

DERECHO BANCARIO

La banca deberá asumir las pérdidas por fraudes digitales sufridos por sus clientes, incluso con autenticación reforzada

[TS, Sala de lo Civil, Sección 1ª, de 9 de abril de 2025, STS: 1671/2025, Recurso: 1151/2023](#)
[Ponente: Excmo. Sr. D. Manuel Almenar Belenguer.](#)

Antecedentes – Formulación de la pretensión y contestación – Doctrina sobre la responsabilidad del proveedor de servicios de pago en operaciones no autorizadas (sinopsis de Fernando Zunzunegui y María Jesús Sánchez-Cabezudo Tovar)

Antecedentes: “[...] D. Martin es titular [...] de la cuenta corriente y/o depósito [...] en la entidad Unicaja Banco S.A. [...] [E]l 24 de febrero de 2021 [...] D. Martin recibió un aviso de Google, en el que se le informaba que se había detectado una vulneración de su cuenta de correo electrónico @gmail, comprobándose un acceso no autorizado, ante lo cual, minutos después y como medida de prevención [...] **procedió al cambio de contraseña de la cuenta de correo.** [...] El mismo 24 de febrero, D. Martin recibió en su teléfono móvil, varios mensajes SMS con códigos para la materialización a través del sistema digital de transferencias que no obedecían a órdenes emitidas por él, **lo que puso en conocimiento del personal de la sucursal del banco.** En fechas 27 de febrero y 2 y 12 de marzo de 2021, Google Play y Google Ads realizaron varios cargos no autorizados en la cuenta [...], lo que **D. Martin comunicó a la entidad bancaria, reiterando su preocupación por los SMS recibidos,** al tiempo que presentaba la pertinente reclamación a Google, que la rechazó el 15 de marzo, al no haber podido confirmar que se hubiera producido algún tipo de actividad fraudulenta. [...] El 16 de marzo, [...] recibió un email de Google en su dirección de correo de @gmail con el siguiente mensaje: «Alerta de seguridad crítica, se ha bloqueado un intento de inicio de sesión. Alguien acaba de usar tu contraseña para intentar iniciar sesión en tu cuenta». Inmediatamente, procedió a cambiar la contraseña, y, al día siguiente, 17 de marzo, **el actor acudió a la oficina bancaria, donde informó sobre lo sucedido y solicitó la cancelación de la tarjeta y la emisión de otra nueva.** [...] Entre la noche del 17 y la mañana del 18 de marzo de 2021 se realizaron quince transferencias bancarias [...]. **La mayoría de las mencionadas transferencias se efectuaron a favor de delincuentes conocidos por la Policía [...].** El demandante no supo lo sucedido hasta la mañana del día 18 de marzo, cuando el personal de la sucursal, alertado por una llamada del personal del Banco Santander S.A., que había detectado el ingreso realizado en una cuenta sospechosa, le preguntó si durante la noche había hecho transferencias por valor de 83.000 €, a lo que respondió que no. Al acceder a la banca electrónica y comprobar la realidad de la información, **el mismo día 18 presentó la correspondiente denuncia en la comisaría de la Policía Nacional, lo que motivó la incoación de las diligencias previas n.º 1017/21021 por el Juzgado de Instrucción n.º 11 de Zaragoza.** En atención a la reclamación del actor, Ibercaja Banco S.A. solicitó la restitución de las cantidades dispuestas a las distintas entidades de destino, consiguiendo la devolución de 27.218,10 €, que fueron reintegrados al actor. En el presente procedimiento y con base en los mencionados hechos, D. Martin ejercita una acción de **responsabilidad contractual frente a Ibercaja Banco S.A** [...] por los daños y perjuicios causados por el incumplimiento de las obligaciones asumidas por la demandada en el contrato de banca a distancia y en el contrato de cuenta corriente y/o depósito. [...] La demandada Ibercaja Banco S.A. se opone a la demanda y solicita su desestimación. Alega que [...] **todas las transferencias realizadas cumplen las exigencias impuestas en la normativa aplicable** [...] de servicios de pago, [...] ya que se ejecutaron con **identificación correcta del titular o usuario de las cuentas de origen y empleo de un doble factor de autenticación,** consistente en el envío mediante SMS de un código/clave, que debía incorporar el usuario-titular del servicio «Ibercaja Directo», para continuar, consentir, confirmar y hacer efectiva la operación. La sentencia de instancia estima la demanda y condena a la demandada a abonar al actor la cantidad reclamada. [...] La entidad Ibercaja Banco S.A. presentó recurso de apelación, que fue desestimado por la Audiencia Provincial.

[...] La entidad demandada Ibercaja Banco S.A. formula recurso de casación contra la expresada sentencia, que fundamenta en dos motivos que seguidamente se analizarán. [...]” [Énfasis añadido]

Formulación del motivo de recurso: “[...] [I]bercaja Banco S.A. denuncia que [...] las transferencias controvertidas no deben ser consideradas operaciones no autorizadas, por haber sido realizadas por terceros que habrían utilizado las credenciales del usuario Sr. Martin -extremo no acreditado-, cuando lo cierto es que habían sido correctamente autorizadas y registradas en los sistemas informáticos de la entidad, en cumplimiento y conforme a las condiciones contractuales pactadas con el actor en sendos contratos de cuenta y de servicio «Ibercaja Directo». [...] [I]nsiste la recurrente, en todas transferencias se llevó a cabo la identificación correcta del usuario con un **doble factor de autenticación**, que consistió (i) en que el titular accede al sistema digital con su clave de usuario y contraseña o clave de firma, y (ii) se envía mediante SMS, de forma exclusiva y con validez temporal [...], un código para confirmar la operación, al teléfono móvil que el titular ha facilitado en la oficina para operar a través de la banca online. **Si tales credenciales eran conocidas por terceros y las emplearon para, a través del móvil del actor, ejecutar las operaciones en la banca digital, no cabe imputar responsabilidad alguna a la demandada [...]**” [Énfasis añadido]

Doctrina sobre la responsabilidad del proveedor de servicios de pago en operaciones no autorizadas: “[...] El motivo debe ser desestimado. [...] La controversia radica en determinar [...] qué debe entenderse por «operaciones de pago no autorizadas». [...] [E]s preciso significar que la Audiencia ha declarado probado que las operaciones de pago se ejecutaron por terceras personas, ajenas y sin el consentimiento del demandante, lo que comporta rechazar de plano las dudas sugeridas por la recurrente. [...] **[L]a 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.** [...] [L]a expresión «operaciones no autorizadas» incluye aquellas que se han iniciado con las claves de usuario y contraseña del usuario 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. [...] [Q]ue la entidad bancaria acredite que la operación fue autenticada, registrada con exactitud y contabilizada, **no es suficiente para eximirle de responsabilidad. Ha de probar que la operación no resultó afectada por un fallo técnico u otra deficiencia del servicio prestado, y, dado que el cliente niega que la operación fuera consentida, que no hubo por parte de este último fraude, incumplimiento deliberado o negligencia grave.** [...] [N]os encontramos, de un lado, ante una conducta diligente del titular de la cuenta, que informó, inmediata y reiteradamente, al personal de entidad de lo que estaba sucediendo, cumpliendo la obligación que expresamente le imponía la normativa comunitaria y nacional; y, de otro lado, ante un servicio que se presta defectuosamente por el proveedor, tanto por no tomar en consideración la información recibida pese a su gravedad, como por omitir la adopción de medidas que posibilitaran la detección de eventuales maniobras fraudulentas. [...] Desestimar el recurso de casación interpuesto por Ibercaja Banco S.A. [...]” [Énfasis añadido]

[Texto completo de la sentencia](#)