Administración de Justicia

JUZGADO DE 1ª INSTANCIA Nº 04 DE MÓSTOLES
Plaza Ernesto Peces Nº 2 , Planta 1 - 28931
Tfno: 916647308
Fax: 916187808
instancia4_mostoles@madrid.org
[redacted]
Procedimiento: Juicio Verbal [redacted]
Materia: Contratos bancarios
NEGOCIADO P
Demandante: D. [redacted]
PROCURADOR Dña. [redacted]
Demandado: UNICAJA BANCO, S.A.U.
[redacted]

SENTENCIA Nº [redacted]/2023

MAGISTRADO- JUEZ: D. [redacted]
Lugar: Móstoles
Fecha: catorce de noviembre de dos mil veintitrés

Vistos por **D.** [redacted] **Magistrado-Juez del Juzgado de Primera Instancia número cuatro de los de Móstoles y su Partido, los presentes Autos de JUICIO VERBAL 1173/2023**, instados por D. [redacted], representado por la procuradora SRA. [redacted] y asistida por la letrada SRA. [redacted] contra UNICAJA BANCO S.A., representada por el procurador y asistida por la letrada [redacted].

ANTECEDENTES DE HECHO

PRIMERO.- Por la representación de D. [redacted] se formula por medio de escrito presentado con fecha 31 de mayo de 2023 demanda de juicio verbal contra UNICAJA BANCO S.A., en base a los hechos que expone en su escrito rector, solicitando que se dicte sentencia de conformidad con el suplico del mismo.

SEGUNDO.- Mediante decreto de fecha 25 de septiembre de 2023 se admite a trámite la demanda, emplazándose a la demandada UNICAJA BANCO S.A. por plazo de diez días, con traslado de las copias del escrito de demanda y documentos acompañados, sin que por la parte demandada se presentara la contestación a la demanda en plazo. Ninguna de las partes ha solicitado la celebración de vista.

FUNDAMENTOS JURÍDICOS

PRIMERO.- DEL OBJETO DEL LITIGIO.-
Por la representación de D. [redacted] se formula demanda de juicio verbal contra UNICAJA BANCO S.A., en reclamación de la cantidad de 2.200 euros más los intereses legales desde su cobro indebido.

Madrid

Administración de Justicia

SEGUNDO.- DE LA RESPONSABILIDAD BANCARIA Y DE LA LEGISLACION DE SERVICIOS DE PAGO.-

Como ya expresa la SAP de Madrid de 23 de abril de 2015 (Roj: SAP M 6576/2015-ECLI:ES:APM:2015:6576), citada en la SAP de Valencia, Sección 6ª, núm. 254/2022 de 13 junio (JUR 2022\321509), en relación a la diligencia exigible a las entidades bancarias, la jurisprudencia del Tribunal Supremo, Sala Primera, viene declarando desde la STS de 15 de julio de 1988 (RJ 1988, 5717) que "la diligencia exigible a una entidad bancaria no es la diligencia de un buen padre de familia, sino la de un "comerciante experto" que aconseja "gran tacto", "cuidado extremo" a la hora de llevar a cabo las órdenes del cliente, y que "en este punto aparece un criterio objetivo a tener en cuenta a la hora de delimitar responsabilidades, que no es otro que el constituido por las concretas instrucciones dadas por el cliente –STS de 20 de mayo de 1988. El banco, en cuanto mandatario, debe ejecutar las instrucciones del cliente, con sus abonos y cargos -SSTS 15 de julio de 1993, 19 de diciembre de 1995 y 21 de noviembre de 1997-, lo que reitera la STS de 30 de junio de 2005, que hace referencia a que el "artículo 255 del Código de Comercio establece que en el contrato de comisión mercantil en lo no previsto por el comitente debe ser consultado éste por el comisionista y que los contratos de comercio han de ser ejecutados de buena fe, según el artículo 57 del mismo Cuerpo legal".

Por otro lado, el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, regula los servicios de pago que se relacionan, incluyendo "c) La ejecución de operaciones de pago, incluida la transferencia de fondos, a través de una cuenta de pago en el proveedor de servicios de pago del usuario u otro proveedor de servicios de pago", incluyendo la forma de prestación de dichos servicios, el régimen jurídico de las entidades de pago, el régimen de transparencia e información aplicable a los servicios de pago, así como los derechos y obligaciones respectivas tanto de los usuarios de los servicios de pago como de los proveedores de los mismos:

En esta sentido, dispone en su artículo 41 –"Obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas"-, que "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". Igualmente, en el artículo 42 se recogen las obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago, concretando: "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 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 (…). 2. El proveedor de servicios de pago soportará los riesgos derivados del envío de un instrumento

Madrid

Administración de Justicia

de pago al usuario de servicios de pago o del envío de cualesquiera elementos de seguridad personalizados del mismo".

En cualquier caso, como señala la SAP de Ourense, Sección 1ª, núm. 311/2023 de 12 mayo (JUR 2023\293249), que cita la SAP de Madrid, sección 11ª, núm. 74/2022, el conocido "riesgo operacional", que debe ser asumido por los bancos en virtud de su posición de garante al ser una pieza clave para evitar la comisión de fraudes..."

TERCERO.- DE LA CARGA DE LA PRUEBA.-

La regla general sobre la carga de la prueba aplicable a la prestación de servicios que no tenga adjetivada una especial peligrosidad o requiera de un particular cuidado ha de ser la regla general del art. 217 de la LEC, de manera que cuando se trata de prestaciones contractuales o no contractuales, del tenor del art. 1.101 y 1.902 del CC, en relación al art. 217.2 de la LEC se desprenderá que corresponde al perjudicado demandante la carga de la prueba de la culpa del causante del daño demandado. Ahora bien, no es así cuando "una disposición legal expresa" -art 217.6- de la LEC- imponga al demandado la carga de probar que hizo cuanto le era exigible para prevenir el daño; o cuando tal inversión de la carga de la prueba venga reclamada por los principios de "disponibilidad y facilidad probatoria" a los que se refiere el artículo 217.7 de la LEC, y ello sin perjuicio de que en aplicación de lo dispuesto en el artículo 386 de la LEC el tribunal pueda imputar a culpa del demandado el resultado dañoso acaecido cuando, por las especiales características de éste y conforme a una máxima de la experiencia, pertenezca a una categoría de resultados que típicamente se produzcan (sean realización de un riesgo creado) por impericia o negligencia, y no proporcione el demandado al tribunal una explicación causal de ese resultado dañoso que, como excepción a aquella máxima, excluya la culpa por su parte.

En este sentido, el artículo 44 del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que:

ª1. 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".

Añade el artículo 45.2 párrafo 2º que "(…) De conformidad con el artículo 44.1, corresponderá al proveedor de servicios de iniciación de pagos demostrar que, dentro de su

Madrid

Administración de Justicia

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".

El artículo 46 del mismo texto legal regula la responsabilidad del ordenante, en caso de operaciones de pago no autorizadas, en los siguientes términos:

"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:

"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" (…).

Como expresa la SAP de Ourense, Sección 1ª, núm. 311/2023 de 12 mayo (JUR 2023\293249), de la normativa expresada se desprende que la entidad que presta el servicio de pago únicamente podrá exonerarse de la responsabilidad, acreditando la culpa grave del usuario que emite la orden de pago. En similares términos, para la SAP de Ourense, Sección 1ª, núm. 311/2023 de 12 mayo (JUR 2023\293249), con cita de las SSAP de Madrid, Sección 11ª, de 28 de febrero de 2022 y Sección 9ª, núm. 178/2015 de 4 mayo (JUR 201551311), salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante, la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la carga de la prueba de que la orden de pago "no se vio afectada por un fallo técnico o cualquier otra deficiencia". Podemos hablar de una responsabilidad cuasi-objetiva, por cuanto la entidad que presta los servicios sólo puede exonerarse mediante la prueba de la culpa grave del ordenante; interpretación acorde no sólo con la literalidad de la norma, sino con el espíritu y finalidad de la misma (art. 3 del CC). Igualmente, para la SAP de Madrid (Sección 9ª), núm. 178/2015 de 4 mayo (JUR 2015\151311), se establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago, con inversión de la carga probatoria, al presumirse la falta de autorización, si el titular lo niega. Este sistema de responsabilidad civil, tan solo cesa cuando el cliente ha actuado fraudulentamente o con negligencia grave a la hora de aplicar los medios razonables de protección de seguridad personalizados de que haya sido provisto, o en el caso de que no haya comunicado a la entidad el pago no autorizado, en cuanto tenga conocimiento del mismo, siempre y

Madrid

Administración de Justicia

cuando la entidad disponga de un sistema de comunicación adecuado, gratuito y disponible, en todo momento, que le permita al usuario del servicio efectuar la comunicación de la actuación fraudulenta.

En similares términos, SSAP de Asturias, Sección 1ª, núm. 351/2012 de 18 septiembre (JUR 2012\369519); Granada, Sección 5ª, núm. 212/2022 de 20 junio (JUR 2022\303953); Jaén, Sección 1ª, núm. 1355/2022 de 14 diciembre (JUR 2023\123097); Almería, Sección 1ª, núm. 99/2023 de 31 enero. JUR 2023\166836); Islas Baleares, Sección 5ª, núm. 132/2023 de 17 febrero (JUR 2023\200863); Asturias, Sección 7ª, núm. 353/2023 de 30 junio (JUR 2023\356143); Valencia, Sección 9ª, núm. 130/2013 de 23 abril (JUR 2013\254877) y Albacete, Sección 2ª, de 23 de febrero de 2012.

La lógica de la norma de acceso a la fuente de la prueba y facilidad probatoria en lo que hace a la implementación de medidas de seguridad en la prestación de un servicio que se da por las entidades de crédito a sus clientes a través de una oficina virtual que se desenvuelve en redes bien de internet, bien de comunicaciones móviles, se presenta como criterio más que de razonable atención al caso en el que la propia seguridad y debida reserva de la red se contrapone al acceso por parte de un tercero distinto al titular de la misma que asume poner en la red pública un conjunto de comunicaciones para permitir operaciones bancarias que requiere de soluciones tecnológicas muy avanzadas que minimicen las amenazas contra la autenticidad, integridad y la confidencialidad de los datos que circulan a través de la red. Por tanto, no es cierto que la carga de la prueba sobre la implementación de medidas de seguridad adecuadas, suficientes, eficientes y actuales al nivel de riesgo en la red bancaria de banca online lo sea a cargo del usuario del sistema, pues el marco de responsabilidad establecido para el caso de operaciones de pagos hechos por proveedores de servicios no autorizadas o ejecutadas incorrectamente, es el de la cuasi-objetividad tal cual se desprende de la regulación específica sobre la materia, sin perjuicio del régimen general de la carga de la prueba –SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

Desde el punto de vista del derecho de consumo -no está en cuestión la condición de usuario del demandante-, el artículo 147 del TRLGDCU dispone que "Los prestadores de servicios serán responsables de los y perjuicios causados a los consumidores o usuarios, salvo que prueben que han cumplido las exigencias y requisitos reglamentariamente establecidos y demás cuidados y diligencias que exige la naturaleza del servicio". Este precepto -como recuerda la STS núm. 185/2016, de 18 de marzo (RJ 2016, 983), citada en la SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-, no concreta el supuesto de hecho al que se refiere y por tanto ha de aplicarse con cautela, debiendo "ponderarse si el evento dañoso acaecido evidencia, o no, un defecto -un déficit de la seguridad que legítimamente cabía esperar- del servicio prestado; y tener presente “la disponibilidad y facilidad probatoria que corresponda a cada una de las partes del litigio”. Además, la norma citada se complementa con el art. 148 conforme al cual "se responderá de los daños originados en el correcto uso de los servicios, cuando por su propia naturaleza, o por estar así reglamentariamente establecido, incluyan necesariamente la garantía de niveles determinados de eficacia o seguridad, en condiciones objetivas de determinación, y supongan controles técnicos, profesionales o sistemáticos de calidad, hasta llegar en debidas condiciones al consumidor y usuario", precepto del que se desprende el fundamento de la responsabilidad presunta del proveedor de servicios en el ámbito de la sociedad de la información, en particular cuando no aparece vinculada exclusivamente a la falta de específicas medidas de autoprotección por parte de aquellos sino a la falta de un especial

Madrid

Administración de Justicia

cuidado en atención a la naturaleza del servicio de que se trata, al modo empresarial de su prestación y al rol que en este desempeña un usuario típico, ponderado el hecho de que si el evento dañoso acaece es porque hay un déficit de la seguridad que legítimamente no cabía esperar del servicio prestado. Y dado que se produce -cuando el evento ocurre- dentro de un ámbito que se halla bajo el control del empresario prestador del servicio, que es quien cuenta con la información sobre las medidas de cuidado exigibles, y en su caso adoptadas, a fin de reducir el riesgo de riesgos, es el proveedor quien deviene responsable del daño -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

El Tribunal Supremo, en STS de 23 de julio de 2001 (RJ 2001, 8411), citada en la SAP de Murcia, Sección 1ª, núm. 398/2013 de 30 julio (JUR 2013\307044), ya expresa que "el art. 25 de la Ley General para la Defensa de los Consumidores y Usuarios establece un principio de inversión de la carga de la prueba, haciendo recaer sobre el productor o suministrador de los productos o servicios la carga de probar que el origen de los daños y perjuicios se encuentra en la conducta culposa del usuario o de las personas por las que debe responder, cometido que no ha logrado alcanzar el banco demandado".

En conclusión, la responsabilidad del proveedor de los servicios de banca online es de riesgo y consecuentemente, es por ley que a la entidad corresponde acreditar que la operación ordenada sí fue auténtica y que no estuvo afectada por un fallo técnico o por otra deficiencia como, por ejemplo, por un ataque informático de naturaleza fraudulenta al sistema bancario que hubiera permitido el acceso a las cuentas de sus clientes y disponer ilícitamente, de las mismas ordenando operaciones en detrimento de aquellos.

CUARTO.- DE LOS FRAUDES INFORMATICOS Y DEL PHISHING.-

Antes de analizar las pretensiones formuladas, es imprescindible proporcionar una definición del phishing, para determinar ante que abuso informático nos encontramos.

Efectivamente, siguiendo la SAP de Alicante, Sección 8ª, núm. 107/2018, de 12 marzo (AC 2018\818), la banca electrónica está siendo objeto de transferencias no autorizadas por el cliente y que vienen antecedidas por el método delictivo conocido como "phishing" que constituye una modalidad específica de fraude informático que visualiza las deficiencias de seguridad del sistema informático de una entidad y que trae causa en el uso de las redes telemáticas. De acuerdo con la Agencia Española de Protección de Datos (Resolución del Expediente núm. E/00762/2004, de 24 de mayo de 2006): el objetivo de los ataques de "phishing" es la obtención de forma engañosa y fraudulenta de los códigos de usuarios y contraseñas de clientes de Banca Electrónica, al objeto de realizar transferencias no autorizadas… Su operatoria comienza con la adquisición en internet de un "paquete de herramientas", que incluyen programas informáticos e información necesaria para realizar los ataques. Esta información incluye "listas de equipos comprometidos" que pueden ser utilizados bien para mandar correos electrónicos, bien para alojar páginas web falsificadas. Incluyen además "bases de datos de direcciones de correo electrónico". Una vez en posesión del paquete, se remiten los correos electrónicos con carácter indiscriminado (buscando contactar con clientes de la entidad financiera) informando de la necesidad de conectarse a una página web que parece pertenecer a la citada entidad y portar los códigos de acceso y contraseñas de clientes. Dicha página web se suele alojar en un equipo conectado a Internet cuya seguridad se haya [visto] comprometida", sin conocimiento de su usuario, y que se encuentra normalmente en un país distinto al de los destinatarios del ataque. De esta forma se constituye un "fichero de datos personales con códigos de usuarios y contraseñas de clientes" recabados de forma engañosa y fraudulenta, que se ubica normalmente en el mismo

Madrid

Administración de Justicia

"equipo remoto comprometido" en el que se aloja la página web falsificada. Con los datos obtenidos se realizan transferencias a cuentas de colaboradores situados en España los cuales a su vez retiran el dinero en efectivo y tras descontar una comisión realizan transferencias monetarias internacionales mediante entidades especializadas".

En similares términos, para la SAP de Madrid, Sección 9ª, núm. 178/2015 de 4 mayo (JUR 2015\151311), el phishing se origina con la suplantación de la identidad del banco por parte del phisher con la finalidad de adquirir información confidencial sobre contraseñas de cuentas bancarias, tarjetas de crédito o cualquier otra información en relación con el banco, que permita entrar en las cuentas de los usuarios en Internet de banca electrónica. El internauta recibe un correo electrónico o cualquier mensaje instantáneo, a través del cual se le informa de que debe cambiar sus claves bancarias, proporcionándole un link a través del cual pueda acceder a la página Web de la supuesta entidad bancaria y allí realizar la modificación aconsejada. En la mayoría de los métodos de phishing se utilizan técnicas de engaño, a través de las cuales el phisher utiliza contra la víctima el propio código de programa del banco o servicio similar, adquiriendo la página Web la verdadera apariencia de la entidad bancaria. Igualmente, resulta muy habitual que el internauta reciba un correo en el que se le informe de que debe verificar sus cuentas, seguido por un enlace que parece la página Web oficial de la entidad bancaria.

El phishing, como indica el Instituto Nacional de Ciberseguridad de España (INCIBE) es una modalidad de fraude llevada a cabo mediante el envío de un correo electrónico por parte de un ciber-delincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico –SAP de Almería, Sección 1ª, núm. 99/2023 de 31 enero (JUR 2023\166836)-.

Por otro lado, como indica la doctrina jurisprudencial, el contrato de cuenta corriente es una figura atípica que encuentra su singularidad, desde el punto de vista de los titulares de la cuenta, en el llamado servicio de caja, encuadrable, dentro del marco general de la comisión mercantil y de acuerdo con el cual el Banco, en cuanto mandatario, ejecuta las instrucciones del cliente (abonos, cargos...) y, como contraprestación, recibe determinadas comisiones, asumiendo la responsabilidad propia de un comisionista -STS de 21 de noviembre 1997 (EDJ 1997/7846). Además, la transferencia bancaria es un servicio que forma parte del contrato de servicio de caja entre un proveedor de servicios de pago (el banco) y sus clientes y sirve de medio de pago mediante el débito en la cuenta del ordenante y abono en la del beneficiario, tratándose en suma de un procedimiento financiero de movimiento de la moneda. Se trata de un medio de pago consistente en una orden dada al banco (banco emisor) por parte de un cliente (ordenante) a fin de que, con cargo a su cuenta, abone un determinado importe en otra cuenta del mismo o distinto banco (banco destinatario) abierta a nombre de un tercero (beneficiario) o del propio ordenante. Las transferencias se regulan en la Ley 16/2009, de 13 de noviembre, de Servicios de Pago. La Ley 16/2009, de 13 de noviembre, de Servicios de Pago define la orden de pago como "toda instrucción cursada por un ordenante o beneficiario a su proveedor de servicios de pago por la que se solicite la ejecución de una operación de pago" (art. 2.16 de la LSP). Desde un punto de vista contractual toda transferencia constituye una forma de ejecución de obligaciones contractuales previamente asumidas, ejecución obligada cuando se dan las condiciones pactadas, de ordinario, que haya provisión de fondos. Es por ello que se entiende que la orden de transferencia constituye una declaración de voluntad o mandato (en

Madrid

Administración de Justicia

el sentido del art. 254 del CCo) en virtud del cual el banco asume la realización de transferencias por cuenta del cliente como parte del contrato de servicio de caja. Dado el carácter negocial de la orden de pago, ésta puede pactarse que tenga lugar en cualquier forma, incluida la electrónica. En particular, el consentimiento a las operaciones de pago por el usuario, en el ámbito de la banca electrónica, supone que el cliente deba haber firmado un contrato de adhesión a los servicios de banca electrónica. El art. 25.1 de la LSP establece al respecto que "el ordenante y su proveedor de servicios de pago acordarán la forma en que se dará el consentimiento, así como el procedimiento de notificación del mismo", negocio jurídico que determina que la transferencia se entienda autorizada por el ordenante de acuerdo con el mismo precepto de la LSP. El consentimiento del ordenante se prestará, según el medio utilizado para prestar dicho consentimiento, mediante, o la firma de la autorización y orden de transferencia correspondiente, o verbalmente a través de la vía telefónica o a través de banca por internet o electrónica -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

Por otro lado, tanto en la banca telefónica como por internet, el proveedor de servicios de pago, o lo que es lo mismo, el banco emisor, debe implementar las medidas necesarias para asegurar la autenticación e identidad del ordenante a la hora de prestar su consentimiento. Por ello y para su ejecución, el banco debe comprobar en todo caso la autenticidad de la orden y, salvo pacto en contrario, que existe saldo suficiente. De ordinario, para la realización de transferencias ordinarias con cargo a una cuenta vinculada es preciso que el cliente haya de autenticar la operación mediante la introducción de las claves previamente facilitadas por la entidad de crédito con la que contrata, con respecto a las cuales tendrá unos deberes de custodia. La falsedad de la transferencia (es decir, que el ordenante no sea el titular de la cuenta) es un riesgo a cargo del banco porque, en principio, el deudor sólo se libera pagando al verdadero acreedor por lo que, si el banco cumple una orden falsa, habrá de reintegrar en la cuenta correspondientes las cantidades cargadas. Una excepción a esta distribución de riesgos se produce en el caso de que el titular haya creado o elevado el riesgo de falsificación de forma imputable en el caso concreto (STS 15 de julio de 1988 (RJ 1988, 5717) -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

Los servicios que prestan las entidades de crédito a sus clientes a través de su oficina virtual se desenvuelven en redes TCP/IP (Internet) o WAP (comunicaciones móviles). Siendo Internet una red pública de comunicaciones, la seguridad de las operaciones bancarias precisa de soluciones tecnologías avanzadas a los efectos de garantizar tanto la autenticidad como la integridad y la confidencialidad de los datos. Por estos motivos las entidades prestadoras del servicio de banca online deben dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones. Consecuencia derivada de la omisión, insuficiencia o defectuoso funcionamiento de las adoptadas es que han de ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

QUINTO.- DE LA VALORACIÓN DE LA PRUEBA Y DE LA JURISPRUDENCIA APLICABLE.-

Por tanto, lo importante a los efectos de la resolución de las pretensiones formuladas, no es tanto la existencia de diligencia en la actuación de la entidad de crédito demandada, sino, si esta ha probado que los actores incurrieron en fraude, incumplimiento deliberado o

Madrid

Administración de Justicia

negligencia grave en relación a las operaciones no autorizadas cuya devolución reclama a través de la presente demanda. Y tal prueba no se ha logrado en las presentes actuaciones.

Como ya se reconoce por la propia parte actora en el escrito inicial de demanda, "el 11 de junio de 2022, recibió un SMS de Liberbank (actual UNICAJA) en el que se le informaba de que se había detectado un acceso inusual a su cuenta online y que, si no reconocía ese nuevo dispositivo, verificara sus datos a través del enlace "https://s.id/liberbank-ayuda". Que accedió al enlace, que lo llevó a la banca online, y entró a través de su usuario y contraseña, con el objeto de que bloquearan dicho acceso inusual que le indicaban en el SMS. Dos días después, el 13 de junio de 2023, recibió una llamada desde el número [redacted], indicándole que lo contactaban desde el departamento de seguridad de la banca digital de Unicaja porque habían detectado accesos inusuales en su cuenta desde dispositivos no habituales. En dicha llamada, le indican que, para bloquear dichos accesos, le iban a enviar unos códigos por SMS los cuales les tendría que facilitar para poder solucionarlo (…)".

De esta forma, en el supuesto analizado, no ofrece duda de que, si bien las operaciones fueron autorizadas, registradas con exactitud y contabilizadas, sin que interviniera fallo técnico alguno, nos encontramos con el típico fraude denominado phishing, ya ampliamente explicado, y la forma en que se articuló la operación fraudulenta -de una complejidad y grado de perfección, difícilmente detectable por un cliente de las características del demandante-, no permitió a la actora, cuyo comportamiento en cualquier caso no puede considerarse diligente, detectar que algo anómalo estaba sucediendo, siendo evidente que el formato empleado por los delincuentes era totalmente apto para provocar el error en la demandante.

Y debemos empezar descartando, ante la ausencia de toda alegación y prueba a tal fin, cualquier atisbo de "mala fe en el proceder del demandante" en las operaciones fraudulentas que provocaron su empobrecimiento patrimonial, y, por ende, cualquier actuación fraudulenta por parte del actor. Tampoco se acredita que hubiera incurrido en negligencia grave, lo que tampoco ha sostenido la entidad demandada, que ha verificado la contestación a la demanda fuera de plazo. Parafraseando la SAP de Valencia, Sección 6ª, núm. 254/2022 de 13 junio (JUR 2022\321509), esta última interpretación nos parece más acorde con la protección debida al usuario de los servicios bancarios, y a las obligaciones propias de las entidades que ofrecen los servicios telemáticos, que son conocedoras de las crecientes actuaciones ilícitas o estafas que proliferan aprovechando las nuevas tecnologías, y que desarrollan mecanismos técnicos con el fin de ofrecer un sistema lo más seguro posible para el usuario, como parte igualmente de su oferta de servicios.

Efectivamente, no cabe duda que hubo un déficit de protección en el sistema de seguridad por parte de la entidad bancaria demandada. Por la parte demandada ni siquiera se ha explicado ni acreditado cuáles eran los niveles de seguridad existentes –en general se deduce del escrito de demanda la existencia de un único nivel de seguridad al cliente, que disponía de un código de usuario y una clave/contraseña para acceder a la Banca digital, siendo además muy probable la existencia de un segundo nivel de seguridad consistente en una segunda clave/contraseña para la realización de transferencias en el marco de la Banca Digital-. Tampoco se ha ofrecido una explicación satisfactoria sobre los reintegros en cajero automático efectuados. Igualmente existe una absoluta orfandad alegatoria y probatoria sobre la eventual adopción de medidas concretas de seguridad para dicho tipo de fraude conocido del phishing. No puede obviarse que la entidad era consciente de los ataques que venían produciéndose contra sus clientes y, a pesar de ello, no cambio el sistema de

Madrid

Administración de Justicia

autenticación -pues dicha modalidad fraudulenta de movimientos de cuenta es una práctica extendida-, pudiendo haber evitado el fraude si hubiese reforzado, como estaba a su alcance, el sistema de seguridad. No consta ningún filtro adicional de seguridad para evitarlo, ni se han aportado estudios sobre dicho riesgo; no constando tampoco que informara de esta situación al cliente, mediante la remisión de las oportunas advertencias mediante un medio de comunicación eficaz. En definitiva, la entidad demandada no actuó diligentemente, en previsión del fraude con el nivel máximo de seguridad, ya que no detectó el phishing sufrido por el actor, a pesar de que los phishers realizaron las conductas típicas y actuaron con el modus operandi característico en este tipo de fraudes informáticos. Efectivamente, no resulta acreditado que la entidad demandada hubiera previsto y establecido un sistema de autorización de pagos con autenticación reforzada, lo que implica que el prestador de servicios asume la responsabilidad patrimonial por un riesgo perfectamente descrito tanto para el usuario como para el prestador de servicios como es la defraudación con el procedimiento de phishing. El artículo 97 de 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, impone la obligación a los Estados miembros de velar por que los proveedores de servicios de pago apliquen la autenticación reforzada de clientes 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.

En otros términos, no se ha acreditado por la demandada la observancia de los deberes de diligencia que le eran exigibles en la autenticación de las operaciones de pago, pues ni prueba haber implementado un mecanismo "antiphishing" de protección de los usuarios de los instrumentos de pago por ella emitidos frente al uso fraudulento por un tercero de páginas imitativas de las propias para hacerse con las credenciales del instrumento –resulta indiferente que no se produjera fallo del sistema, en cuanto que, su responsabilidad no deriva de tal hecho, sino de no haber adoptado las medidas de seguridad precisas para evitar o minorar las consecuencias para el cliente de haber sufrido un fraude en red-. En definitiva, se entiende que media un incumplimiento contractual del banco al ejecutar una orden de pago sin comprobar su legitimidad, es decir, que provenía efectivamente del titular (o autorizado) de la cuenta, al no disponer de un sistema adecuado de seguridad que previniera tal tipo de órdenes fraudulentas. Y es exigible a la demandada la responsabilidad patrimonial cuasi objetiva legalmente establecida, según sentir general de la jurisprudencia menos de las Audiencias Provinciales, que, obviamente, supone un paso más en la protección al consumidor que el previsto en el art. 148 del TRLGDCU, puesto que viene a excusar al consumidor de la negligencia en que pueda haber incurrido por facilitar sus datos personales y claves de confirmación o firma electrónica en virtud de la acción defraudatoria de terceros.

En cualquier caso, no basta con medidas genéricas de protección o avisos estereotipados de cuidado, sino que la seguridad de las operaciones bancarias precisa de soluciones tecnológicas avanzadas, a efectos de garantizar tanto la autenticidad como la integridad y confidencialidad de los datos. De esta manera, no son los clientes los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, ni prevenir con su asesoramiento experto dichos riesgos.

Parafraseando la SAP de Albacete, Sección 2ª, de 23 de febrero de 2012, citada en la SAP de Asturias, Sección 1ª, núm. 351/2012 de 18 septiembre (JUR 2012\369519), quien resultó engañado o burlado no fue tanto el titular de la cuenta sino la entidad financiera y

Madrid

Administración de Justicia

proveedora del servicio que tenía su custodia y los medios de seguridad para protegerla, por lo que es ésta quien debe responder, salvo en los supuestos específicos legalmente indicados, y más allá de cualquier grado de diligencia mayor o menor de dicha entidad.

Como expresa la SAP de Madrid, Sección 20ª, de 20 de mayo de 2022, citada en la SAP de Asturias, Sección 7ª, núm. 285/2023 de 12 mayo (JUR 2023\312886), en la Directiva 2015/2036 la negligencia que le 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. Para la SAP de Vizcaya, Sección 3ª, núm. 429/2016 de 10 noviembre (AC 2016\2241), precisamente a la entidad bancaria demandada le incumbe proteger a sus clientes de cuantas conductas se realicen a través de la banca electrónica y ello en cuanto que precisamente este tipo de fraude comienza con la posibilidad de que los defraudadores interesan las claves de acceso a los clientes de los bancos (en este incide la mecánica delictiva)… Dichas circunstancias vienen a contemplar un sistema bancario electrónico diseñado por la entidad demandada adoleciendo de seguridad, la oferta a los clientes para operar a través de dicha banca electrónica y que es un hecho conocido de que cada vez se impone más por las entidades bancarias a los clientes, eliminando los servicios en ventanilla, se publicita por ser seguro contener los filtros para detectar fraudes y operar de forma fiable siendo así que en cuanto se ha probado la mecánica de la facilidad para operar por terceros no autorizados a través de la banca electrónica de la demandada, difícilmente podemos decir de que el Banco demandado no haya incurrido en negligencia grave de sus obligaciones, se han permitido efectuar operaciones bancarias sin superar ningún filtro cuando la legislación bancaria tiende precisamente a establecer que se efectúen y se establezcan diferentes controles por los bancos en protección de los clientes, tendiendo a establecerse una responsabilidad cuasi objetiva de las entidades bancarias en cuanto deben soportar los riesgos de su actividad profesional en cuanto que se establece con el cliente una responsabilidad contractual del servicio de depósito, custodia y pagos de las cuentas del cliente.

Igualmente, como expresa la SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818), la responsabilidad en estos supuestos no puede atribuirse directamente al supuesto ordenante de la transferencia por entenderse ésta autorizada al haberse realizado de acuerdo con los sistemas de autenticación del banco. Los sistemas de autenticación se establecen por los proveedores de servicios de pago y si un banco no ha sido capaz de limitar el acceso al canal de banca electrónica no puede pretender que el presunto ordenante víctima de esta práctica fraudulenta sea el único responsable, pues es el banco quien tiene responsabilidad respecto del buen funcionamiento y la seguridad del mismo. Dispone a tal efecto el art. 25.1 de la LSP que "Las operaciones de pago se considerarán autorizadas cuando el ordenante haya dado el consentimiento para su ejecución. A falta de tal consentimiento la operación de pago se considerará no autorizada". Por tanto, en el caso de órdenes de pago y transferencias fraudulentas ésta disposición supone que si la orden de pago o transferencia emitida por el cliente contiene una manifestación voluntad que actúa como causa del pago al tercero o la remisión de fondos al beneficiario, a "sensu contrario" puede afirmarse que sin dicha declaración de voluntad la operación de pago o transferencia de fondos se considerará no autorizada. Las medidas de seguridad no solamente están destinadas a proteger la seguridad de las órdenes de pago emitidas por los clientes, sino que su eficacia exonera a las entidades de crédito de sus responsabilidades frente a las órdenes de pago no emitidas por sus clientes de tal forma que el incumplimiento de este específico

Madrid

Administración de Justicia

deber de vigilancia da lugar a una responsabilidad por "culpa in vigilando" o responsabilidad objetiva por el mal funcionamiento de los servicios de banca electrónica.

En base a este fundamento la SAP de Barcelona, Sección 11ª, de 23 de julio 2015 declaró la responsabilidad de la entidad bancaria por cargos y extracciones de efectivo no autorizados que tuvieron su origen en la introducción por los delincuentes de un mensaje fraudulento en la página oficial del banco a través del cual se canalizó la operación -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-. Este mismo hecho, considerado una infracción de los deberes de vigilancia del banco, fue la causa por la que la entidad bancaria fue condenada en la SAP de Valencia, Sección 9ª, de 23 de abril de 2013 (JUR 2013, 254877) -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-. La SAP de Barcelona, Sección 14ª, de 7 de marzo de 2013 (JUR 2013, 171665) condenó a la entidad bancaria a devolver a una empresa víctima de "phising" una cantidad por cuanto la entidad bancaria no adoptó las medidas de seguridad adicionales previstas en las Condiciones Generales del contrato al haberse producido movimientos inusuales de fondos de la cuenta corriente y ser transferidos a cuentas sospechosas de su control por "muleros" que la entidad debió detectar -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-. La SAP de Zaragoza de fecha 14 de mayo de 2013 (JUR 2013, 197766) condenó a la entidad bancaria señalando que la Ley de Servicios de Pago expresa con claridad que, salvo una tardanza injustificada del usuario del servicio de banca electrónica en comunicar la irregularidad de las operaciones, será el banco quien deberá devolverle de inmediato el importe de la operación no autorizada y, en su caso, restablecerá la cuenta de pago en que haya adeudado dicho importe al estado que habría existido de no haberse efectuado la operación de pago no autorizada. Por ello y salvo actuación fraudulenta o negligencia grave del titular de la cuenta, la responsabilidad de la operación es del banco al que corresponde además probar el correcto funcionamiento del sistema informático -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-. La SAP de Madrid de 4 de mayo de 2015 (JUR 2015, 151311) -la víctima facilitó sus claves y contraseñas a una página web clonada que simulaba ser la del banco-, expresa que el artículo 31 de la Ley 16/09 de 13 de noviembre de Servicios de Pago establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago con inversión de la carga probatoria al presumirse la falta de autorización de la orden de pago o transferencia si el cliente lo niega -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

Añade la SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)- que, a falta de prueba hemos de afirmar que la entidad financiera no cumplió con los deberes de seguridad frente a los riesgos concretos que podrían derivarse del funcionamiento de su plataforma de banca digital, deberes que no se cumplen con la mera literalidad genérica de los contratos suscritos, ni con la firma o suscripción de los mismos, pues son de índole material y técnico que han de fluir a través de diversos niveles de seguridad que pueden constituir opciones de la entidad pero no frente a sus clientes usuarios del sistema en caso de fallo del mismo pues, en tales casos, constituye objetivamente la omisión de una medida esencial en tanto tienen por objeto garantizar la autenticación de la orden de pago como, por lo demás, se desprende del propio tener del contrato de banca próxima. En consecuencia, es la prestadora de los servicios de pago quien tiene la obligación de facilitar un sistema de banca telemática segura, y no son sus clientes-usuarios los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, ni prevenir con un asesoramiento experto los mismos, no pudiendo en suma la parte obligada legalmente a ofrecer un modelo de servicio de caja que requiere de un especial nivel de seguridad, objetar que el usuario debía

Madrid

Administración de Justicia

conocer aspectos técnicos tales como identificar una web como falsa -cuando no consta que fuera burda y por tanto, evidente de toda falsedad-, ni que no eran fallos técnicos sino riesgos fraudulentos, determinados comportamientos de la plataforma que, no se olvide, son tan factibles que incluso el contrato de banca directa alude -para eludir responsabilidades el prestador- al riesgo de fallos técnicos, errores, interrupciones, desconexiones, sobrecargas y otras formas de defectos en la conexión. Si con carácter general el banco tiene la obligación, dice la STS 311/16, de 12 de mayo (RJ 2016, 2039), de comprobar la veracidad de la firma del ordenante -lo que no deja de ser una obviedad-, tanto más relevante lo es el ámbito de la banca electrónica a través de cualquiera de los sistemas ya existentes y que prestan un elevado nivel de garantía como son las claves aleatorias remitidas por la entidad directamente al usuario para cada operación y la firma electrónica. En conclusión, resulta evidente que en el caso hubo un incumplimiento contractual del banco al ejecutar una orden de pago sin comprobar su legitimidad, es decir, que provenía efectivamente del titular (o autorizado) de la cuenta, al no disponer de un sistema adecuado de seguridad que previniera tal tipo de órdenes fraudulentas ni adoptar medidas concretas y específicas en el caso cuando toma conocimiento de una situación operativa anormal que debió, cuando menos de forma puntual y excepcional, a verificar cualquiera orden que se diera en relación a las cuentas de la demandante. La no acreditación de las necesarias medidas de seguridad, la acreditación de la diligencia de la usuaria, y la inacreditación de la conducta posterior a la denuncia del fraude por el banco, omitiendo las medidas necesarias para evitar, en su caso, la pérdida definitiva del dinero, constituyen los presupuestos que permiten apreciar la realidad de una causalidad adecuada entre la conducta omisiva de la entidad y el resultado dañoso.

SEXTO.- DE LAS COSTAS PROCESALES.-

De conformidad con lo establecido en el artículo 394 LEC, procede imponer a la parte demandada el abono de las costas procesales.

V I S T O S los preceptos legales citados y demás de general y pertinente aplicación

F A L L O

Que estimando la demanda formulada por la representación de D. [redacted] debo condenar y condeno a UNICAJA BANCO S.A., a que abone a la actora la suma de 2.200 euros más los intereses legales desde la interpelación judicial, condenando a la parte actora al abono de las costas procesales.

Notifíquese la presente resolución a las partes, haciéndoles saber que CONTRA LA MISMA NO CABE INTERPONER RECURSO ALGUNO, todo ello al amparo de lo establecido en el artículo 455.1 LEC, en su nueva redacción dada por la Ley 37/2011, de 10 de octubre, de medidas de agilización procesal –"las sentencias dictadas en toda clase de juicio, los autos definitivos y aquéllos otros que la ley expresamente señale, serán apelables, con excepción de las sentencias dictadas en los juicios verbales por razón de la cuantía cuando ésta no supere los 3.000 euros"-.

Así por esta mi sentencia, juzgando en primera Instancia lo pronuncio, mando y firmo.

Madrid

Administración de Justicia

PUBLICACIÓN.- Leída y publicada ha sido la anterior sentencia por el Ilmo. Sr. Magistrado-Juez que la suscribe, en el día de la fecha. Doy fe.

[redacted]

Madrid

[redacted]

Administración de Justicia

JUZGADO DE 1ª INSTANCIA Nº 04 DE MÓSTOLES
Plaza Ernesto Peces Nº 2 , Planta 1 - 28931
Tfno: 916647308
Fax: 916187808
instancia4_mostoles@madrid.org
[redacted]
Procedimiento: Juicio Verbal 1173/2023
Materia: Contratos bancarios
NEGOCIADO P
Demandante: D. [redacted]
PROCURADOR Dña. [redacted]
Demandado: UNICAJA BANCO, S.A.U.
PROCURADOR D. [redacted]

SENTENCIA Nº [redacted]

MAGISTRADO- JUEZ: D. [redacted]
Lugar: Móstoles
Fecha: catorce de noviembre de dos mil veintitrés

Vistos por **D.** [redacted]**, Magistrado-Juez del Juzgado de Primera Instancia número cuatro de los de Móstoles y su Partido, los presentes Autos de JUICIO VERBAL 1173/2023**, instados por D. [redacted], representado por la procuradora SRA. [redacted] y asistida por la letrada SRA. [redacted] contra UNICAJA BANCO S.A., representada por el procurador [redacted] y asistida por la letrada [redacted]

ANTECEDENTES DE HECHO

PRIMERO.- Por la representación de D. [redacted] se formula por medio de escrito presentado con fecha 31 de mayo de 2023 demanda de juicio verbal contra UNICAJA BANCO S.A., en base a los hechos que expone en su escrito rector, solicitando que se dicte sentencia de conformidad con el suplico del mismo.

SEGUNDO.- Mediante decreto de fecha 25 de septiembre de 2023 se admite a trámite la demanda, emplazándose a la demandada UNICAJA BANCO S.A. por plazo de diez días, con traslado de las copias del escrito de demanda y documentos acompañados, sin que por la parte demandada se presentara la contestación a la demanda en plazo. Ninguna de las partes ha solicitado la celebración de vista.

FUNDAMENTOS JURÍDICOS

PRIMERO.- DEL OBJETO DEL LITIGIO.-
Por la representación de [redacted] se formula demanda de juicio verbal contra UNICAJA BANCO S.A., en reclamación de la cantidad de 2.200 euros más los intereses legales desde su cobro indebido.

Madrid

Administración de Justicia

SEGUNDO.- DE LA RESPONSABILIDAD BANCARIA Y DE LA LEGISLACION DE SERVICIOS DE PAGO.-

Como ya expresa la SAP de Madrid de 23 de abril de 2015 (Roj: SAP M 6576/2015-ECLI:ES:APM:2015:6576), citada en la SAP de Valencia, Sección 6ª, núm. 254/2022 de 13 junio (JUR 2022\321509), en relación a la diligencia exigible a las entidades bancarias, la jurisprudencia del Tribunal Supremo, Sala Primera, viene declarando desde la STS de 15 de julio de 1988 (RJ 1988, 5717) que "la diligencia exigible a una entidad bancaria no es la diligencia de un buen padre de familia, sino la de un "comerciante experto" que aconseja "gran tacto", "cuidado extremo" a la hora de llevar a cabo las órdenes del cliente, y que "en este punto aparece un criterio objetivo a tener en cuenta a la hora de delimitar responsabilidades, que no es otro que el constituido por las concretas instrucciones dadas por el cliente –STS de 20 de mayo de 1988. El banco, en cuanto mandatario, debe ejecutar las instrucciones del cliente, con sus abonos y cargos -SSTS 15 de julio de 1993, 19 de diciembre de 1995 y 21 de noviembre de 1997-, lo que reitera la STS de 30 de junio de 2005, que hace referencia a que el "artículo 255 del Código de Comercio establece que en el contrato de comisión mercantil en lo no previsto por el comitente debe ser consultado éste por el comisionista y que los contratos de comercio han de ser ejecutados de buena fe, según el artículo 57 del mismo Cuerpo legal".

Por otro lado, el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, regula los servicios de pago que se relacionan, incluyendo "c) La ejecución de operaciones de pago, incluida la transferencia de fondos, a través de una cuenta de pago en el proveedor de servicios de pago del usuario u otro proveedor de servicios de pago", incluyendo la forma de prestación de dichos servicios, el régimen jurídico de las entidades de pago, el régimen de transparencia e información aplicable a los servicios de pago, así como los derechos y obligaciones respectivas tanto de los usuarios de los servicios de pago como de los proveedores de los mismos:

En esta sentido, dispone en su artículo 41 –"Obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas"-, que "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". Igualmente, en el artículo 42 se recogen las obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago, concretando: "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 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 (…). 2. El proveedor de servicios de pago soportará los riesgos derivados del envío de un instrumento

Madrid

Administración de Justicia

de pago al usuario de servicios de pago o del envío de cualesquiera elementos de seguridad personalizados del mismo".

En cualquier caso, como señala la SAP de Ourense, Sección 1ª, núm. 311/2023 de 12 mayo (JUR 2023\293249), que cita la SAP de Madrid, sección 11ª, núm. 74/2022, el conocido "riesgo operacional", que debe ser asumido por los bancos en virtud de su posición de garante al ser una pieza clave para evitar la comisión de fraudes..."

TERCERO.- DE LA CARGA DE LA PRUEBA.-

La regla general sobre la carga de la prueba aplicable a la prestación de servicios que no tenga adjetivada una especial peligrosidad o requiera de un particular cuidado ha de ser la regla general del art. 217 de la LEC, de manera que cuando se trata de prestaciones contractuales o no contractuales, del tenor del art. 1.101 y 1.902 del CC, en relación al art. 217.2 de la LEC se desprenderá que corresponde al perjudicado demandante la carga de la prueba de la culpa del causante del daño demandado. Ahora bien, no es así cuando "una disposición legal expresa" -art 217.6- de la LEC- imponga al demandado la carga de probar que hizo cuanto le era exigible para prevenir el daño; o cuando tal inversión de la carga de la prueba venga reclamada por los principios de "disponibilidad y facilidad probatoria" a los que se refiere el artículo 217.7 de la LEC, y ello sin perjuicio de que en aplicación de lo dispuesto en el artículo 386 de la LEC el tribunal pueda imputar a culpa del demandado el resultado dañoso acaecido cuando, por las especiales características de éste y conforme a una máxima de la experiencia, pertenezca a una categoría de resultados que típicamente se produzcan (sean realización de un riesgo creado) por impericia o negligencia, y no proporcione el demandado al tribunal una explicación causal de ese resultado dañoso que, como excepción a aquella máxima, excluya la culpa por su parte.

En este sentido, el artículo 44 del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que:

ª1. 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".

Añade el artículo 45.2 párrafo 2º que "(…) De conformidad con el artículo 44.1, corresponderá al proveedor de servicios de iniciación de pagos demostrar que, dentro de su

Madrid

Administración de Justicia

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".

El artículo 46 del mismo texto legal regula la responsabilidad del ordenante, en caso de operaciones de pago no autorizadas, en los siguientes términos:

"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:

"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" (…).

Como expresa la SAP de Ourense, Sección 1ª, núm. 311/2023 de 12 mayo (JUR 2023\293249), de la normativa expresada se desprende que la entidad que presta el servicio de pago únicamente podrá exonerarse de la responsabilidad, acreditando la culpa grave del usuario que emite la orden de pago. En similares términos, para la SAP de Ourense, Sección 1ª, núm. 311/2023 de 12 mayo (JUR 2023\293249), con cita de las SSAP de Madrid, Sección 11ª, de 28 de febrero de 2022 y Sección 9ª, núm. 178/2015 de 4 mayo (JUR 201551311), salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante, la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la carga de la prueba de que la orden de pago "no se vio afectada por un fallo técnico o cualquier otra deficiencia". Podemos hablar de una responsabilidad cuasi-objetiva, por cuanto la entidad que presta los servicios sólo puede exonerarse mediante la prueba de la culpa grave del ordenante; interpretación acorde no sólo con la literalidad de la norma, sino con el espíritu y finalidad de la misma (art. 3 del CC). Igualmente, para la SAP de Madrid (Sección 9ª), núm. 178/2015 de 4 mayo (JUR 2015\151311), se establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago, con inversión de la carga probatoria, al presumirse la falta de autorización, si el titular lo niega. Este sistema de responsabilidad civil, tan solo cesa cuando el cliente ha actuado fraudulentamente o con negligencia grave a la hora de aplicar los medios razonables de protección de seguridad personalizados de que haya sido provisto, o en el caso de que no haya comunicado a la entidad el pago no autorizado, en cuanto tenga conocimiento del mismo, siempre y

Madrid

Administración de Justicia

cuando la entidad disponga de un sistema de comunicación adecuado, gratuito y disponible, en todo momento, que le permita al usuario del servicio efectuar la comunicación de la actuación fraudulenta.

En similares términos, SSAP de Asturias, Sección 1ª, núm. 351/2012 de 18 septiembre (JUR 2012\369519); Granada, Sección 5ª, núm. 212/2022 de 20 junio (JUR 2022\303953); Jaén, Sección 1ª, núm. 1355/2022 de 14 diciembre (JUR 2023\123097); Almería, Sección 1ª, núm. 99/2023 de 31 enero. JUR 2023\166836); Islas Baleares, Sección 5ª, núm. 132/2023 de 17 febrero (JUR 2023\200863); Asturias, Sección 7ª, núm. 353/2023 de 30 junio (JUR 2023\356143); Valencia, Sección 9ª, núm. 130/2013 de 23 abril (JUR 2013\254877) y Albacete, Sección 2ª, de 23 de febrero de 2012.

La lógica de la norma de acceso a la fuente de la prueba y facilidad probatoria en lo que hace a la implementación de medidas de seguridad en la prestación de un servicio que se da por las entidades de crédito a sus clientes a través de una oficina virtual que se desenvuelve en redes bien de internet, bien de comunicaciones móviles, se presenta como criterio más que de razonable atención al caso en el que la propia seguridad y debida reserva de la red se contrapone al acceso por parte de un tercero distinto al titular de la misma que asume poner en la red pública un conjunto de comunicaciones para permitir operaciones bancarias que requiere de soluciones tecnológicas muy avanzadas que minimicen las amenazas contra la autenticidad, integridad y la confidencialidad de los datos que circulan a través de la red. Por tanto, no es cierto que la carga de la prueba sobre la implementación de medidas de seguridad adecuadas, suficientes, eficientes y actuales al nivel de riesgo en la red bancaria de banca online lo sea a cargo del usuario del sistema, pues el marco de responsabilidad establecido para el caso de operaciones de pagos hechos por proveedores de servicios no autorizadas o ejecutadas incorrectamente, es el de la cuasi-objetividad tal cual se desprende de la regulación específica sobre la materia, sin perjuicio del régimen general de la carga de la prueba –SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

Desde el punto de vista del derecho de consumo -no está en cuestión la condición de usuario del demandante-, el artículo 147 del TRLGDCU dispone que "Los prestadores de servicios serán responsables de los y perjuicios causados a los consumidores o usuarios, salvo que prueben que han cumplido las exigencias y requisitos reglamentariamente establecidos y demás cuidados y diligencias que exige la naturaleza del servicio". Este precepto -como recuerda la STS núm. 185/2016, de 18 de marzo (RJ 2016, 983), citada en la SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-, no concreta el supuesto de hecho al que se refiere y por tanto ha de aplicarse con cautela, debiendo "ponderarse si el evento dañoso acaecido evidencia, o no, un defecto -un déficit de la seguridad que legítimamente cabía esperar- del servicio prestado; y tener presente "la disponibilidad y facilidad probatoria que corresponda a cada una de las partes del litigio". Además, la norma citada se complementa con el art. 148 conforme al cual "se responderá de los daños originados en el correcto uso de los servicios, cuando por su propia naturaleza, o por estar así reglamentariamente establecido, incluyan necesariamente la garantía de niveles determinados de eficacia o seguridad, en condiciones objetivas de determinación, y supongan controles técnicos, profesionales o sistemáticos de calidad, hasta llegar en debidas condiciones al consumidor y usuario", precepto del que se desprende el fundamento de la responsabilidad presunta del proveedor de servicios en el ámbito de la sociedad de la información, en particular cuando no aparece vinculada exclusivamente a la falta de específicas medidas de autoprotección por parte de aquellos sino a la falta de un especial

Madrid

Administración de Justicia

cuidado en atención a la naturaleza del servicio de que se trata, al modo empresarial de su prestación y al rol que en este desempeña un usuario típico, ponderado el hecho de que si el evento dañoso acaece es porque hay un déficit de la seguridad que legítimamente no cabía esperar del servicio prestado. Y dado que se produce -cuando el evento ocurre- dentro de un ámbito que se halla bajo el control del empresario prestador del servicio, que es quien cuenta con la información sobre las medidas de cuidado exigibles, y en su caso adoptadas, a fin de reducir el riesgo de riesgos, es el proveedor quien deviene responsable del daño -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

El Tribunal Supremo, en STS de 23 de julio de 2001 (RJ 2001, 8411), citada en la SAP de Murcia, Sección 1ª, núm. 398/2013 de 30 julio (JUR 2013\307044), ya expresa que "el art. 25 de la Ley General para la Defensa de los Consumidores y Usuarios establece un principio de inversión de la carga de la prueba, haciendo recaer sobre el productor o suministrador de los productos o servicios la carga de probar que el origen de los daños y perjuicios se encuentra en la conducta culposa del usuario o de las personas por las que debe responder, cometido que no ha logrado alcanzar el banco demandado".

En conclusión, la responsabilidad del proveedor de los servicios de banca online es de riesgo y consecuentemente, es por ley que a la entidad corresponde acreditar que la operación ordenada sí fue auténtica y que no estuvo afectada por un fallo técnico o por otra deficiencia como, por ejemplo, por un ataque informático de naturaleza fraudulenta al sistema bancario que hubiera permitido el acceso a las cuentas de sus clientes y disponer ilícitamente, de las mismas ordenando operaciones en detrimento de aquellos.

CUARTO.- DE LOS FRAUDES INFORMATICOS Y DEL PHISHING.-

Antes de analizar las pretensiones formuladas, es imprescindible proporcionar una definición del phishing, para determinar ante que abuso informático nos encontramos.

Efectivamente, siguiendo la SAP de Alicante, Sección 8ª, núm. 107/2018, de 12 marzo (AC 2018\818), la banca electrónica está siendo objeto de transferencias no autorizadas por el cliente y que vienen antecedidas por el método delictivo conocido como "phishing" que constituye una modalidad específica de fraude informático que visualiza las deficiencias de seguridad del sistema informático de una entidad y que trae causa en el uso de las redes telemáticas. De acuerdo con la Agencia Española de Protección de Datos (Resolución del Expediente núm. E/00762/2004, de 24 de mayo de 2006): el objetivo de los ataques de "phishing" es la obtención de forma engañosa y fraudulenta de los códigos de usuarios y contraseñas de clientes de Banca Electrónica, al objeto de realizar transferencias no autorizadas… Su operatoria comienza con la adquisición en internet de un "paquete de herramientas", que incluyen programas informáticos e información necesaria para realizar los ataques. Esta información incluye "listas de equipos comprometidos" que pueden ser utilizados bien para mandar correos electrónicos, bien para alojar páginas web falsificadas. Incluyen además "bases de datos de direcciones de correo electrónico". Una vez en posesión del paquete, se remiten los correos electrónicos con carácter indiscriminado (buscando contactar con clientes de la entidad financiera) informando de la necesidad de conectarse a una página web que parece pertenecer a la citada entidad y portar los códigos de acceso y contraseñas de clientes. Dicha página web se suele alojar en un equipo conectado a Internet cuya seguridad se haya [visto] comprometida", sin conocimiento de su usuario, y que se encuentra normalmente en un país distinto al de los destinatarios del ataque. De esta forma se constituye un "fichero de datos personales con códigos de usuarios y contraseñas de clientes" recabados de forma engañosa y fraudulenta, que se ubica normalmente en el mismo

Madrid

Administración de Justicia

"equipo remoto comprometido" en el que se aloja la página web falsificada. Con los datos obtenidos se realizan transferencias a cuentas de colaboradores situados en España los cuales a su vez retiran el dinero en efectivo y tras descontar una comisión realizan transferencias monetarias internacionales mediante entidades especializadas".

En similares términos, para la SAP de Madrid, Sección 9ª, núm. 178/2015 de 4 mayo (JUR 2015\151311), el phishing se origina con la suplantación de la identidad del banco por parte del phisher con la finalidad de adquirir información confidencial sobre contraseñas de cuentas bancarias, tarjetas de crédito o cualquier otra información en relación con el banco, que permita entrar en las cuentas de los usuarios en Internet de banca electrónica. El internauta recibe un correo electrónico o cualquier mensaje instantáneo, a través del cual se le informa de que debe cambiar sus claves bancarias, proporcionándole un link a través del cual pueda acceder a la página Web de la supuesta entidad bancaria y allí realizar la modificación aconsejada. En la mayoría de los métodos de phishing se utilizan técnicas de engaño, a través de las cuales el phisher utiliza contra la víctima el propio código de programa del banco o servicio similar, adquiriendo la página Web la verdadera apariencia de la entidad bancaria. Igualmente, resulta muy habitual que el internauta reciba un correo en el que se le informe de que debe verificar sus cuentas, seguido por un enlace que parece la página Web oficial de la entidad bancaria.

El phishing, como indica el Instituto Nacional de Ciberseguridad de España (INCIBE) es una modalidad de fraude llevada a cabo mediante el envío de un correo electrónico por parte de un ciber-delincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública, etc.) con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Para ello, adjuntan archivos infectados o enlaces a páginas fraudulentas en el correo electrónico –SAP de Almería, Sección 1ª, núm. 99/2023 de 31 enero (JUR 2023\166836)-.

Por otro lado, como indica la doctrina jurisprudencial, el contrato de cuenta corriente es una figura atípica que encuentra su singularidad, desde el punto de vista de los titulares de la cuenta, en el llamado servicio de caja, encuadrable, dentro del marco general de la comisión mercantil y de acuerdo con el cual el Banco, en cuanto mandatario, ejecuta las instrucciones del cliente (abonos, cargos...) y, como contraprestación, recibe determinadas comisiones, asumiendo la responsabilidad propia de un comisionista -STS de 21 de noviembre 1997 (EDJ 1997/7846). Además, la transferencia bancaria es un servicio que forma parte del contrato de servicio de caja entre un proveedor de servicios de pago (el banco) y sus clientes y sirve de medio de pago mediante el débito en la cuenta del ordenante y abono en la del beneficiario, tratándose en suma de un procedimiento financiero de movimiento de la moneda. Se trata de un medio de pago consistente en una orden dada al banco (banco emisor) por parte de un cliente (ordenante) a fin de que, con cargo a su cuenta, abone un determinado importe en otra cuenta del mismo o distinto banco (banco destinatario) abierta a nombre de un tercero (beneficiario) o del propio ordenante. Las transferencias se regulan en la Ley 16/2009, de 13 de noviembre, de Servicios de Pago. La Ley 16/2009, de 13 de noviembre, de Servicios de Pago define la orden de pago como "toda instrucción cursada por un ordenante o beneficiario a su proveedor de servicios de pago por la que se solicite la ejecución de una operación de pago" (art. 2.16 de la LSP). Desde un punto de vista contractual toda transferencia constituye una forma de ejecución de obligaciones contractuales previamente asumidas, ejecución obligada cuando se dan las condiciones pactadas, de ordinario, que haya provisión de fondos. Es por ello que se entiende que la orden de transferencia constituye una declaración de voluntad o mandato (en

Madrid

Administración de Justicia

el sentido del art. 254 del CCo) en virtud del cual el banco asume la realización de transferencias por cuenta del cliente como parte del contrato de servicio de caja. Dado el carácter negocial de la orden de pago, ésta puede pactarse que tenga lugar en cualquier forma, incluida la electrónica. En particular, el consentimiento a las operaciones de pago por el usuario, en el ámbito de la banca electrónica, supone que el cliente deba haber firmado un contrato de adhesión a los servicios de banca electrónica. El art. 25.1 de la LSP establece al respecto que "el ordenante y su proveedor de servicios de pago acordarán la forma en que se dará el consentimiento, así como el procedimiento de notificación del mismo", negocio jurídico que determina que la transferencia se entienda autorizada por el ordenante de acuerdo con el mismo precepto de la LSP. El consentimiento del ordenante se prestará, según el medio utilizado para prestar dicho consentimiento, mediante, o la firma de la autorización y orden de transferencia correspondiente, o verbalmente a través de la vía telefónica o a través de banca por internet o electrónica -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

Por otro lado, tanto en la banca telefónica como por internet, el proveedor de servicios de pago, o lo que es lo mismo, el banco emisor, debe implementar las medidas necesarias para asegurar la autenticación e identidad del ordenante a la hora de prestar su consentimiento. Por ello y para su ejecución, el banco debe comprobar en todo caso la autenticidad de la orden y, salvo pacto en contrario, que existe saldo suficiente. De ordinario, para la realización de transferencias ordinarias con cargo a una cuenta vinculada es preciso que el cliente haya de autenticar la operación mediante la introducción de las claves previamente facilitadas por la entidad de crédito con la que contrata, con respecto a las cuales tendrá unos deberes de custodia. La falsedad de la transferencia (es decir, que el ordenante no sea el titular de la cuenta) es un riesgo a cargo del banco porque, en principio, el deudor sólo se libera pagando al verdadero acreedor por lo que, si el banco cumple una orden falsa, habrá de reintegrar en la cuenta correspondientes las cantidades cargadas. Una excepción a esta distribución de riesgos se produce en el caso de que el titular haya creado o elevado el riesgo de falsificación de forma imputable en el caso concreto (STS 15 de julio de 1988 (RJ 1988, 5717) -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

Los servicios que prestan las entidades de crédito a sus clientes a través de su oficina virtual se desenvuelven en redes TCP/IP (Internet) o WAP (comunicaciones móviles). Siendo Internet una red pública de comunicaciones, la seguridad de las operaciones bancarias precisa de soluciones tecnologías avanzadas a los efectos de garantizar tanto la autenticidad como la integridad y la confidencialidad de los datos. Por estos motivos las entidades prestadoras del servicio de banca online deben dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones. Consecuencia derivada de la omisión, insuficiencia o defectuoso funcionamiento de las adoptadas es que han de ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

QUINTO.- DE LA VALORACIÓN DE LA PRUEBA Y DE LA JURISPRUDENCIA APLICABLE.-

Por tanto, lo importante a los efectos de la resolución de las pretensiones formuladas, no es tanto la existencia de diligencia en la actuación de la entidad de crédito demandada, sino, si esta ha probado que los actores incurrieron en fraude, incumplimiento deliberado o

Madrid

Administración de Justicia

negligencia grave en relación a las operaciones no autorizadas cuya devolución reclama a través de la presente demanda. Y tal prueba no se ha logrado en las presentes actuaciones.

Como ya se reconoce por la propia parte actora en el escrito inicial de demanda, "el 11 de junio de 2022, recibió un SMS de Liberbank (actual UNICAJA) en el que se le informaba de que se había detectado un acceso inusual a su cuenta online y que, si no reconocía ese nuevo dispositivo, verificara sus datos a través del enlace "https://s.id/liberbank-ayuda". Que accedió al enlace, que lo llevó a la banca online, y entró a través de su usuario y contraseña, con el objeto de que bloquearan dicho acceso inusual que le indicaban en el SMS. Dos días después, el 13 de junio de 2023, recibió una llamada desde el número , indicándole que lo contactaban desde el departamento de seguridad de la banca digital de Unicaja porque habían detectado accesos inusuales en su cuenta desde dispositivos no habituales. En dicha llamada, le indican que, para bloquear dichos accesos, le iban a enviar unos códigos por SMS los cuales les tendría que facilitar para poder solucionarlo (…)".

De esta forma, en el supuesto analizado, no ofrece duda de que, si bien las operaciones fueron autorizadas, registradas con exactitud y contabilizadas, sin que interviniera fallo técnico alguno, nos encontramos con el típico fraude denominado phishing, ya ampliamente explicado, y la forma en que se articuló la operación fraudulenta -de una complejidad y grado de perfección, difícilmente detectable por un cliente de las características del demandante-, no permitió a la actora, cuyo comportamiento en cualquier caso no puede considerarse diligente, detectar que algo anómalo estaba sucediendo, siendo evidente que el formato empleado por los delincuentes era totalmente apto para provocar el error en la demandante.

Y debemos empezar descartando, ante la ausencia de toda alegación y prueba a tal fin, cualquier atisbo de "mala fe en el proceder del demandante" en las operaciones fraudulentas que provocaron su empobrecimiento patrimonial, y, por ende, cualquier actuación fraudulenta por parte del actor. Tampoco se acredita que hubiera incurrido en negligencia grave, lo que tampoco ha sostenido la entidad demandada, que ha verificado la contestación a la demanda fuera de plazo. Parafraseando la SAP de Valencia, Sección 6ª, núm. 254/2022 de 13 junio (JUR 2022\321509), esta última interpretación nos parece más acorde con la protección debida al usuario de los servicios bancarios, y a las obligaciones propias de las entidades que ofrecen los servicios telemáticos, que son conocedoras de las crecientes actuaciones ilícitas o estafas que proliferan aprovechando las nuevas tecnologías, y que desarrollan mecanismos técnicos con el fin de ofrecer un sistema lo más seguro posible para el usuario, como parte igualmente de su oferta de servicios.

Efectivamente, no cabe duda que hubo un déficit de protección en el sistema de seguridad por parte de la entidad bancaria demandada. Por la parte demandada ni siquiera se ha explicado ni acreditado cuáles eran los niveles de seguridad existentes –en general se deduce del escrito de demanda la existencia de un único nivel de seguridad al cliente, que disponía de un código de usuario y una clave/contraseña para acceder a la Banca digital, siendo además muy probable la existencia de un segundo nivel de seguridad consistente en una segunda clave/contraseña para la realización de transferencias en el marco de la Banca Digital-. Tampoco se ha ofrecido una explicación satisfactoria sobre los reintegros en cajero automático efectuados. Igualmente existe una absoluta orfandad alegatoria y probatoria sobre la eventual adopción de medidas concretas de seguridad para dicho tipo de fraude conocido del phishing. No puede obviarse que la entidad era consciente de los ataques que venían produciéndose contra sus clientes y, a pesar de ello, no cambio el sistema de

Madrid

Administración de Justicia

autenticación -pues dicha modalidad fraudulenta de movimientos de cuenta es una práctica extendida-, pudiendo haber evitado el fraude si hubiese reforzado, como estaba a su alcance, el sistema de seguridad. No consta ningún filtro adicional de seguridad para evitarlo, ni se han aportado estudios sobre dicho riesgo; no constando tampoco que informara de esta situación al cliente, mediante la remisión de las oportunas advertencias mediante un medio de comunicación eficaz. En definitiva, la entidad demandada no actuó diligentemente, en previsión del fraude con el nivel máximo de seguridad, ya que no detectó el phishing sufrido por el actor, a pesar de que los phishers realizaron las conductas típicas y actuaron con el modus operandi característico en este tipo de fraudes informáticos. Efectivamente, no resulta acreditado que la entidad demandada hubiera previsto y establecido un sistema de autorización de pagos con autenticación reforzada, lo que implica que el prestador de servicios asume la responsabilidad patrimonial por un riesgo perfectamente descrito tanto para el usuario como para el prestador de servicios como es la defraudación con el procedimiento de phishing. El artículo 97 de 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, impone la obligación a los Estados miembros de velar por que los proveedores de servicios de pago apliquen la autenticación reforzada de clientes 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.

En otros términos, no se ha acreditado por la demandada la observancia de los deberes de diligencia que le eran exigibles en la autenticación de las operaciones de pago, pues ni prueba haber implementado un mecanismo "antiphishing" de protección de los usuarios de los instrumentos de pago por ella emitidos frente al uso fraudulento por un tercero de páginas imitativas de las propias para hacerse con las credenciales del instrumento –resulta indiferente que no se produjera fallo del sistema, en cuanto que, su responsabilidad no deriva de tal hecho, sino de no haber adoptado las medidas de seguridad precisas para evitar o minorar las consecuencias para el cliente de haber sufrido un fraude en red-. En definitiva, se entiende que media un incumplimiento contractual del banco al ejecutar una orden de pago sin comprobar su legitimidad, es decir, que provenía efectivamente del titular (o autorizado) de la cuenta, al no disponer de un sistema adecuado de seguridad que previniera tal tipo de órdenes fraudulentas. Y es exigible a la demandada la responsabilidad patrimonial cuasi objetiva legalmente establecida, según sentir general de la jurisprudencia menos de las Audiencias Provinciales, que, obviamente, supone un paso más en la protección al consumidor que el previsto en el art. 148 del TRLGDCU, puesto que viene a excusar al consumidor de la negligencia en que pueda haber incurrido por facilitar sus datos personales y claves de confirmación o firma electrónica en virtud de la acción defraudatoria de terceros.

En cualquier caso, no basta con medidas genéricas de protección o avisos estereotipados de cuidado, sino que la seguridad de las operaciones bancarias precisa de soluciones tecnológicas avanzadas, a efectos de garantizar tanto la autenticidad como la integridad y confidencialidad de los datos. De esta manera, no son los clientes los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, ni prevenir con su asesoramiento experto dichos riesgos.

Parafraseando la SAP de Albacete, Sección 2ª, de 23 de febrero de 2012, citada en la SAP de Asturias, Sección 1ª, núm. 351/2012 de 18 septiembre (JUR 2012\369519), quien resultó engañado o burlado no fue tanto el titular de la cuenta sino la entidad financiera y

Madrid

Administración de Justicia

proveedora del servicio que tenía su custodia y los medios de seguridad para protegerla, por lo que es ésta quien debe responder, salvo en los supuestos específicos legalmente indicados, y más allá de cualquier grado de diligencia mayor o menor de dicha entidad.

Como expresa la SAP de Madrid, Sección 20ª, de 20 de mayo de 2022, citada en la SAP de Asturias, Sección 7ª, núm. 285/2023 de 12 mayo (JUR 2023\312886), en la Directiva 2015/2036 la negligencia que le 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. Para la SAP de Vizcaya, Sección 3ª, núm. 429/2016 de 10 noviembre (AC 2016\2241), precisamente a la entidad bancaria demandada le incumbe proteger a sus clientes de cuantas conductas se realicen a través de la banca electrónica y ello en cuanto que precisamente este tipo de fraude comienza con la posibilidad de que los defraudadores interesan las claves de acceso a los clientes de los bancos (en este incide la mecánica delictiva)… Dichas circunstancias vienen a contemplar un sistema bancario electrónico diseñado por la entidad demandada adoleciendo de seguridad, la oferta a los clientes para operar a través de dicha banca electrónica y que es un hecho conocido de que cada vez se impone más por las entidades bancarias a los clientes, eliminando los servicios en ventanilla, se publicita por ser seguro contener los filtros para detectar fraudes y operar de forma fiable siendo así que en cuanto se ha probado la mecánica de la facilidad para operar por terceros no autorizados a través de la banca electrónica de la demandada, difícilmente podemos decir de que el Banco demandado no haya incurrido en negligencia grave de sus obligaciones, se han permitido efectuar operaciones bancarias sin superar ningún filtro cuando la legislación bancaria tiende precisamente a establecer que se efectúen y se establezcan diferentes controles por los bancos en protección de los clientes, tendiendo a establecerse una responsabilidad cuasi objetiva de las entidades bancarias en cuanto deben soportar los riesgos de su actividad profesional en cuanto que se establece con el cliente una responsabilidad contractual del servicio de depósito, custodia y pagos de las cuentas del cliente.

Igualmente, como expresa la SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818), la responsabilidad en estos supuestos no puede atribuirse directamente al supuesto ordenante de la transferencia por entenderse ésta autorizada al haberse realizado de acuerdo con los sistemas de autenticación del banco. Los sistemas de autenticación se establecen por los proveedores de servicios de pago y si un banco no ha sido capaz de limitar el acceso al canal de banca electrónica no puede pretender que el presunto ordenante víctima de esta práctica fraudulenta sea el único responsable, pues es el banco quien tiene responsabilidad respecto del buen funcionamiento y la seguridad del mismo. Dispone a tal efecto el art. 25.1 de la LSP que "Las operaciones de pago se considerarán autorizadas cuando el ordenante haya dado el consentimiento para su ejecución. A falta de tal consentimiento la operación de pago se considerará no autorizada". Por tanto, en el caso de órdenes de pago y transferencias fraudulentas ésta disposición supone que si la orden de pago o transferencia emitida por el cliente contiene una manifestación voluntad que actúa como causa del pago al tercero o la remisión de fondos al beneficiario, a "sensu contrario" puede afirmarse que sin dicha declaración de voluntad la operación de pago o transferencia de fondos se considerará no autorizada. Las medidas de seguridad no solamente están destinadas a proteger la seguridad de las órdenes de pago emitidas por los clientes, sino que su eficacia exonera a las entidades de crédito de sus responsabilidades frente a las órdenes de pago no emitidas por sus clientes de tal forma que el incumplimiento de este específico

Madrid

Administración de Justicia

deber de vigilancia da lugar a una responsabilidad por "culpa in vigilando" o responsabilidad objetiva por el mal funcionamiento de los servicios de banca electrónica.

En base a este fundamento la SAP de Barcelona, Sección 11ª, de 23 de julio 2015 declaró la responsabilidad de la entidad bancaria por cargos y extracciones de efectivo no autorizados que tuvieron su origen en la introducción por los delincuentes de un mensaje fraudulento en la página oficial del banco a través del cual se canalizó la operación -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-. Este mismo hecho, considerado una infracción de los deberes de vigilancia del banco, fue la causa por la que la entidad bancaria fue condenada en la SAP de Valencia, Sección 9ª, de 23 de abril de 2013 (JUR 2013, 254877) -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-. La SAP de Barcelona, Sección 14ª, de 7 de marzo de 2013 (JUR 2013, 171665) condenó a la entidad bancaria a devolver a una empresa víctima de "phising" una cantidad por cuanto la entidad bancaria no adoptó las medidas de seguridad adicionales previstas en las Condiciones Generales del contrato al haberse producido movimientos inusuales de fondos de la cuenta corriente y ser transferidos a cuentas sospechosas de su control por "muleros" que la entidad debió detectar -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-. La SAP de Zaragoza de fecha 14 de mayo de 2013 (JUR 2013, 197766) condenó a la entidad bancaria señalando que la Ley de Servicios de Pago expresa con claridad que, salvo una tardanza injustificada del usuario del servicio de banca electrónica en comunicar la irregularidad de las operaciones, será el banco quien deberá devolverle de inmediato el importe de la operación no autorizada y, en su caso, restablecerá la cuenta de pago en que haya adeudado dicho importe al estado que habría existido de no haberse efectuado la operación de pago no autorizada. Por ello y salvo actuación fraudulenta o negligencia grave del titular de la cuenta, la responsabilidad de la operación es del banco al que corresponde además probar el correcto funcionamiento del sistema informático -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-. La SAP de Madrid de 4 de mayo de 2015 (JUR 2015, 151311) -la víctima facilitó sus claves y contraseñas a una página web clonada que simulaba ser la del banco-, expresa que el artículo 31 de la Ley 16/09 de 13 de noviembre de Servicios de Pago establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago con inversión de la carga probatoria al presumirse la falta de autorización de la orden de pago o transferencia si el cliente lo niega -SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)-.

Añade la SAP de Alicante, Sección 8ª, núm. 107/2018 de 12 marzo (AC 2018\818)- que, a falta de prueba hemos de afirmar que la entidad financiera no cumplió con los deberes de seguridad frente a los riesgos concretos que podrían derivarse del funcionamiento de su plataforma de banca digital, deberes que no se cumplen con la mera literalidad genérica de los contratos suscritos, ni con la firma o suscripción de los mismos, pues son de índole material y técnico que han de fluir a través de diversos niveles de seguridad que pueden constituir opciones de la entidad pero no frente a sus clientes usuarios del sistema en caso de fallo del mismo pues, en tales casos, constituye objetivamente la omisión de una medida esencial en tanto tienen por objeto garantizar la autenticación de la orden de pago como, por lo demás, se desprende del propio tener del contrato de banca próxima. En consecuencia, es la prestadora de los servicios de pago quien tiene la obligación de facilitar un sistema de banca telemática segura, y no son sus clientes-usuarios los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, ni prevenir con un asesoramiento experto los mismos, no pudiendo en suma la parte obligada legalmente a ofrecer un modelo de servicio de caja que requiere de un especial nivel de seguridad, objetar que el usuario debía

Madrid

Administración de Justicia

conocer aspectos técnicos tales como identificar una web como falsa -cuando no consta que fuera burda y por tanto, evidente de toda falsedad-, ni que no eran fallos técnicos sino riesgos fraudulentos, determinados comportamientos de la plataforma que, no se olvide, son tan factibles que incluso el contrato de banca directa alude -para eludir responsabilidades el prestador- al riesgo de fallos técnicos, errores, interrupciones, desconexiones, sobrecargas y otras formas de defectos en la conexión. Si con carácter general el banco tiene la obligación, dice la STS 311/16, de 12 de mayo (RJ 2016, 2039), de comprobar la veracidad de la firma del ordenante -lo que no deja de ser una obviedad-, tanto más relevante lo es el ámbito de la banca electrónica a través de cualquiera de los sistemas ya existentes y que prestan un elevado nivel de garantía como son las claves aleatorias remitidas por la entidad directamente al usuario para cada operación y la firma electrónica. En conclusión, resulta evidente que en el caso hubo un incumplimiento contractual del banco al ejecutar una orden de pago sin comprobar su legitimidad, es decir, que provenía efectivamente del titular (o autorizado) de la cuenta, al no disponer de un sistema adecuado de seguridad que previniera tal tipo de órdenes fraudulentas ni adoptar medidas concretas y específicas en el caso cuando toma conocimiento de una situación operativa anormal que debió, cuando menos de forma puntual y excepcional, a verificar cualquiera orden que se diera en relación a las cuentas de la demandante. La no acreditación de las necesarias medidas de seguridad, la acreditación de la diligencia de la usuaria, y la inacreditación de la conducta posterior a la denuncia del fraude por el banco, omitiendo las medidas necesarias para evitar, en su caso, la pérdida definitiva del dinero, constituyen los presupuestos que permiten apreciar la realidad de una causalidad adecuada entre la conducta omisiva de la entidad y el resultado dañoso.

SEXTO.- DE LAS COSTAS PROCESALES.-

De conformidad con lo establecido en el artículo 394 LEC, procede imponer a la parte demandada el abono de las costas procesales.

V I S T O S los preceptos legales citados y demás de general y pertinente aplicación

F A L L O

Que estimando la demanda formulada por la representación de D. [redacted], debo condenar y condeno a UNICAJA BANCO S.A., a que abone a la actora la suma de 2.200 euros más los intereses legales desde la interpelación judicial, condenando a la parte actora al abono de las costas procesales.

Notifíquese la presente resolución a las partes, haciéndoles saber que CONTRA LA MISMA NO CABE INTERPONER RECURSO ALGUNO, todo ello al amparo de lo establecido en el artículo 455.1 LEC, en su nueva redacción dada por la Ley 37/2011, de 10 de octubre, de medidas de agilización procesal –"las sentencias dictadas en toda clase de juicio, los autos definitivos y aquéllos otros que la ley expresamente señale, serán apelables, con excepción de las sentencias dictadas en los juicios verbales por razón de la cuantía cuando ésta no supere los 3.000 euros"-.

Así por esta mi sentencia, juzgando en primera Instancia lo pronuncio, mando y firmo.

Madrid

Administración de Justicia

PUBLICACIÓN.- Leída y publicada ha sido la anterior sentencia por el Ilmo. Sr. Magistrado-Juez que la suscribe, en el día de la fecha. Doy fe.

Madrid

Este documento es una copia auténtica del documento SENTENCIA firmado electrónicamente por [redacted]

Administración de Justicia

JUZGADO DE 1ª INSTANCIA Nº 04 DE MÓSTOLES
Plaza Ernesto Peces Nº 2 , Planta 1 - 28931
Tfno: 916647308
Fax: 916187808
instancia4_mostoles@madrid.org
[redacted]

Procedimiento: Juicio Verbal [redacted]
Materia: Contratos bancarios
NEGOCIADO P
Demandante: D./Dña. [redacted]
PROCURADOR D./Dña. [redacted]
Demandado: UNICAJA BANCO, S.A.U.
PROCURADOR D./Dña. [redacted]

DILIGENCIA DE CONSTANCIA.- En Móstoles, a catorce de noviembre de dos mil veintitrés.

La extiendo yo, el/la Letrado/a de la Administración de Justicia, para hacer constar que en el día de hoy, se integra la sentencia en el sistema de gestión procesal para su firma por el juez, una vez debidamente firmada, procédase a su notificación a las partes, quedando en el sistema de gestión procesal el original de la sentencia, dejándose testimonio suficiente en autos, de lo que doy fe.

El/la Letrado/a de la Administración de Justicia

Madrid

[redacted]