Notificado: 15/12/2023

JUZGADO DE PRIMERA INSTANCIA Nº 27 DE VALENCIA

Av. PROFESOR LOPEZ PIÑERO (CIUDAD DE LA JUSTICIA), 14º-5ª Dcha (zona AZUL) (antigua Avd. Del Saler)

N.I.G.: **46250-42-1-2023-0007461**

Procedimiento: Juicio verbal (250.2) [VRB] Nº 000307/2023

SENTENCIA Nº 000371/2023

MAGISTRADO/A-JUEZ QUE LA DICTA: D/Dª MARIA ANGELES BARONA ARNAL

Lugar: VALENCIA

Fecha: trece de diciembre de dos mil veintitrés.

PARTE DEMANDANTE: [redacted]
Abogado: PALOMAR PEREZ, JUAN PABLO
Procurador: [redacted]

PARTE DEMANDADA EVO BANCO SA
Abogado: [redacted]
Procurador: [redacted]

OBJETO DEL JUICIO: Contratos en general.

La Titular de este Juzgado de Primera Instancia número 27 de VALENCIA , DOÑA Mª ÁNGELES BARONA ARNAL , ha dictado la siguiente resolución judicial en Valencia, el 13 de diciembre de 2023.

VISTOS los presentes autos que integran el procedimiento de Juicio Verbal tramitado en este Juzgado con el número 307/23 , interpuestos por el Procurador D. [redacted] en nombre y representación de Dª [redacted] y con la dirección del Letrado D. Juan Pablo Palomar Pérez contra EVO BANCO SA representado por la Procuradora Dª [redacted] y con la dirección del Letrado D [redacted] sobre reclamación de cantidad, se ha dictado la presente resolución con fundamento en los siguientes:

ANTECEDENTES DE HECHO

PRIMERO.- Que por el Procurador [redacted] en nombre y representación de Dª [redacted] se presentó demanda de juicio verbal contra EVO BANCO SA , en la que tras exponer los hechos y fundamentos de derecho que estimaba aplicables terminaba solicitando que se dicte sentencia por la que se declare que la demandada es responsable de los daños y perjuicios causados a la actora según obra especificado en el cuerpo de la demanda, y al amparo del art 1101 CC se le condene por dolo y/o negligencia a indemnizar a la demandante por los daños y perjuicios sufridos equivalentes

a la pérdida patrimonial experimentada. Esta pérdida de valor patrimonial se cuantifica en 5980 €, más los intereses legales de esta cantidad desde la fecha de la reclamación extraprocesal hasta intereses legales de esta cantidad desde la fecha de reclamación extraprocesal hasta la fecha de la sentencia y los intereses judiciales del art 576 LEC desde la fecha de la sentencia hasta su completo pago, con imposición de costas a la demandada.

SEGUNDO.- Admitida a trámite la demanda se dio traslado de la misma a la parte demandada para su contestación en el plazo de diez días.

Dentro del plazo compareció la Procuradora Dª. [redacted] en nombre y representación de la parte demandada, personándose y presentando escrito de contestación a la demanda en el que tras exponer los hechos y fundamentos de derecho que estimaba aplicables terminaba solicitando que se dicte sentencia desestimando la demanda y ello con imposición de costas a la parte actora.

TERCERO.- Señalada fecha para la celebración de la vista comparecieron las partes y tras la práctica de la prueba propuesta y admitida quedaron los autos conclusos para dictar sentencia.

FUNDAMENTOS DE DERECHO

PRIMERO.- Tal y como ha quedado planteado por las partes la cuestión controvertida y reconocido por la propia demandada que la hoy actora fue objeto de un ciberataque con aplicación de una técnica de ingeniería social, sobre la plataforma de banca on line de la entidad, a través del envío de un mensaje SMS al móvil de la actora el día 1 de septiembre de 2022 y efectuándose una compra mediante la utilización de la tarjeta de débito por importe de 3990 € y otra compra con la tarjeta de crédito por importe de 1990 €, la única cuestión que ha de ser analizada queda limitada a determinar si tal y como se sostiene por la demandada la demandante, con su actuación no guardó la debida diligencia relativa a los elementos de seguridad de su tarjeta y así facilitó a los estafadores las calves necesarias para operar en su cuenta y saltándose todos las advertencias de EVO y advertencias que se contienen en el documento nº 2 aportado por la entidad.

Y para resolver la cuestión debatida, hemos de partir de que 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 (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.

La ley cambiaria se ampara en el principio general de que el daño que resulte del

pago de un cheque falso o falsificado será imputado al librado, a no ser que el librador haya sido negligente en la custodia del talonario de cheques, o hubiere procedido con culpa. Este principio se recoge hoy en la Ley Servicios de Pago, articulo 36 y siguientes , pues 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 a su proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud, y que no se vio afectada por un fallo técnico o cualquier otra deficiencia. El registro por el proveedor de servicios de la utilización del instrumento de pago no bastará necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que este actuó de manera fraudulenta o incumplió deliberadamente o por negligencia grave una o varias de sus obligaciones previstas en la propia ley.

En este sentido, el artículo 41 de la Ley de Servicios de Pago , establece que es obligación del usuario: " 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" .

El art. 42 de la LSP , establece que el proveedor de servicios deberá:

" 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.

Esta sustitución podrá venir motivada por la incorporación al instrumento de pago de nuevas funcionalidades, no expresamente solicitadas por el usuario, siempre que en el contrato marco se hubiera previsto tal posibilidad y la sustitución se realice con carácter gratuito para el cliente.

c) Garantizará que en todo momento estén disponibles medios adecuados y gratuitos que permitan al usuario de servicios de pago efectuar una notificación en virtud del artículo 41.b), o solicitar un desbloqueo con arreglo a lo dispuesto en el artículo 40.4. A este respecto, el proveedor de servicios de pago facilitará, también gratuitamente, al usuario de dichos servicios, cuando éste se lo requiera, medios tales que le permitan demostrar que ha efectuado dicha comunicación, durante los 18 meses siguientes a la misma.

d) Ofrecerá al usuario de servicios de pago la posibilidad de efectuar una notificación en virtud del artículo 41.b), gratuitamente y cobrar, si acaso, únicamente los costes de sustitución directamente imputables al instrumento de pago.

e) Impedirá cualquier utilización del instrumento de pago una vez efectuada la notificación en virtud del artículo 41.b)

2. El proveedor de servicios de pago soportará los riesgos derivados del envío de un instrumento de pago al usuario de servicios de pago o del envío de cualesquiera elementos de seguridad personalizados del mismo".

El art. 43 respecto a operaciones de pago no autorizadas, establece que;" El usuario de servicios de pago obtendrá la rectificación por parte del proveedor de servicios de pago de una operación de pago no autorizada o ejecutada incorrectamente únicamente si el usuario de servicios de pago se lo comunica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación, incluso las cubiertas por el artículo 60, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo.

Los plazos para la notificación establecidos en el párrafo primero no se aplicarán cuando el proveedor de servicios de pago no le haya proporcionado ni puesto a su disposición la información sobre la operación de pago con arreglo a lo establecido en el título II.

2. Cuando intervenga un proveedor de servicios de iniciación de pagos, el usuario de servicios de pago deberá obtener la rectificación del proveedor de servicios de pago gestor de cuenta en virtud del apartado 1, sin perjuicio de lo dispuesto en el artículo 45.2, y el artículo 60.1

Teniendo en cuenta que los servicios que prestan las entidades de crédito a sus clientes a través de su oficina virtual se desenvuelven en redes TCP/IP (Internet)y 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 .

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. En este sentido la propia actora ha sido víctima de tales hechos, denunciados ante la Comisaria , que no ha podido, a día de hoy, averiguar su autoría, al no haber obtenido ninguna línea de investigación viable.

De acuerdo con la Agencia Española de Protección de Datos (R Expediente N° : NUM000, 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 "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 ".

La responsabilidad en estos supuestos no puede atribuirse directamente al supuesto ordenante de la transferencia por entenderse que 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. Por tanto, en el caso de órdenes de pago y transferencias fraudulentas puede afirmarse que sin dicha declaración de voluntad la operación de pago o transferencia de fondos, presuntamente realizada por la titular de los 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 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. Y en este sentido, la Audiencia Provincial de Zaragoza de fecha 14 de mayo de 2013, condenó a Barclays Bank a reintegrar 20.947 euros al cliente víctima de phishing. La Sentencia señala 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" .

En consecuencia, a lo expuesto, hay responsabilidad bancaria por los defectos de seguridad del sistema que determina la ejecución de órdenes de pago no autorizadas por su cliente, con la única excepción de que el banco acredite la culpa o negligencia de la víctima. Constituye por tanto obligación esencial de las entidades prestadoras del servicio de banca online el dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones por lo que, en el supuesto de insuficiencia o mal funcionamiento de las adoptadas, deben ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema.

En el caso de autos, necesariamente hemos de concluir en el mal funcionamiento o insuficiencia de las medidas de seguridad adoptadas por la entidad bancaria y no cabe sostener en modo alguno la existencia de culpa o negligencia de la hoy actora.

Por todo ello, hemos de concluir que existió un deficiente funcionamiento de la normativa sobre seguridad en el pago y, por lo tanto, le corresponde al banco la responsabilidad de abono de la cantidad defraudada.

Por consiguiente, acreditado el incumplimiento por la entidad bancaria demandada de sus obligaciones en los sistemas de pago online o a distancia, la demanda debe ser estimada.

SEGUNDO.- Conforme a lo dispuesto en el artículo 394 de la Ley de Enjuiciamiento Civil y al ser estimada la demanda procederá condenar en costas a la parte demandada.

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

FALLO

Que estimo la demanda interpuesta por el Procurador D. [redacted] en nombre y representación de Dª [redacted] contra EVO BANCO SA D. [redacted] y en consecuencia condeno a la citada demandada a abonar la suma de 5.980 €, más los intereses legales desde la fecha de interpelación extrajudicial y ello con expresa condena en costas a la parte demandada.

Contra la presente resolución cabe la interposición de recurso de **APELACIÓN** ante este Tribunal (artículo 455 LEC), dentro del plazo de **VEINTE DÍAS** hábiles contados desde el día siguiente a su notificación. En la interposición del recurso el apelante deberá exponer las alegaciones en que se base la impugnación, además de citar la resolución apelada y los pronunciamientos que impugna (art. 458 LEC).

INFORMACION SOBRE EL DEPÓSITO PARA RECURRIR

De conformidad con la D.A. 15ª de la LOPJ, para que sea admitido a trámite el recurso de apelación contra esta resolución deberá constituir un depósito de 50 €, que le será devuelto sólo en el caso de que el recurso sea estimado.

El depósito deberá constituirlo ingresando la citada cantidad en el banco BANCO SANTANDER, en la cuenta correspondiente a este expediente nº [redacted] indicando, en el campo "concepto" el código "02 Civil-Apelación" y la fecha de la resolución recurrida con el formato DD/MM/AAAA

En el caso de realizar el ingreso mediante transferencia bancaria, tras completar el Código de Cuenta Corriente nº [redacted] se indicará en el campo "concepto" el número de cuenta el código y la fecha que en la forma expuesta en el párrafo anterior.

En ningún caso se admitirá una consignación por importe diferente al indicado. En el caso de que deba realizar otros pagos en la misma cuenta, deberá verificar un ingreso por cada concepto, incluso si obedecen a otros recursos de la misma o distinta clase.

Están exceptuados de la obligación de constituir el depósito quienes tengan reconocido el derecho a litigar gratuitamente, el Ministerio Fiscal, Estado, Comunidades Autónomas,

entidades locales y organismos autónomos dependientes de los tres anteriores.

Llévese el original de esta resolución al Libro de Sentencias Civiles, que al efecto existe en la Secretaría de este Juzgado, quedando en las actuaciones testimonio de la misma.

Así por esta mi sentencia, definitivamente juzgando en esta instancia, lo pronuncio, mando y firmo.

E/

PUBLICACIÓN.- Leída y publicada fue la anterior sentencia por la Sra. Juez que la dictó, estando celebrando audiencia pública en mi presencia, de lo que yo, el Secretario, doy fe.