe 2.000,00 EUR. Clave de seguridad: 537334".

E inmediatamente, Unicaja envió al teléfono del actor el siguiente mensaje: "UNIVIA: Transferencia internacional, Cuenta de Abono: MT62 PAPY 3683 6000 0026 7637, importe 3.000,00 EUR. Clave de seguridad: 826223".

El demandante, facilitó las referidas claves a la persona con la que estaba hablando en la creencia de que se trataba de personal del banco y de que su finalidad era cancelar las transferencias que él no había autorizado.

A través del engaño de que fue víctima el demandante, personas desconocidas detrajeron del saldo de su cuenta un total de 5.000 euros mediante dos transferencias.

SEGUNDO. Partiendo de los hechos expuestos y centrada la controversia en si el comportamiento adoptado por las partes litigantes debe ser calificado como negligente, en el cumplimiento de las obligaciones que para cada una de ellos se

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

deriva de los contratos de cuenta bancaria que les vincula y las consecuencias a extraer de todo ello, el marco normativo de que debe partirse viene constituido por el RDL 19/2018, la Directiva 2015/2366 y el Reglamento delegado 2018/389 de la Comisión. Como se indica en la sentencia de 21 de diciembre de 2.021 de la de la Audiencia provincial de Pontevedra, en la que se analiza un supuesto de hecho similar al presente, el marco normativo del que debe partirse es el siguiente:

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. Considerando (72): "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 servicios aporte pruebas de la presunta negligencia, puesto que los medios a disposición del ordenante son limitados en esos casos".

El Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017 por el que se complementa la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros.

"Artículo 2. Requisitos generales de autenticación.

1. Los proveedores de servicios de pago dispondrán de mecanismos de supervisión de las operaciones que les permitan detectar operaciones de pago no autorizadas o fraudulentas a efectos de la aplicación de las medidas de seguridad a que se hace referencia en el artículo 1, letras a) y b).

Dichos mecanismos se basarán en el análisis de las operaciones de pago teniendo en cuenta los elementos que caractericen al usuario de servicios de pago en el contexto de un uso normal de las credenciales de seguridad personalizadas.

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

2.Los proveedores de servicios de pago garantizarán que los mecanismos de supervisión de las operaciones tengan en cuenta, como mínimo, todos los factores basados en el riesgo siguientes: a) listas de elementos de autenticación comprometidos o sustraídos; b) el importe de cada operación de pago; c) supuestos de fraude conocidos en la prestación de servicios de pago; d) señales de infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación; e) en caso de que el dispositivo o el programa informático de acceso sea facilitado por el proveedor de servicios de pago, un registro de la utilización del dispositivo o el programa informático de acceso facilitado al usuario de los servicios de pago y de su uso anormal.

Artículo 3. Revisión de las medidas de seguridad.

"La aplicación de las medidas de seguridad a que se refiere el artículo 1 deberá documentarse, probarse periódicamente, evaluarse y auditarse de conformidad con el marco jurídico aplicable al proveedor de servicios de pago por auditores con experiencia en el ámbito de la seguridad y los pagos informáticos y funcionalmente independientes, ya pertenezcan al organigrama del propio proveedor de servicios de pago o sean externos a él…".

Y el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera:

"Artículo 41. Obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas.

El usuario de servicios de pago habilitado para utilizar un instrumento de pago: a) utilizará el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del instrumento de pago que deberán ser objetivas, no discriminatorias y proporcionadas y, en particular, en cuanto reciba un instrumento de pago, tomará todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas;

b) en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, lo notificará al proveedor de servicios de pago o a la entidad que este designe, sin demora indebida en cuanto tenga conocimiento de ello.

Artículo 42. Obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago.

1. El proveedor de servicios de pago emisor de un instrumento de pago:

a) Se cerciorará de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento, sin perjuicio de las obligaciones que

PRINCIPADO DE ASTURIAS

incumben al usuario de servicios de pago con arreglo al artículo 41.
b) Se abstendrá de enviar instrumentos de pago que no hayan sido solicitados, salvo en caso de que deba sustituirse un instrumento de pago ya entregado al usuario de servicios de pago. Esta sustitución podrá venir motivada por la incorporación al instrumento de pago de nuevas funcionalidades, no expresamente solicitadas por el usuario, siempre que en el contrato marco se hubiera previsto tal posibilidad y la sustitución se realice con carácter gratuito para el cliente.
c) Garantizará que en todo momento estén disponibles medios adecuados y gratuitos que permitan al usuario de servicios de pago efectuar una notificación en virtud del artículo 41.b), o solicitar un desbloqueo con arreglo a lo dispuesto en el artículo 40.4. A este respecto, el proveedor de servicios de pago facilitará, también gratuitamente, al usuario de dichos servicios, cuando éste se lo requiera, medios tales que le permitan demostrar que ha efectuado dicha comunicación, durante los 18 meses siguientes a la misma.
d) Ofrecerá al usuario de servicios de pago la posibilidad de efectuar una notificación en virtud del artículo 41.b), gratuitamente y cobrar, si acaso, únicamente los costes de sustitución directamente imputables al instrumento de pago.
e) Impedirá cualquier utilización del instrumento de pago una vez efectuada la notificación en virtud del artículo 41.b).
2. El proveedor de servicios de pago soportará los riesgos derivados del envío de un instrumento de pago al usuario de servicios de pago o del envío de cualesquiera elementos de seguridad personalizados del mismo.
Artículo 43. El usuario de servicios de pago obtendrá la rectificación por parte del proveedor de servicios de pago de una operación de pago no autorizada o ejecutada incorrectamente únicamente si el usuario de servicios de pago se lo comunica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación, incluso las cubiertas por el artículo 60, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo. Los plazos para la notificación establecidos en el párrafo primero no se aplicarán cuando el proveedor de servicios de pago no le haya proporcionado ni puesto a su disposición la información sobre la operación de pago con arreglo a lo establecido en el título II.
Artículo 44. Prueba de la autenticación y ejecución de las operaciones de pago.
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

ADMINISTRACION DE JUSTICIA

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.
Artículo 45 Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas.
1. Sin perjuicio del artículo 43 de este Real decreto-ley, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada.
Artículo 46 Responsabilidad del ordenante en caso de operaciones de pago no autorizadas.
1. No obstante lo dispuesto en el artículo 45, el ordenante podrá quedar obligado a soportar, hasta un máximo de 50 euros, las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado, sustraído o apropiado indebidamente por un tercero, salvo que:

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

a) al ordenante no le resultara posible detectar la pérdida, la sustracción o la apropiación indebida de un instrumento de pago antes de un pago, salvo cuando el propio ordenante haya actuado fraudulentamente, o
b) la pérdida se debiera a la acción o inacción de empleados o de cualquier agente, sucursal o entidad de un proveedor de servicios de pago al que se hayan externalizado actividades.
El ordenante soportará todas las pérdidas derivadas de operaciones de pago no autorizadas si el ordenante ha incurrido en tales pérdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 41. En esos casos, no será de aplicación el importe máximo contemplado en el párrafo primero.
En todo caso, el ordenante quedará exento de toda responsabilidad en caso de sustracción, extravío o apropiación indebida de un instrumento de pago cuando las operaciones se hayan efectuado de forma no presencial utilizando únicamente los datos de pago impresos en el propio instrumento, siempre que no se haya producido fraude o negligencia grave por su parte en el cumplimiento de sus obligaciones de custodia del instrumento de pago y las credenciales de seguridad y haya notificado dicha circunstancia sin demora.
2. Si el proveedor de servicios de pago del ordenante no exige autenticación reforzada de cliente, el ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta. En el supuesto de que el beneficiario o el proveedor de servicios de pago del beneficiario no acepten la autenticación reforzada del cliente, deberán reembolsar el importe del perjuicio financiero causado al proveedor de servicios de pago del ordenante.
3. Salvo en caso de actuación fraudulenta, el ordenante no soportará consecuencia económica alguna por la utilización, con posterioridad a la notificación a que se refiere el artículo 41.b), de un instrumento de pago extraviado o sustraído.
4. Si el proveedor de servicios de pago no tiene disponibles medios adecuados para que pueda notificarse en todo momento el extravío o la sustracción de un instrumento de pago, según lo dispuesto en el artículo 42.1.c), el ordenante no será responsable de las consecuencias económicas que se deriven de la utilización de dicho instrumento de pago, salvo en caso de que haya actuado de manera fraudulenta.
Artículo 64. Ausencia de responsabilidad cuando concurran circunstancias excepcionales e imprevisibles.
La responsabilidad establecida con arreglo a los Capítulos II y III de este Título no se aplicará en caso de circunstancias excepcionales e imprevisibles fuera del control de la parte

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

que invoca acogerse a estas circunstancias, cuyas consecuencias hubieran sido inevitables a pesar de todos los esfuerzos en sentido contrario, o en caso de que a un proveedor de servicios de pago se le apliquen otras obligaciones legales.

Artículo 68. Autenticación.

1. Los proveedores de servicios de pago aplicarán la autenticación reforzada de clientes, en la forma, con el contenido y con las excepciones previstas en la correspondiente norma técnica aprobada por la Comisión Europea, cuando el ordenante:

a) acceda a su cuenta de pago en línea;

b) inicie una operación de pago electrónico;

c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos.

6. No obstante, no será preciso aplicar la autenticación reforzada de clientes a la que se refiere el apartado 1 a los supuestos indicados en el artículo 98.1.b) de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015".

TERCERO. De acuerdo con la normativa expuesta, "el proveedor de servicios de pago se encuentra sujeto al cumplimiento de específicas obligaciones de protección en la emisión de los instrumentos de pago y en los procesos de autenticación de las operaciones de pago cuya finalidad es minimizar la probabilidad de ejecución de operaciones no autorizadas.

En relación con los instrumentos de pago ha de cumplir con las obligaciones sobre emisión y uso seguro que se establecen en el artículo 42.1 RDL 19/2018.

Los procesos o mecanismos de autenticación de las operaciones de pago deben cumplir con los requisitos que establece el Reglamento Delegado 2018/389, lo que exige:

a) Implementar las medidas de seguridad previstas en el artículo 1, que han de incluir el procedimiento de autenticación reforzada de clientes, con las salvedades específicamente señaladas.

b) Incluir mecanismos de supervisión de las operaciones que permitan al proveedor de servicios de pago detectar operaciones de pago no autorizadas o fraudulentas. A tal efecto el proveedor de servicios de pago ha de tener en cuenta la totalidad de los factores de riesgo enumerados en el artículo 2, y, entre ellos, los supuestos de fraude conocidos en la prestación de servicios de pago.

c) Auditar las medidas, en las condiciones del artículo 3.

Por su parte, el usuario de los servicios de pago deberá cumplir con las obligaciones que se establecen en el artículo 41 RDL 19/2010: a) Usar del instrumento de pago conforme a lo pactado y tomar las medidas razonables a fin de proteger sus

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

credenciales de seguridad personalizadas; b) En cuanto tenga conocimiento de haber perdido la posesión del instrumento de pago o de haber sido este utilizado sin su autorización, lo notificará sin demora indebida al proveedor de servicios de pago.

El régimen de la responsabilidad por las pérdidas derivadas de operaciones de pago por uso fraudulento de un instrumento de pago por un tercero se determina interpretando de manera integrada las previsiones del artículo 46 con la regulación general de las pérdidas por operaciones de pago no autorizadas del artículo 45 y con el régimen de la carga probatoria que se establece en el artículo 44 (todos del RDL 19/2018).

Será el proveedor de los servicios de pago quien habrá de responder de las pérdidas de importe superior a 50 euros por las operaciones de pago resultantes del uso fraudulento del instrumento de pago por un tercero; responderá de la totalidad de la pérdida cuando al ordenante no le hubiera sido posible detectar el posible uso fraudulento antes de que éste se hubiese materializado o cuando la pérdida se debiera a la acción u omisión de cualquier persona de la que el proveedor de servicios hubiera de responder.

En cambio, el ordenante será quien soporte la totalidad de las pérdidas cuando concurran dos requisitos: a) La operación de pago fue autenticada y registrada con exactitud y no se vio afectada por ninguna deficiencia del servicio prestado por el proveedor de servicios de pago; b) El ordenante actuó de manera fraudulenta, o incumpliendo deliberadamente o por negligencia grave alguna de las obligaciones recogidas en el artículo 41 RDL 19/2018.

Al proveedor de servicios de pago le corresponde la carga procesal de acreditar tanto su propio comportamiento diligente en la autenticación de la operación de pago como el fraude o la negligencia grave del ordenante. La prueba de la diligencia en el procedimiento de autenticación deberá realizarse en relación a las exigencias del Reglamento Delegado 2018/389. La prueba del fraude del ordenante requerirá de la acreditación de hechos de los que pudiera llegar a inferirse que aquel actuó con engaño para beneficiarse de la operación de pago. La prueba de la negligencia grave del ordenante requerirá de la acreditación de las circunstancias concurrentes en la operación de pago de las que quepa inferir que la misma pudo realizarse porque aquel obró con una significativa falta de diligencia al usar del instrumento de pago o al proteger sus credenciales.

Cuando el proveedor de servicios de pago no acredite el cumplimiento de los deberes de diligencia propios en la autenticación habrá de responder de la pérdida resultante del uso fraudulento del instrumento de pago por un tercero salvo

PRINCIPADO DE ASTURIAS

que concurra el fraude del ordenante." (SAP Pontevedra 21/12/21).

CUARTO. Una vez detallada la normativa de aplicación, a la vista del contenido de la documental aportada cabe afirmar que el actor ha sido víctima de un fraude, hecho que no es negado por la parte demandada.

El tipo de fraude sufrido por el actor se describe en la sentencia de la Audiencia Provincial de Cantabria de 10 de octubre de 2.023 en los siguientes términos: "De acuerdo con la definición dada por la Agencia Española de Protección de Datos, en resolución de fecha 24 de mayo de 2006, "el objetivo de los ataques de "phishing" es la obtención de forma engañosa y fraudulenta de los códigos de usuarios y contraseñas de clientes de Banca Electrónica, al objeto de realizar transferencias no autorizadas... Su operatoria comienza con la adquisición en internet de un "paquete de herramientas", que incluyen programas informáticos e información necesaria para realizar los ataques. Esta información incluye "listas de equipos comprometidos" que pueden ser utilizados bien para mandar correos electrónicos, bien para alojar páginas web falsificadas. Incluyen además "bases de datos de direcciones de correo electrónico". Una vez en posesión del paquete, se remiten los correos electrónicos con carácter indiscriminado (buscando contactar con clientes de la entidad financiera) informando de la necesidad de conectarse a una página web que parece pertenecer a la citada entidad y portar los códigos de acceso y contraseñas de clientes. Dicha página web se suele alojar en un equipo conectado a Internet cuya seguridad se haya [visto] comprometida", sin conocimiento de su usuario, y que se encuentra normalmente en un país distinto al de los destinatarios del ataque. De esta forma se constituye "un fichero de datos personales con códigos de usuarios y contraseñas de clientes" recabados de forma engañosa y fraudulenta, que se ubica normalmente en el mismo "equipo remoto comprometido" en el que se aloja la página web falsificada. Con los datos obtenidos se realizan trasferencias a cuentas de colaboradores situados en España los cuales a su vez retiran el dinero en efectivo y tras descontar una comisión realizan transferencias monetarias internacionales mediante entidades especializadas."

Habitualmente se hace efectiva a través del envío de correos electrónicos o SMS engañosos, en los que se imita el lenguaje, formato e imagen de las entidades bancarias o financieras suplantando su identidad y, solicitando los datos personales de las víctimas alegando diferentes motivos. Los métodos empleados para este tipo fraude son diversos (clonación de tarjetas, skimming o carcasa superpuesta, el pharming o introducirse en un servidor a través de hackers,

ADMINISTRACION DE JUSTICIA

capturando claves, contraseñas, etc.) y no necesariamente llega a descubrirse en todos los supuestos el concreto método empleado; si bien es evidente, en cualquier caso, que se trata de una operación no autorizada por el titular de la cuenta corriente, el cual ve sustraído sus datos y claves de una manera fraudulenta, a través de medios técnicos".

QUINTO. Aplicando la normativa indicada al supuesto aquí analizado, la primera conclusión que se alcanza es que no cabe apreciar en el demandante un comportamiento negligente de la gravedad y entidad para con base en el mismo hacerle responsable. Como se indica en la Directiva 2015/2036 la negligencia que hace responder al cliente, es la que se deriva de una conducta caracterizada por un grado significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que ha sido inducido por un delincuente profesional. Tampoco puede calificarse como grave dicho comportamiento conforme a la normativa del código civil, pues siendo exigible al demandante la diligencia que exija la naturaleza de la obligación y correspondan a las circunstancias de las personas, tiempo y lugar (art. 1.104 del cc), el método fraudulento empleado es de una complejidad y grado de perfección, difícilmente detectable por un consumidor medio. Ha de tenerse en cuenta que el SMS fue recibido dentro de la línea de mensajes procedentes de la entidad bancaria, creando una apariencia de legitimidad. Que el interlocutor se identificó como personal de Unicaja desde un número de teléfono que en la pantalla del terminal telefónico del actor se identificaba como procedente de Málaga, con el mismo número empleado por las oficinas de Unicaja en Málaga.

En supuestos similares nuestra Audiencia Provincial no ha considerado esta conducta constitutiva de negligencia grave. Así, la Sentencia de la Sección 5ª de fecha 22 de junio de 2.023 declara: "La única negligencia imputable al consumidor radica en haber confiado en el SMS recibido en su móvil, en la línea de mensajes de la demandada, y consignar en la página a la que resultó redireccionada las claves de acceso a su usuario, lo que esta Sala no ha considerado constitutivo de una negligencia grave en atención a la distribución de la responsabilidad regulado en la LSP. En la reciente sentencia de veinte de abril de dos mil veintitrés señalamos, en un supuesto análogo: "... la prueba allegada por el banco al respecto, que se redujo a una certificación del empleado de la demandada responsable del Departamento de Banca Digital aparece desmentido o, al menos, resulta insuficiente para probar, como le corresponde a la recurrente, aquella actuación negligente del cliente basada en la comunicación a terceros o cuidado de la clave de acceso. Como señala la sentencia de la

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

Sec. 3ª de la AP de Burgos de 5 de diciembre de 2022 a propósito del fraude por phishing, "la mayor parte de las AAPP han apreciado responsabilidad del proveedor de servicios de pago cuando lo único que ha hecho el usuario es descargarse estos programas maliciosos, sin introducir un segundo código de autenticación. Así, SSAP Zaragoza sección 5 del 1 de julio de 2022 (ROJ: SAP Z 1482/2022), Granada sección 5 del 20 de junio de 2022 (ROJ: SAP GR 957/2022), Valencia sección 6 del 13 de junio de 2022 (ROJ: SAP V 2622/2022), Madrid sección 20 del 20 de mayo de 2022 (ROJ: SAP M 7327/2022), y Pontevedra sección 6 del 21 de diciembre de 2021 (ROJ: SAP PO 3078/2021)".

Ciertamente, en el caso de autos, el comportamiento del actor no puede considerarse diligente, pero para hacer soportar al cliente las consecuencias, es preciso apreciar en él una negligencia y que además sea grave, que en la normativa europea antes referida se equipara a la comisión de un fraude, actuación en la que no se ha acreditado incurriese el demandante. En primer lugar, ha de tenerse en cuenta que el mensaje tenía apariencia de legitimidad, pues, lo recibió el actor en la misma línea que el resto de mensajes enviados por Unicaja, por lo que, el hecho de haber pinchado en el link que se le ofrecía no se estima constitutivo de grave negligencia. En segundo lugar, en la página a la que accedió, que tenía la apariencia de ser la de Unicaja, se le informaba de que iba a recibir una llamada de uno de sus agentes y la persona que le llamó se identificó como personal de Unicaja llamando desde un teléfono supuestamente procedente de Málaga, por lo que, cualquier cliente medio en su misma situación hubiera pensado que efectivamente estaba recibiendo una llamada de Unicaja.

Por otro lado, si bien el hecho de haber facilitado las claves recibidas por SMS constituye un acto imprudente, el mismo ha ser valorado en las circunstancias personales, de tiempo y lugar, en las que se produjo. Así, ante la indicación por parte del interlocutor (que el demandante creía que era de Unicaja) de que le facilitase las claves que le iban a enviar a su móvil para anular las transferencias, el contenido del mensaje recibido no era suficientemente clarificador, pues se limitaba a decir: "Transferencia internacional, Cuenta de Abono....Importe: EUR. Clave:…". No indica si es para autorizar o anular ese movimiento, por lo que, en las circunstancias en las que lo recibió el demandante, en el entorno que habían propiciado los delincuentes, haciendo creer al actor que estaba hablando con personal del banco y por otro lado, la situación estresante que estaba viviendo el demandante, angustiado porque creía que se habían realizado dos transferencias desde su cuenta que él no había autorizado, cualquier usuario medio podría haber pensado que, tal como le indicaba el interlocutor, la finalidad era anular las

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

transferencias no autorizadas. Atendiendo a dichas circunstancias considero que haber facilitado las claves inducido por el engaño de un delincuente no puede ser calificado como negligencia grave.

Por lo que se refiere a la posición de la demandada, como proveedora del servicio, venía obligada a adoptar una serie de medidas de seguridad y dotarse de mecanismos de supervisión que permitieran detectar operaciones fraudulentas en la prestación de servicios de pago, tal como señala el artículo 2 del Reglamento Delegado 2018/389, pues como se indica también en la sentencia citada de la Audiencia de Pontevedra, "incluyendo la técnica del phishing, la creación y puesta en la red de páginas que clonan las del sitio oficial de las entidades emisoras de instrumentos de pago, el deber de diligencia de la entidad demandada exigía dotarse de la tecnología antiphishing precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas, lo que, de producirse, impediría que el defraudador pudiera hacerse con las credenciales del usuario del instrumento de pago por ella emitido, pues la rotura del enlace del correo electrónico haría ya ineficaz cualquier conducta que frente al mismo pudiera observar el usuario receptor".

Por lo expuesto, no habiendo quedado acreditado que la entidad demandada cumpliera en la forma que le es exigible los deberes de diligencia en la autenticación de las operaciones de pago y no apreciándose que el demandante incurriera en negligencia grave en el cumplimiento de sus deberes de custodia y uso de la cuenta, ha de declararse la responsabilidad de la entidad demandada como proveedora de los servicios de pago usados de manera fraudulenta por un tercero y por tanto es quien debe responder de las pérdidas sufridas por el demandante con tales operaciones.

Por lo expuesto, procede estimar la pretensión actora y condenar a la demandada a abonar al actor la suma de 5.000 euros, más los intereses del art. 576 LEC.

SEXTO. Junto con la acción de reclamación de cantidad, solicita la parte demandante la declaración de nulidad de la cláusula del contrato de cuenta bancaria que fija una comisión o gastos por reclamación de posiciones deudoras de 45 euros. La parte demandada se ha allanado a dicha pretensión por lo que, de conformidad con lo dispuesto en el art. 21 LEC, procede declarar la nulidad de la referida cláusula y, en aplicación de lo previsto en el art. 1.303 CC, condenar a la parte demandada a restituir al actor las cantidades que haya percibido en aplicación de la misma, más los intereses legales desde la fecha de su cobro.

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

SÉPTIMO. En cuanto a las costas procesales, la estimación de la demanda conlleva su imposición a la parte demandada, por aplicación del criterio objetivo del vencimiento que se contiene en el art. 394.1 LEC.

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

FALLO

Estimo la demanda formulada por la Procuradora Sra. Revuelta Capellín, en representación de don
, frente a la entidad "Unicaja Banco, S.A" y:

1.- Declaro la nulidad de la cláusula del contrato de cuenta bancaria suscrito por las partes el 5 de octubre de 2.021 que establece una comisión o gastos de reclamación de posiciones deudoras de 45 euros y condeno a la demandada a restituir al actor las cantidades percibidas en aplicación del referida cláusula más los intereses legales devengados desde su cobro.

2.- Condeno a la demandada a abonar al actor la suma de 5.000 euros, más los intereses legales moratorios devengados desde la fecha de esta resolución y hasta su completo pago.

Con imposición de las costas a la parte demandada.

Notifíquese esta sentencia a las partes.

Contra esta resolución cabe interponer recurso de apelación en el plazo de veinte días desde su notificación; debiendo constituir previamente un depósito de 50 euros, mediante su consignación en la Cuenta de Depósitos y Consignaciones de este Juzgado.

Así lo pronuncio, mando y firmo, Coral Gutiérrez Presa, Magistrada-Juez del Juzgado de Primera Instancia nº 3 de Gijón.

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

La difusión del texto de esta resolución a partes no interesadas en el proceso en el que ha sido dictada sólo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contuvieran y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutelar o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda.

Los datos personales incluidos en esta resolución no podrán ser cedidos, ni comunicados con fines contrarios a las leyes.

PRINCIPADO DE ASTURIAS

FIRMA (1): Coral Gutierrez Presa (10/03/2024 09:40)

Firmado digitalmente por NOMBRE GARCIA LOPEZ ALFREDO - NIF 71633818L
Fecha: 2024.03.12 14:34:38 +01:00