JUZGADO DE PRIMERA INSTANCIA Nº 17 DE VALENCIA

N.I.G.: [redacted]
Procedimiento: Juicio verbal (250.2) [VRB] - 001610/2022-6

De: D/ña. [redacted]
Abogado/a Sr/a. PALOMAR PEREZ, JUAN PABLO
Procurador/a Sr/a.

Contra: D/ña. CAIXABANK SA
Procurador/a Sr/a. [redacted]
Abogado/a Sr/a. [redacted]

S E N T E N C I A Nº 349/2023

En Valencia, a 12 de diciembre de 2023

S.S.ª, D. Jesús Ángel López Sanz, Magistrado del Juzgado de Primera Instancia nº 17 de esta ciudad, habiendo visto los presentes autos de juicio verbal n.º 1610/2022, sobre acción de reclamación de cantidad, promovidos por D. [redacted], defendido por el letrado Sr. Palomar Pérez, contra "CAIXBANK, S.A.", representada por la procuradora Sra. [redacted] y defendida por el letrado Sr. [redacted].

ANTECEDENTES DE HECHO

PRIMERO.- La actora interpuso demanda de juicio verbal sobre acción de reclamación de cantidad contra la demandada, y tras establecer los hechos y fundamentos de derecho que tuvieron por conveniente, terminaron solicitando que se dictara sentencia por la que se condenase a la demandada a pagarle la cantidad de 1.500 € con sus intereses legales desde la fecha de la reclamación extraprocesal hasta la fecha de la sentencia y los del Art. 576 de la Ley de Enjuiciamiento Civil desde la fecha de la sentencia hasta su completo pago, y al pago de las costas.

Basó el actor su reclamación en que es cliente de la entidad demandada, con quien tiene un contrato de tarjeta de débito; el 17/01/2022 a las 8,04 horas se inició un ciberataque sobre la plataforma de banca on line del actor a través del envío a su dispositivo móvil de un mensaje SMS al que se dio la apariencia de haber sido remitido por CAIXABANK que manifestaba que no podía utilizar su Tarjeta Débito y que tenía que activar el nuevo sistema de seguridad web en un enlace, lo cual provino de un ciberdelicuente, tal como queda acreditado en la página web analizadora de enlaces sospechosos "Virus Total" recomendada por la "Oficina de Seguridad del Internauta" del Instituto Nacional de Seguridad, que lo registró como tal enlace sospechoso de

actuaciones de phishing en fecha 12 de julio de 2022. No obstante, el actor creyó de buena fe que tal mensaje provenía realmente de su entidad bancaria, y por una fuerza mayor no pudo percibir la existencia de un engaño al venir encabezado por la leyenda "CAIXABANK", al igual lo hacían otros mensajes de carácter auténtico que en otras ocasiones le habían precedido, al ofrecer como enlace un dominio que se iniciaba con la extensión "https", entorno que por lo común se considera como seguro en internet, lo que infundió en el actor, dentro de ese marco visual de "aparente veracidad", un sentimiento de temor hacia la seguridad de su cuenta, lo cual, unido a la confianza de que, efectivamente, pretendía protegérsele frente a la utilización no autorizada de sus datos bancarios, lo que le llevó a seguir las instrucciones y pulsar el referido enlace, lo que le redirigió a través de la web internet a un dominio de internet que a su vez aparentaba la pagina web de CAIXABANK (*"página espejo"*), la cual le solicitó toda una serie de datos bajo el pretexto de solventar la incidencia de seguridad, los cuales fueron suministrados de buena fe por el actor; tales datos entregados a petición del requirente fueron en concreto su numero de DNI y su contraseña de acceso a la plataforma on line. Transcurridos unos segundos, el actor entró en su plataforma de banca on line, a fin y efecto de confirmar el correcto estado de sus cuentas de depósito, y en tal momento pudo comprobar con estupefacción que había sido objeto de un engaño y que se había producido dos operaciones de pago en concepto de compra a la entidad BINANCE por importes de 500 euros y 1.000 euros.

Valga añadir que en ningún momento recibió de la entidad CAIXABANK llamada telefónica o mensaje por SMS, previamente a la ejecución de tales pagos. De igual forma, en ningún momento suministró a la entidad CAIXABANK código numérico ni de ningún otro tipo a tal efecto.

Desde la fecha en que acaecieron los hechos descritos, han sido permanentes las visitas efectuadas a su oficina bancaria a los efectos de que se le proporcionara solución a una situación de la que él no se consideraba en absoluto responsable, por cuanto consideraba haber actuado diligentemente en todo momento. Ello no obstante, los empleados de su oficina bancaria hicieron caso omiso a las reiteradas reclamaciones recibidas.

SEGUNDO.- Admitida la demanda se emplazó a la demandada, la cual se opuso a la demanda, y tras establecer los hechos y fundamentos de derecho que tuvo por conveniente, terminó solicitando que se dictara sentencia por la que se desestimase la demanda, alegando que las transacciones se realizaron de forma electrónica con la tarjeta bancaria del actor y para ello, además de instalarse la aplicación de CaixaBankNow y CaixaBank Sign se tuvieron que introducir los datos de la tarjeta (nombre completo, numeración, CVV) y demás otros datos de carácter personal del demandante para la autenticación de la compra en mediante un

sistema de seguridad reforzada como es la aplicación de CaixaBank Sign.

Tres días después de que se produjeran los hechos y cuando ya era conocedor del fraude que se le había cometido, unido además a que conocía que él mismo propició el fraude al abrir el enlace que estaba inserto en el mensaje SMS recibido y consiguientemente facilitar todos sus datos de carácter personal y bancario, interpuso el actor una denuncia ante la Dirección General de la Policía Nacional de Valencia, el la que afirmó que en ningún momento había facilitado sus claves a nadie, cosa que, como se puede comprobar con el escrito de demanda presentado de contrario, no reviste veracidad alguna. Es más, en tal denuncia el demandante no hizo alusión alguna a la responsabilidad de CAIXABANK sobre dicha transferencia supuestamente fraudulenta, pese a las afirmaciones vertidas ahora en la demanda, por lo que de ello se extrae que la demandada no había llevado a cabo ningún incumplimiento de sus obligaciones ni mucho menos había actuado con negligencia. Más bien todo lo contrario, de entre las palabras del Sr. [redacted] se puede entrever cómo señala haber sido víctima de un presunto delito de estafa.

En realidad, fue el Sr. [redacted] quien propició dicho fraude al haber recibido un SMS y acceder al enlace que contenía el mismo y facilitar todos sus datos personales y bancarios, lo que provocó una suplantación de su identidad. Tanto es así que el propio demandante reconoce y acredita junto con su demanda1, que el enlace al que accedió provino de un ciberdelicuente y que la página web "Virus Total" recomendada por la "Oficina de Seguridad del Internauta" del INCIBE, lo registró como enlace sospechoso de actuaciones de phishing en fecha de 12 de julio de 2022.

Por tanto, es evidente que el demandante conoce que los hechos que ahora son objeto del presente procedimiento son, en realidad, constitutivos de un presunto delito de estafa y por ello ya inició la vía penal oportuna a través de la denuncia aportada. Y sobre todo, es evidente que el Sr. [redacted] es plenamente conocedor de que dichos hechos se tratan en realidad, del comúnmente conocido como "SMISHING" y en el que ninguna responsabilidad puede tener la demandada.

Por otro lado, ni que decir cabe que en cuanto el Sr. [redacted] se dirigió a CAIXABANK e informó de los hechos, la demandada automáticamente inició el mecanismo establecido y, tras la cancelación de las tarjetas bancarias, procedió a comprobar si las operaciones habían contado con los sistemas de verificación de CAIXABANK y CAIXABANK PAYMENTS & CONSUMER. Pero, desde luego, CAIXABANK en nada más podía intervenir ahí, más allá de verificar si había existido alguna deficiencia o fallo o en los sistemas de pago o si, por el contrario, las operaciones habían contado con todos pasos y había sido autenticada por la parte demandante, cosa que así fue.

Las órdenes de pago cuya devolución se solicita a CAIXABANK en el presente procedimiento son totalmente acordes a derecho y

cuentan con consentimiento, pues tal y como figura en el detalle de dichas operaciones, las órdenes de pago contaron con la autentificación reforzada, es decir, con la autenticación del titular de la tarjeta vía notificación por medio de CaixaBankNow. Otra cosa es que, como se ha adelantado, fuera precisamente la negligencia grave del Sr. [redacted], lo que propició las mismas. Pero insistimos, nada de ello podrá serle reprochado a CAIXABANK. Más bien al contrario, cumplió en todo momento con sus obligaciones contractuales dado que las transacciones se completaron tras haber confirmado la identidad de la titular de la tarjeta mediante un sistema de autenticación reforzada.

Los proveedores de servicios de pago deben dotarse de medidas suficientes que garanticen al usuario del sistema la seguridad de las operaciones, por lo que en aquellos casos en los que exista suficiente y buen funcionamiento de las medidas adoptadas no puede hacerse responsable a la entidad bancaria. Normalmente las medidas de seguridad establecidas por los bancos y las entidades de pago se articulan en varios niveles de seguridad complementarios y compatibles entre sí. El primer nivel, consiste en un código de usuario y contraseña o clave privada que cada cliente podrá configurar para acceder a la oficina virtual o banca online. Y en otro nivel de seguridad se sitúa la conocida *"autenticación reforzada"* que son aquellos datos únicamente conocidos por el cliente que permiten autorizar, y por ende, consentir la operación. Y en el caso de autos, dicha autenticación reforzada se llevó a cabo mediante: (i) el dispositivo desde el que se accedió a CaixaBankNow, que estaba previamente enrolado y (ii) el conocimiento de las credenciales de acceso a CaixaBankNow, datos que, desgraciadamente, el Sr. Pérez como reconoce en la demanda, facilitó al presunto estafador. Así pues, el supuesto fraude no se pudo perpetuar sin la necesaria cooperación del Sr. [redacted], tanto es así que el presunto estafador necesitó del DNI y la clave de acceso del demandante a la banca online –que recordemos, fueron facilitadas por el Sr. [redacted] y así lo afirma en la demanda–, para con ello finalizar el proceso de compra autenticando la misma. Por consiguiente, para realizar una compra mediante comercio seguro se solicitan los siguientes datos:

- i. Datos de la tarjeta bancaria (numeración PAN, fecha de caducidad y número de seguridad CVV).
- ii. En la pasarela de pago, antes de confirmar dicho pago, la página web, solicita que se acceda a CaixaBankNow para confirmar el pago.
- iii. Por lo que, por ello, se debe de acceder a CaixaBankNow con las credenciales (personales e intransferibles) para confirmar la operación, que figura como pendiente.
- iv. Una vez se ha confirmado la operación, el pago se ha realizado y el proceso de compra finaliza.

Por ende, así es como el sistema se asegura que es el

auténtico titular de la tarjeta quien está intentando realizar la transacción. Hasta que no se confirma la operación por el titular de la tarjeta bancaria después de haber introducido el usuario y contraseña para acceder a CaixaBankNow, la operación no se podrá realizar y figurará como pendiente, lo que aumenta exponencialmente el nivel de seguridad.

El funcionamiento de autorización a través de la aplicación del dispositivo móvil es muy sencillo y se activa cuando se está intentando realizar una compra online con los datos de la tarjeta o intentando realizar cualquier transacción. Antes de finalizar la operación se activa el sistema de confirmación en dos pasos, en este caso, mediante la confirmación a través de la aplicación. En ese momento, se recibe una notificación que solo servirá para esa operación y en ese instante. Y es que, como medida de seguridad, esa notificación tiene una duración de tiempo limitada. Si no se usa en el tiempo que aparece en la pantalla de pasarela de pago, la notificación caduca y se debe volver a solicitar la autenticación vía notificación.

Precisamente, esta información viene ampliamente explicada y desarrollada en el Informe Pericial Informático de fecha 23 de marzo de 2022 emitido por EVIDENTIA, que, además de confirmar que CAIXABANK goza de un sistema de seguridad adecuado ratifica que todas las operaciones efectuadas a través de banca online gozan de un doble sistema de autenticación reforzada, tal y como exige la normativa que resulta de aplicación.

Además, como también recoge el informe pericial, y permite la Directiva Europea 2015/2366, existen supuestos en los que se pueden realizar exenciones de autenticación reforzada en algunas operaciones, como es el caso, por ejemplo, de operaciones de escasa cuantía o beneficiarios de confianza.

A mayor abundamiento, las tarjetas VISA, como la que fueron contratadas, cuentan con la tecnología de autenticación *3-D Secure 2.0*. *3-D Secure* (anteriormente denominado '*Verified by Visa*') proporciona una capa de seguridad adicional previa a la autenticación para las transacciones de comercio electrónico. Permite el intercambio de datos entre el comerciante, el emisor de la tarjeta y, cuando proceda, el consumidor, para así validar que la transacción está siendo ordenada por el legítimo propietario de la cuenta.

Asimismo, las operaciones realizadas con la tarjeta VISA cuentan con un sistema analítico predictivo denominado *Visa Advanced Authorization* para detectar actividades que se clasifican como sospechosas. Se trata de un algoritmo que evalúa determinados atributos relativos a cada una de las transacciones realizadas en menos de un milisegundo para generar una calificación que predice la probabilidad de que las compras sean fraudulentas de forma que se pueda aprobar o rechazar la transacción. Todas estas medidas de seguridad se producen con carácter previo o durante el transcurso de la transacción y, como se puede comprobar, se cumple con lo exigido por el propio RDLSP

al contar no solo con un mecanismo de doble autenticación (mediante la confirmación de la operación mediante la aplicación instalada en la aplicación), sino que existen sofisticados sistemas que permiten detectar operaciones fraudulentas.

No obstante lo anterior, cabe señalar que los sistemas de seguridad de CAIXABANK no se limitan al momento de la operación, sino que continúan una vez la misma ha sido ejecutada. Así, todos los titulares de una tarjeta emitida por CAIXABANK PAYMENTS & CONSUMER, E.F.C., E.P., S.A.U. cuentan con el servicio CaixaBankProtect. Este servicio consiste en el envío de alertas sobre las operaciones realizadas con la tarjeta. Esas alertas se envían a través de mensajería SMS o de aplicaciones específicas como notificaciones *push* en aplicaciones móviles o mediante correo electrónico. Las alertas informan, por ejemplo, sobre operaciones con un importe que supera los 500 euros o las primeras compras realizadas en el extranjero, cualquiera que sea su importe. Otra cosa es que desgraciadamente, pese a haber recibido esas alertas el Sr. [redacted] facilitara los datos al presunto estafador.

También como medida de seguridad, y que de nuevo el Sr. [redacted] obvio por completo, CAIXABANK pone a disposición de todos los titulares de tarjetas un número de asistencia 24 horas al día y 365 días al año, en el que pueden solicitar el bloqueo de las tarjetas, avisar del robo de las mismas o de las credenciales asociadas a éstas. También pueden comunicar si sospechan que han sido víctima de un fraude o si han identificado una operación que no reconocen sin necesidad de desplazarse a una oficina de atención al público de CAIXABANK o esperar a que comience su horario de atención al público. Se trata del teléfono gratuito 900 40 40 90. Sin embargo, el Sr. [redacted] prefirió esperarse y personarse en la oficina, permitiendo de nuevo, una vez más, que el fraude se cometiera. Pues si hubiera llamado a dicho teléfono gratuito mi representada habría bloqueado su banca online y las tarjetas de crédito emitidas por CAIXABANK PAYMENTS & CONSUMER.

Por si no fuera suficiente, el Instituto Nacional de Ciberseguridad de España (en adelante, INCIBE) pone a disposición de todos los ciudadanos un teléfono de contacto, denominada "*Línea de ayuda en Ciberseguridad*", donde el Sr. Pérez podría haber consultado cualquier duda acerca de los correos electrónicos que recibió y a los que accedió antes de facilitar sus datos bancarios a terceros. Por ello, se trata de un hecho conocido por la sociedad, puesto que son continuos los anuncios en medios de telecomunicación en los que el propio INCIBE informa a los ciudadanos de la existencia de dicho teléfono de contacto.

Por último, aunque no menos importante, CAIXABANK facilita a sus clientes información periódica un boletín de noticias con consejos sobre seguridad, información actualizada del modus operandi de los delincuentes y con novedades en las medidas de seguridad que adoptan en CAIXABANK. Esta información también se puede consultar fácilmente desde la web de particulares de

CAIXABANK. Igualmente, al acceder a la plataforma de clientes o banca online, denominado CaixaBankNow, aparecen advertencias de seguridad.

Pero es que, además, los propios antivirus que cualquier ciudadano debe tener instalado en sus dispositivos advierten a sus usuarios del auge de las estafas financieras, recordando los consejos de seguridad que deben llevarse a cabo. Otra cosa es que, de nuevo el Sr. [redacted] incumpliera con sus obligaciones contractuales y ni tan siquiera tuviera instalado en su terminal móvil un antivirus.

En este sentido, debemos recordar que tanto en los medios de comunicación como en las redes sociales o en la propia red se difunden y divulgan asiduamente los peligros de toda índole que acechaban a la realización de compras online o distintas modalidades de fraude como el *phishing, smishing o SIM Swapping*, peligros que siempre han estado protegidos por férreas medidas de seguridad y que, para el caso que nos ocupa, se encontraban a la vanguardia entre sus competidores. Y es que, recordamos, las órdenes de pago se verificaron no solo mediante los datos personales del Sr. [redacted], sino que se autentificaron mediante un sistema reforzado como fue la notificación en la aplicación de CaixaBankNow.

En conclusión: el sistema de seguridad de la banca electrónica de CAIXABANK era, y es, absolutamente adecuado al nivel de riesgo que conlleva esta forma de operar en la realización de compras con la tarjeta de débito VISA, ya sea en comercios físicos o virtuales.

En este sentido, cuando la información proporcionada por la entidad bancaria sobre las medidas de seguridad es correcta y queda evidenciado el correcto funcionamiento de estas medidas, entra en juego la diligencia de actuación que lleva a cabo el usuario del sistema para poderse dilucidar la responsabilidad en la que, en su caso, incurriría el banco. Estas medidas de seguridad no solamente están destinadas a proteger la seguridad de las compras con tarjeta realizadas por los clientes –siendo ésta evidentemente su máxima finalidad– sino que, además, su eficacia exonera a las entidades de crédito de sus responsabilidades frente a las compras no autorizadas por sus clientes cuando estos han actuado de forma negligente como, por ejemplo, compartiendo las claves recibidas en su dispositivo móvil o autorizando operaciones no reconocidas a través de la aplicación CaixaBankNow.

Tal y como se afirma en el escrito de demanda presentada de contrario, el Sr. [redacted] recibió un mensaje SMS que contenía un enlace que abrió, y en los cuales facilitó todos sus datos personales y bancarios que se les iba solicitando. Por tanto, no es controvertido que el Sr. [redacted] fue víctima de un fraude conocido como "*smishing*": En este sentido, el Instituto Nacional de Ciberseguridad -INCIBE- en su página web, informa que el *SMISHING* es un tipo de fraude caracterizado por el envío de un

SMS a un usuario simulando ser una entidad legítima con el objetivo de robarle información y realizar un cargo económico. Es decir, como hemos visto la estafa comienza con un defraudador que recopila datos personales sobre la víctima mediante el envío de un SMS. Y una vez obtiene dichos datos, suplanta su identidad llevando a cabo, la contratación de nuevos productos o la realización de cargos sobre sus tarjetas, e incluso las órdenes de transferencias. Ahora bien, son muchas las advertencias que día a día, y desde diferentes medios se publican acerca de este tipo de fraudes. Indicando expresamente a los consumidores de la importancia de no acceder a correos electrónicos, SMS o páginas web sospechosas, sobre todo, no ejecutar enlaces que éstos puedan contener, y lo más importante, no revelar nunca los datos personales ni bancarios. La información acerca de la necesidad de extremar las precauciones para prevenir este tipo de fraudes es de dominio público, y el Sr. [redacted] tenía acceso a la misma.

En todo caso, el delito del que fue víctima el Sr. [redacted] consta de tres fases.

- La fase inicial en el que el estafador obtiene los datos personales de la víctima, en este caso, con el envío de un SMS al que el Sr. [redacted] contestó facilitando sus datos personales y bancarios. Y es que, sobre lo que no hay duda, es que en esta fase el Sr. [redacted] tuvo una participación directa en la consecución del fraude, pues si hubiera actuado diligentemente y no hubiera facilitado sus datos personales al presunto estafador, tales como nombre completo y apellidos, número de DNI, usuario y contraseña, éste no hubiera suplantar la identidad y efectuar las compras que son objeto de Autos. De hecho, precisamente el Informe Pericial sobre los sistemas de seguridad de CAIXABANK que se ha adjuntado como Documento número 4 confirma que en este tipo de fraudes siempre se da necesariamente la colaboración activa del cliente.
- La segunda fase es aquella en la que, una vez ha obtenido los datos personales, el defraudador procede a introducir todos los datos bancarios en el procedimiento de compra online, tales como número de tarjeta bancaria, fecha de caducidad y CVV.
- La tercera y última fase es aquella en la que el estafador, una vez que posee todos los datos del cliente, procede a realizar las órdenes de pago. Esto es, puesto que el presunto estafador disponía del usuario y de la clave de acceso a la banca online del Sr. [redacted] procedió a confirmar la operación de compra en CaixaBankNow, tras introducir el usuario y contraseña de acceso a la aplicación.

Es decir, como bien indica Banco de España, una vez el defraudador ha obtenido todos los datos del cliente defraudado, a efectos de la entidad financiera, las operaciones son realizadas como si fuera el cliente quien las está llevando a cabo, pues el sistema de seguridad de doble autenticación reforzada funciona correctamente. Insistimos, como el propio Banco de España explica en su Portal Bancario, en este tipo de fraude los sistemas de

seguridad de las entidades financieras de doble autenticación de la operación funcionan correctamente. Lo que por desgracia es materialmente imposible que la entidad financiera puede controlar, es si ese cliente ha sido suplantado previamente por su propia cooperación.

En conclusión, todos estos hechos distan mucho de ser una actuación diligente del cliente por lo que en modo alguno puede ser responsable de ello la demandada.

Para llevar a cabo las compras con tarjeta, lo primero que tuvo que hacer el presunto estafador fue acceder a la página web donde pretendía efectuar las compras online mediante la tarjeta de débito con número [redacted] cuya titularidad corresponde al Sr. [redacted]. En primer lugar, el presunto estafador accedió, como se ha indicado, a la página web donde pretendía efectuar la compra, en este caso y tal y como se puede comprobar en el documento relativo al detalle de las operaciones accedió a la página web BINANCE e inició el proceso de compra. A continuación, el supuesto delincuente, debió instalarse en su terminal móvil la aplicación de la entidad CAIXABANK. Para ello, introdujo el usuario del Sr. [redacted] esto es su Documento Nacional de Identidad -que previamente el demandante le había facilitado- y su contraseña -que el Sr. [redacted] también le había facilitado- y justo a continuación procedió al *"enrolamiento del dispositivo"*. Tras ello, continuó con el proceso de compra y efectuó el pago. Posteriormente, una vez el presunto estafador ya tenía acceso a la banca online -a la que recordemos, había accedido con las claves personales facilitadas por el Sr. [redacted]- y se encontraba dentro de la banca online del demandante, efectuó los siguientes pasos: a. En primer lugar, autorizó la compra tras observar el aviso de que existía una operación pendiente de verificar y confirmar. En segundo lugar, confirmó la autorización. Finalmente, en la tienda online, el proceso de compra se finaliza exitosamente.

Pues bien, si observamos el detalle de las operaciones, todas y cada una de ellas consta autenticada -y por ende con consentimiento-, al haberse autorizado la compra vía CaixaBankNow como medio de autenticación reforzado. En consecuencia, y en contra de lo alegado en la demanda, las órdenes de pago fueron confirmadas mediante un sistema de autenticación reforzada y, por tanto, gozan de consentimiento. Al respecto, debemos recordar a la parte actora que, desde el 1 de enero de 2021, tanto las entidades bancarias, como otros proveedores de pago (como pueden ser establecimientos o tiendas online), deben aplicar la autenticación reforzada en las operaciones de sus clientes, y precisamente esa autenticación reforzada es el consentimiento en este tipo de transacciones. Por tanto, habiendo acreditado CAIXABANK que las dos órdenes de pago objeto de autos constan debidamente autenticadas, no cabe más que concluir que las mismas son válidas. Otra cosa es que el cliente haya sido víctima de un fraude -en el que recordemos, en nada intervino mi representada

al contrario de lo que sí hizo él mismo al no haber sido diligente en la custodia de sus datos personales-. Así pues, los sistemas funcionaron correctamente y no cabe duda de que las operaciones quedaron debidamente registradas, autenticadas y contabilizadas con exactitud, tal y como se desprende del propio Documento número 15 en el que aparecen todos los detalles de las operaciones realizadas: fecha, hora, importe, comercio, actividad del comercio, tarjeta utilizada, e, forma de autorización, etc. Es más, de contrario se imputa a CAIXABANK responsabilidad por el simple hecho de tratarse de pagos con tarjeta para terminar concluyendo que mi representada debía haber detectado las órdenes de pago como fraudulentas y, por ende, paralizarlas. Sin embargo, de nuevo, yerra la parte actora en tales conclusiones por dos motivos muy significativos y que prefiere, una vez más, no relatar al Juzgador:

1. Para poder llegar a la conclusión de si CAIXABANK puede o no paralizar una transacción online debemos contextualizar este tipo de operaciones. Así, según informó el Banco de España y el Banco Central Europeo: *"En 2020, el número total de operaciones de pago efectuadas con instrumentos distintos del efectivo en la zona del euro, que incluyen todos los tipos de servicios de pago, se incrementó un 3,7 % en comparación con el año anterior y se situó en 101.600 millones de operaciones, y el importe total aumentó un 8,7 % hasta situarse en 167,3 billones de euros. Los pagos con tarjeta representaron el 47 % del total de operaciones, mientras que las transferencias supusieron el 23 % y los adeudos directos el 22 %. El número de transferencias en la zona del euro se incrementó un 3,2 % en 2020, hasta alcanzar 23.100 millones de operaciones, y el importe total creció un 10,3 % y se situó en 155,8 billones de euros. La importancia relativa del número de operaciones electrónicas siguió aumentando, y la proporción de operaciones electrónicas en relación con las operaciones en papel ahora es de aproximadamente quince a una"*.

Por tanto, dentro de este contexto de millones de operaciones al día, y teniendo en cuenta que CAIXABANK cuenta con más de 20 millones de clientes, es perfectamente entendible que los supervisores y el legislador confirmen que una operación de pago se entenderá debidamente ejecutada y realizada cuando cuente con el doble sistema de autenticación o autenticación reformada. Pues de lo contrario, exigir a las entidades financieras que fiscalizaran cada una de las operaciones que se llevaran a cabo por sus clientes, no solo sería materialmente imposible, sino que incluso colapsaría el sistema financiero en sí.

Pero no solo es que CAIXABANK no deba fiscalizar las operaciones, sino que, además, en el caso de autos las dos transacciones que hoy nos ocupan ni tan siquiera podrían resultar sospechosas en tanto en cuanto el Sr. [redacted] habitualmente realizaba compras con tarjeta y transacciones en Internet, como son las compras a través de la plataforma PayPal.

Así pues, el Sr. [redacted] conocía a la perfección el

funcionamiento de las compras con su tarjeta y sabía de la necesidad de no revelar a terceros nunca, bajo ningún concepto, sus datos personales ni bancarios. Si desgraciadamente lo hizo y ello propició el fraude, no cabe más que concluir que el demandante actuó con total negligencia en la custodia de sus elementos de seguridad.

No hay dudas de que efectivamente el Sr. [redacted] actuó negligentemente al facilitar a un tercero sus datos personales que provocaron la autenticación de las operaciones que ahora dice no reconocer y, por ende, actuó sin atenerse a las condiciones que regulaban su uso, ya que no adoptó las medidas razonables para proteger los elementos de seguridad de esta, propiciando que el fraude se materializada. Y todo ello, reiteramos, sin olvidar que el Sr. [redacted] venía realizando compras online con cierta asiduidad, pudiéndose afirmar que estaba familiarizado con el sistema. Pero, sin embargo, no actuó con la diligencia que le era exigible, dando lugar a que con su comportamiento se produjera el fraude del que, desgraciadamente, fue víctima.

Con ello, la parte demandante incumplió, y de una manera grave, las obligaciones que le impone el artículo 41 del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera de utilizar el instrumento de pago de conformidad con las condiciones que regulen su emisión o utilización y no tomó las medidas razonables a fin de proteger los elementos de seguridad personalizados del mismo, por lo que no procede acceder a la pretensión deducida en la demanda.

Pero es que, además, como se profundizará en los Fundamentos de Derecho el artículo 46 del mismo texto legal establece la responsabilidad para el caso de que el usuario no haya tomado las medidas necesarias para proteger esos elementos de seguridad, como precisamente ocurrió en el caso de autos.

De modo que es el propio RDL de Servicios de Pago el que imputa la responsabilidad de la operación ejecutada por el banco al cliente en aquellos casos -como el que hoy nos ocupa- en el que el cliente hubiera actuado fraudulentamente o con negligencia grave a la hora de adoptar los medios razonables de protección sobre los elementos de seguridad personalizados que hubieran sido facilitados por el banco, motivo por el cual, debe ser desestimada la demanda. Y es que, en el caso que nos ocupa, las operaciones contaron con un sistema de autenticación reforzada para autorizar las compras que se estaba realizando.

CAIXABANK facilitó en todo momento toda la información relativa a la seguridad del sistema de compra con tarjeta, pues como se ha explicado, mi representada no solo concedía esta información a través de los empleados de banca, sino que en el propio contrato suscrito con la parte actora y en la propia página web de la entidad constaba toda la información en materia de seguridad.

Por ello, siendo el propio Sr. [redacted] el que ha actuado

negligentemente al no haber tomado las precauciones que la ley le imponía, y sobre las que fue debidamente informado desde la suscripción de su contrato de tarjeta, ninguna obligación extracontractual se ha incumplido.

Y es un hecho notorio que tras un proceso de compra y posterior fusión a día de hoy CAIXABANK ostenta la posición de BANKIA. Y no es un hecho controvertido, que en su día el Sr. Pérez con quien formalizó ambos contratos de tarjeta de crédito fue con BANKIA. Ahora bien, tal y como siempre se informó al demandante, tanto BANKIA en su momento como CAIXABANK ahora, se limitan a comercializar las tarjetas de crédito, siendo CAIXABANK PAYMENTS & CONSUMER, E.F.C., E.P., S.A.U. la entidad de pago y emisora de la tarjeta utilizada para efectuar las operaciones no reconocidas por la parte demandante. En este sentido cabe señalar que, a pesar de encontrarse dentro del mismo grupo empresarial, CAIXABANK PAYMENTS & CONSUMER, E.F.C., E.P., S.A.U. es una sociedad independiente a CAIXABANK, S.A. Así pues, CAIXABANK, S.A. tiene su domicilio social en calle Pintor Sorolla, 2-4, 46002 Valencia, con NIF A08663619, inscrita en el Registro Mercantil de Valencia, Tomo 10370, Folio 1, Hoja V-178351, e inscrita en el Registro Administrativo Especial del Banco de España con el número 2100. Mientras que CAIXABANK PAYMENTS & CONSUMER, E.F.C., E.P., S.A.U. está domiciliada en Caleruega 102, 28033 Madrid, con CIF A08980153, inscrita en el Registro Mercantil de Madrid, Tomo 36.556, Folio 29, Hoja M-656492, e inscrita con el n.º 8776 en el Registro de Establecimientos de Crédito del Banco de España.

Es más, en acreditación de que efectivamente es CAIXABANK PAYMENTS & CONSUMER, E.F.C., E.P., S.A.U y no CAIXABANK, S.A. la titular de los derechos y obligaciones acerca de las tarjetas de crédito se adjunta el testimonio notarial de fecha 30 de mayo de 2022 otorgado por el Ilustre Notario de Barcelona Don [redacted] y en el que se hace constar:

"1º.- El día 7 de octubre de 2021 CAIXABANK, S.A. y CAIXABANK PAYMENTS & CONSUMER, E.F.C., E.P., S.A., mediante escritura autorizada por mí con número 13.649 de protocolo, elevado a público el contrato privado de compraventa del negocio de emisión y tarjetas proveniente de Bankia, S.A. el cual se encontraba sujeto al cumplimiento de varias condiciones suspensivas.

2º.- Que el día 15 de noviembre de 2021, mediante diligencia otorgada por mí a la mencionada escritura, los comparecientes dejaron constancia del cumplimiento de la última de las condiciones suspensivas, y en consecuencia, CAIXABANK, S.A. transmitió a CAIXABANK PAYMENTS & CONSUMER, E.F.C., E.P., S.A.U. el negocio de emisión y tarjetas provenientes de BANKIA, S.A.".

Igualmente se adjunta como DOCUMENTO NÚMERO 1 BIS el testimonio notarial de fecha 26 de marzo de 2021 otorgado por Ilmo. Notario de Valencia Don [redacted] que acredita la fusión por absorción de BANKIA, S.A. y CAIXABANK, S.A.

Asimismo, también se puede comprobar de las condiciones generales

a las que se suscriben todos aquellos quienes formalizan contrato de tarjeta bancaria con CAIXABANK PAYMENTS & CONSUMER, E.F.C., E.P., S.A.U., que esta entidad actúa a través de su agente, el cual es CAIXABANK.

Es por ello por lo que CAIXABANK, S.A. no ostenta la legitimación pasiva en el presente procedimiento pues es CAIXABANK PAYMENTS & CONSUMER, E.F.C., E.P., S.A.U. el proveedor de servicios de pago y quien estaría obligado a cumplir con las disposiciones del Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (en lo sucesivo, 'RDLSP'), al que hace referencia la parte contraria en su demanda para exigir la responsabilidad de mi mandante. Así pues, el propio artículo 10 y siguientes de la citada norma establece el régimen jurídico de las entidades de pago, como lo es CAIXABANK PAYMENTS & CONSUMER, E.F.C., E.P., S.A.U. indicando expresamente en su artículo 10.2 que "las entidades de pago no podrán llevar a cabo la captación de depósitos", actividad que sí que realizaría CAIXABANK, S.A., como es público y notorio.

TERCERO.- Celebrada la vista el día señalado, se practicaron las pruebas declaradas pertinentes, tras lo cual quedaron los autos conclusos para sentencia.

CUARTO.- En la tramitación del presente procedimiento se han observado todas las prescripciones legales.

FUNDAMENTOS DE DERECHO

PRIMERO.- La demandada alega, en primer lugar, la falta de legitimación pasiva, que no puede ser apreciada.

La demanda se basa en la responsabilidad de la demandada como proveedora de servicios de pago, por lo que es irrelevante a estos efectos quién es el titular del negocio de las tarjetas, porque la demanda no se funda en dicha condición.

Además, no se ha aportado ningún contrato de tarjeta en el que sea contratante "Caixabank Payments & Consumer", ni tampoco que pruebe que se comunicara al actor que el proveedor de servicios de pago hubiese cambiado después de que en noviembre de 2021 se cediese a dicha entidad el negocio de tarjetas.

Por si fuera poco, el documento n.º 18 de la contestación a la demanda prueba que Caixabank asumió frente al actor la condición de proveedor de servicios de pago, lo que le impide

ahora negarlo, so pena de ir contra sus propios actos, lo que está proscrito en nuestro Derecho.

SEGUNDO.- Entrando en el fondo del asunto, recordemos que el Art. 36 del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, considera autorizadas las operaciones de pago cuando el ordenante haya dado el consentimiento para su ejecución, y, a falta de tal consentimiento, la operación de pago se considerará no autorizada.

El Art. 41 impone al usuario de servicios de pago habilitado para utilizar un instrumento de pago utilizarlo de conformidad con las condiciones que regulen la emisión y utilización del instrumento de pago y tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas.

El Art. 42 impone al proveedor de servicios de pago emisor de un instrumento de pago la obligación de cerciorarse de que las credenciales de seguridad personalizadas del instrumento de pago sólo 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.

El Art. 44 prevé que 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. Y 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. A estos efectos, 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. Y atribuye al proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, la carga de probar que el usuario del servicio de pago cometió fraude o negligencia grave.

El Art. 45 dispone que, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine, en cuyo caso el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada.

Por último, el Art. 46 impone al ordenante soportar todas las pérdidas derivadas de operaciones de pago no autorizadas si 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; y le deja 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, pero 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.

TERCERO.- De la regulación reseñada se deduce que la responsabilidad establecida respecto de la entidad proveedora del servicio de pago es cuasiobjetiva y se articula a través de la inversión de la carga de la prueba: se presume la falta de autorización de la operación cuando el titular lo niega. Y esta responsabilidad cede cuando el cliente actúa fraudulentamente o con negligencia grave en la observancia de las condiciones que regulen la emisión y utilización del instrumento de pago, o en la protección de sus credenciales de seguridad personalizadas, o cuando no haya comunicado a la entidad el pago no autorizado en cuanto haya tenido conocimiento del mismo.

En este sentido la SAP de Salamanca de 21 de junio de 2021 ha declarado que "...los deberes de seguridad que los bancos deben observar para llegar a consolidar un espacio seguro de actuación han tenido su reflejo legal armonizando nuestro ordenamiento interno con la normativa europea sobre la materia. Y así, la Ley 16/2009, de 13 de noviembre, de servicios de pago, que incorporó a nuestro ordenamiento la Directiva sobre servicios de pago en el mercado interior, que fue aprobada como Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2005/65/CE y 2006/48/CE y por la que se derogó la Directiva 97/5/CE. Esta Ley 16/2009 introdujo en un capítulo que reguló los riesgos operativos y de seguridad de los proveedores de servicios de pago. Todo ello en la idea, resaltada en el Preámbulo de la Ley, de que la regulación de los servicios de pago ha de promover, en particular, un entorno que propicie el desarrollo

ágil de las transacciones de pago, unas reglas comunes respecto a su operatividad, un abanico suficientemente amplio de opciones de pago para los usuarios y unas normas de protección efectiva para los mismos. Pues bien, en los artículos 27 y ss se establece un régimen de responsabilidad de las indemnizaciones por daños y perjuicios en caso de que se ejecute una operación de pago no autorizada, a cargo del proveedor de servicios de pago, que le obliga a devolver de inmediato el importe de la operación no autorizada y, en su caso, restablecer en la cuenta de pago en que se haya adeudado dicho importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada. Responsabilidad que solo cede en caso de actuación fraudulenta o del incumplimiento, deliberado o por negligencia grave, del titular de la cuenta en cuestión, respecto a la obligación que asume de adoptar "las medidas razonables a fin de proteger los elementos de seguridad personalizados" que se le hayan facilitado. En esa misma línea, el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, derogó la Ley 16/2009, e incorporó parcialmente a nuestro ordenamiento jurídico el marco europeo creado por 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 y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) n.° 1093/2010 y se deroga la Directiva 2007/64/CE, en sustitución de la del 2007, que junto al Reglamento (UE) 2015/751 del Parlamento Europeo y del Consejo, de 29 de abril de 2015 . Esta nueva norma, actualmente en vigor, asumió como principales objetivos facilitar y mejorar la seguridad en el uso de sistemas de pago a través de internet, reforzar el nivel de protección al usuario contra fraudes y abusos potenciales, respecto del previsto en la Ley 16/2009, de 13 de noviembre, así como promover la innovación en los servicios de pago a través del móvil y de internet. En la misma línea de proteger al consumidor del servicio, exige ahora

sistemas de autenticación reforzada, y reproduce un sistema similar de responsabilidad a cargo del proveedor del servicio, que solo cede, como en el supuesto anterior, en caso de actuación fraudulenta o del incumplimiento, deliberado o por negligencia grave; que lo será solo en caso de actuación fraudulenta, cuando el proveedor no ha establecido el sistema de autenticación reforzada..."

Pues bien, en este caso el actor recibió u mensaje que parecía ser de la demandada, que le reenvió a un enlace en el que le pidió los datos de su DNI y el código de seguridad, tras lo cual se produjeron los cargos en la cuenta. Es decir, que se produjo un fraude por un tercero que simuló necesitar los datos para activar la tarjeta que se suponía desactivada, correspondiendo pues a la demandada acreditar que el actor actuó fraudulentamente o con negligencia grave, lo que no consta, pues el mero hecho de facilitar los datos al estafador no es una negligencia grave, ya que es un hecho notorio la habilidad con que logran hacerse pasar por las entidades autorizadas para reclamar las claves y datos de los clientes, y además la demandada no ha aportado prueba alguna de lo contrario.

Como recuerda la SAP de Logroño de 17 de febrero de 2023, tratándose de operaciones no autorizadas, 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 u otra deficiencia del servicio prestado por el proveedor de servicios de pago, lo cual responde al hecho de haber sido la Banca la que principalmente se ha beneficiado de las nuevas tecnologías porque su uso le ha permitido abaratar costes mediante el sistema de que sean los clientes los que realicen materialmente las operaciones que antes llevaban a cabo sus empleados en las oficinas o sucursales bancarias, lo que les ha permitido despedir a muchos de aquéllos y cerrar muchas de éstas. Y en esa situación resulta justo que sea el banco el que se haga cargo de ese margen de riesgo que ha introducido el uso de las nuevas tecnologías y que antes, cuando las operaciones se hacían presencialmente, era inexistente. El banco es perfectamente consciente que en esta dinámica de contratación, es el dispositivo de telefonía móvil el que habitualmente más se utiliza por los clientes para la realización de estas operaciones on line; no en vano, los bancos facilitan e incentivan su uso mediante la creación de sus propias apps, cuyo uso preconizan y publicitan de forma insistente entre sus clientes. Por eso no puede el banco pretender exonerarse de responsabilidad con el argumento de que no responde de la seguridad de esos dispositivos, cuando resulta que es el propio banco quien,

mediante la creación apps, facilita cuando no incentiva su utilización por los clientes para realizar este tipo de operaciones, sin que conste que el banco, cuando facilita o difunde esta utilización, se preocupe de cuál es concretamente el rango o nivel de seguridad que presenta cada uno de los dispositivos de sus clientes a través de los cuales se realizan las operaciones.

Por ello, debe estimarse la demanda.

CUARTO.- En materia de costas, y por aplicación del Art. 394 de la Ley de Enjuiciamiento Civil, procede condenar a la demandada al estimarse la demanda.

FALLO

1.- ESTIMO la demanda presentada por D. [redacted] contra "CAIXBANK, S.A."

2.- CONDENO a la demandada a pagar al demandante la cantidad de 1.500 € con sus intereses legales desde la fecha de la reclamación extraprocesal hasta la fecha de la sentencia y los del Art. 576 de la Ley de Enjuiciamiento Civil desde la fecha de la sentencia hasta su completo pago.

3.- CONDENO a la demandada a pagar al demandante las costas procesales.

Notifíquese a las partes la presente resolución haciéndoles saber que es firme y que contra la misma no cabe interponer recurso alguno.

Así por ésta mi sentencia, lo pronuncio, mando y firmo.

PUBLICACIÓN.- Leída y publicada fue la anterior sentencia por el Sr. Juez que la suscribe, estando celebrando audiencia pública en el mismo día de su fecha, de lo que yo, el Secretario, doy fe.

En Valencia, a 12 de diciembre de 2023.