[redacted]
Procuradora dels Tribunals
Tel./ Fax: [redacted]

Advocat: [redacted]
Client: ASSOCIACIÓ ACU-ABAE CATALUNYA
Contrari: BANCO SANTANDER S.A
Autos: [redacted]
Notificat: [redacted]

**CIV - Sección Civil y de Instrucción del TI de Vilanova i la Geltrú. Plaza nº 5 - (Sección Civil. Juzgado de Primera Instancia e Instrucción nº 5 de Vilanova i la Geltrú)**

**Servicio Común de Tramitación de Vilanova. Sección Civil**

Calle Ronda Ibérica, 175, Planta 3 - Vilanova I La Geltrú - C.P.: 08800

TEL.: 936571050
FAX: 936571054
EMAIL:mixt5.vilanovailageltru@xij.gencat.cat

Entidad bancaria BANCO SANTANDER:
Para ingresos en caja. Concepto: 0800000003052724
Pagos por transferencia bancaria: IBAN ES55 0049 3569 9200 0500 1274.
Beneficiario: Servicio Común de Tramitación de Vilanova. Sección Civil
Concepto: 0800000003052724

N.I.G.: 0830742120240253490

**Juicio verbal (250.2) (VRB[redacted]**

**-**

Materia: Juicio verbal (resto de casos)

Parte demandante/ejecutante: ASSOCIACIÓ ACU-ABAE CATALUNYA
Procurador/a: [redacted]
Abogado/a:

Parte demandada/ejecutada: BANCO SANTANDER S.A
Procurador/a: [redacted]
Abogado/a:

# SENTENCIA Nº 49/2026

Vilanova I La Geltrú, 3 de marzo de 2026

Vistos por mí, Don [redacted] Magistrado-Juez de la Sección Civil y de Instrucción del Tribunal de Instancia de Vilanova i la Geltrú, Plaza nº5, los presentes autos de Juicio Verbal nº 527/2024, instados por el Procurador de los Tribunales Sra. [redacted], en nombre y representación de la ASSOCIACIÓ ACU-ABAE CATALUNYA, asistida por el Letrado Sr. [redacted], frente a BANCO DE SANTANDER, S.A., representada por el Procurador de los Tribunales Sr. [redacted] y asistida por el Letrado Sr. [redacted], sobre RECLAMACIÓN DE CANTIDAD POR RESPONSABILIDAD CONTRACTUAL POR INCUMPLIMIENTO DE LAS OBLIGACIONES DE LA ENTIDAD BANCARIA procede dictar la presente resolución en base a los siguientes:

## A N T E C E D E N T E S  D E  H E C H O

***PRIMERO.-*** Por la indicada presentación procesal de la actora se interpuso demanda de juicio ordinario de fecha 16 de julio de 2024 en la que, expuestos los hechos y alegados los fundamentos jurídicos en que basa su pretensión, termina por suplicar del Juzgado se dicte sentencia de conformidad con los pedimentos contenidos en la misma.

***SEGUNDO.-*** Por turnada la anterior demanda, correspondió a este Juzgado, y posteriormente se dictó decreto por el que se admitió a trámite con sus documentos y copias, emplazándose a la parte demandada a fin de que se personase en autos y contestase a la demanda en el término improrrogable de veinte días, trámite que cumplimento presentando escrito de contestación a la demanda el día 17 de julio de 2025.

***TERCERO.-*** En virtud de diligencia de ordenación se convocó a las partes a la vista, celebrándose la misma en el día y hora fijada al efecto, el 2 de marzo de 2026, con el resultado que obra en autos, al cual me remito en aras a la brevedad. Como prueba se admitió exclusivamente la documental y el interrogatorio del actor, [redacted]. Practicada la prueba se dio a las partes la oportunidad de hacer sus respectivas conclusiones y quedaron los autos vistos para Sentencia.

***CUARTO.-*** En la tramitación de este procedimiento se han seguido los preceptos y prescripciones legales.

## F U N D A M E N T O S  D E  D E R E C H O

**PRIMERO**.- **<u>Pretensiones de las partes.</u>**

La parte actora alega en su demanda que, [redacted] era titular de la tarjeta de débito número 5489 0185 0802 8702 del Banco Santander. El día 21 de marzo de 2022 recibió un SMS fraudulento haciéndose pasar por Banco Santander y diciéndole que se había hecho una compra de 800 euros, adjuntándole un enlace para que si no había sido él quien había realizado dicha compra pudiera cancelarla. Tras acceder al enlace los siguientes movimientos con su tarjeta ese día entre las 17:42 y las 17:54 horas: 3 compras de 1.500 euros y una compra de 1.000 euros. El actor considera que la entidad bancaria demandada no ha cumplido debidamente sus obligaciones de custodia respecto de las cuentas bancarias y servicio de banca electrónica y por ello reclama la cuantía total de 5.500 euros, con los intereses legales y las costas del juicio.

La entidad bancaria demandada se opone a la demanda y solicita su desestimación íntegra. Considera que Banco Santander cumplió con sus obligaciones de diligencia, seguridad, autenticación reforzada y registro contable de las operaciones, produciéndose el fraude por la negligencia del actor al haber facilitado sus credenciales a terceros. Además, el actor ni tan siquiera aporta con la demanda los SMS o llamadas que recibió.

**SEGUNDO.- <u>Objeto de la controversia.</u>**

En el acto de la audiencia previa quedaron fijados como puntos de controversia, con la aceptación de las partes, los siguientes.

- Quién es el responsable por los 4 movimientos fraudulentos: el cliente o el banco. Si el responsable es la entidad bancaria por no tener correctos sistemas de seguridad, autenticación y registro contable de las operaciones o si el responsable es el cliente por incumplir los deberes de custodia facilitándole las credenciales a terceros.
- De lo anterior, si la entidad bancaria demandada debe responder por los importes defraudados a través de la técnica delictiva del phising.
- Las costas.

**TERCERO.- <u>Sobre las normativa aplicable a los deberes de custodia de las entidades bancarias.</u>**

El marco normativo aplicable a los deberes de diligencia del banco en la custodia de cuentas bancarias, servicios de pago y banca electrónica se integra por el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, así como la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior y 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.

El citado Real Decreto-ley establece, en su artículo 36.1, el principio esencial de que *"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"*.

Partiendo del principio general del consentimiento del cliente a las operaciones bancarias el núcleo del régimen de responsabilidad por ellas se reparte entre el usuario (artículo 41) y la entidad bancaria (artículo 42).

Así, el artículo 41 del Real Decreto-ley impone al usuario la obligación de tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas y notificar sin demora su extravío o utilización no autorizada cuando recoge que:

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

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

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

Por su parte, el artículo 42 del Real Decreto-ley, de forma paralela, impone al proveedor de servicios de pago, entre otras, la obligación de "cerciorarse de que las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago", "garantizar que en todo momento estén disponibles medios adecuados que permitan al usuario de servicios de pago efectuar una notificación (de extravío o utilización no autorizada)" e "impedir cualquier utilización del instrumento de pago una vez efectuada" dicha notificación cuando dice que:

*"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"*.

Por su parte, la piedra angular del sistema, reside en el artículo 44 del Real Decreto-ley, que regula la prueba de la autenticación y ejecución de las operaciones de pago. Así, su apartado 1º establece de manera taxativa que *"Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago"*. El precepto anterior invierte la carga de la prueba. A continuación el apartado 2º del mismo artículo recoge que *"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"*. Y finalmente el apartado 3º del mismo artículo expresa que *"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"*.

El régimen anteriormente descrito se complementa con los artículos 45 y 46 del del Real Decreto-ley.

El artículo 45 al regular la "responsabilidad del proveedor de servicios de pago en caso de operaciones de pago no autorizadas" ordena al proveedor devolver el importe de la operación no autorizada de inmediato y, a más tardar, al final del día hábil siguiente a su notificación cuando expresa que *"(…) en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine. En 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 (…)"*.

Por su parte, el artículo 46 regula la "responsabilidad del ordenante en caso de operaciones de pago no autorizadas" determinando que *"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"*.

A este marco legal nacional se añade el mandato del 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, cuyo artículo 2 impone a los proveedores de servicios de pago el deber de disponer de *"mecanismos de supervisión de las operaciones que les permitan detectar operaciones de pago no autorizadas o fraudulentas"*. A continuación el mismo artículo recoge que *"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) 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"*.

Esta normativa conforma, por tanto, un sistema de protección del usuario que trasciende la mera comprobación formal de credenciales, imponiendo a la entidad bancaria obligaciones activas de vigilancia y control.

La interpretación y alcance de este régimen de responsabilidad ha sido precisados de manera definitiva por la jurisprudencia del Tribunal Supremo, en concreto por la Sentencia 571/2025 del Tribunal Supremo, Sala Primera, de lo Civil, de 9 de abril de 2025, recurso 1151/2023 la cual ha establecido con claridad que la responsabilidad del proveedor de los servicios de pago, en los casos de operaciones no autorizadas o ejecutadas incorrectamente, tiene carácter cuasi objetivo cuando su fundamento jurídico segundo en su apartado 6º recoge que:

*"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, 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"*.

En síntesis, la responsabilidad cuasi objetiva de la entidad bancaria se manifiesta en en un doble sentido:
- En primer lugar, una vez notificada la operación no autorizada, el proveedor debe responder por ella, salvo que acredite la existencia de fraude del usuario hacia el banco.
- En segundo lugar, cuando el usuario niegue haber autorizado la operación, corresponde al proveedor acreditar no solo su correcta autenticación y registro, sino también "que no se vio afectada por un fallo técnico u otra deficiencia del servicio".

Además, la citada sentencia al definir el concepto de "deficiencia del servicio" precisa que dicho concepto *"no significa error o fallo del sistema informático o electrónico (…), sino que abarca cualquier falta de diligencia o mala praxis en la prestación del servicio"*, subraya, además, que el grado de diligencia exigiblea la entidad bancaria *"no es el propio del buen padre de familia"*, sino que, dada la naturaleza profesional de la actividad y los riesgos que implica, especialmente en una relación empresario-consumidor se le *"obliga a elevar el nivel de diligencia a un plano superior, como es el del ordenado y experto comerciante"* y que esta elevación del estándar de diligencia es fundamental para comprender el alcance de las obligaciones de custodia que pesan sobre la entidad bancaria.

En coherencia con lo anterior, la misma Sentencia concreta las exigencias de dicha diligencia profesional, señalando que *"las buenas prácticas pasan por adoptar las medidas de seguridad necesarias para garantizar el correcto funcionamiento del sistema de servicios de pago"*. Entre ellas, se destacan

específicamente aquellas prácticas *"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"*, poniendo como ejemplos la *"reiteración de transferencias sin solución de continuidad, horario en que se producen, importe de las mismas, destinatarios, antecedentes en el uso de la cuenta"*. Asímismo, menciona las medidas *"dirigidas a incrementar el control y vigilancia cuando se han recibido noticias o alertas de un posible aumento del riesgo"*.

Las distintas Audiencias Provinciales también han perfilado la responsabilidad de la entidad bancaria.

Así, la Sentencia 360/2025 de la Audiencia Provincial de Zaragoza, Sección 4ª, de 16 de septiembre 2025, recurso 116/2024 sobre la diligencia de la entidad bancaria en la detección de anomalías recoge en su fundamento jurídico segundo que:

*"Resulta evidente que los demandantes sufrieron una penetración de delincuentes en su/sus dispositivos, que les permitieron conocer sus claves bancarias y acceder a la Banca electrónica de Ibercaja, así como controlar su teléfono móvil y efectuar las operaciones no autorizadas [...] lo que evidencia* ***la ausencia de los controles automáticos a los que alude el Tribunal Supremo, que hubieran evitado o minimizado el riesgo*** *que, por ignorado, se convirtió en daño efectivo para los demandantes. Y ello lo ha calificado el Tribunal Supremo como* ***falta de diligencia o mala praxis en la prestación del servicio generadora de responsabilidad para la prestadora del servicio*** *(…)".*

Por su parte, la Sentencia 371/2023 de la Audiencia Provincial de Alicante, Sección 9ª, de 23 de junio de 2023, recurso 172/2023 sobre la responsabilidad ante negligencias en la ejecución de las operaciones no autorizadas recoge en su fundamento jurídico segundo que:

*"(…)* ***la intervención de la entidad demandada supone una injerencia negligente en el nexo causal tan determinante que, especialmente en estos***

***supuestos en los que normativamente se predica una especial protección de los usuarios de servicios online, llega a romper la relación de causalidad****, pues de no haberse producido, el daño tampoco.* ***La inicial negligencia de las usuarias del servicio demandantes, hubiera podido ser fácilmente subsanada mediante una actuación diligente de la sucursal****. Es clásica ya la doctrina jurisprudencial que mantiene que el criterio de la prohibición de regreso que justifica negar la imputación del resultado dañoso, tendrá lugar cuando en el proceso causal que desembocó en aquél, puesto en marcha por el posible responsable, se ha incardinado sobrevenidamente la conducta dolosa o gravemente imprudente de un tercero".*

Finalmente, la Sentencia 493/2013 la Audiencia Provincial de Castellón, Sección 3ª, de 19 de diciembre de 2013, recurso 485/2013 también sobre el régimen de responsabilidad por operaciones fraudulentas recoge en su fundamento jurídico segundo que:

"***Salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante (art 32), la responsabilidad será del proveedor del servicio de pago****, lo que supone que a él le corresponde la carga de la prueba de que la orden de pago 'no se vio afectada por un fallo técnico o cualquier otra deficiencia' (art 30).*"

En consecuencia, a la luz de este marco normativo y jurisprudencial, se sintetizan las obligaciones de custodia y diligencia que incumben a las entidades bancarias como proveedoras de servicios de pago en las siguientes:

1. La obligación de garantizar medios de notificación gratuitos y permanentemente accesibles (art. 42.1.c del Real Decreto-ley 19/2018).
2. La obligación de bloquear inmediatamente el instrumento tras una notificación de uso no autorizado (art. 42.1.e del Real Decreto-ley 19/2018).
3. La obligación de implementar y mantener sistemas automatizados de supervisión que analicen el riesgo en tiempo real, considerando el perfil del usuario, el importe, la frecuencia, el horario y otros indicadores anómalos (art. 2 Reglamento Delegado UE 2018/389).

4. La obligación de reaccionar con medidas reforzadas ante cualquier alerta o notificación previa del cliente sobre posibles vulneraciones.
5. La obligación de actuar con la diligencia de un ordenado y experto comerciante, lo que implica una vigilancia activa y proactiva.
6. La obligación de reembolsar de inmediato las cantidades objeto de operaciones no autorizadas, una vez notificadas (art. 45.1 del Real Decreto-ley 19/2018).
7. La obligación probatoria de acreditar, en caso de controversia, la ausencia de deficiencia en el servicio y, en su caso, el fraude o negligencia grave del usuario (art. 44 del Real Decreto-ley 19/2018).

Por tanto, la entidad bancaria en su responsabilidad cuasi objetiva debe adoptar medidas para prevenir que se hagan operaciones fraudulentas en detrimento del cliente y deberá responder por tales operaciones fraudulentas salvo que concurra fraude del consumidor hacia la entidad bancaria o esta demuestre que el usuario actuó incumpliendo deliberamente o con negligencia grave sus obligaciones en relación con sus credenciales de seguridad.

**CUARTO.- <u>Valoración de la prueba practicada y responsabilidad por las operaciones fraudulentas.</u>**

El hecho controvertido fijado en la audiencia previa se centra, de un lado, en determinar si la entidad bancaria Banco Santander cumplió los deberes de diligencia que le eran exigibles en la prestación del servicio de banca electrónica, y, de otro, si el actor incurrió en conducta fraudulenta o negligencia grave al facilitar a terceros sus credenciales, así como, en consecuencia, a quién corresponde la responsabilidad por los 4 movimientos fraudulentos ejecutados el día 21 de marzo de 2022, por un importe total de 5.500 euros.

En el acto del juicio se practicó el interrogatorio del actor, quien manifestó que el día 21 de marzo de 2022 recibió SMS con enlaces sobre las 15 horas y se le enlazaba a una web en la que le pedían la clave de acceso y la firma electrónica. Su número de teléfono es el 639970232. Cree que no le pidieron

nada más. No notó ese día problemas en su línea telefónica y tenía con él su teléfono móvil. A las horas su mujer recibió una llamada supuestamente de Banco Santander. Los SMS los tenía en su móvil y los mostró a los Mossos d'Esquadra al denunciar los hechos. Los SMS decían que se le había hecho un cobro de 499 euros y que si no era él que clicase en el enlace. No ha sido llamado por ningún Juzgado de Instrucción para declarar sobre los hechos. No facilitó datos bancarios a nadie. Además, de denunciar puso una reclamación en Banco Santander y le explicaron que ellos no le habían llamado y que habían usado un teléfono espejo haciéndose pasar por Banco Santander.

En cuanto a la documental obrante en autos cabe comenzar manifestando que por la parte actora no se han presentado los sms que recibió ni el registro de llamadas de su teléfono móvil siendo cierto que debía haberlos aportados con arreglo a los principios de distribución de la carga de la prueba del artículo 217.2 de la Ley de Enjuiciamiento Civil ya que tenía la facilidad y disponibilidad probatoria para ello. Por más que el perjudicado manifieste que los mostró a los Mossos d'Esquadra, ni se adjuntaron a la denuncia, ni tal circunstancia consta en ella, pero en todo caso, eso no eximía a la parte actora de presentarlos en este juicio.

Sin embargo, en el presente caso, la prueba más relevante es la propia documental aportada por el banco, que como se verá a continuación es la que perjudica precisamente a la entidad bancaria demandada.

Así, la entidad bancaria ha aportado documentación que acredita que la secuencia técnica de las operaciones fue del siguiente modo:
- A las 17:36:56 del día del fraude se mandó por SMS un código OTP para registrar un nuevo dispositivo, emitiéndose una notificación push a las 17:38:25 horas. Es cierto que el número de móvil era el del actor 639970232. La IP de la notificación push era 31.4.241.67.
- A las 17:40:34 y a las 17:41:04 horas se enviaron al móvil del actor (639970232) dos SMS con códigos OTP para la consulta del PIN de la tarjeta de crédito.

- A las 17:48:12 horas se recibió notificación *push* informando del cambio de límite de la tarjeta asociadas a la cuenta. Se utilizó para esta notificación la IP de la notificación push era 31.4.241.67.

Sin embargo, la entidad demandada a pesar de aportar el registro del envío de los SMS con códigos OTP para la gestión del alta del dispositivo y del cambio del PIN de la tarjeta no ha aportado registro alguno que acredite el envío de los correspondientes códigos de un solo uso (OTP) para la autenticación de cada una de las cuatro compras individuales realizadas entre las 17:42 y las 17:54 horas.

Conforme al artículo 44 del Real Decreto-ley 19/2018, correspondía al proveedor de servicios de pago demostrar que la totalidad de las operaciones de pago fueron autenticadas, registradas con exactitud y contabilizadas. Al no aportar los registros de los SMS OTP supuestamente enviados para autorizar cada compra, la entidad no solo incumple la carga probatoria que legalmente le incumbe, sino que impide a este tribunal verificar si el sistema de doble autenticación funcionó correctamente en cada una de las transacciones fraudulentas o si, por el contrario, una vez alterados los límites de las tarjetas, las compras se cursaron sin las exigidas medidas de seguridad reforzada, lo que constituiría una deficiencia adicional del servicio. Esta laguna probatoria debe ser interpretada, en aplicación del principio de facilidad probatoria arículo 217.7 de la Ley de Enjuiciamiento Civil y de la regla de la carga de la prueba, en perjuicio de la parte que disponía de tales registros y ha omitido su aportación, confirmando así la falta de diligencia del banco en la custodia de la cuenta de su cliente.

La cronología en el fraude descrita anteriormente no resulta suficiente para enervar la pretensión del actor sino que más bien su análisis evidencia precisamente la falta de diligencia debida por la entidad bancaria

Así, en cuanto al proceso de alta de dispositivo la entidad bancaria certifica que el alta del dispositivo desde el que se cometió el fraude se produjo desde la dirección IP 31.4.241.67. Si se consulta en cualquier página web sobre

geolocalización de IP's (hecho notorio), como por ejemplo https://www.geolocation.com/, resulta que tal IP está geolocalizada en Vielha. Este dato contrasta frontalmente con el domicilio del actor sito en Vilanova i la Geltrú como se puede observar en la denuncia (documento 5 de la demanda). Un sistema de supervisión de operaciones configurado con la diligencia de un "ordenado y experto comerciante" (véase la Sentencia 571/2025 del Tribunal Supremo, Sala Primera, de lo Civil, de 9 de abril de 2025, recurso 1151/2023 anteriormente citada) debería haber detectado esta incongruencia como un factor de riesgo significativo. Así, nos hallamos ante una operación que supuestamente se habría llevado a cabo desde una localidad a 277 km del domicilio del demandante sin relación con el perfil habitual del cliente. La ausencia de una alerta o bloqueo ante este hecho puede ser considerada como una falta de diligencia inexcusable.

Por otro lado, también concurre una falta de control en la escalada del fraude ya que una vez que se superó el primer filtro (el alta anómala del dispositivo), el sistema bancario permitió que, en un lapso de tiempo extraordinariamente breve (entre las 17:42 y las 17:54 horas), se realizaran hasta 4 compras por un importe considerablemente elevado, un total de 5.500 euros, en un mismo comercio (compra en El Corte Inglés por internet). De hecho, llaman la atención los elevados importes de las operaciones de 1.000 y 1.500 euros y que se repitan los importes en tres de las operaciones, siendo unos importes de cifras muy redondas. La Sentencia 571/2025 del Tribunal Supremo, Sala Primera, de lo Civil, de 9 de abril de 2025, recurso 1151/2023 anteriormente citada es muy clara al señalar que las buenas prácticas exigen medidas orientadas a detectar de forma automática "la reiteración de transferencias sin solución de continuidad" o el "importe de las mismas". En este caso, se produjeron múltiples operaciones en menos de 15 minutos que eran ciertamente sospechosas por su reiteración y cifras. Un sistema diligente debería haber activado, como mínimo, una alerta o bloqueo temporal de seguridad ante un patrón de gasto tan inusual y concentrado en el tiempo, máxime cuando se realizaba desde un dispositivo recién dado de alta en circunstancias geográficas anómalas. La pasividad del sistema permitió la consumación íntegra del fraude.

Sobre la falta de aportación de los SMS con los códigos OTP para las 4 compras por el banco  cabe remarcar nuevamente que conforme al artículo 44 del Real Decreto-ley 19/2018, correspondía al proveedor de servicios de pago demostrar que la totalidad de las operaciones de pago fueron autenticadas. Al no aportar los registros de los SMS con los códigos OTP supuestamente enviados para autorizar cada compra, la entidad no solo incumple la carga probatoria que legalmente le incumbe, sino que impide a este Juzgador verificar si el sistema de doble autenticación funcionó correctamente en cada una de las transacciones fraudulentas o si, por el contrario, una vez alterados los límites de las tarjetas, las compras se cursaron sin las exigidas medidas de seguridad reforzada, lo que constituiría una deficiencia adicional del servicio.

Por lo que respecta a la falta de aportación por el actor de los SMS que se usaron en el mecanismo de *phishing* ello no resulta relevante en el presente litigio. Así, debe decirse que la carga de probar la autorización de las 4 operaciones fraudulentas y de la diligencia del servicio corresponde a la entidad bancaria (artículo 44 del Real Decreto-ley 19/2018). Por otro lado, la propia documental bancaria acredita el hecho nuclear del fraude ya que la operativa se realizó desde una dirección IP extraña al domicilio del actor y se dio un dispositivo de alta en el mismo día del fraude, lo que constituye una anomalía que un sistema diligente debió detectar con independencia de los medios concretos (SMS, llamadas desde teléfono “espejo” o páginas webs simuladas) el tercero (*phisher*) hubiera obtenido las credenciales.

De lo anteriormente expuesto, puede llegarse a la conclusión de que la entidad bancaria no ha logrado probar que su servicio no se vio afectado por una deficiencia. Por el contrario, la prueba por ella misma aportada demuestra que su sistema de seguridad no reaccionó ante indicios claros de fraude (añta de dispositivo el día del fraude, geolocalización IP incompatible con el domicilio del cliente, operativa masiva en minutos) incumpliendo así las obligaciones de supervisión activa y control de riesgos impuestas por el artículo 2 del

Reglamento Delegado (UE) 2018/389 y la jurisprudencia del Tribunal Supremo en los términos ya descritos.

Una vez establecida esa deficiencia del servicio bancario, procede analizar si el banco ha conseguido probar, como le exige el artículo 44.3 del Real Decreto-ley 19/2018, que el actor incurrió en negligencia grave en la custodia de sus credenciales.

Este Juzgador considera que el solo hecho de que el actor introdujera sus claves en un enlace fraudulento no puede ser reputado como una circuntancia que exonere al banco de su responsabilidad. Ello, se debe a que dicha posible negligencia del usuario debe ponerse en contexto de las obligaciones de seguridad del banco, que son primarias y más exigentes.

Así, pese a ser cierto que el artículo 41 del Real Decreto-ley 19/2018 impone al usuario la obligación de adoptar "medidas razonables" para proteger sus credencialesla Jurisprudencia del Tribunal Supremo ha fijado un listón muy alto para apreciar la concurrencia de la "negligencia grave". De este modo, no cualquier descuido del usuario merece la calificación de negligencia grave, especialmente cuando el fraude se comete mediante técnicas de cibercriminalidad avanzada (como el *phishing*), de carácter muy sofisticado y difíciles de distinguir para un usuario medio.

En el presente caso, la negligencia del banco en sus deberes de seguridad y sistemas de alertas fue determinante de que se cometieran las operaciones fraudulentas. De hecho, el fraude no pudo consumarse por la mera introducción de las claves por el actor en la página web simulada, sino porque el sistema bancario falló claramente en su deber de supervisión. Como señala la la Sentencia 371/2023 de la Audiencia Provincial de Alicante, Sección 9ª, de 23 de junio de 2023, recurso 172/2023 *"(…)* ***la intervención de la entidad demandada supone una injerencia negligente en el nexo causal tan determinante que, especialmente en estos supuestos en los que normativamente se predica una especial protección de los usuarios de***

***servicios online, llega a romper la relación de causalidad****, pues de no haberse producido, el daño tampoco.* ***La inicial negligencia de las usuarias del servicio demandantes, hubiera podido ser fácilmente subsanada mediante una actuación diligente de la sucursal****.* La negligencia inicial del usuario podría haber sido fácilmente subsanada mediante una actuación diligente de la entidad bancaria en sus deberes de supervisión y alerta.

Dicho de otro modo si el banco hubiera actuado con la diligencia exigible, desplegando medidas antifraude ante las operaciones anómalas tales como el bloqueo de la operativa o alertando al usuario, el daño no se habría producido, independientemente de que el actor hubiera "picado" inicialmente en el *phishing*. Por lo tanto, la conducta del actor, aunque imprudente, no alcanza el grado de "negligencia grave" necesario para romper el nexo de causalidad y exonerar al banco, cuya responsabilidad es, cuasi-objetiva como expone la Jurisprudencia sobradamente expuesta.

En consecuencia, al no haber acreditado la entidad bancaria demandada la concurrencia de negligencia grave del actor, y al haber quedado probado, con la documental que ella misma aportó, que su servicio adoleció de una deficiencia en los mecanismos de supervisión y control de operaciones anómalasla debe declararse la responsabilidad de la entidad bancaria demandada por las cuatro operaciones fraudulentas de conformidad con lo dispuesto en el artículo 45 del Real Decreto-ley 19/2018.

Por todo ello, procede estimar íntegramente la demanda y condenar a la entidad bancaria demandada a satisfacer al actor la cantidad de 5.500 euros.

**QUINTO.- <u>Intereses.</u>**

La cantidad por la que se estima la demanda (5.500 euros) devengará los intereses de los artículos 1100 y 1108 del Código Civil desde la primera reclamación fehaciente (reclamación a Banco Santander de 23 de marzo de

2022, documento 6 de la demanda) y los intereses del artículo 576 de la Ley de Enjuiciamiento Civil desde que se dicta esta resolución.

**SEXTO.- Recursos.**

Conforme al artículo 455 y siguientes de la Ley de Enjuiciamiento Civil, frente a la sentencia dictada en el presente procedimiento cabe interponer **recurso de apelación**.

**SÉPTIMO.- Costas.**

Habiéndose estimado íntegramente la demanda procede imponer las costas a la parte demandada en virtud del artículo 394 de la Ley de Enjuiciamiento Civil y del principio de vencimiento del pleito (*victus victori in expensis est condemnandus*).

Vistos los artículos citados y demás de general y pertinente aplicación,

## F A L L O

SE ESTIMA ÍNTEGRAMENTE la demanda interpuesta por el Procurador Sra. Arbonés Ojeda, en nombre y representación de la ASSOCIACIÓ ACU-ABAE CATALUNYA contra BANCO DE SANTANDER, S.A. y se condena a BANCO DE SANTANDER, S.A. a pagar a D. JULIÁN [redacted] la cantidad de 5.500 euros con los intereses del fundamento jurídico quinto de esta resolución.

Se imponen a la demandada las costas del presente proceso.

Notifíquese esta resolución a las partes haciéndoles saber que contra esta resolución cabe recurso de apelación que se interpondrá ante este mismo Juzgado en el plazo de VEINTE DÍAS a contar del siguiente a su notificación y será resuelto por la Ilma. Audiencia Provincial de Barcelona. De conformidad con la Disposición Adicional 5ª LOPJ, modificada por la LO 1/2009, de 3 de noviembre, es preciso que, con carácter previo a la admisión del recurso, se consigne en la Cuenta de Consignaciones y Depósitos del Juzgado la cantidad de 50 euros en concepto de depósito para recurrir.

Además, deberá autoliquidarse la tasa correspondiente si el procedimiento así lo exige.

Líbrese testimonio de la presente sentencia que se unirá a los presentes autos, quedando el original en el libro de sentencias de este Juzgado.

Así, por esta mi Sentencia, la pronuncio, mando y firmo.

**PUBLICACIÓN.-** Leída y publicada ha sido la anterior sentencia por el Magistrado-Juez Don [redacted] de la Sección Civil y de Instrucción del Tribunal de Instancia de Vilanova i la Geltrú, Plaza nº5, de lo que como Letrada de la Administración de Justicia certifico.

Lo acuerdo y firmo.
El Magistrado

Puede consultar el estado de su expediente en el área privada de seujudicial.gencat.cat

Los interesados quedan informados de que sus datos personales han sido incorporados al fichero de asuntos de esta Oficina Judicial, donde se conservarán con carácter de confidencial, bajo la salvaguarda y responsabilidad de la misma, dónde serán tratados con la máxima diligencia.

Quedan informados de que los datos contenidos en estos documentos son reservados o confidenciales y que el tratamiento que pueda hacerse de los mismos, queda sometido a la legalidad vigente.

Los datos personales que las partes conozcan a través del proceso deberán ser tratados por éstas de conformidad con la normativa general de protección de datos. Esta obligación incumbe a los profesionales que representan y asisten a las partes, así como a cualquier otro que intervenga en el procedimiento.

El uso ilegítimo de los mismos, podrá dar lugar a las responsabilidades establecidas legalmente.

En relación con el tratamiento de datos con fines jurisdiccionales, los derechos de información, acceso, rectificación, supresión, oposición y limitación se tramitarán conforme a las normas que resulten de aplicación en el proceso en que los datos fueron recabados. Estos derechos deberán ejercitarse ante el órgano judicial u oficina judicial en el que se tramita el procedimiento, y las peticiones deberán resolverse por quien tenga la competencia atribuida en la normativa orgánica y procesal.

Todo ello conforme a lo previsto en el Reglamento EU 2016/679 del Parlamento Europeo y del Consejo, en la Ley Orgánica 3/2018, de 6 de diciembre, de protección de datos personales y garantía de los derechos digitales y en el Capítulo I Bis, del Título III del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.