Juzgado de Primera Instancia nº 3 de Granollers

Calle Josep Umbert, 124, planta 4a - Granollers - C.P.: 08402
TEL.: 936934585
FAX: 936934582
EMAIL:instancia3.granollers@xij.gencat.cat

N.I.G.: 0809642120238163874

Juicio verbal (250.2) (VRB)[redacted]

Materia: Juicio verbal sobre productos y activos financieros

Entidad bancaria BANCO SANTANDER:
Para ingresos en caja. Concepto: [redacted]
Pagos por transferencia bancaria: IBAN ES55 0049 3569 9200 0500 1274.
Beneficiario: Juzgado de Primera Instancia nº 3 de Granollers
Concepto: [redacted]

Parte demandante/ejecutante: [redacted]
Procurador/a: Consol Cuadra Baile
Abogado/a: Òscar Serrano Castells

Parte demandada/ejecutada: BANCO BILBAO VIZCAYA ARGENTARIA, S.A.
Procurador/a: Isabel Fuentes Angulo
Abogado/a:

SENTENCIA N° 200/2024

En Granollers, a diecisiete de junio de dos mil veinticuatro.

Vistos por mí, Dª. Mª José Dorel Bruscas, Magistrado-Juez en sustitución del Juzgado de Primera Instancia n° 3 de los de Granollers y su partido, los presentes autos de **Juicio Verbal** seguidos en este Juzgado y registrados bajo el **n° 9**[redacted], en los que figura como parte demandante **Dª** [redacted], representada por la Procuradora de los Tribunales Dª. Consol Cuadra Baile y asistida por el Letrado D. Oscar Serrano Castells y, como parte demandada **la entidad financiera BANCO BILBAO VIZCAYA ARGENTARIA, S.A.,** representada por la Procuradora de los Tribunales Dª Isabel Fuentes Angulo y bajo la dirección de la Letrado Dª. [redacted], sobre reclamación de cantidad.

ANTECEDENTES DE HECHO

PRIMERO.- Que, en fecha 16 de mayo de 2023, por la Procuradora de los Tribunales Dª. Consol Cuadra Baile, en nombre y representación de Dª [redacted], se presentó telemáticamente escrito, que por reparto correspondió a este Juzgado, por el que interponía Demanda de Juicio Ordinario en reclamación de cantidad contra la entidad financiera BANCO BILBAO VIZCAYA ARGENTARIA, S.A. y en la que, tras exponer los hechos y alegar los fundamentos

de derecho que estimó pertinentes, terminó Suplicando se dicte Sentencia por la que:

1.- Se declare el incumplimiento de las obligaciones legales y contractuales que le eran de cumplimiento, declarando la responsabilidad de BBVA, S.A. en la incorrecta custodia y ejecución de las operaciones realizadas contra la cuenta titularidad de la demandante no autorizadas por ella.

2.- Se condene a la entidad demanda a abona a la actora el importe de los daños y perjuicios causados junto con los intereses legales de dicha cantidad desde la fecha de su cargo en cuenta e igualmente se retroceda el importe de 4.690,00 euros, todo ello con especial condena en costas a la demandada.

SEGUNDO.- Que, tras subsanarse los defectos formales existentes, mediante Decreto de fecha 26 de junio de 2023 se admitió a trámite la demanda, acordándose dar traslado de la misma a la parte demandada a fin de que en el término legalmente establecido al efecto compareciese en autos y contestase la demanda, trámite que evacuó en tiempo y forma mediante escrito de fecha 14 de ju1io de 2023 por el que se oponía a la demanda formulada de contrario en base a los hechos y fundamentos de derecho que estimó pertinentes, Suplicando se dicte Sentencia por la que se desestime la demanda con imposición de las costas a la demandante.

TERCERO.- Mediante Diligencia de Ordenación de fecha 31 de julio pasado se tuvo por contestada la demanda acordando señalar fecha para la celebración de la correspondiente vista, la cual hubo de suspenderse en reiteradas ocasiones por causa justificada, señalándose finalmente para el día 31 de enero del presente año, llevándose a cabo en el día y hora señalados al efecto con la asistencia de ambas partes debidamente representadas y asistidas de letrado, afirmándose y ratificándose en dicho acto las mismas en sus respectivos escritos de demanda y contestación, solicitándose el recibimiento del pleito a prueba, proponiéndose la documental, testifical y pericial, llevándose a cabo, tras su admisión, con el resultado que obra en autos, acordándose la más documental propuesta y, una vez cumplimentada, se puso de manifiesto a las partes para que llevasen a cabo el trámite de conclusiones, lo que hicieron ambas mediante la presentación de sendos escritos en fecha 13 de junio del año en curso por los que mantenían ambas sus posiciones, quedando tras lo cual los presentes autos en el día de hoy conclusos para Sentencia.

CUARTO.- En la sustanciación del presente procedimiento, se han observado todos los términos y las prescripciones legales existentes al efecto.

FUNDAMENTOS DE DERECHO

PRIMERO.- En el presente procedimiento, se ejercita por la parte actora, una acción de carácter personal, dirigida frente a la entidad demandada al objeto de que, en virtud del contrato de tarjeta de crédito nº [redacted] suscrito entre las partes, vinculado a la cuenta bancaria de la que era titular la demandante en la entidad demandada, así como el contrato de servicios banca online que le permitía acceder a su cuenta desde su ordenador y dispositivo móvil, se llevaron a cabo varias operaciones con dicha tarjeta, así como con otras tres tarjetas que no son reconocidas por la misma y que en la madrugada del 1 de septiembre de 2022 se abrieron a nombre de la demandante, concretamente la tarjeta AHORA BBVA nº [redacted], la AQUA CREDITO MAS nº 4[redacted] y la TARJETA AQUA DEBITO nº [redacted], tarjetas creadas "ex novo" sin la autorización de la misma, utilizándose todas ellas sin el consentimiento de la actora para llevar a cabo hasta un total de 18 operaciones consecutivas por un importe total de 1.610,00 euros con la primera a través de cinco operaciones, 955,00 euros con la segunda en un total de cuatro operaciones, 1.175,00 euros con la tercera en un total de cinco operaciones y 950,00 euros con la última en un total de cuatro operaciones, lo que determina un importe total de 4.690,00 euros que se reclaman mediante la presente en concepto de daños y perjuicios sufridos por la actora por incumplimiento por parte de la entidad financiera de sus obligaciones legales y contractuales, al haberse iniciado el 31 de agosto y 1 de septiembre de 2022 sobre la plataforma de banco online de la actora un ciberataque, con aplicación de una técnica de ingeniería social, a través del envío de un mensaje SMS a su dispositivo móvil, con la apariencia de haber sido remitido por BBVA entremezclándolo dentro del hilo de mensajes SMS auténticos provenientes de tal entidad bancaria, siendo el texto del mensaje el siguiente:

"*Su cuenta ha sido suspendida. Por seguridad es obligatorio instalar BBVA Protect para prevenir mensajes fraudulentos. Descarga: https://bbva.movil#descarga.click#*"

La demandante, creyendo que tal mensaje provenía realmente de su entidad bancaria, al constatar que se

entremezclaba dentro del hilo de mensajes de BBVA, junto a mensajes auténticos de tal entidad, al visualizar que mostraba un link encabezado por la extensión "https" (normalmente perteneciente a páginas web verdaderas) y que el mismo hacía constar la leyenda "BBVA" en la convicción de que se pretendía protegerle frente a una utilización fraudulenta de su tarjeta de pago, pulsó dicho enlace que le redirigió a través de la web internet a un domicilio de internet que a su vez aparentaba la página web de BBVA donde se le solicitó y facilitó el DNI y contraseña, creyendo estar al habla con un empleado de la entidad, produciéndose ese mismo día, de madrugada, pocos minutos después, las 18 operaciones señaladas anteriormente, ello tras haber dado de alta incluso tres nuevas tarjetas de crédito, no llamando la atención de la entidad financiera quien, pese a las horas en que se dieron de alta dichos contratos de tarjeta y que la actora ya era titular de una, no extremó las precauciones de seguridad pertinentes, siendo los beneficiarios terceros ajenos a la demandante, cliente de la entidad demandada, ascendiendo la suma de tales operaciones, tal y como se ha señalado anteriormente a la cantidad total de 4.690,00 euros, no habiendo recibido SMS alguno de BBVA con clave de autenticación de doble factor, siendo cargada tal cantidad por la entidad bancaria a través de los diferentes cargos en fecha 31 de agosto de 2022 con su tarjeta y posteriormente el 1 de septiembre de 2022 en las tres tarjetas que se abrieron a su nombre ignorando dicho extremo.

La demandante detectó que algo no iba bien en su terminal Android Galaxy S9 con la Banca móvil, al conectarse desde su IP [redacted] a las 23:22 horas del 31 de agosto de 2022, poniéndose inmediatamente (00:51 horas) en contacto con la entidad, tal y como se acredita de la Documental aportada a la demanda (Documento nº 5), remitiendo un correo electrónico que obtuvo respuesta de la entidad a las 00:53 horas del 1 de septiembre por movimientos sospechosos con la única tarjeta de la que era consciente porque era la única que tenía, acabada en [redacted], lo que motivó que se personase al día siguiente en la oficina para ver qué había pasado, interponiendo denuncia el 1 de septiembre de 2022 sobre las 11:57 horas, la cual fue ampliada a las 15:40 horas cuando en la entidad le indicaron que tenía otras tres tarjetas de crédito que ella no había contratado y con las que se habían efectuado igualmente operaciones, interponiendo por tanto denuncia policial ese mismo día, formulando reclamación a la entidad que fue desestimada.

Reclamándose por tanto la cuantía de los pagos que se dicen fraudulentos, dado que existiría responsabilidad de la

entidad por haber podido disponer de trazabilidad de la aplicación, evidenciando que las conexiones se habrían efectuado desde un dispositivo distinto de los habituales; por no existir negligencia de la demandante al ser que las claves de seguridad fueron conservadas diligentemente y no existir sustracción de la tarjeta, la numeración identificativa de tal documento, ya que nunca fue guardada junto a su instrumento de pago, ni en formato abierto alguno detectable por terceros, y por no haber autenticado la operación adecuadamente, no habiendo autorizado tampoco la contratación de otras tres tarjetas de crédito teniendo ya una vigente, no teniendo lógica alguna hacerlo de madrugada y para llevar a cabo compras vía internet cuando de la vida de las operaciones bancarias de la actora no se desprendía dicha trayectoria.

La parte demandada se opone a la demanda y solicita la desestimación de la demanda alegando que no ha cumplido la actora ninguna de sus obligaciones, que la responsabilidad sería de la demandante por haber revelado los datos de acceso a su banca electrónica y el número de la tarjeta y CVV de la misma, es decir, hubo una negligencia muy grave por su parte ya que las operaciones fueron autenticadas con las correspondientes códigos TP remitidos a su teléfono móvil y que la entidad lleva advirtiendo a sus clientes de que tomen medidas para evitar estos fraudes.

SEGUNDO.- Así las cosas, no existe controversia entre las partes en que se llevaron a cabo los 18 cargos fraudulentos utilizando los datos de la demandante y las tarjetas de crédito de la que era titular y que se crearon el mismo momento de la utilización fraudulenta, otras tres tarjetas de crédito a su nombre y respecto de la misma cuenta de cargo de la que era titular la actora. El Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, en su artículo 41 respecto a las obligaciones a cargo del usuario establece 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 éste designe, sin demora indebida en cuanto tenga conocimiento de ello".

En cuanto a la demandada, en el caso que nos ocupa, sus obligaciones se reflejan en el artículo 44 del mismo Texto legal que señala:

"1.- Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá al 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.

4.- El proveedor de servicios de pago conservará la documentación y los registros que le peritan acreditar el cumplimiento de las obligaciones establecidas en este Título y sus disposiciones de desarrollo y las facilitará al usuario en el caso de que así e sea solicitado, durante, al menos, seis años. No obstante, el proveedor de servicios de pago conservará la documentación relativa al nacimiento,

modificación y extinción de la relación jurídica que le une con cada usuario de servicios de pago al menos durante el periodo en que, a tenor de las normas sobre prescripción puedan resultarles convenientes para promover el ejercicio de sus derechos contractuales o sea posible que les llegue a ser exigido el cumplimiento de sus obligaciones contractuales.

Lo dispuesto en este apartado se extiende sin perjuicio de lo establecido en la Ley 18/2018, de 28 de abril de prevención del blanqueo de capitales y de la financiación del terrorismo, así como en otras disposiciones nacionales o de la Unión Europea aplicables".

Por lo tanto, si bien el usuario tiene la obligación de tomar las precauciones necesarias para evitar el uso indebido o fraudulento de su tarjeta, que es lo que en el presente le achaca la demandada para eximirse de responsabilidad, es el prestador quien tiene la obligación y carga de probar la negligencia del usuario, lo que ha pretendido hacer en el presente con la pericial aportada y ratificada en el acto de la vista.

No es controvertido en el presente la relación contractual ni la titularidad de la tarjeta bancaria acabada en [redacted] por la demandante, sí la utilización de dicha tarjeta con su autorización en los cinco cargos que se llevaron a cabo en la noche del 31 de agosto y madrugada del 1 de septiembre de 2022 y contratación de las tres tarjetas de crédito utilizadas en 13 de las 18 operaciones fraudulentas llevadas a cabo. La demandante, ha relatado, tanto en el escrito de demanda como en el interrogatorio practicado que, a primera hora de la mañana del 1 de septiembre de 2022, ya que los hechos sucedieron de madrugada, siendo en dicho momento que se le comunica que ha sufrido un fraude de duplicidad de SIM y le dan el extracto de su tarjeta acabada en [redacted] para que pueda presentar la correspondiente denuncia (Documento ° 6 de la demanda), regresando posteriormente a la entidad para comprobar el estado de sus cuentas, siendo en dicho momento que se le indicó que e habían dado de alta tres tarjetas (TARJETA AHORA BBVA acabada en [redacted], AQUE CREDITO MAS acabada en [redacted] y TARJETA AQUA DEBIDO acabada en [redacted] haciendo un total de 18 movimiento, aconsejándole la entidad que reseteara el móvil, motivando que, como se ha señalado, ampliase la denuncia que previamente había interpuesto ante la policía.

Por tanto, es un hecho acreditado que la diligencia de la demandante ha quedado más que acreditada, pues las dos

denuncias junto con los extractos aportados de las cuatro tarjetas son inmediatas a conocer los hechos, cumpliendo con ello con la obligación que, según el artículo 41 del Real Decreto-ley 19/2018, incumbe a la misma como cliente de la entidad financiera, habiéndolo hecho con total celeridad.

No se acredita por la entidad demandada, que es a quien incumbe su prueba, cómo los defraudadores obtuvieron el número de tarjeta y el CVV de la misma por mucho que la demandante pinchase en el enlace que se le remitió en nombre de la entidad financiera ya que, por máxima de la experiencia, sólo puede obtenerse la misma o por un clonado de la tarjeta o por acceso de la aplicación con los datos que la demandante facilitó o por haberlo facilitado ella personalmente. Ninguna de las tres se acredita ya que, de ser la segunda de ellas como pretende la demandada, habrá que valorar a continuación qué grado de diligencia puso o no la demandante en facilitar los datos al pinchar en el enlace, ya que ello conllevó también al parecer la contratación de tres tarjetas nuevas de crédito en su nombre que facilitó la entidad, siendo algo inusual dicho hecho, algo que la propia entidad debería haber observado, teniendo en cuenta las horas en las que se llevó a cabo la contratación y que la cliente ya era titular de una tarjeta de crédito.

En específico, hecho reconocido por la propia demandada, se realizaron las siguientes operaciones.

.- Cinco operaciones con la tarjeta nº [redacted] por un importe total de 1.610,00 euros.

.- Cuatro operaciones con la tarjeta nº [redacted], tarjeta nueva dada de alta por un importe total de 955,00 euros.

.- Cinco operaciones con la tarjeta nº [redacted], tarjeta nueva dada de alta por un importe total de 1.175,00 euros.

.- Cuatro operaciones con la tarjeta nº [redacted], tarjeta nueva dada de alta, por un importe total de 950 euros.

Por la parte demandada se señala, amparándose para ello en su informe pericial, que los pagos fraudulentos fueron confirmados por el sistema OTP-SMS, consistiendo dicho sistema en que se envía un sms al móvil que figura en los datos de la aplicación de banca online, conteniendo un código numérico que se ha de introducir para completar la operación. La demandante niega haber recibido ninguno de los 13 sms de confirmación de las tarjetas nuevas, cuya

existencia incluso desconocía hasta que por la entidad financiera se le dijo que habían sido contratadas dicha madrugada cuando pidió un extracto bancario, así como de los otros cinco de la única tarjeta que tenía, el enlace primero al que pinchó y que derivó en toda la operativa posterior.

Del informe pericial aportado por la demandada, no figura en ningún momento a qué terminal se enviaron dichos OPT-SMS pese a que el perito en su declaración afirmó que sí se enviaron, pero también hay que decir que la declaración de dicho perito, desde el momento en que reconoció que era empleado de la entidad demandada, no puede tenerse en cuenta como prueba plena, ya que concurre en el mismo, causa de tacha.

La parte demandada manifiesta que no ha incumplido ninguna de sus obligaciones legales ni contractuales, y que la operación fraudulenta objeto del presente procedimiento lo ha sido como consecuencia de la actuación negligente de la Sra. [redacted] que accedió a un enlace y reveló los datos de acceso a su banca electrónica de BBVA, puesto que las operaciones en cuestión fueron llevadas a cabo a través de comercio electrónico seguro, siendo necesario para la emisión de las mismas introducir los datos de la tarjeta correspondiente (16 dígitos, fecha de caducidad y CVV) y la autentificación mediante segundo factor de seguridad, en este caso a través de un código OTP enviado por SMS al teléfono móvil de la demandante, tal y como se ha indicado anteriormente, por lo que fue necesario acceder a la banca online de la actora con su usuario y contraseña, revelar los códigos OPT remitidos para autorizar la contratación de dos tarjetas a través de la banca online, revelar los códigos OTP remitidos para revelar el detalle de cada una de las cuatro tarjetas y revelar los 18 códigos OTP remitidos para autorizar cada una de las operaciones realizadas, por lo que incurrió en una actuación de negligencia grave, si bien dicho extremo, no ha sido acreditado de modo alguno pro la entidad demandada que es a quien incumbe la carga de la prueba en dicho sentido, no pudiéndose escudar dicha entidad que ha realizado diversas campañas de concienciación de todos sus clientes para evitar que sean víctimas de ciberataques, puesto que no consta qué actuaciones en concreto se llevaron a cabo con la demandante en dicho sentido.

Al respecto hay que decir que el hecho de que se hagan anuncios de cybersegridad en artículos publicados, noticias, videos de youtube o en sedes sociales, o el enlace a "consejos de seguridad", no significa que la información

necesaria para evitar un fraude estuviera al alcance de la demandante.

Cuestión distinta es si a cada vez que accediera a la web a la app de banca online la Sra. [redacted] le apareciese una ventana emergente avisando de que no facilite sus datos personales, lo que no se ha acreditado por la demandada.

Cuesta creer que por la entidad demandada se cumpliese con todos los requisitos legales cuando se permiten hasta 18 operaciones consecutivas con todos los signos de ser fraudulentas, máxime cuando gran parte de las mismas se corresponden con unas tarjetas de crédito de las que ni siquiera era titular la demandante, que se contrataron a unas horas intempestivas y sin fundamento alguno, puesto que eran para adquirir productos para cuyo pago no era necesario la contratación de otra tarjeta, y que se achaque una falta de diligencia en la demandante a la que se dice autorizó los 18 cargos que se llevaron a cabo de madrugada, cuando NUNCA HABÍA PROCEDIDO DE ESE MODO, siendo que inmediatamente a percatarse del posible fraude habido con la única tarjeta de la que era consciente se puso en contacto inmediatamente con la entidad, tal y como se acredita de la documental aportada, tanto por teléfono como por correo electrónico, tal y como se acreditó de la más documental acompañada en la vista del juicio por la parte demandante, correo electrónico enviado por el servicio de la entidad BBVA a las 01:08 horas del 1 de septiembre de 2022 donde se indica a la demandante que le adjuntan "documentación previa a la firma" lo que evidencia un grave error en los sistemas de seguridad del banco, ya que la entidad permitió que una persona siguiese operando con las cuentas de la demandante a pesar de que minutos antes la misma había advertido a la entidad lo sucedido y la propia entidad había enviado un correo de bloqueo.

Como bien señala la parte demandante, la entidad demandada no ha acreditado, pese al requerimiento que se le efectuó al respecto, incumbiendo a dicha parte la prueba, desde qué dispositivo de confianza de la actora se llevaron a cabo las operaciones fraudulentas, únicamente el número de teléfono de la misma que les constaba, siendo la propia actora la que identificó el mismo como teléfono móvil Android marca y modelo SAMSUNG GALAXY S6, si bien no consta de prueba alguna que fuese desde el mismo que se autorizasen las operaciones ya que el de la actora es un SM/G908F y las conexiones se hacen desde SM-G960F, acreditándose de la documentación acompañada por la demandada que en el transcurso de las operaciones fraudulentas, se utilizaron

dispositivos distintos al de la demandante, pues se utilizó un nuevo dispositivo WINDOWS 10 y desde una IP distinta a la habitualmente utilizada de conexión por la misma, constando igualmente acreditado que la activación de las tarjetas se llevó a acabo desde una IP y dispositivo diferentes a los habituales de la Sra [redacted], no advirtiendo dicho hecho la entidad a la cliente, lo que implica una negligencia grave de la demandada, no así de la demandante.

TERCERO.- Por tanto, no puede entenderse, tal y como pretende la mercantil demandada que fuese la conducta culposa de la actora la que permitió el pago, al facilitar el acceso a sus datos, pues como ha indicado la jurisprudencia, la legislación aplicable establece en estos supuestos una responsabilidad cuasi objetiva para la entidad bancaria, de la que sólo puede eximirse si acredita la concurrencia de actuación fraudulenta o culpa grave del cliente (en este sentido SSAAPP de Badajoz de 7 de febrero de 2013, de Alicante de 12 de marzo de 2018, de Madrid de 13 de enero de 2023 o de la Rioja de 17 de febrero de 2023, entre otras). Dicha interpretación se desprende de lo establecido en el Real Decreto-ley 19/2018, de 23 de noviembre de servicios de pago y otras medidas urgentes en materia financiera, el cual indica en su artículo 36.1 que las operaciones de pago se considerarán autorizadas "*cuando el ordenante haya dado el consentimiento para su ejecución*". También indica este precepto que, a falta de ese consentimiento "*la operación de pago se considerará no autorizada*".

Además, el artículo 44 anteriormente indicado, establece una presunción de falta de autorización cuando es negada por el usuario. A mayor abundamiento, ha de valorarse que en el presente caso no resulta controvertido que el actor no autorizó los referidos cargos, pues la mercantil demandada no cuestiona en su contestación que el demandante fuese víctima de una maquinación fraudulenta a través del engaño propio del phising, sino que lo achaca a su propia negligencia, cuando si algo ha quedado acreditado de su interrogatorio en el plenario, es que la demandante actuó con toda la diligencia que se le puede exigir a una persona (diligencia de un buen padre de familia) a quien contactan a través de un enlace habitual y con toda la apariencia de provenir de la propia entidad BBVA, y que en cuanto se percató de que algo no iba bien con su terminal lo pone en conocimiento inmediatamente, dadas además las horas en que suceden los hechos, de la propia entidad, tanto telefónicamente como por correo, que en cuanto se abre la oficina acude a la misma para ver qué ha pasado, que en

cuanto se percata en un primer momento de la única tarjeta de la que tiene conocimiento, que se ha usado fraudulentamente y con los documentos que se le facilitan en la entidad financiera, acude a la Policía Mossos d´Esquadra para interponer la denuncia, la cual amplió posteriormente al cerciorarse tras acudir de nuevo a la entidad de los movimientos realmente habidos en su cuenta, enterándose en dicho momento de la contratación de otras tres tarjetas de crédito, limitándose tras ello a seguir los pasos que se le indicaban para recuperar el dinero que se le había sustraído.

Por otro lado, de los artículos 45 y 46 de la ley, se desprende que, en el caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago deberá devolver al cliente el importe de la misma, salvo que este último haya actuado de manera fraudulenta o con negligencia grave. Si concurriera este último supuesto, el cliente "*soportará todas las pérdidas derivadas de operaciones de pago no autorizadas*". Además, en virtud del artículo 44.3 del mismo texto legal, en referencia a la carga de la prueba, en estos casos corresponde a la entidad bancaria "*probar que el usuario del servicio de pago cometió fraude o negligencia grave*", lo que no ha hecho en el presente, tal y como se ha expuesto en el Fundamento anterior.

Desde esta perspectiva, debemos valorar que la mercantil demandada no ha probado en modo alguno que la actora haya actuado de manera fraudulenta o con negligencia grave, limitándose a manifestar que el demandante no fue diligente en su actuar al introducir la contraseña que por sms le llegó aceptando con ello la operación al dar a los autores del engaño delictivo los datos. Sin embargo, no podemos olvidar que, para trasladar al cliente los efectos del riesgo de estos cargos fraudulentos, que no se ha acreditado fueran autorizados los 18 por introducir los SMS la Sra. [redacted], no exigiendo la ley la concurrencia de una culpa leve o de tipo medio, sino que por el contrario, nuestra legislación indica que la negligencia debe ser grave. Y, en este caso, no puede calificarse, tal y como se ha expuesto anteriormente, como grave la falta de diligencia de la actora.

En estos supuestos de phishing, ha de valorarse que nos encontramos ante conductas delictivas muy elaboradas, a menudo perpetradas por profesionales del engaño que simulan con precisión los formatos auténticos de las entidades bancarias e inducen a error con cierta facilidad. Las dificultades para la detección del fraude por parte de los

usuarios se evidencian ante la multitud de procedimientos penales que se tramitan en nuestros órganos judiciales por estafas de este tipo. Por ello, ha de valorarse que el legislador no ha querido trasladar a los usuarios la carga de atribuirles la responsabilidad por estas operaciones no autorizadas y de exigirles que procedan con un cuidado extremo ante su carencia de medios para detectar estos fraudes.

En cambio, son las entidades bancarias las que se benefician por la introducción de las mejoras tecnológicas y las que deben contar con instrumentos adecuados para la detección de las actuaciones fraudulentas. En consecuencia, la ley ha optado por un sistema de responsabilidad cuasi objetiva, que atribuye a las entidades bancarias el deber de restitución ante operaciones no aceptadas, con la excepción de conductas de los usuarios que sean maliciosas o gravemente negligentes. Dichas razones nos deben llevar a valorar que la conducta del actor no puede suponer una negligencia grave, tal y como señaló en un caso similar la SAP de Madrid de 13 de enero de 2023 que dijo: "*no podemos calificar la posible negligencia de la demandante en la conservación de sus claves como "grave" en ningún caso. Estamos ante un tipo de fraude muy específico del que es fácil ser víctima, sin que ello implique una actuación negligente del cliente, dado lo bien articulada en su ejecución que está esta modalidad de fraude*".

Además, cabe añadir que no ha quedado acreditado que la entidad bancaria haya actuado con una diligencia adecuada a las circunstancias del caso. En este sentido, no se ha alegado ni mucho menos probado, que la mercantil demandada hubiera proporcionado a la actora de forma personalizada los mecanismos anti-phishing de supervisión suficientes, de carácter reforzado, para detectar y evitar este tipo de fraude, sin que puedan resultar suficientes los avisos de carácter genérico de la web del banco. Este Juzgador comparte las reflexiones de la SAP de la Rioja de 17 de febrero de 2023 al señalar que: "*El banco debe actuar con la diligencia exigible, que no es sólo la reglamentariamente prevista, sino la adecuada a las circunstancias de personas, lugar y tiempo. Entre estas, cobran especial relevancia datos tales como el perfil del cliente, los movimientos inusuales, los importes dispuestos, la hora en que se hace la operación… Y no basta con medidas genéricas de protección o avisos estereotipados de cuidado, pues tales avisos ostentarían la calificación de "fórmulas predispuestas" vacías de contenido. No son los clientes los que deben prevenir ni averiguar las modalidades de riesgos que el*

sistema conlleva o estar al tanto de los mismos, ni prevenir con su asesoramiento experto dichos riesgos". Este deber especial de diligencia que cabe atribuir a la entidad bancaria, habría de llevarle también a diseñar sistemas de control ante movimientos inusuales o ante cargos que se salgan de lo habitual.

En el presente caso, en el contexto del engaño fraudulento, se produjo una modificación del límite máximo de seguridad diario establecido en el contrato de tarjeta de crédito, sin que la entidad bancaria efectuara las comprobaciones que confirmaran que era su cliente el que había llevado a cabo esa variación contractual tan relevante que en el presente supuso retirar en el límite de la noche del 31 de agosto de 2022 y madrugada del 1 de septiembre de 2022 nada menos que 4.690,00 euros en 18 cargos sucesivos entre cuatro tarjetas diferentes de las que resultaba una misma titular que únicamente tenía inicialmente contratada una, algo que, teniendo en cuenta el cliente y la dinámica habitual del mismo, debería haber llamado la atención de la demandada. Precisamente dicha circunstancia es la que lleva al Banco de España a emitir en más de una ocasión informe que indica que la entidad financiera se ha apartado de los buenos usos y prácticas financieras, al no haber restituido a su cliente la cuantía de la operación no autorizada.

En consecuencia, al quedar acreditados los hechos alegados por la demandante y no quedar probada la concurrencia de negligencia grave en la conducta del actor, debe ser estimada íntegramente la demanda.

CUARTO.- De conformidad con lo dispuesto en los artículos 1.108 y siguientes del Código Civil, las cantidades objeto de reclamación devengarán el interés legal del dinero desde la fecha de interpelación judicial incrementados en dos puntos desde sentencia, ex artículo 576 de la LEC hasta el completo abono de la suma objeto de condena.

QUINTO.- Respecto a las costas procesales causadas en el presente procedimiento, teniendo en cuenta el principio del vencimiento objetivo que rige nuestro sistema procesal y lo dispuesto en el artículo 394 de la Ley de Enjuiciamiento Civil, al estimarse íntegramente la demanda, las costas de este procedimiento deben imponerse a la entidad demandada.

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

F A L L O

Que, **estimando íntegramente** la demanda formulada por la Procuradora de los Tribunales Dª Consol Cuadra Baile, en nombre y representación de **Dª.** [redacted] contra la entidad financiera **BANCO BILBAO VIZCAYA ARGENTARIA, S.A. (BBVA, S.A.)**, DEBO:

1.- DECLARAR Y DECLARO la responsabilidad de la mercantil demandada en la incorrecta ejecución de las dieciocho operaciones objeto de este procedimiento que fueron realizadas contra la cuenta de la actora.

2.**- DECLARAR Y DECLARO que se han producido daños y perjuicios a la demandante** por importe total de 4.690,00 euros como resultado de dichas operaciones.

3.**- CONDENAR Y CONDENO a la mercantil demandada a abonar a la actora la cantidad de CUATRO MIL SEISCIENTOS NOVENTA EUROS (4.690,00 euros**) en concepto de daños y perjuicios más los intereses legales desde la interpelación judicial incrementados en dos puntos desde sentencia.

Todo ello, con imposición de las costas causadas en el presente procedimiento a la parte demandada.

Líbrese testimonio de la presente resolución para su unión a los autos principales, y llévese el original al libro de Sentencias de este Juzgado.

Notifíquese la presente resolución a las partes, haciéndoles saber que la misma no es firme, y que contra ella cabe interponer Recurso de Apelación para su resolución por la Ilma. Audiencia Provincial de Barcelona.

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

PUBLICACIÓN.- Leída y publicada ha sido la anterior sentencia por el mismo Magistrado Juez que la dictó, hallándose en audiencia pública en el mismo día de su fecha, doy fe.