SENTENCIA: 00139/2025

Modelo: N30090 SENTENCIA JUICIO VERBAL UN SOLO MAGISTRADO

PLAZA CONCEPCIÓN ARENAL, Nº 1, 4ª PLANTA

32003 OURENSE

-Teléfono: 988 687057/58/59/60 Fax: 988 687063

Correo electrónico: seccion1.ap.ourense@xustiza.gal

Equipo/usuario: ML

N.I.G. 32054 42 1 2023 0007771

ROLLO: RPL RECURSO DE APELACION (LECN) 0000633 /2024

Juzgado de procedencia: XDO. PRIMEIRA INSTANCIA N.7 de OURENSE

Procedimiento de origen: JVB JUICIO VERBAL 0001105 /2023

Recurrente: BANCO SANTANDER SA

Procurador: [redacted]

Recurrido: [redacted]

Procurador: [redacted]

APELACIÓN CIVIL

La Audiencia Provincial de Ourense, constituida por la Sra. magistrada Dña. Ángela Domínguez-Viguera Fernández, presidenta, ha pronunciado, en nombre de S.M. El Rey, la siguiente

S E N T E N C I A NÚM. 139/2025

En la ciudad de Ourense a veinticuatro de febrero de dos mil veinticinco.

VISTOS, en grado de apelación, por esta Audiencia Provincial, actuando como Tribunal Civil, los autos de juicio verbal n.º 1105/2023 procedentes del Juzgado de Primera Instancia n.º 7 de Ourense, rollo de apelación n.º 633/24, entre partes, como apelante, Banco Santander SA, representada por la procuradora [redacted]

[redacted], y, como apelado, [redacted], representado por la procuradora [redacted].

I - ANTECEDENTES DE HECHO

Primero.- Por el Juzgado de Primera Instancia n.º 7 de Ourense, se dictó sentencia en los referidos autos, en fecha 10 de junio de 2024, cuya parte dispositiva es del tenor literal siguiente: "FALLO: Que DEBO ESTIMAR Y ESTIMO ÍNTEGRAMENTE la demanda interpuesta por la Procuradora [redacted], en nombre y representación de [redacted] contra BANCO SANTANDER, S.A. y, en consecuencia, se declara que la entidad Banco Santander ha incumplido el contrato de cuenta bancaria n.º [redacted], en relación a la ejecución de operaciones por tercero no autorizado, CON CONDENA a la parte demandada a satisfacer a la actora la cantidad de 4.299,49, importe que se incrementará

con los intereses legales devengados desde la fecha de su anotación en cuenta, todo ello con condena en costas a la parte demandada".

Segundo.- Notificada la anterior sentencia a las partes, se interpuso por la representación procesal de Banco Santander SA recurso de apelación en ambos efectos habiendo formulado oposición al mismo la representación procesal de [redacted], y seguido por sus trámites legales, se remitieron los autos a esta Audiencia Provincial para su resolución.

Tercero.- En la tramitación de este recurso se han cumplido las correspondientes prescripciones legales.

Se acepta la fundamentación jurídica de la sentencia apelada en tanto no contradiga lo expuesto a continuación.

II - FUNDAMENTOS DE DERECHO

Primero. - Como se expone en la sentencia apelada, se ejercitó en la demanda acción de responsabilidad civil frente a la entidad bancaria demandada con fundamento en los artículos 43-1º y 45 del Real Decreto Ley 19/2018, de 23 de noviembre, que regula los servicios de pago y otras medidas urgentes en materia financiera, con el argumento de haberse realizado distintos cargos no autorizados por el demandante en cuenta corriente de su titularidad, por parte de terceras personas no identificadas, desde el extranjero y de modo fraudulento.

El demandante alegó que no había infringido el deber de custodia de sus claves y credenciales bancarias, ni incurrido en conducta negligente o fraudulenta.

La entidad bancaria se había opuesto a la viabilidad de la demanda, alegando que, necesariamente, debía haber mediado negligencia o incumplimiento de las obligaciones impuestas en el artículo 41 a) del Real Decreto Ley 19/2018 al titular de la cuenta, pues teniéndose por acreditada la intervención fraudulenta de un tercero, sostiene que los adeudos controvertidos en la cuenta del actor sólo pudieron producirse por infracción del deber de custodia, que le obligaba a mantener a buen recaudo sus credenciales bancarias de seguridad de modo que no pudieran ser conocidas por un tercero.

La parte demandada apelante alega que debe tenerse por probada la negligencia grave del usuario a consecuencia de la realización de los cargos controvertidos en su cuenta bancaria, lo cual, y a su juicio, sólo habría podido tener lugar obteniendo el defraudador las credenciales de seguridad necesarias para la realización de tales cargos, y con tal fundamento sostiene en su recurso que la juzgadora de instancia incurrió en error al valorar la prueba e infracción de lo dispuesto en el artículo 217 LEC.

Segundo.- El motivo de recurso no se estima, al haber efectuado la juzgadora de instancia una correcta valoración de la prueba practicada.

Ha resultado acreditado y no cuestionado por la entidad demandada, que durante el período comprendido entre el 8 y el 22 de septiembre de 2022, se efectuaron diversos cargos fraudulentos y no autorizados por el demandante en la cuenta corriente bancaria de su titularidad, abierta en la entidad demandada mediante un contrato de cuenta corriente y depósito en su día concertado. La apertura de dicha cuenta bancaria tenía asociada la utilización de una tarjeta de crédito, como servicio de pago (producto 4B Master). Durante el período indicado, se realizaron numerosas compras en distintos

establecimientos comerciales de la ciudad de París, ciudad a la que no se había desplazado el actor en esas fechas. Todas las compras realizadas, en su mayoría en forma presencial, fueron efectuadas mediante tal medio de pago electrónico y cargadas en la cuenta del actor abierta en la entidad demandada. Tan pronto como el demandante advirtió la realización de tales disposiciones bancarias no autorizadas, presentó denuncia ante las dependencias policiales, en 27 de septiembre de 2022 (pocos días después) poniendo en conocimiento de la entidad bancaria tales hechos.

El demandante no había facilitado sus claves o credenciales bancarias a persona alguna, o, cuando menos, no resultó probado, ni había sido víctima de ninguna sustracción de la tarjeta o de sus claves bancarias, ni había detectado en su teléfono móvil signos de jaqueo. La mayoría de las operaciones fueron realizadas en forma presencial desde París (Francia) como se expuso, a donde nunca se había desplazado el actor, el cual tampoco era titular de un teléfono de la marca Apple, como se probó, compatible con la aplicación de pago Apple Pay, utilizada para realizar algunas de las operaciones no autorizadas desde el país extranjero, lo que excluye cualquier actuación fraudulenta por parte del actor.

Ni se ha acreditado que hubiese incurrido en cualquier clase de negligencia mediante el extravío de sus claves bancarias, por lo que, como bien argumenta la sentencia apelada, todo apunta a una clonación de tarjeta o captura de claves o contraseñas a través de hackers, lo que pone de manifiesto el fallo de las medidas de seguridad y control que incumbía adoptar al proveedor de los servicios de pago, y en modo alguno negligencia por parte del usuario. Siendo diversos los modos empleados para realizar este tipo de fraudes (clonación de tarjetas, pharming o introducirse en un servidor a través de hackers capturando claves o contraseñas).

La probada realidad de una operación fraudulenta de la que fue víctima el demandante, con falta absoluta de consentimiento del titular de la cuenta en relación a tales disposiciones bancarias, conduce a su nulidad de pleno derecho conforme a lo dispuesto en el artículo 1261 del Código Civil.

A la misma conclusión conduce la responsabilidad que deriva del contrato de depósito bancario "con la consecuencia prevista en el art. 307.3 del Código de Comercio, según la cual, al quedar el dinero depositado confundido con el patrimonio del depositario, éste ha de soportar los riesgos derivados de su deber de conservar la cosa depositada".

Como ha reiterado la jurisprudencia "hay responsabilidad bancaria por los defectos de seguridad del sistema que determina la ejecución de órdenes de pago no autorizadas por su cliente, con la única excepción de que el banco acredite la culpa o negligencia de la víctima."

Tercero.- Para el caso de que aquella verificación se realice a través de medios técnicos, la entidad bancaria habrá de asegurarse que estos son lo suficientemente adecuados y seguros para efectuarla sin error, y en caso de que no sea así y exista un defecto de seguridad o se muestren de cualquiera manera insuficientes, habrá de responder de los daños que se originen al cliente de la entidad, pues es aquella entidad la que ha hecho uso de unos medios que se demostraron ineficaces para cumplir su obligación de verificación.

- Esta responsabilidad debe ser, por tanto, cuasi objetiva, excluible únicamente en supuestos de dolo o culpa imputable a la víctima. De esta manera, la exclusión no puede basarse simplemente en la utilización de un sistema que cumpla con los estándares mínimos de seguridad exigidos, sino únicamente en un actuar doloso o (gravemente) negligente del usuario de los servicios de pago.

- Debe tenerse en cuenta asimismo que estos mecanismos de pago (tanto por medio de tarjetas, como a través de la banca a distancia o digital) no sólo los articula la entidad financiera a través de las correspondientes aplicaciones y software, sino que potencia su utilización por sus clientes y usuarios bancarios (en tanto la misma se beneficia de la extensión generalizada de estos servicios online, al evitar costes asociados a la atención de sus clientes), por lo que tiene -y debe- implementar todas las medidas de seguridad necesarias para evitar fraudes, incluida la suplantación de identidad y si el fraude es externo, es decir a través de estafas informáticas, lo único que puede exigirse al usuario es que el dispositivo que utilice para la realización de este tipo de operaciones tenga un mantenimiento (razonable) de seguridad."

- Es la entidad bancaria quien dispone los medios técnicos necesarios para la verificación de la identidad del cliente, por lo que hacer recaer en este último los riesgos de un fallo del sistema o la falta de adaptación de éste a las técnicas defraudatorias más modernas produciría no sólo una injusticia palmaria, sino también un efecto económico y técnico adverso, consistente en el estancamiento de las medidas de seguridad.

- Es evidente que si, quien dispone de los medios técnicos de seguridad y tiene la capacidad para mejorar el sistema, únicamente tiene que cumplir con un estándar mínimo y no responde de los fallos sobrevenidos del mismo, la consecuencia ineludible será un desfase del sistema y una precarización de la situación de los usuarios de los sistemas de banca electrónica, únicamente evitable atribuyéndole a las entidades bancarias la responsabilidad activa de velar por la seguridad de las operaciones y mejorar constantemente sus sistemas de verificación y seguridad; lo que, en fin, sólo se puede conseguir atribuyéndoles responsabilidad para el caso de que éstos fallen o se demuestren ineficientes.

- A esta concepción responde el reciente Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que transpone al ordenamiento jurídico español la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, derogando la anterior Ley 16/2009, de 13 de noviembre, de servicios de pago.

- Señala el art. 36.1 de esta norma que "las operaciones de pago se considerarán autorizadas cuando el ordenante haya dado el consentimiento para su ejecución" y que "a falta de tal consentimiento la operación de pago se considerará no autorizada."

- Este precepto ha de ponerse en relación con el art. 44 que, referido a la prueba de la autenticación y ejecución de las operaciones de pago, dispone que:

"1. Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, corresponderá al proveedor de servicios de pago demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago.

2. A los efectos de lo establecido en el apartado anterior, el registro por el proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, de la utilización del instrumento de pago no bastará, necesariamente, para demostrar que la operación de 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."

Estas obligaciones del usuario de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizadas, a que se refiere el art. 41 del RD-Ley, son:

a) utilizar 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, tomar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas; y

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

- El régimen establecido por estos preceptos se completa con los arts. 43, 45 y 46 del mismo cuerpo legal:

Art. 43. Notificación y rectificación de operaciones de pago no autorizadas o ejecutadas incorrectamente.

"1. El usuario de servicios de pago obtendrá la rectificación por parte del proveedor de servicios de pago de una operación de pago no autorizada o ejecutada incorrectamente únicamente si el usuario de servicios de pago se lo comunica sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones que sea objeto de reclamación, incluso las cubiertas por el artículo 60, y, en todo caso, dentro de un plazo máximo de trece meses contados desde la fecha del adeudo."

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."

"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."

"Responsabilidad cuasi objetiva de la entidad bancaria, que ya se venía reconociendo en base a la anterior Ley de Servicios de Pago de 2009....

- El nuevo texto normativo, no hace sino reforzar este sistema de responsabilidad cuasi objetiva, como corrobora la aplicación del mismo por la jurisprudencia más reciente de las Audiencias Provinciales. En este sentido, pueden citarse las SSAP de Madrid núm. 184/2022, de 20 de mayo, y núm. 24/2023, de 13 de enero;

la SAP de Zaragoza núm. 804/2022, de 1 de julio; la SAP de Cantabria núm. 679/2022, de 19 de septiembre; o la SAP de Valladolid núm. 689/2022, de 19 de octubre, entre otras.

- La responsabilidad del proveedor de servicios de pago será excluible únicamente cuando el usuario de los servicios haya actuado fraudulentamente o haya incumplido, deliberadamente o por negligencia grave, una o varias de sus obligaciones en relación con los instrumentos de pago y las credenciales de seguridad personalizadas. En caso contrario, y siempre que el usuario lo comunique sin demora injustificada, el proveedor de los servicios de pago habrá de rectificar la operación no autorizada y devolver al usuario el importe de la misma.

- Asimismo, corresponde a la entidad financiera la prueba, por un lado, de que las operaciones de pago fueron correctamente autenticadas, registradas con exactitud y contabilizadas, y que no se vieron afectadas por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago; y, por otro lado, que el ordenante actuó de manera fraudulenta, o incumpliendo deliberadamente o por negligencia grave alguna de las obligaciones; sin que el registro por el proveedor de servicios de pago baste 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."

La postura mayoritaria de las Audiencias Provinciales en torno a la responsabilidad de las entidades bancarias ante fraudes conocidos como phising, en interpretación del artículo 41 y ss. del Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, han apreciado una responsabilidad cuasi-objetiva de la entidad bancaria que presta servicios de pago que tan solo cesa si acredita que el cliente actuó fraudulentamente o con negligencia grave a la hora de aplicar los medios razonables de protección de seguridad personalizados de que haya sido provisto, o en el caso de que no haya comunicado a la entidad el pago no autorizado en cuanto tenga conocimiento del mismo. Ello implica, además, que la carga de la prueba de esas circunstancias exoneratorias y la paralela inexigibilidad de otra conducta incumba a la entidad. En este sentido se pronuncian, entre otras muchas, las SSAP Cádiz (Sec. 2ª) núm. 473/2023, de 23 de noviembre; Huelva (Sec. 2ª) núm. 643/2023, de 16 de octubre; Pontevedra (Sec. 3ª) núm. 447/2023, de 18 de septiembre; Oviedo (Sec. 5ª) núm. 236/2023, de 22 de junio; Cuenca núm. 125/2023, de 16 de mayo; Zaragoza (Sec. 4ª) núm.

117/2023, de 10 de marzo; La Rioja núm. 49/2023, de 17 de febrero; Madrid (Sec. 10ª) núm. 24/2023, de 13 de enero; Almería (Sec. 1ª) núm. 99/2023, de 31 de enero; Jaén (Sec. 1ª) núm. 1355/2022, de 14 de diciembre; Madrid (Sec. 11ª) núm. 74/2022, de 28 de febrero; Bizcaia (Sec. 3ª) núm. 429/2016, de 10 de noviembre, que cita la SAP de Madrid (Sec. 9ª) núm. 178/2015, de 4 de mayo 2015, entre otras.

Consideraciones que conducen a la íntegra confirmación de la sentencia apelada.

Cuarto.- Dada la íntegra desestimación del recurso de apelación interpuesto, las costas de la alzada han de imponerse a la parte apelante.

Procede decretar la pérdida del depósito constituido para apelar.

Por lo expuesto la Sección Primera de la Audiencia Provincial pronuncia el siguiente

FALLO

:

Se desestima el recurso de apelación interpuesto por la representación procesal de Banco Santander SA contra la sentencia dictada el 10 de junio de 2024 por el Juzgado de Primera Instancia n.º 7 de Ourense en autos de juicio verbal n.º 1105/2023 -rollo de Sala n.º 633/2024-, cuya resolución se confirma, con imposición de las costas del recurso a la parte apelante.

Se decreta la pérdida del depósito constituido para apelar al cual se dará el oportuno destino legal.

La presente resolución es firme y contra la misma no cabe recurso alguno.