ADMINISTRACION DE JUSTICIA

TRIBUNAL DE INSTANCIA
SECCION CIVIL
PLAZA Nº 4
MURCIA

SENTENCIA: 00267 / 2026

AVDA. JUSTICIA S/N. CIUDAD DE LA JUSTICIA. FASE II. 1ª PLANTA
Teléfono: 968272359
Correo electrónico: [redacted]

SERVICIO COMÚN TRAMITACION CIVIL, FAMILIA, INFANCIA Y CAPACIDAD - MURCIA

Equipo/usuario: SGM
Modelo: N04390 SENTENCIA DE TEXTO LIBRE ART 447 LEC

N.I.G: 30030 42 1 2025 0006650
ORD PROCEDIMIENTO ORDINARIO 0000350 / 2025
Procedimiento de origen: /
Sobre: OTRAS MATERIAS

DEMANDANTE, DEMANDANTE: [redacted]
Procurador/a: [redacted]
Abogado/a: CARLOS ARNAU MARTINEZ, CARLOS ARNAU MARTINEZ

DEMANDADO: ABANCA CORPORACION BANCARIA SA
Procurador/a: [redacted]
Abogado/a: [redacted]

PROCEDIMIENTO: Juicio Declarativo Ordinario 350/2025

SENTENCIA

En Murcia, a catorce de septiembre del año dos mil veintiséis.

Vistos por su S.Sª, **Dª** [redacted], **Magistrada número 4 en la Sección Civil del Tribunal de Instancia de Murcia (antiguo JPI-4)**, los precedentes autos de **Juicio Declarativo Ordinario nº 350/25** seguidos en este Juzgado a instancias de **Dª** [redacted] **y Dª.** [redacted] representadas por la procuradora **Dª.** [redacted] y defendidas por el letrado **D. CARLOS ARNAU MARTÍNEZ** contra **la entidad ABANCA CORPORACIÓN BANCARIA, S.A. (en adelante, "ABANCA")** representada por el procurador [redacted] y defendida por la letrada [redacted], que versa sobre reclamación de cantidad; y

ANTECEDENTES DE HECHO

PRIMERO: Por la procuradora Dª. [redacted] en nombre y representación de Dª. [redacted] y Dª.

ADMINISTRACION DE JUSTICIA

[redacted] se presentó demanda de juicio ordinario contra Abanca Corporación Bancaria, SA que fue turnada a este Juzgado, en la cual solicitaba previa alegación de los hechos y fundamentos de derecho, que se dictara sentencia por la que estimando la demanda se condene a la demandada a abonar a mis representadas el importe de VEINTICUATRO MIL EUROS (24.000 €), más intereses legales y costas.

SEGUNDO: Admitida a trámite la demanda, se acordó emplazar a la parte demandada para que en el plazo de veinte días contestase la demanda formulada en su contra con los apercibimientos legales correspondientes.

TERCERO: Emplazado en legal forma la parte demandada, por el procurador [redacted] en nombre y representación de Abanca Corporación Bancaria, SA se presentó escrito oponiéndose a la demanda interpuesta y solicitando que se desestimase la demanda, con expresa imposición de costas a la parte actora.

CUARTO: Se tuvo por contestada la demanda y se acordó citar a las partes para la celebración de la audiencia previa, siendo citadas las partes personadas en legal forma. El día señalado tuvo lugar la celebración de la citada audiencia previa, en la que las partes ratificaron sus respectivos escritos y dieron cumplimiento al resto de las previsiones legales y recibido el pleito a prueba, por la parte actora se propusieron las de: - documental por reproducida, y por la parte demandada se propuso: – documental por reproducida y - pericial, admitiéndose las mismas en los términos que constan en el soporte audiovisual, y convocando a las partes para la celebración del juicio.

QUINTO: El día señalado tuvo lugar la celebración del juicio correspondiente, en el que se practicaron las pruebas por el orden legal y tras la conclusión de las mismas, por la parte actora se informó sobre las conclusiones de hecho y de derecho correspondientes a este proceso, tras lo cual quedaron los autos vistos para sentencia.

SEXTO: En la tramitación de este procedimiento se han cumplido todas las formalidades legales.

FUNDAMENTOS DE DERECHO

PRIMERO: Planteamiento.

Ejercitan Dª. [redacted] y Dª. [redacted], en la presente litis, acción de responsabilidad por culpa contractual y extracontractual en base a lo establecido el artículo 41 y concordantes de Real Decreto-ley 19/2018 de 23 de noviembre, de servicios de pago y otras

ADMINISTRACION DE JUSTICIA

medidas urgentes en materia financiera contra la entidad Abanca Corporación Bancaria, SA solicitando se condene a la entidad crediticia demandada a que le reintegre la cantidad de 24.000 €.

Alega la representación procesal de la parte actora, con fundamento en su pretensión, que el día 03/10/2.024, sobre las 19:07 h aproximadamente la Sra. [redacted] recibió un SMS en su número de teléfono, aparentemente remitido por Abanca, en el que se le avisaba de un inicio de sesión desde un nuevo dispositivo y se le remitía a un enlace a una web con aspecto de Abanca y un número de incidencia ([redacted]), todo ello a través del chat habitual de comunicación entre actora y la Entidad, por ello no le generó duda alguna; poco después, a las 19:27 h., le enviaron otro SMS desde otro número identificado como de Abanca indicándole que se había abierto una incidencia y le habían asignado un gestor ([redacted]), quien la llamó seguidamente diciéndole que tenía que hacer una serie de gestiones, indicándole que al día siguiente la volverían a llamar, lo que consta en la segunda parte del SMS, siendo este el modo de operar de Abanca; ese mismo día a las 19:27 h. recibe la llamada de una agente con acento gallego y le indica que han detectado un acceso a su cuenta desde Badajoz, requiriéndole para hacer unas comprobaciones, entre ellas otra llamada para comprobar si su móvil tiene un virus, así como un mensaje que le informa de que se va a realizar una transferencia desde su cuenta; seguidamente recibe otro mensaje en el que le facilitan una clave para la banca electrónica de la Entidad, con la excusa de que es necesario para anular la transferencia (SMS del 3 de Octubre de las 19:45 h.), e inmediatamente recibe un SMS en el que se le comunica que la transferencia se ha anulado con éxito, esto es, recibe 3 SMS durante la llamada (19:45 h.; 20:02 h y 20:07), a consecuencia de lo cual la Sra. [redacted] enumera a la agente que le llama los cargos que hay en su cuenta así como las claves ([redacted]) para anular la transferencia de 24.000 € y le envían un SMS indicando que ha sido "anulada con éxito" (20:07 h); asimismo refiere que el cargo de 24.000 € se realizó en la cuenta [redacted] siendo Dª. [redacted] titular de la misma y Dª [redacted] autorizada; de igual modo expresa que el día 4 de octubre interpuso la correspondiente denuncia ante la Policía Nacional, en El Carmen y, asimismo, puso en conocimiento de la Entidad estos hechos, tan pronto tuvo conocimiento de lo sucedido; al hilo de lo expuesto resalta que con esta conducta la entidad demandada contravino las obligaciones que pesan sobre ella, reguladas en el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

En base a los razonamientos expuestos, interesa que se condene a la entidad financiera demandada a que abone los daños y perjuicios causados al Sras. [redacted] y [redacted] que ascienden a 24.000 € más los intereses legales y costas del procedimiento.

ADMINISTRACION DE JUSTICIA

Frente a dicha pretensión se alza la representación procesal de la entidad financiera alegando, en esencia, que el relato de hechos de la demanda evidencia que la demandante realizó una conducta imprudente facilitando las claves de confirmación que permitieron que se ejecutaran las operaciones litigiosas, por lo que, en el presente caso, no resulta de aplicación lo prevenido en el artículo 46.1 del RDLSP; de igual modo apunta que para el caso de que las actoras hubieren sido víctimas de un fraude, no se le podría imputar a ABANCA responsabilidad alguna sino a su propia negligencia grave, habida cuenta que no tomaron las medidas razonables a fin de proteger sus claves de seguridad personalizadas; asimismo destaca que la causa del perjuicio que ahora se reclama deriva simplemente de que las actoras le facilitaran el código que ABANCA les envió por SMS y que era meridianamente claro: "Para realizar el envío de 24.000 EUR, introduce el [redacted] código [redacted] exclusivo para Banca ELECTRÓNICA de ABANCA. Si no eres tú [redacted]; al propio tiempo resalta que la Sra. [redacted] reúne conocimientos y experiencia elevada, por lo que debió observar mayor diligencia en su conducta, adiciona que las demandantes eran conocedoras de este tipo de riesgos ya que fueron destinatarias de numerosas compañas antifraude, por lo que debieron percatarse del fraude; en suma considera que las actoras incurrieron con su actuación en una clara negligencia grave, siendo este el sentir de numerosas audiencias provinciales, en supuestos idénticos al que nos ocupa.

De igual modo indica que la operación litigiosa se realizó cumpliendo Abanca con todos los controles exigidos por el RDLSP, lo que la exime de responsabilidad; asimismo subraya que no hubo ninguna brecha se seguridad en los sistemas de la entidad, habida cuenta que el fraude responde a que las demandantes le facilitaron verbalmente al tercero desconocido el código OTP destinado a la confirmación de la transferencia; al propio tiempo refiere que Abanca ni podía ni tenía obligación legal de bloquear la banca electrónica ni las operaciones autorizadas por el cliente, precisando que en el contrato marco la Entidad demandada no se reservó la facultad de paralizar operaciones inusuales (art. 40.2 del RDLSP); finalmente resalta que a pesar de que las transferencias no pueden ser revocadas lo que sí pueden hacer las entidades bancarias es, una vez se pone en su conocimiento la existencia de un posible fraude, solicitar a la entidad beneficia de los fondos su devolución, dependiendo dicha devolución del receptor y de su entidad bancaria, adiciona que en este caso, Abanca inició los trámites y consiguió que la entidad beneficiaria de los fondos, [redacted] en España, bloqueara la cantidad transferida a tiempo, si bien, solicitó la firma de una carta de garantías por parte de la Sra. [redacted] para proceder a su devolución, habiéndose negado ésta a firmar la carta, por lo que la falta de recuperación es achacable únicamente a la Sra. [redacted].

ADMINISTRACION DE JUSTICIA

SEGUNDO: Doctrina jurisprudencial. Normativa aplicable

Como regla general, y sin perjuicio de la posibilidad de repetir contra el proveedor de servicios de iniciación de pagos, es el proveedor de servicios de pago el que responde de la restitución al ordenante del importe de las operaciones de pago no autorizadas.

Como excepción a esa regla general, se atribuye al ordenante esa responsabilidad cuando actúe de manera fraudulenta, o bien incumpla deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el art. 41, entre las que se incluyen la de tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas.

Correlativa a esa obligación es la norma sobre la carga de la prueba, establecida en el art. 44.3, según la cual es al proveedor de Servicios de pago a quien le incumbe probar que el usuario del Servicio de pago cometió fraude o negligencia grave, porque como ha señalado la jurisprudencia, la responsabilidad de aquél es una responsabilidad cuasi-objetiva.

En el caso de autos, la cuestión litigiosa se centra en determinar si la demandante, Sra. [redacted], usuaria del servicio de pago, cometió negligencia grave, toda vez que la existencia de fraude por su parte aparece totalmente descartada.

Al respecto la Entidad financiera demandada considera que la coactora Sra. [redacted] faltando a la diligencia que era exigible cedió todas sus credenciales de seguridad: clave de usuario, contraseña y códigos a su interlocutor telefónico para que se realizara la transferencia litigiosa y con ello permitió que se consumara el fraude o estafa del que fue víctima.

De cara a la resolución de la presente litis se estima oportuno traer a colación la reciente Sentencia del Tribunal Supremo de fecha 9 de abril de 2025 (**Roj:** STS 1671/2025 - **ECLI:**ES:TS:2025:1671) que en su Fundamento de Derecho Segundo 2.-, y por lo que se refiere a la normativa aplicable refiere que:

"La respuesta a la cuestión discutida exige recordar concretar la normativa aplicable. 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, que derogó la *Directiva 2007/64/CE, explica en su Considerando 7* el objetivo de la reforma:

«En los últimos años, han aumentado los riesgos de seguridad de los pagos electrónicos, debido a la mayor complejidad técnica de estos, el incesante incremento del volumen de pagos electrónicos en todo el mundo y los nuevos tipos de servicios de pago. Disponer de servicios de pago fiables y seguros es condición esencial para el buen funcionamiento del mercado de servicios de pago, por lo que los usuarios de esos servicios deben gozar de la debida protección frente a tales riesgos. Los servicios de pago son esenciales para el mantenimiento de actividades económicas y sociales de vital importancia.»

Y en los Considerandos 70, 71 y 72 se aborda el problema de las operaciones de pago no autorizadas o ejecutadas incorrectamente, precisando las respectivas obligaciones y responsabilidad del usuario y del proveedor de los servicios de pago y ofreciendo pautas para valorar la diligencia exigible:

«(70) Para reducir los riesgos y las consecuencias de operaciones de pago no autorizadas o que hayan sido ejecutadas incorrectamente, **el usuario de servicios de pago debe informar al proveedor de servicios de pago, lo antes posible, sobre toda reclamación en relación con operaciones de pago supuestamente no autorizadas o ejecutadas incorrectamente** , siempre y

cuando el proveedor de servicios de pago haya respetado sus obligaciones de información con arreglo a la presente Directiva. Si el usuario de servicios de pago respeta el plazo de notificación, debe poder hacer valer esas reclamaciones dentro de los plazos de prescripción nacionales. [...]

(71) En caso de una operación de pago no autorizada, el proveedor de servicios de pago deberá devolver inmediatamente el importe de dicha operación al ordenante. No obstante, cuando haya una sospecha fundada de que una operación no autorizada es el resultado de una conducta fraudulenta del usuario de servicios de pago y la sospecha se funde en motivos objetivos comunicados a la autoridad nacional pertinente, el proveedor de servicios de pago tendrá la posibilidad de efectuar, en un plazo razonable, una investigación antes de devolver el importe al ordenante. A fin de evitar perjuicios al ordenante, la fecha de valor del abono de la devolución no debe ser posterior a la fecha de adeudo del importe. A fin de ofrecer incentivos para que el usuario de servicios de pago comunique sin demora a su proveedor de servicios de pago toda pérdida o robo de un instrumento de pago y reducir así el riesgo de operaciones de pago no autorizadas, el usuario solo debe ser responsable por un importe muy limitado, salvo en caso de fraude o grave negligencia por su parte. A este respecto, parece adecuado fijar un importe de 50 EUR con vistas a garantizar una protección elevada y homogénea del usuario dentro de la Unión. **No se le debe imputar responsabilidad al ordenante, cuando este se encuentre en una posición que no le permite tener conocimiento del extravío, el robo o la sustracción del instrumento de pago** . Asimismo, **una vez que el usuario de servicios de pago haya comunicado al proveedor de servicios de pago que su instrumento de pago puede haber sido objeto de uso fraudulento, no deben exigírsele responsabilidades por las ulteriores pérdidas que pueda ocasionar el uso no autorizado del instrumento** . [...]

(72) A la hora de evaluar la posible negligencia o la negligencia grave del usuario de servicios de pago, deben tomarse en consideración todas las circunstancias. Las pruebas de una presunta negligencia, y el grado de esta, deben evaluarse con arreglo a la normativa nacional. No obstante, si el concepto de negligencia supone un incumplimiento del deber de diligencia, **la negligencia grave tiene que significar algo más que la mera negligencia, lo que entraña una conducta caracterizada por un grado significativo de falta de diligencia** . Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros. Se deben considerar nulas las cláusulas contractuales y las condiciones de prestación y utilización de instrumentos de pago mediante las cuales aumente la carga de la prueba sobre el consumidor o se reduzca la carga de la prueba sobre el emisor. Además, en situaciones específicas y, más concretamente, cuando el instrumento de pago no esté presente en el punto de venta, como en el caso de los pagos en línea, resulta oportuno que el proveedor de servicios aporte pruebas de la presunta negligencia, puesto que los medios a disposición del ordenante son limitados en esos casos.»

Con relación a las medidas de seguridad que deben adoptarse, los Considerandos 91 y 96 indican:

«(91) Los proveedores de servicios de pago son responsables de las medidasde seguridad. Dichas medidas deben ser proporcionales a los riesgos de seguridad existentes. Los proveedores de servicios de pago deben establecer un marco que permita paliar los riesgos y mantener procedimientos eficaces de gestión de incidentes. (96) [...] Es necesario que las credenciales de seguridad personalizadas se utilicen adecuadamente, para limitar los riesgos de captación de datos mediante suplantación de identidad (phising) y otras actividades fraudulentas. A tal fin, el usuario debe poder confiar en la adopción de medidas que protejan la confidencialidad y la integridad de sus credenciales personalizadas de seguridad. Entre estas medidas figuran, en particular, los sistemas de cifrado basados en dispositivos personales del ordenante (lectores de tarjetas o teléfonos móviles, por ejemplo) o facilitados al ordenante por su proveedor de servicios de pago gestor de cuentas por otros cauces (por SMS o mensaje de correo electrónico por ejemplo). Las medidas, incluidos los sistemas habituales de cifrado, que pueden dar lugar a códigos de autenticación como las contraseñas de un solo uso, pueden aumentar la seguridad de las operaciones de pago; la utilización de este tipo de códigos de autenticación por los usuarios de servicios de pago debe considerarse compatible con sus obligaciones respecto de los instrumentos de pago y las credenciales de seguridad personalizadas...»

Estas indicaciones se plasman en los *arts. 64* y *69 y ss. de la Directiva 2015/2366* . Así, el art. 64, titulado «Consentimiento y retirada del consentimiento», dispone:

«1. Los Estados miembros velarán por que las operaciones de pago se consideren autorizadas únicamente cuando el ordenante haya dado su consentimiento a que se ejecute la operación de pago. [...]

2. El consentimiento para la ejecución de una operación de pago o de una serie de operaciones de pago se dará en la forma acordada entre el ordenante y el proveedor de servicios de pago. El consentimiento para la ejecución de una operación de pago podrá darse también por conducto del beneficiario o del proveedor de servicios de iniciación de pagos.

En ausencia de consentimiento, la operación de pago se considerará no autorizada.

[...] 4. El ordenante y el proveedor o proveedores de servicios de pago correspondientes convendrán en el procedimiento de notificación del consentimiento.»

Los arts. 69 y 70 de la Directiva regulan las obligaciones del usuario y del proveedor de servicios de pago en relación con los instrumentos de pago. Así, el art. 69 ordena:

«1. 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;

b) en caso de extravío, robo 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.

2. En particular, a los efectos del apartado 1, letra a), el usuario de servicios de pago, en cuanto reciba un instrumento de pago, tomará todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas del instrumento de pago.»

Y, paralelamente, el art. 70.1 establece respecto del proveedor de servicios de pago las siguientes obligaciones:

«a) se asegurará de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar el instrumento, sin perjuicio de las obligaciones que incumben al usuario de servicios de pago con arreglo al artículo 69;

[...]

c) garantizará que en todo momento estén disponibles medios adecuados que permitan al usuario de servicios de pago efectuar una notificación en virtud del artículo 69, apartado 1, letra b), o solicitar un desbloqueo del instrumento de pago en virtud del artículo 68, apartado 4; el proveedor de servicios de pago facilitará al usuario de dichos servicios, cuando este así lo solicite, medios que le permitan demostrar que ha efectuado dicha notificación durante los dieciocho meses siguientes a la misma;

d) ofrecerá al usuario de servicios de pago la posibilidad de efectuar una notificación en virtud del artículo 69, apartado 1, letra 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 69, apartado 1, letra b).»

El art. 71.1 de la Directiva prevé la obligación del proveedor de servicios de pago de rectificar la operación si el usuario lo comunica sin demora injustificada:

«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 notifica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación, incluso las cubiertas por el artículo 89, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo.»

Y el art. 72 añade, en relación con la prueba de la autenticación y ejecución de las operaciones de pago, cuando el usuario niegue haberla autorizado o alegue que se ejecutó de manera incorrecta:

«1. Los Estados miembros exigirán que, cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que esta se ejecutó de manera incorrecta, corresponda 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. [...]

2. Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ejecutada, la utilización de un instrumento de pago registrada por el proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, no bastará necesariamente para demostrar que la operación de pago ha sido autorizada por el ordenante, ni que este ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 69. El proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, aportará pruebas para demostrar que el usuario del servicio de pago ha cometido fraude o negligencia grave.»

Por último, los arts. 73 y 74 de la Directiva ordenan el régimen de responsabilidad del proveedor y del usuario en caso de operaciones de pago no autorizadas. El art. 73.1 señala:

«1. Sin perjuicio del artículo 71, los Estados miembros velarán por que, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devuelva a este 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 a la autoridad nacional

pertinente. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada...»

Y el art. 74.1 contempla la posibilidad de que, en determinados casos, el ordenante pueda quedar obligado a soportar las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado o robado, hasta un máximo de 50 €.

3.- El *Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017* , por el que se complementa la *Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo* en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros, avanza un paso más en esta línea y, además de desarrollar el contenido y las exigencias en materia de autenticación reforzada, impone en su art. 2 a los proveedores de servicios de pago el deber de incorporar mecanismos de supervisión que les permitan detectar operaciones de pago no autorizadas o fraudulentas a efectos de la adopción de terminadas medidas de seguridad:

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

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

2. Los proveedores de servicios de pago garantizarán que los mecanismos de supervisión de las operaciones tengan en cuenta, como mínimo, todos los factores basados en el riesgo siguientes: a) listas de elementos de autenticación comprometidos o sustraídos; b) el importe de cada operación de pago; c) supuestos de fraude conocidos en la prestación de servicios de pago; d) señales de infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación; e) 1. en caso de que el dispositivo o el programa informático de acceso sea facilitado por el proveedor de servicios de pago, un registro de la utilización del dispositivo o el programa informático de acceso facilitado al usuario de los servicios de pago y de su uso anormal.»

4.- La mencionada *Directiva 2015/2366* ha sido traspuesta al ordenamiento jurídico interno por el *Real Decreto Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, cuyos arts. 36* y *41* a *46* reproducen casi miméticamente los preceptos que se acaban de transcribir. Así, el art. 36.1 proclama:

«1. Las operaciones de pago se considerarán autorizadas cuando el ordenante haya dado el consentimiento para su ejecución. A falta de tal consentimiento la operación de pago se considerará no autorizada. El consentimiento para la ejecución de una operación de pago podrá darse también por conducto del beneficiario o del proveedor de servicios de iniciación de pagos.

El ordenante y su proveedor de servicios de pago acordarán la forma en que se dará el consentimiento, así como el procedimiento de notificación del mismo.»

El art. 41 recoge las obligaciones del usuario en relación con los instrumentos de pago y las credenciales de seguridad personalizadas, indicando que:

«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.»

Y el art. 42.1 del Real Decreto Ley reitera el contenido del art. 71.1 de la Directiva, con el matiz de insistir en el carácter gratuito de los medios que permitan al usuario efectuar la notificación a que hace referencia el art. 41.b).

Lo mismo sucede con los arts. 43 y 44, en relación con los arts. 71 y 72 de la Directiva. En particular, el art. 44 atribuye al proveedor de los servicios de pago la carga de la prueba de 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, así como que el usuario del servicio de pago cometió fraude o negligencia grave:

«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. [...]

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

ADMINISTRACION DE JUSTICIA

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. [...]»

Igualmente, los arts. 45 y 46 del Real Decreto Ley recogen lo dispuesto en los arts. 73 y 74 de la Directiva acerca de la responsabilidad del proveedor de servicios de pago y del usuario en caso de operaciones de pago no autorizadas. En este sentido, el art. 45.1 establece:

«1. Sin perjuicio del artículo 43 de este real decreto-ley, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada.»

Y el art. 46, después de recoger en su apartado 1 la posibilidad de que el ordenante pueda quedar obligado a soportar, hasta un máximo de 50 €, las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado, sustraído o apropiado indebidamente por un tercero, vincula la responsabilidad del ordenante a la existencia de fraude o por incumplimiento deliberado o por negligencia grave de las obligaciones que pesan sobre el mismo:

«1. No obstante lo dispuesto en el artículo 45, el ordenante podrá quedar obligado a soportar, hasta un máximo de 50 euros, las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado, sustraído o apropiado indebidamente por un tercero, salvo que:

a) al ordenante no le resultara posible detectar la pérdida, la sustracción o la apropiación indebida de un instrumento de pago antes de un pago, salvo cuando el propio ordenante haya actuado fraudulentamente, o

b) la pérdida se debiera a la acción o inacción de empleados o de cualquier agente, sucursal o entidad de un proveedor de servicios de pago al que se hayan externalizado actividades.

El ordenante soportará todas las pérdidas derivadas de operaciones de pago no autorizadas si el ordenante ha incurrido en tales pérdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 41. En esos casos, no será de aplicación el importe máximo contemplado en el párrafo primero.

En todo caso, el ordenante quedará exento de toda responsabilidad en caso de sustracción, extravío o apropiación indebida de un instrumento de pago cuando las operaciones se hayan efectuado de forma no presencial utilizando únicamente los datos de pago impresos en el propio instrumento, siempre que no se haya producido fraude o negligencia grave por su parte en el cumplimiento de sus obligaciones de custodia del instrumento de pago y las credenciales de seguridad y haya notificado dicha circunstancia sin demora.

2. Si el proveedor de servicios de pago del ordenante no exige autenticación reforzada de cliente, el ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta. En el supuesto de que el beneficiario o el proveedor de servicios de pago del beneficiario no acepten la autenticación reforzada del cliente, deberán reembolsar el importe del perjuicio financiero causado al proveedor de servicios de pago del ordenante.

3. Salvo en caso de actuación fraudulenta, el ordenante no soportará consecuencia económica alguna por la utilización, con posterioridad a la notificación a que se refiere el artículo 41.b), de un instrumento de pago extraviado o sustraído.

4. Si el proveedor de servicios de pago no tiene disponibles medios adecuados para que pueda notificarse en todo momento el extravío o la sustracción de un instrumento de pago, según lo dispuesto en el artículo 42.1.c), el ordenante no será responsable de las consecuencias económicas que se deriven de la utilización de dicho instrumento de pago, salvo en caso de que haya actuado de manera fraudulenta.»

5.- Al margen de la normativa expuesta, la *sentencia del Tribunal de Justicia de 2 de septiembre de 2021 (C-337/20*), con ocasión de examinar el alcance del *art. 58 de la anterior Directiva 2007/64* , aporta siquiera sea de modo indirecto unas pautas orientativas sobre la diligencia exigible al usuario de los servicios de pago.

En este sentido, en las conclusiones del abogado general Sr. Henrik Saugmandsgaard, presentadas el 8 de julio de 2021 y asumidas por el Tribunal de Justicia, se dice:

«38. Por lo que respecta, en primer lugar, al tenor de los *artículos 58* y *60 de la Directiva 2007/64* , cabe señalar que el artículo 58 introduce una obligación general de notificación de cualquier operación no autorizada o ejecutada incorrectamente, de modo que el usuario del servicio solo obtendrá la rectificación de una operación no autorizada o ejecutada incorrectamente si notifica dicha operación a su proveedor de servicios, notificación que deberá efectuarse a más tardar en los trece meses de la fecha del adeudo correspondiente.

39. El artículo 60 de dicha Directiva se refiere específicamente a la responsabilidad del proveedor de servicios de pago en caso de operaciones no autorizadas. Su apartado 1 establece que, sin perjuicio del artículo 58, los Estados miembros velarán por que el proveedor de servicios devuelva de inmediato al ordenante el importe de la operación no autorizada.

40. La expresión «sin perjuicio del *artículo 58» que figura en el artículo 60 de la Directiva 2007/64* significa que lo dispuesto en este artículo no se establece en detrimento del artículo 58 de dicha Directiva. De ello se desprende, en mi opinión, que la responsabilidad del proveedor en caso de operaciones no autorizadas está supeditada a que el usuario del servicio respete el procedimiento de notificación previsto en el artículo 58 de dicha Directiva, cuyo plazo no puede exceder de los trece meses siguientes a la fecha del adeudo.

41. El considerando 31 de la *Directiva 2007/64* pone de manifiesto que se trata efectivamente de una condición al establecer que *si* el usuario del servicio de pago respeta el plazo de la notificación, debe tener la posibilidad de presentar su reclamación relativa al carácter no autorizado del pago.

[...]

51. A continuación, tanto en el caso de operaciones no autorizadas como de operaciones ejecutadas de manera incorrecta, el *artículo 59 de la Directiva 2007/64* , relativo a la carga de la prueba, establece que corresponde al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada.

52. Debo subrayar que este artículo 59 efectúa una inversión de la carga de la prueba, haciendo que esta no recaiga sobre quien alega la existencia de una operación no autorizada, a saber, el usuario del servicio de pago, sino sobre el proveedor de servicios de pago. De ello se desprende que, durante un período de trece meses, este último está sujeto a una obligación de devolución casi automática e inmediata de la operación que el usuario no ha autorizado.

53. De este modo, **el legislador de la Unión ha establecido un régimen de responsabilidad basado en tres elementos esenciales y vinculados entre sí** , a saber: una obligación de notificación que recae sobre el usuario del servicio de pago, establecida en el *artículo 58 de la Directiva 2007/64* ; la atribución de la carga de la prueba al proveedor de esos servicios, que figura en el artículo 59 de dicha Directiva, y, por último, en caso de falta de prueba, la responsabilidad de ese proveedor, de conformidad con los artículos 60 y 75 de dicha Directiva, en función de que la operación no haya sido autorizada, no haya sido ejecutada o haya sido ejecutada incorrectamente.

[...]

86. De este modo, existe un equilibrio entre, en primer lugar, la obligación de información que recae sobre el proveedor de servicios de pago, en segundo lugar, el deber de diligencia que incumbe al usuario del servicio de pago asociado a una obligación de notificación dentro de un plazo concreto y, en tercer lugar, la responsabilidad estricta del proveedor, sin que el usuario tenga que demostrar una falta o negligencia.»

La posterior *sentencia del Tribunal de Justicia de 2 de septiembre de 2021 (C-337/20*), tras indicar que, para interpretar una disposición del Derecho de la Unión, no solo debe tenerse en cuenta su tenor literal, sino también el contexto en el que se inscribe y los objetivos perseguidos por la normativa de la que forma parte, declara:

«32 En primer lugar, por lo que respecta, por una parte, al texto del *apartado 1 del artículo 60 de la Directiva 2007/64* , titulado «Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas», conviene indicar que este artículo dispone que, sin perjuicio del *artículo 58 de la citada Directiva, los Estados* miembros velarán por que, en el caso de una operación de pago no autorizada, el proveedor de servicios de pago devuelva de inmediato al ordenante el importe de tal operación y, en su caso, por que restablezca en la cuenta de pago en la cual se haya adeudado el importe el estado que habría existido de no haberse efectuado la operación de pago no autorizada.

[...]

39 En el sistema de este régimen de responsabilidad, la obligación de notificación por el usuario de servicios de pago de cualquier operación no autorizada es condición para que dicho régimen pueda aplicarse en favor del usuario, denominado también ordenante en determinadas disposiciones de la *Directiva 2007/64* .

40 A continuación, el artículo 59 de esta Directiva incluye en el régimen de responsabilidad por operaciones no autorizadas un mecanismo de carga de la prueba favorable al usuario de servicios de pago. En esencia, la carga de la prueba recae sobre el proveedor de servicios de pago,

que debe probar que la operación de pago fue autenticada, registrada con exactitud y contabilizada. En la práctica, el régimen de prueba establecido en dicho artículo 59 lleva, desde el momento en que la notificación prevista en el artículo 58 de la citada Directiva se ha efectuado dentro del plazo previsto en él, a someter al proveedor de servicios de pago a una obligación de devolución inmediata, de conformidad con el artículo 60, apartado 1, de dicha Directiva. [...]

63 Así, como ha señalado, en esencia, el Abogado General en el *punto 86 de sus conclusiones, el régimen de responsabilidad previsto en el artículo 60, apartado 1, de la Directiva 2007/64* se basa en un equilibrio entre la obligación de información que recae sobre el proveedor de servicios de pago y la obligación de notificación de cualquier operación no autorizada dentro de un plazo de trece meses que incumbe al usuario de servicios de pago, que permite fundamentar la responsabilidad estricta del proveedor, sin que el usuario tenga que demostrar una falta o negligencia.»

6.- Con arreglo a la normativa comunitaria y nacional aplicable y a la jurisprudencia comunitaria recaída en interpretación de la regulación de la que trae causa la primera, podemos concluir:

1.º El usuario de servicios de pago debe adoptar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas y, en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, ha de notificarlo al proveedor de servicios de pago de manera inmediata, tan pronto tenga conocimiento de ello.

2.º En caso de que se produzca una operación de pago no autorizada o ejecutada incorrectamente, si el usuario de servicios de pago se lo comunica sin demora injustificada, el proveedor debe proceder a su rectificación y reintegrar el importe de inmediato, salvo que tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España.

3.º Cuando un usuario niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, incumbe al proveedor la carga de 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.

4.º El mero hecho del registro por el proveedor 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, correspondiendo al proveedor la prueba de que el usuario del servicio de pago cometió fraude o negligencia grave.

En suma, la responsabilidad del proveedor de los servicios de pago, en los casos de operaciones no autorizadas o ejecutadas incorrectamente, tiene carácter cuasi objetivo, en el doble sentido de que, primero, notificada la existencia de una operación no autorizada o ejecutada incorrectamente, el proveedor debe responder salvo que acredite la existencia de fraude; y, segundo, cuando el usuario niegue haber autorizado la operación o alegue que ésta se ejecutó incorrectamente, corresponde al proveedor acreditar 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, sin que el simple registro de la operación baste para demostrar que fue autorizada ni que el usuario ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave.

Profundizando en este último punto, la expresión «operaciones no autorizadas» incluye aquellas que se han iniciado con las claves de usuario y contraseña del usuario -necesarias para acceder al sistema de banca digital- y confirmado mediante la inserción del SMS enviado por el propio sistema al dispositivo móvil facilitado por el usuario, siempre que éste niegue haberlas autorizado, en cuyo caso el banco deberá acreditar 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 que presta.

A este respecto, la mención «deficiencia del servicio» no significa error o fallo del sistema informático o electrónico -posibilidad que estaría prevista en el concepto de «fallo técnico»-, sino que abarca cualquier falta de diligencia o *mala praxis* en la prestación del servicio, en el entendimiento de que el grado de diligencia exigible al proveedor de los servicios de pago no es el propio del buen padre de familia, sino que la naturaleza de la actividad y los riesgos que entraña el servicio que se presta, sobre todo en una relación empresario/consumidor, obliga a elevar el nivel de diligencia a un plano superior, como es el del ordenado y experto comerciante.

Lógicamente, las buenas prácticas pasan por adoptar las medidas de seguridad necesarias para garantizar el correcto funcionamiento del sistema de servicios de pago, entre las cuales destacan las orientadas a detectar de forma automática la concurrencia de indicios de que puede tratarse de una operación anómala y generar una alerta o un bloqueo temporal (v.gr. reiteración de transferencias sin solución de continuidad, horario en que se producen, importe de las mismas,

ADMINISTRACION DE JUSTICIA

destinatarios, antecedentes en el uso de la cuenta...), o las dirigidas a incrementar el control y vigilancia cuando se han recibido noticias o alertas de un posible aumento del riesgo." (…)

TERCERO: Valoración al caso concreto

En el presente caso no se discute que se emplearon claves y/o códigos personales de la demandante. Ahora bien en el marco de esta regulación legal, ut supra transcrita, el consentimiento no se entiende prestado por el solo hecho de que la operación de pago se haya realizado mediante la utilización de las claves personales, sino que es necesario que provenga de la usuaria o, en caso de que ésta niegue su intervención, que se acredite fraude, incumplimiento deliberado o, al menos, negligencia grave por parte del usuario, cuya prueba recae sobre la entidad bancaria; cuando la usuaria ha notificado de forma inmediata la existencia de una operación no autorizada, la entidad ha de proceder a su rectificación, salvo que demuestre que hubo fraude imputable a la usuaria.

O dicho de otro modo el hecho de que la entidad financiera acredite que la operación fue autenticada, registrada con exactitud y contabilizada, no es suficiente para eximirle de responsabilidad, además ha de probar que la operación no resultó afectada por un fallo técnico u otra deficiencia del servicio prestado, y, dado que la clienta niega que la operación fuera consentida, que no hubo por parte de esta último fraude, incumplimiento deliberado o negligencia grave.

En el presente caso la entidad demandada no ha probado tales extremos, dado que la documental obrante en autos revela que el día 3 de octubre de 2024, a las 19:07 h, la Sra. [redacted] recibió un mensaje SMS en su móvil de Abanca, en el que se la avisa de un inicio de sesión desde un nuevo dispositivo, remitiéndole a un enlace, a una web con aparente aspecto de Abanca y un número de incidencia. Ese mismo día a las 19:27 h recibió otro SMS desde otro número de teléfono identificado como Abanca y se le indica que se había abierto una incidencia y que le habían asignado un gestor ([redacted]), quien la llamó seguidamente y le indicó que al día siguiente tenía que realizar una serie de gestiones y le comunicó que habían detectado un acceso a su cuenta desde Badajoz, de igual modo le requirió para realizar unas comprobaciones consistentes en realizar otra llamada para comprobar si su móvil tenía un virus y el envió otro mensaje en el que se le informe que se va a realizar una transferencia desde su cuenta; seguidamente recibió otro mensaje en el que le facilitan una clave para la banca electrónica de la Entidad, con la excusa de que es necesario para anular la transferencia y acto seguido recibió un SMS en el que se le comunica que la transferencia se ha anulado con éxito. La Sra. [redacted], comunicó a la entidad los hechos anteriores al día siguiente que dieron lugar a la apertura de la correspondiente incidencia. El 4 de octubre de 2024 se interpuso denuncia.

A partir de tales hechos, debe indicarse que corresponde al proveedor de tales servicios la carga de la prueba que el

usuario de los mismos cometió fraude o negligencia grave y a tenor de los hechos ya expuestos, no puede calificarse de negligencia o culpa grave la actuación de la actora al recibir el mensaje SMS de un inicio de sesión desde un nuevo dispositivo y hacer uso de un enlace a una Web con aspecto y a nombre de Abanca ni el resto de actuaciones, que tras dicha y previa acción engañosa, realizó.

Al propio tiempo no está de más recordar que los avances de la tecnología actual hacen relativamente sencillo diseñar sistemas o aplicaciones informáticas idóneas para detectar ciertas anomalías en la prestación de los servicios de pago. Operaciones que, tratándose de empresas o sociedades con un concreto objeto social, pueden calificarse como ordinarias, deben inmediatamente levantar sospechas y dar lugar a una respuesta cuando afectan a personas físicas ajenas a tales actividades. A este respecto, sería suficiente un control automático de determinados factores, como el número y sucesión de operaciones, el intervalo en que se ejecutan, la hora del día, su importe, entidades de destino..., para generar un aviso que reforzara los requisitos de confirmación y minimizara los posibles riesgos.

De lo hasta el momento expuesto se colige que nos encontramos, de un lado, ante una conducta diligente de la actora, que informó de forma inmediata a la entidad de lo que había sucedido, cumpliendo la obligación que expresamente le imponía la normativa comunitaria y nacional; y, de otro lado, ante un servicio que se presta defectuosamente por el proveedor por no adoptar medidas de seguridad que eviten maniobras fraudulentas.

CUARTO: Responsabilidad legal prevista en el RDL 19/2018 de servicios de pago, art. 43 y ss.

Se alega por la entidad financiera demandada que ha cumplido con rigurosidad sus obligaciones, la identificación del usuario, la autentificación de la operación realizada y la aplicación del doble factor de autenticación impuesta por la normativa de servicios de pago, sin que haya sufrido ningún tipo de incidencia técnica y/o brecha de seguridad, por lo que de conformidad con lo establecido en el *art.44 RDL 19/2018*, *Abanca* no debe responder.

El art. 44 RDL establece que en caso de que el usuario niegue haber autorizado una operación de pago ya autorizada, el cumplimiento de las obligaciones relativas a la autenticación, registro y contabilización de la operación de pago fue autenticada, no exime de responsabilidad al proveedor de servicio, sino que deberá acreditar además que la operación no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado, sin que mero registro de la utilización del instrumento de pago baste 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.

ADMINISTRACION DE JUSTICIA

En el presente caso Abanca debe probar, lo que no ha logrado, que la operación no se vio afectada por un fallo técnico.

De otro lado, el hecho de que el conocimiento de las claves por el tercero no sea imputable a la entidad bancaria tampoco la libera de obligación de responder ni traslada al usuario la obligación de soportar las pérdidas, ya que el proveedor de servicios de pago, además de demostrar que el servicio se prestó correctamente, debe acreditar la concurrencia de fraude o incumplimiento deliberado o gravemente negligente por parte de la usuaria, y, en relación con este extremo no se ha probado fraude ni incumplimiento doloso o por negligencia grave de las obligaciones que correspondían a la demandante, la que fue víctima de un engaño, perpetrado con evidente pericia por el delincuente, y tampoco aquí observó el usuario una conducta que pudiera calificarse como de gravemente negligente y notificó al proveedor de servicios de pago la utilización no autorizada del instrumento de pago, tan pronto tuvo conocimiento de ello.

Por consiguiente las consecuencias dañosas de la actuación de la parte actora no puede afirmarse que estén al alcance de ser previstas por una persona media ni menos aún puede ser conceptuada como de negligencia grave, debiendo ser la entidad bancaria la que aumente las medidas de seguridad específicas ante este tipo de prácticas delictivas, cada vez más generalizadas.

Los argumentos hasta el momento expuestos conducen a la estimación de la demanda y a la condena de Abanca Corporación Bancaria, SA a que abone a Dª. [redacted] y Dª. [redacted] la cantidad de 24.000 euros

QUINTO: Intereses

En cuanto a los intereses, es objeto de aplicación el artículo 1100 y 1108 del Código Civil en relación con el artículo 576 de la Ley de Enjuiciamiento Civil y se devengarán desde la fecha de la presente resolución hasta el completo pago de la deuda.

SEXTO: Costas

La estimación la demanda conlleva, por aplicación de lo dispuesto en el artículo 394.1 de la Ley de Enjuiciamiento Civil, la condena en costas a parte demandada.

Vistos los preceptos legales citados, los invocados por la parte actora y demás de pertinente aplicación al caso de autos.

FALLO

Que estimando la demanda presentada por la procuradora **Dª.** [redacted] en nombre y representación de **Dª** [redacted] **y Dª.** [redacted] contra **la entidad ABANCA CORPORACIÓN BANCARIA, S.A. (en adelante,**

ADMINISTRACION DE JUSTICIA

"ABANCA") representada por el procurador [redacted] **debo condenar al parte demandada a que abone a la parte actora**, la cantidad de **VEINTICUATRO MIL EUROS (24.000 €)**, más los intereses legales de dicha cantidad desde la fecha de la sentencia hasta el completo pago de la deuda, así como las costas causadas en esta instancia.

Esta sentencia no es firme, y contra la misma **cabe recurso de apelación** que deberá ser interpuesto **en el plazo** de **veinte días** desde la notificación de la presente resolución, a través de escrito presentado en la forma prevista en el artículo 458 de la Ley de Enjuiciamiento Civil, para su **conocimiento y fallo** por la **Audiencia Provincial de Murcia. Para la interposición de dicho recurso** es necesario la **constitución de depósito por importe de 50 €** en la cuenta de depósitos y consignaciones del Juzgado ([redacted]) de acuerdo con lo establecido en la disposición adicional decimoquinta de la LOPJ, lo que deberá ser acreditado a la presentación del recurso

Así por esta mi Sentencia, de la que se expedirá testimonio para su unión a los autos lo pronuncio, mando y firmo.