JUZGADO DE PRIMERA INSTANCIA Nº 3

ORIHUELA

Plaza SANTA LUCIA,S/N
TELÉFONO: 965359567

[redacted]

Procedimiento: Asunto Civil 000955/2022

Demandante: CRISTINA [redacted]
Abogado:
Procurador: [redacted]

Demandado: CAJA RURAL CENTRAL SCC
Abogado:

SENTENCIA 238/2022

En Orihuela, a 13 de octubre de 2022, vistos por mí, D. Antonio Morente Espinosa, Magistrado del Juzgado de Primera Instancia Nº 3 de esta ciudad y su partido, los presentes autos de juicio verbal 955/2022, promovidos por la Procuradora Dña. [redacted], en nombre y representación de Dña. Cristina [redacted], asistida por el Letrado D. Juan Pablo Palomar Pérez, contra la mercantil Caja Rural Central Sociedad Cooperativa de Crédito, representada por la Procuradora Dña. [redacted] y asistida por el Letrado D. [redacted], por responsabilidad civil contractual, procede dictar, en nombre de Su Majestad El Rey Felipe VI de España, lo siguiente.

ANTECEDENTES DE HECHO

PRIMERO: El 11 de julio de 2022 se registró demanda presentada por la Procuradora Dña. [redacted], en nombre y representación de Dña. [redacted] con el siguiente suplico:

Teniendo por presentado este escrito de demanda junto con los documentos que se acompañan y copias de todo ello, se sirva admitirlo a trámite, me tenga por comparecida y parte en la representación que ostento en el proceso de DÑA. [redacted], por promovido el correspondiente JUICIO VERBAL contra CAJA RURAL CENTRAL SOCIEDAD COOPERATIVA DE CRÉDITO, y previos los trámites oportunos, interesa se dicte sentencia estimando íntegramente la presente demanda, y en virtud de tal sentencia estimatoria DECLARE que la demandada es responsable de los daños y perjuicios causados a mi mandante según obra especificado en el cuerpo de la presente demanda, y al amparo

[redacted]

del artículo 1.101 del Código Civil se le CONDENE por dolo y/o negligencia a INDEMNIZAR A LA DEMANDANTE POR LOS DAÑOS Y PERJUICIOS sufridos, equivalentes a la pérdida patrimonial experimentada. Esta pérdida de valor patrimonial se cuantifica en CUATRO MIL NOVECIENTOS OCHENTA Y CINCO EUROS (4.985- €), más los intereses legales de esta cantidad desde la fecha de la reclamación extraprocesal hasta la fecha de la sentencia y los intereses judiciales del art. 576 de la LEC desde la fecha de la sentencia hasta su completo pago; con imposición de costas a la parte demandada.

SEGUNDO: Por decreto de 29 de julio de 2022 fue admitida a trámite dicha demanda, una vez subsanados los defectos apreciados en la misma, siendo notificada la misma a la demandada.

TERCERO: El 14 de septiembre de 2022 se registró escrito de contestación a la demanda, solicitando la desestimación de la misma con imposición de costas a la parte actora.

CUARTO: El 13 de octubre de 2022 se celebró la vista. Admitida la prueba propuesta por las partes y practicada la misma, se dio trámite de conclusiones por la complejidad del asunto, quedando el juicio visto para sentencia.

En el referido acto de la vista se indicó a las partes que se continuaría el procedimiento a pesar de que las entidades requeridas no remitieran la información solicitada, no recurriendo ninguna de las partes dicha decisión o formulado protesto.

FUNDAMENTOS DE DERECHO

PRIMERO: La demanda presentada tiene por finalidad lograr la indemnización de los importes que se habrían sustraído de la cuenta abierta por la actora en la entidad demandada mediante el uso fraudulento de la tarjeta de débito asociada a la misma, exponiendo la demandante como dichos cargos se realizaron sin que por la entidad demandada se adoptaran las correspondientes medidas de seguridad, puesto que se realizaron, por ejemplo, desde un teléfono que no era el de la actora, así como sin enviar el correspondiente sms a fin de comunicar los códigos necesarios para autorizar diversas operaciones.

Ante dicha petición, la parte demandada considera que se ha actuado en todo momento con total diligencia por su parte, siendo la demandante vista de delincuencia cibernética.

SEGUNDO: La sentencia de la sección tercera de la Audiencia Provincia de Badajoz de 16 de junio de 2022, desestimatoria del recurso interpuesto contra la sentencia de primera instancia que estimó la demanda interpuesta contra la entidad bancaria, expone: "El actor solicita la condena de la entidad demandada a reintegrarle la cantidad total de 5496,45 euros (en tres disposiciones sucesivas de 2.699 euros, 2.195 euros y 602,45 euros el día 11-9-2020) de la cuenta asociada a la tarjeta de débito que tenía contratada con la entidad del que se habría dispuesto sin su consentimiento mediante el uso fraudulento de los datos del instrumento de pago. La entidad demandada afirma que el demandante habría sufrido un fraude mediante la técnica del phishing y que habría de soportar las pérdidas pues actuó con grave negligencia al contestar a un SMS fraudulento, aportando sus claves de seguridad, lo que propició que el defraudador pudiera instalar su tarjeta en la aplicación Apple Pay del terminal del defraudador y que éste pudiera, una vez instalada, realizar compras con la tarjeta por ese total importe. No se discute, pues, que las operaciones de pago mediante las que se detrajeron de la cuenta bancaria que el demandante tenía en la entidad demandada respondieron a órdenes de pago / compra realizadas por un tercero que usó de manera fraudulenta de los datos de una tarjeta de débito de aquél.

En el RDL 19/2018, de 23 de noviembre se regulan las obligaciones del proveedor y del usuario de los servicios de pago y el régimen de responsabilidad de ambos, así como la carga de la prueba de tales circunstancias que, en lo que aquí respecta, son:

- art. 41 (obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas): utilizar el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del instrumento de pago y, en particular, en cuanto reciba un instrumento de pago, tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas;

- art. 42 (obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago): El proveedor de servicios de pago emisor de un instrumento de pago se cerciorará de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento, sin perjuicio de las obligaciones que incumben al usuario de servicios de pago con arreglo al artículo 41;

- art. 44 (prueba de la autenticación y ejecución de las operaciones de pago): "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".

- art. 45.1 (Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizada :"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 (...) 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"

- art. 46 (Responsabilidad del ordenante en caso de operaciones de pago no autorizadas): "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 (...)"

- art. 68 (autenticación): "1. Los proveedores de servicios de pago aplicarán la autenticación reforzada de clientes, en la forma, con el contenido y con las excepciones previstas en la correspondiente norma técnica aprobada por la Comisión Europea, cuando el ordenante: a) acceda a su cuenta de pago en línea; b) inicie una operación de pago electrónico; c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos. 2. En lo que se refiere a la iniciación de las operaciones de pago electrónico mencionada en el apartado 1, letra b) respecto de las operaciones remotas de pago electrónico, los proveedores de servicios de pago aplicarán una autenticación reforzada de clientes que incluya elementos que asocien dinámicamente la operación a un importe y un beneficiario determinados. 3. En los casos a los que se refiere el apartado 1, los proveedores de servicios de pago contarán con medidas de seguridad adecuadas para proteger la confidencialidad y la integridad de las credenciales de seguridad personalizadas de los usuarios de los servicios de pago. 4. Los apartados 2 y 3 se aplicarán asimismo cuando los pagos se inicien a través de un proveedor de servicios de iniciación de pagos. Los apartados 1 y 3 se aplicarán asimismo cuando la información se solicite a través de un proveedor de servicios de pago que preste servicios de información sobre cuentas. (...)".

Pues bien, en lo que respecta a la responsabilidad por operaciones de pago fraudulentas, el proveedor de servicios de pago se encuentra sujeto al cumplimiento de específicas obligaciones de protección en la emisión de los instrumentos de pago y en los procesos de autenticación de las operaciones de pago cuya finalidad es minimizar la probabilidad de ejecución de operaciones no autorizadas y en relación con los instrumentos de pago ha de cumplir con las obligaciones sobre emisión y uso seguro que se establecen en el mencionado art. 42.1 RDL 19/2018 y será el proveedor de los servicios de pago quien habrá de responder por las operaciones de pago resultantes del uso fraudulento del instrumento de pago por un tercero, y siempre que la operación de pago fue autenticada y registrada con exactitud y no se vio afectada por ninguna deficiencia del servicio prestado por el proveedor de servicios de pago, salvo que el ordenante actuara de manera fraudulenta, o incumpliendo deliberadamente o por negligencia grave alguna de las obligaciones recogidas en el art. 41 RDL 19/2018 .

De esta manera, al proveedor de servicios de pago le corresponde la carga procesal de acreditar tanto su propio comportamiento diligente en la autenticación de la operación de pago como, en su caso, el fraude (requerirá de la acreditación de hechos de los que pudiera llegar a inferirse que aquel actuó con engaño para beneficiarse de la operación de pago) o la negligencia grave del ordenante (requerirá de la acreditación de las circunstancias concurrentes en la operación de pago de las que quepa inferir que la misma pudo realizarse porque aquel obró con una significativa falta de diligencia al usar del instrumento de pago o al proteger sus credenciales).

Pues bien, de la prueba practicada, si bien es posible acreditar que la entidad actora ha cumplido con su obligación 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, sin embargo, no ha demostrado, y a ella correspondía la carga probatoria, que se hubiera producido una negligencia grave en el actuar del actor, que exonere de responsabilidad a la entidad demandada, así como tampoco que hubiera proveído al demandante de los mecanismos de autenticación y supervisión suficientes (reforzados) para detectar y evitar la utilización fraudulenta de su medio de pago, como puede ser el dotarse de la tecnología antiphishing precisa para detectar las páginas o enlaces fraudulentos, impidiendo su acceso, lo que, de haberse producido, hubieran evitado que el defraudador pudiera hacerse con las credenciales del usuario del instrumento de pago por ella emitido, pues la rotura del enlace haría ya ineficaz cualquier conducta que frente al mismo pudiera observar el usuario receptor.

Así, de la lectura del SMS recibido por el actor no es posible concluir, que de haber clicado en el enlace (aunque él lo niegue), se derive su falta de diligencia en la protección de las credenciales del instrumento de pago. No ha de olvidarse que en el phishing se usan técnicas para ganarse la confianza del usuario del instrumento de pago y aprovecharse de una simulación cada vez más perfeccionada. A ello debiera responderse por la entidad bancaria también con mecanismos de protección cada vez mayores y mejores. Así, no podía la entidad desconocer que frecuentemente mediante esta técnica el tercero defraudador utiliza los datos de la tarjeta para activarla en una aplicación de pago, por lo que debiendo conocer que el teléfono desde el que se le había solicitado la activación no se encontraría entre los que hubiera registrado su nombre el actor, la comunicación del número de terminal telefónico devenía exigible para que aquélla pudiera conocer que era un tercero quien podría disponer de los datos de la tarjeta mediante la aplicación de pago que se activaría.

De lo expuesto se concluye que la entidad demandada no habría acreditado la observancia de los deberes de diligencia que le eran exigibles en la autenticación de las operaciones de pago, pues ni habría probado haber implementado un mecanismo antiphising de protección de los usuarios de los instrumentos de pago por ella emitidos frente al uso fraudulento por un tercero para hacerse con las credenciales del instrumento; ni habría puesto en conocimiento del usuario los datos necesarios para que este conociera que se trataba de instalar su tarjeta en una aplicación de pago de un terminal de un tercero; ni tampoco de avisarle por el mecanismo habitual de contacto con el cliente que se estaba intentando adquirir determinados productos a precios ciertamente importantes en comercios electrónicos situados en el extranjero, a fin de que el demandante hubiera podido, con carácter previo, dar su visto bueno a las utilizaciones concretas que se pretendían, lo que hubiera permitido conocer tal uso fraudulento, conocimiento que solo adquirió tras examinar los movimientos de su cuenta bancaria.

Por ello, no cabe observar negligencia grave del demandante de los deberes de conducta al usar del instrumento de pago y al dirigirse a un enlace simulado y habrá de ser, en consecuencia, la entidad demandada como proveedora de los servicios de pago usados de manera fraudulenta por un tercero logrando con ello acceder a la cuenta bancaria del demandante, quien haya de responder las pérdidas sufridas por éste con tales operaciones".

La sentencia de 20 de mayo de 2022 de la sección vigésima de la Audiencia Provincial de Madrid, estimatoria en su integridad de la demanda interpuesta contra la entidad bancaria, recoge: "Centrada la discrepancia en si el comportamiento adoptado por las partes aquí enfrentadas debe ser calificado como negligente, en el cumplimiento de las obligaciones que para cada uno de ellos se deriva del contrato de tarjeta de débito que les vincula y las consecuencias a extraer de todo ello, para el análisis del cumplimiento que cada una de las partes ha hecho de las obligaciones que les corresponde como titular y usuario de la tarjeta el demandante y como prestadora del servicio de pago la demandada, el marco normativo de que debe partirse viene constituido por el RDL 19/2018, que derogó la Ley 16/2009 a la que se remite la sentencia de primera instancia. La Directiva 2015/2366 y el Reglamento delegado 2018/389 de la Comisión , interpretado todo ello conforme a las reglas y principios básicos establecidos en el cc, respecto de las obligaciones y contratos y ello a la vista de todas las circunstancias concurrentes en el supuesto de hecho enjuiciado. Como se indica en la sentencia nº 539/2021 de 21 de diciembre de la Sec. 6ª (Sede Vigo) de la Audiencia provincial de Pontevedra , (ponente el Ilmo Sr. José Ferrer González), en la que se analiza un supuesto de hecho similar al presente, el marco normativo del que debe partirse es el siguiente:

" Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015 , sobre servicios de pago en el mercado interior

Considerando:

(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.

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 . En vigor desde el 14 de septiembre de 2019 (artículo 38)

Artículo 1 Objeto

El presente Reglamento establece los requisitos que deben cumplir los proveedores de servicios de pago a efectos de la aplicación de medidas de seguridad que les permitan hacer lo siguiente:

a) aplicar el procedimiento de autenticación reforzada de clientes, de conformidad con el artículo 97 de la Directiva (UE) 2015/2366 ;

b) eximir de la aplicación de los requisitos de seguridad de la autenticación reforzada de clientes, bajo determinadas condiciones limitadas y basadas en el nivel de riesgo, el importe de la operación de pago y la frecuencia con que se repite, y el canal de pago empleado para la ejecución de dicha operación;

c) proteger la confidencialidad y la integridad de las credenciales de seguridad personalizadas del usuario de servicios de pago;

d) establecer estándares abiertos comunes y seguros para la comunicación entre los proveedores de servicios de pago gestores de cuenta, los proveedores de servicios de iniciación de pagos, los proveedores de servicios de información sobre cuentas, los ordenantes, los beneficiarios y otros proveedores de servicios de pago en relación con la provisión y la utilización de servicios de pago en aplicación del título IV de la Directiva (UE) 2015/2366 .

Artículo 2 Requisitos generales de autenticación .

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

[redacted] [redacted]

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) 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.

Artículo 3 Revisión de las medidas de seguridad

1.La aplicación de las medidas de seguridad a que se refiere el artículo 1 deberá documentarse, probarse periódicamente, evaluarse y auditarse de conformidad con el marco jurídico aplicable al proveedor de servicios de pago por auditores con experiencia en el ámbito de la seguridad y los pagos informáticos y funcionalmente independientes, ya pertenezcan al organigrama del propio proveedor de servicios de pago o sean externos a él.

....

12. El RDL 19/2018 derogó la ley 16/2009 de 13 de noviembre de servicios de pago (disposición derogatoria única) y dispuso, en cuanto al régimen transitorio, que los contratos de servicios de pago suscritos con anterioridad a su entrada en vigor seguirían siendo válidos pero en todo caso habría de aplicarse las disposiciones de carácter imperativo que resulte más favorables para los consumidores y microempresas (Disposición Transitoria quinta). La Disposición Final 13ª estableció un régimen de entrada en vigor de la norma de manera escalonada que, partiendo de la general vigencia desde el día 25 de noviembre de 2018 (el siguiente a la fecha de publicación de la norma en el BOE, DF 13ª.1) culminó el 14 de septiembre de 2019 (18 meses desde la entrada en vigor del Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017, DF 131ª2.b) fecha desde la que habrían de aplicarse los artículos 37, 38, 39 y 68.

[redacted] [redacted]

13. De las normas que en la legislación vigente regulan las obligaciones del proveedor y del usuario de los servicios de pago y el régimen de responsabilidad importa a efectos de este proceso considerar:

Artículo 41. Obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas

El usuario de servicios de pago habilitado para utilizar un instrumento de pago:

a) utilizará el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del instrumento de pago que deberán ser objetivas, no discriminatorias y proporcionadas y, en particular, en cuanto reciba un instrumento de pago, tomará todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas;

b) en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, lo notificará al proveedor de servicios de pago o a la entidad que este designe, sin demora indebida en cuanto tenga conocimiento de ello.

....

Artículo 42. Obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago.

1. El proveedor de servicios de pago emisor de un instrumento de pago:

a) Se cerciorará de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento, sin perjuicio de las obligaciones que incumben al usuario de servicios de pago con arreglo al artículo 41.

b) Se abstendrá de enviar instrumentos de pago que no hayan sido solicitados, salvo en caso de que deba sustituirse un instrumento de pago ya entregado al usuario de servicios de pago.

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

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

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

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

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

Artículo 44. Prueba de la autenticación y ejecución de las operaciones de pago.

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.

Artículo 45 Responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas

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.

....

Artículo 46 Responsabilidad del ordenante en caso de operaciones de pago no autorizadas

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.

Artículo 64. Ausencia de responsabilidad cuando concurran circunstancias excepcionales e imprevisibles.

La responsabilidad establecida con arreglo a los Capítulos II y III de este Título no se aplicará en caso de circunstancias excepcionales e imprevisibles fuera del control de la parte que invoca acogerse a estas circunstancias, cuyas consecuencias hubieran sido inevitables a pesar de todos los esfuerzos en sentido contrario, o en caso de que a un proveedor de servicios de pago se le apliquen otras obligaciones legales.

Artículo 68. Autenticación.

1. Los proveedores de servicios de pago aplicarán la autenticación reforzada de clientes, en la forma, con el contenido y con las excepciones previstas en la correspondiente norma técnica aprobada por la Comisión Europea, cuando el ordenante:

a) acceda a su cuenta de pago en línea;

b) inicie una operación de pago electrónico;

c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos.

....

6. No obstante, no será preciso aplicar la autenticación reforzada de clientes a la que se refiere el apartado 1 a los supuestos indicados en el artículo 98.1.b) de la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 .

TERCERO . Responsabilidad por operaciones de pago fraudulentas.

14. El proveedor de servicios de pago se encuentra sujeto al cumplimiento de específicas obligaciones de protección en la emisión de los instrumentos de pago y en los procesos de autenticación de las operaciones de pago cuya

finalidad es minimizar la probabilidad de ejecución de operaciones no autorizadas.

15. En relación con los instrumentos de pago ha de cumplir con las obligaciones sobre emisión y uso seguro que se establecen en el artículo 42.1 RDL 19/2018 .

16. Los procesos o mecanismos de autenticación de las operaciones de pago deben cumplir con los requisitos que establece el Reglamento Delegado 2018/389 , lo que exige:

- a) Implementar las medidas de seguridad previstas en el artículo 1, que han de incluir el procedimiento de autenticación reforzada de clientes, con las salvedades específicamente señaladas.

- b)Incluir mecanismos de supervisión de las operaciones que permitan al proveedor de servicios de pago detectar operaciones de pago no autorizadas o fraudulentas. A tal efecto el proveedor de servicios de pago ha de tener en cuenta la totalidad de los factores de riesgo enumerados en el artículo 2, y, entre ellos, los supuestos de fraude conocidos en la prestación de servicios de pago.

- c) Auditar las medidas, en las condiciones del artículo 3.

17. El usuario de los servicios de pago deberá cumplir con las obligaciones que se establecen en el artículo 41 RDL 19/2010 : a) Usar del instrumento de pago conforme a lo pactado y tomar las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas; b) En cuanto tenga conocimiento de haber perdido la posesión del instrumento de pago o de haber sido este utilizado sin su autorización, lo notificará sin demora indebida al proveedor de servicios de pago.

18. El régimen de la responsabilidad por las pérdidas derivadas de operaciones de pago por uso fraudulento de un instrumento de pago por un tercero se determina interpretando de manera integrada las previsiones del artículo 46 con la regulación general de las pérdidas por operaciones de pago no autorizadas del artículo 45 y con el régimen de la carga probatoria que se establece en el artículo 44 (todos del RDL 19/2018).

19. Será el proveedor de los servicios de pago quien

[redacted]

habrá de responder de las pérdidas de importe superior a 50 euros por las operaciones de pago resultantes del uso fraudulento del instrumento de pago por un tercero; responderá de la totalidad de la pérdida cuando al ordenante no le hubiera sido posible detectar el posible uso fraudulento antes de que éste se hubiese materializado o cuando la pérdida se debiera a la acción u omisión de cualquier persona de la que el proveedor de servicios hubiera de responder.

20. El ordenante será quien soporte la totalidad de las pérdidas cuando concurran dos requisitos: a) La operación de pago fue autenticada y registrada con exactitud y no se vio afectada por ninguna deficiencia del servicio prestado por el proveedor de servicios de pago; b) El ordenante actuó de manera fraudulenta, o incumpliendo deliberadamente o por negligencia grave alguna de las obligaciones recogidas en el artículo 41 RDL 19/2018 .

21. Al proveedor de servicios de pago le corresponde la carga procesal de acreditar tanto su propio comportamiento diligente en la autenticación de la operación de pago como el fraude o la negligencia grave del ordenante. La prueba de la diligencia en el procedimiento de autenticación deberá realizarse con relación a las exigencias del Reglamento Delegado 2018/389 . La prueba del fraude del ordenante requerirá de la acreditación de hechos de los que pudiera llegar a inferirse que aquel actuó con engaño para beneficiarse de la operación de pago. La prueba de la negligencia grave del ordenante requerirá de la acreditación de las circunstancias concurrentes en la operación de pago de las que quepa inferir que la misma pudo realizarse porque aquel obró con una significativa falta de diligencia al usar del instrumento de pago o al proteger sus credenciales.

22. Cuando el proveedor de servicios de pago no acredite el cumplimiento de los deberes de diligencia propios en la autenticación habrá de responder de la pérdida resultante del uso fraudulento del instrumento de pago por un tercero salvo que concurra el fraude del ordenante."

TERCERO .- La aplicación de la normativa anteriormente indicada al caso presente, nos lleva a estimar la impugnación formulada por el demandante en cuanto, no discutiéndose la forma en que se llegaron a materializar las 6 retiradas de efectivo por un importe total de 6.000 €, iniciadas por una actuación fraudulenta de tercero, no cabe apreciar en el demandante un comportamiento negligente de la gravedad y entidad para con base en el mismo hacerle responsable, ni siquiera de la primera disposición de efectivo realizada con la tarjeta usada de manera fraudulenta por un tercero. Como se indica en la Directiva 2015/2036 la negligencia que le hace responder al cliente, es la que se deriva de una conducta caracterizada por un grado significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que ha sido inducido por un delincuente profesional. Tampoco puede calificarse como grave dicho comportamiento conforme a la normativa del código civil, pues siendo exigible al demandante la diligencia que exija la naturaleza de la obligación y correspondan a las circunstancias de las personas, tiempo y lugar (art. 1.104 del cc), el método fraudulento empleado - phishing- es de una complejidad y grado de perfección, difícilmente detectable por un cliente de las características del demandante, sin que la forma en que se denominaba al Banco en el SMS recibido o el error gramatical al emplear la palabro "lo" en lugar de "le", sean errores de entidad suficiente para detectar con base en ellos el fraude de que estaba siendo objeto. En esas circunstancias, era preciso ser un experto en la materia para poder detectar que la comunicación obedecía a una estafa o fraude. Es cierto que dicho comportamiento no puede considerarse diligente, pero para hacer soportar al cliente las consecuencias, aún parciales como se concluye en la sentencia apelada, es preciso apreciar en él una negligencia y que además sea grave, que en la normativa europea antes referida se equipara a la comisión de un fraude, actuación en la que no se ha acreditado incurriese el demandante, por el hecho de haber pinchado el link que se le ofrecía y facilitar los datos y clave de la tarjeta

CUARTO .- Por el contrario, la responsabilidad exigida a la entidad demandada, como proveedora del servicio, es la que se deriva de la naturaleza de tal prestación y de la posición contractual en la que se encuentran las partes, lo que le obliga a adoptar una serie de medidas de seguridad y dotarse de mecanismos de supervisión que permitieran detectar operaciones fraudulentas en la prestación de servicios de pago, tal como señala el artículo 2 del Reglamento Delegado 2018/389 , pues como se indica también en la sentencia citada de la Audiencia de Pontevedra, incluyendo la técnica del phishing, la creación y puesta en la red de páginas que clonan las del sitio oficial de las entidades emisoras de instrumentos de pago, el deber de diligencia de la entidad demandada exigía dotarse de la tecnología antiphishing precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas, lo que, de producirse, impediría que el defraudador pudiera hacerse con las credenciales del usuario del instrumento de pago por ella emitido, pues la rotura del enlace del correo electrónico haría ya ineficaz cualquier conducta que frente al mismo pudiera observar el usuario receptor. Dicha actuación diligente no puede considerarse acreditada por las información que se facilita a los clientes a través de su página web, en cuanto la efectividad de esas obligaciones preventivas, lo que requerían era implementar en el sistema informático el mecanismo tecnológico adecuado para evitarlo; es decir mediante una con una conducta activa y no simplemente informativa o divulgativa.

De dicha omisión, no puede quedar exonerada por el hecho de que el cliente no tuviera activado el sistema de alarma en la tarjeta utilizada fraudulentamente, pues siendo obligación suya adoptar las medidas de seguridad adecuadas, esa obligación no puede entenderse cumplida con la simple puesta a disposición del cliente, sino que es ella quien debe adoptar una actitud activa para su implantación, no solo ponerla a disposición del cliente.

En consecuencia, la demandada incurrió en un incumplimiento de los deberes de diligencia en la prevención del fraude mediante phishing, que le hace ser responsable del perjuicio total sufrido por el demandante, pues no podía la entidad desconocer que frecuentemente mediante esa técnica el tercero defraudador utiliza los datos de la tarjeta para activarla en una aplicación de pago de la que tiene dominio, por lo que debiendo conocer que el teléfono desde el que se le había solicitado la activación no se encontraría entre los que hubiera registrado su nombre el demandante en su ficha de cliente, la comunicación del número de terminal telefónico devenía exigible para que aquélla pudiera conocer que era un tercero quien podría disponer de los datos de la tarjeta mediante la aplicación de pago que se activaría.

No habiendo quedado acreditado que la entidad demandada cumplió en la forma que le es exigible los deberes de diligencia en la autenticación de las operaciones de pago, pues ni habría probado haber implementado un mecanismo antiphising de protección de los usuarios de los instrumentos de pago por ella emitidos frente al uso fraudulento por un tercero de páginas imitativas de las propias para hacerse con las credenciales del instrumento, ni habría puesto en conocimiento del usuario los datos necesarios para que este conociera que se trataba de instalar su tarjeta en una aplicación de pago de un terminal de un tercero y no apreciándose que el demandante incurrió en negligencia grave

[redacted] [redacted]

en el cumplimiento de sus deberes de custodia y uso de la tarjeta, ha de declararse la responsabilidad de la entidad demandada como proveedora de los servicios de pago usados de manera fraudulenta por un tercero y por tanto es quien debe responder de las pérdidas sufridas por el demandante con tales operaciones, responsabilidad que se hace extensible a la totalidad de la pérdida, pues en momento alguno anterior a que se realizase la última de las operaciones fraudulentas de pago, la entidad demandada había informado a la demandante del número del terminal telefónico desde el que se estaban realizando las órdenes de pago fraudulentas, ni de circunstancia alguna que hubiera permitido conocer al demandante tal uso fraudulento.

La sentencia de la Audiencia Provincial de Pontevedra de 21 de diciembre de 2021, sección sexta, también estimatoria de la demanda, explica: "27. Determinar si la señora Sabina, al abrir el enlace del correo electrónico que le llevó a una página que no era la oficial de la entidad emisora de su tarjeta de débito en la que introdujo los datos de su instrumento de pago y el código de seguridad, incurrió en negligencia grave al usar de instrumento de pago o al cumplir su obligación adoptar las medidas razonables para proteger sus credenciales de seguridad personalizadas requiere considerar la totalidad de las circunstancias concurrentes y en particular la técnica de la que se valió el tercero defraudador para hacerse con las citadas credenciales; el *phishing* .

El *phishing* aparece configurado, en el caso, por dos elementos; a) Envío de un correo electrónico con la apariencia de ser remitido por una entidad con la que el receptor puede tener alguna relación de servicios; b) El correo contiene un enlace a una página que aparenta ser del sitio oficial de la entidad emisora de la tarjeta pero que en realidad pertenece a un dominio bajo el control del *phisher.*

El deber de diligencia de la demandada para asegurar la correcta autenticación de las operaciones de pago exigía de dotarse de mecanismos de supervisión que permitieran detectar operaciones de fraudulentas a cuyo efecto habría de considerar *los supuestos del fraude conocidos en la prestación de servicios de pago* (*artículo 2 del Reglamento Delegado 2018/389*). Es por ello que conocido que la técnica del *phishing* incluye, a menudo, la creación y puesta en la red de páginas que clonan las del sitio oficial de las entidades emisoras de instrumentos de pago, el deber de diligencia de la entidad demandada exigía dotarse de la tecnología *antiphishing* precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas, lo que, de producirse, impediría que el defraudador pudiera hacerse con las credenciales del usuario del instrumento de pago por ella emitido, pues la rotura del enlace del correo electrónico haría ya ineficaz cualquier conducta que frente al mismo pudiera observar el usuario receptor.

A ese mecanismo *antiphishing* parece referirse la entidad demandada cuando en la impugnación del recurso, y antes en la contestación a la demanda, alegaba tener *una posición muy activa y un nivel muy alto de exigencia en la defensa de la seguridad informática de sus clientes;* pero resulta que no se acreditó por medio alguno su implementación en el sistema informático de las operaciones de pago al momento de los hechos objeto del proceso, limitándose la prueba aportada en relación a su actuación en la prevención del phishing a la remisión de correos a los usuarios de los instrumentos de pago que había emitido, entre ellos la demandante, en los que explicaba aquella técnica defraudatoria y realizaba recomendaciones y advertencias que el usuario habría de observar para evitar el conocimiento de las credenciales de su instrumento de pago por el defraudador, correos explicativos insuficientes para entender observada la diligencia propia pues supondría dejar únicamente al cuidado del usuario la evitación de un fraude que debía prevenirse con una conducta activa propia mediante el mecanismo tecnológico adecuado.

La señora Sabina al introducir los datos de su tarjeta de débito en la página que aparentaba ser de la entidad Abanca para abonar el precio de un servicio que aparentemente le habría de prestar la entidad Correos y Telégrafos estaba haciendo uso del instrumento de pago conforme a su propia finalidad, por lo que en relación a las obligaciones que le imponía el *artículo 41 del RDL 19/2018* restaría por determinar si al haber accedido a la página que simulaba ser de la entidad bancaria emisora de la tarjeta desde un enlace de un correo electrónico *impreciso y con dos faltas de ortografía* y haber introducido en aquella no sólo los datos de su tarjeta sino también la clave de activación de una aplicación de pago que un tercero había instalado en un terminal propio habría de determinarse que incurrió en negligencia grave en el deber de protección de sus credenciales de seguridad personalizadas. La lectura atenta del correo electrónico le hubiera permitido a la señora Sabina percatarse tanto de su contenido impreciso, al no identificar el pedido al que se refería, como de las dos faltas de ortografía, datos relevantes para adoptar su decisión de aceptar o no el pago electrónico que se le solicitaba, por lo que en ausencia de tal lectura reflexiva habría de considerarse su falta de diligencia en la protección de las credenciales del instrumento de pago. Pero han de tenerse en cuenta las circunstancias en las que tal decisión se adoptó, previo el engaño premeditado de un tercero para ganarse su confianza, lo que, estimo, debe llevar a que no haya de apreciarse una negligencia grave en la omisión de la lectura atenta del correo electrónico. En el phising se usan técnicas de ingeniería social para ganarse la confianza del usuario del instrumento de pago y aprovecharse de los sesgos cognitivos en la toma de decisiones, lo que, en el caso se habría concretado en la simulación del envío a nombre de una entidad de confianza para la usuaria (Correos y Telégrafos), y en el aprovechamiento del sesgo de confirmación por el cual se tiende a favorecer la información que confirma las opiniones que ya se tenían o que resulta consistente con los hechos ya conocidos (la señora Sabina explicó que estando esperando un pedido de mascarillas creyó que a él se refería la entrega del paquete que se le anunciaba en el correo electrónico).

Los SMS que la entidad demandada envió a la señora Sabina comunicándole el código que había de utilizar para instalar su tarjeta en la aplicación de pago Samsung Pay, y el que le envío después de su activación no proporcionaban información sobre el número del terminal telefónico en el que se había solicitado y después activado la citada aplicación de pago. Tal omisión supone un incumplimiento de los deberes de diligencia en la prevención del fraude mediante phising, pues no podía la entidad desconocer que frecuentemente mediante aquella el tercero defraudador utiliza los datos de la tarjeta para activarla en una aplicación de pago de la que tiene dominio, por lo que debiendo conocer que el teléfono desde el que se le había solicitado la activación no se encontraría entre los que hubiera registrado su nombre la señora Sabina en su ficha de cliente, la comunicación del número de terminal telefónico devenía exigible para que aquélla pudiera conocer que era un tercero quien podría disponer de los datos de la tarjeta mediante la aplicación de pago que se activaría. En tales circunstancias no cabe observar negligencia grave en el acto de la señora Sabina introduciendo la clave de activación de la obligación de pago en la página que simulaba ser de Abanca, pues para que pudiera ponderarse su error (explicó que había entendido que los mensajes se referían al pago que realizaba con su propio teléfono móvil que era de la marca Samsung) como inexcusable le faltaba el dato del número de teléfono en el que la aplicación se activaría, con el que podría haber conocido que el pago no se realizaría mediante el teléfono propio sino mediante el de un tercero.

De lo expuesto se concluye que la entidad demandada no habría acreditado la observancia de los deberes de diligencia que le eran exigibles en la autenticación de las operaciones de pago, pues ni habría probado haber implementado un mecanismo antiphising de protección de los usuarios de los instrumentos de pago por ella emitidos frente al uso fraudulento por un tercero de páginas imitativas de las propias para hacerse con las credenciales del instrumento, ni habría puesto en conocimiento del usuario los datos necesarios para que este conociera que se trataba de instalar su tarjeta en una aplicación de pago de un terminal de un tercero. Se concluye, también, que no cabría observar negligencia grave de la demandante de los deberes de conducta al usar del instrumento de pago y al introducir las credenciales de uso personal en una página que imitaba las del sitio oficial de la entidad emisora de su tarjeta. Habrá de ser, en consecuencia, la entidad demandada como proveedora de los servicios de pago usados de manera fraudulenta por un tercero logrando con ello acceder a la cuenta bancaria de la demandante quien haya de responder las pérdidas sufridas por esta con tales operaciones.

La responsabilidad se extenderá a la totalidad de la pérdida pues en momento alguno anterior a que se realizase la última de las operaciones fraudulentas de pago la entidad demandada había informado a la demandante del número del terminal telefónico desde el que se estaban realizando las órdenes de pago fraudulentas ni de circunstancia alguna (las localidades en las que se ubicaban los establecimientos en los que se realizaban los pagos, que la entidad proveedora de servicios debía analizar si se correspondían con los patrones habituales de las operaciones de la usuaria de la tarjeta) que hubiera permitido conocer tal uso fraudulento, conocimiento que esta solo adquirió tras examinar los movimientos de su cuenta bancaria".

TERCERO: Para la resolución del presente procedimiento, en base a la jurisprudencia citada en el anterior fundamento de derecho, debe señalarse como, para la desestimación de la demanda, es necesario que la entidad demandada acredite, no solo su actuación diligente, sino que la actora, además, actuó de forma negligente.

En su declaración, que ha sido en todo momento coherente y ordenada, sin incurrir en contradicción ni en otro elemento o dato lleve negar credibilidad a la misma, indicó como nunca ha tenido un dispositivo IPhone 13, aportado junto con la demanda justificante de compra del dispositivo móvil empleado en el momento de los hechos, señalando incluso ser una marca que no le gusta usar dado la complejidad de su sistema operativo.

Expuso igualmente como solo accedía a la aplicación bancaria desde su dispositivo móvil, sin usar otro dispositivo, sin que las claves de acceso a la aplicación las tuviese recogidas en algún papel o dispositivo, si que hubiese sufrido algún tipo de robo, hurto o pérdida de su móvil o bolso en los días previos.

La actora relató no tener conocimiento de los hechos por comunicación de la entidad demandada, sino que, al hacer una revisión de sus cuentas en el sofá de su casa tras comer, comprobó que habían desaparecido casi 5.000 euros, lo que le alarmó, dado que solo tenía unos 7.000 euros en cuenta.

En ese momento llamó a la entidad bancaria, constando en autos el registro de la correspondiente llamada, recriminando a la entidad demandada que no hubiese saltado ninguna alarma, informando esta de que había saltado una alarma momentos antes, constando en las actuaciones, tal como indicó el Letrado de la parte actora durante el interrogatorio, la anulación por parte de la entidad bancaria unas tres horas antes de la llamada de la demandante, sin que se hubiese informado a esta.

De la prueba practicada no consta comunicación alguna de la demandada a la actora, sino al contrario, tuvo que ser la actora la que se pusiese en contacto al comprobar el saldo de su cuenta bancaria.

La demandante expuso igualmente no haber recibido sms o correo electrónico en el que se solicitasen datos, ni haber contestado a estos.

En la documentación aportada junto con el escrito de contestación a la demanda se aprecia como, en los días anteriores al bloqueo de la tarjeta, existieron conexiones empleando el número de teléfono y usuario de la demandada, pero desde un terminal diferente, iPhone 13, y con un sistema operativo diferente, IOS, constatando en la documentación aportada por la demandada como la actora empleaba siempre sistema Android y terminales Redmi, lo que corroboraría su versión de los hechos.

Así, en el documento cinco de la contestación, se recoge una activación del servicio push con sistema operativo IOS, o en el documento siente un registro de huella desde un IPhone 13 con sistema operativo IOS, apareciendo en el resto de indicaciones el sistema operativo Android.

Es patente como otra persona, empleando las claves de la actora, desde un terminal diferente, sin que la demandante tuviese conocimiento ni provocase dicha circunstancia, consiguió burlar los diferentes sistemas de seguridad, sistemas que eran responsabilidad de la demandada, sin que la actora actuase de una forma negligente, hecho este que debía acreditar la entidad demandada, por lo que, en base a lo expuesto en el anterior fundamento de derecho, solo cabe estimar la demanda presentada.

CUARTO: De conformidad con el Art. 1100 y 1108 CC y 576 LEC, la parte demandada deberá abonar el interés legal de la cantidad reclamada desde el 5 de mayo de 2022, fecha que consta en el documento veintidós del escrito de demanda, por ser este en el que consta por primera vez la reclamación a la demandada del importe defraudado, aumentando dicho tipo en dos puntos desde el dictado de la presente sentencia.

QUINTO: En aplicación de lo establecido en el Art. 394 LEC, la parte demandada deberá abonar las costas causadas en el presente proceso.

FALLO

Debo estimar y estimo la demanda interpuesta por la Procuradora Dña. [redacted] en nombre y representación de Dña. [redacted] contra la mercantil Caja Rural Central Sociedad Cooperativa de Crédito, condenando a la misma al pago de 4.985 euros, intereses y costas procesales.

MODO DE IMPUGNACIÓN: mediante recurso de **APELACIÓN** ante la Audiencia Provincial de ALICANTE (artículo 455 LECn).

Así por esta sentencia, lo pronuncio, mando y firmo.

[redacted]