



Juzgado de Primera Instancia nº 38 de Barcelona
Avenida Gran Vía de les Corts Catalanes, 111, edifici C, planta 9 - Barcelona - C.P.: 08075

TEL.: 935549438
FAX: 935549538
EMAIL:instancia38.barcelona@xij.gencat.cat

N.I.G.: 0801942120238195456

Juicio verbal (250.2) (VRB) [REDACTED]

Materia: Juicio verbal (resto de casos)

Entidad bancaria BANCO SANTANDER:

Para ingresos en caja, Concepto: [REDACTED]

Pagos por transferencia bancaria: IBAN ES55 0049 3569 9200 0500 1274.

Beneficiario: Juzgado de Primera Instancia nº 38 de Barcelona

Concepto: [REDACTED]

Parte demandante/ejecutante: [REDACTED]

Procurador/a: Pedro Moratal Sendra, Pedro Moratal Sendra
Abogado/a: Óscar Serrano Castells

Parte demandada/ejecutada: BANKINTER, SA

Procurador/a: Ricard Simó Pascual

Abogado/a:

SENTENCIA Nº 396/2024

Magistrada: Claudia Ferrer del Pino

Barcelona, 14 de octubre de 2024

Vistos por mí, Claudia Ferrer del Pino, Magistrada Juez adscrita en refuerzo a este Juzgado de Primera Instancia nº 38 de Barcelona las presentes actuaciones correspondientes a juicio verbal instados por el Procurador Pedro Moratal Sendra en nombre y representación de [REDACTED] contra BANKINTER S.A., y en base a los siguientes

ANTECEDENTES DE HECHO

PRIMERO. - La parte actora presentó a través de la representación procesal indicada, demanda de juicio verbal en reclamación de cantidad, en la que tras alegar los hechos y fundamentos de derecho que tuvo por conveniente, solicitó se dictase sentencia estimatoria de sus pretensiones, frente a la parte demandada.

SEGUNDO. - Admitida a trámite la mentada demanda, se formuló oposición por la parte demandada.

TERCERO. - Celebrada la vista, se practicaron las pruebas y quedaron los autos conclusos para dictar sentencia

FUNDAMENTOS DE DERECHO



Data i hora 14/10/2024 11:52	Signat per Ferrer del Pino, Claudia;
------------------------------------	--------------------------------------



PRIMERO. - La controversia suscitada.

La actora formula demanda de juicio verbal solicitando que:

- 1.- DECLARI l'incompliment de les obligacions legals i contractuals que li eren de compliment així com la responsabilitat de l'entitat financera demandada en la incorrecta custòdia i execució de les operacions realitzades contra els comptes de la meva principal, no autoritzat per ella.
- 2.- CONDEMNI, com a conseqüència de l'anterior, a l'entitat demandada a abonar a la meva representada per concepte de tots els danys i perjudicis causats als demandants, en l'import de 5.102,71 € € junt amb els interessos legals des de la reclamació extrajudicial efectuada el 15 de febrer de 2023.
- 3.- CONDEMNI l'entitat al pagament de les costes causades a aquesta part.

La demandada se opuso a la demanda rechazando haber incurrido en responsabilidad por una orden de pago que fue realizada por el usuario o porque éste incurrió en negligencia grave al permitir que su dispositivo móvil fuera afectado por un malware informático. También excepcionó falta de legitimación activa de una de las actoras y falta de legitimación pasiva para responder de una parte de la reclamación.

SEGUNDO. – Marco normativo y fáctico de la controversia.

La actora ejerce una acción de declaración de responsabilidad contractual y consecuente indemnización al amparo de las reglas generales de obligaciones y contratos y específicamente a tenor del Real decreto Ley 19/2918 de 23 de noviembre de servicios de pagos.

Sin perjuicio de otros que pudieran resultar de los razonamientos y valoración probatoria en esta sentencia, los principales hechos probados que enmarcan la pretensión son:

- 1.- Los actores son clientes del banco demandado BANKINTER S.A. con el que desde el 2001 tienen contratada una cuenta corriente, tarjeta de crédito y otros productos.
- 2.- La Sra. [REDACTED] recibió el día 9 de enero de 2023 en el teléfono móvil sendos SMS de la entidad bancaria informándole de un ingreso de 2.900 euros y un cargo de 4.900 euros por la plataforma de bitcoins BINANCE. No es controvertido que llamaron al Banco y le indicó que fuera a la oficina al día siguiente.
- 3.- Al día siguiente, el matrimonio acudió a la oficina bancaria para informar que los movimientos no estaban autorizados. Así lo reconoció expresamente en juicio la empleada de la oficina. También el 10 de enero de 2023, el Sr. [REDACTED] presentó denuncia ante los Mossos D'Esquadra explicando que no había autorizado a nadie a ingresar los 2.900 euros en su cuenta corriente como tampoco a realizar un cargo BINANCE de 4.900 euros.
- 4.- El día 9 de enero de 2023 en dicha cuenta corriente se produjo un ingreso de 2.900 euros (“movimiento smart cash”) en la cuenta de los actores por la disposición de



Data i hora 14/10/2024 11:52	Signat per Ferrer del Pino, Clàudia;



una línea de Crédito de una tarjeta Smart Cash, modalidad revolving con un TIN anual del 17,52% que tenían contratada con BANKINTER CONSUMER FINANCE EFC, S.A. generándose una comisión de disposición de 87 euros y una primera cuota de 30,62 euros de intereses (documento 12-D). Los 2.900 euros fueron pagados por los actores en 3 cuotas los meses de febrero, marzo y abril de 2023.

5.- El día 12 de enero de 2023 en la cuenta corriente de los actores se cargó un importe de 4.900 euros por la entidad BINANCE (documento 6-D).

**TERCERO. - Excepción de falta de legitimación activa de la Sra. [REDACTED]
y de falta de legitimación pasiva de BANKINTER.**

El demandado alega que una de las actoras, la Sra. [REDACTED] no tiene legitimación activa para pedir una indemnización, pues “el único titular de las tarjetas de crédito y débito con cargo a la cuales se realizaron los dos movimientos supuestamente fraudulentos” es el Sr. [REDACTED]

No se admite la excepción planteada porque se está reclamando un daño sufrido también por la Sra. [REDACTED] cotitular de las cuentas y del dinero que ha perdido y cuya responsabilidad solicita que sea de la demandada.

El demandado también excepciona su legitimación pasiva de la pretensión interesada en la demanda porque “En el presente procedimiento se ha hecho una disposición con cargo a una tarjeta de crédito que nunca fue contratada con BANKINTER SA (sino con BANKINTER CONSUMER FINANCE EFC, S.A.) y cuya disposición, según afirman los demandantes, les ha causado una serie de perjuicios económicos que cifran en 202,71.-€.”

El documento 8-D es la contestación de Bankinter recordando a la demandante sus obligaciones de custodia de la tarjeta de crédito y que es responsable por su uso negligente. El documento 10-D es otra respuesta de Bankinter rechazando la responsabilidad. Por otra parte, la demandada dispone de todos los registros de acceso y uso de la tarjeta, pues los ha aportado al procedimiento. Asimismo, el actor, cliente de la entidad únicamente se ha relacionado con la oficina de la entidad BANKINTER.

En tanto que el actor tiene la condición de consumidor y que es cliente, sin más, de Bankinter, no cabe esgrimir argumentos dotados de tintes acusadamente formalistas para rechazar la legitimación que se discute, como tampoco cabe exigirle que conozca el entramado financiero en función de su actividad (servicios bancarios y emisora de tarjeta de crédito respectivamente), con empresas con el que comparten la designación preponderante de Bankinter, máxime cuando éstas han actuado unitariamente o mejor dicho, es la demandada a través de sus oficinas y empleados la que ha actuado en nombre de las dos, y cuando ha aceptado extraprocesalmente su legitimación pasiva en un acto propio que ahora no puede contradecirse (en el mismo sentido, la SAP León, s.1, de 9 de junio de 2022).

CUARTO. – Estimación de la demanda.



Data i hora 14/10/2024 11:52	Signat per Ferrer del Pino, Clàudia;
------------------------------------	--------------------------------------



El Real Decreto-Ley 19/2018, de 23 de noviembre, de Servicios de pago regula los derechos y obligaciones tanto de los usuarios de los servicios de pago como de los proveedores de los mismos (art.1.1).

Dicha norma en su artículo 41 regula como **obligaciones del usuario** de servicios de pago en relación con los instrumentos de pago y las credenciales de seguridad personalizada las de 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, así como la de en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, notificarlo al proveedor de servicios de pago o a la entidad que este designe, sin demora indebida en cuanto tenga conocimiento de ello.**

El Art 45.1 establece que "*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."*"

Por último, reseñar, respecto de la prueba de la autenticación y ejecución de las operaciones de pago, el art. 44 dispone lo siguiente: "*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. Correspondrá 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.*".



Data i hora 14/10/2024 11:52	Signat per Ferrer del Pino, Claudia;
------------------------------------	--------------------------------------



Tal y como se desprende de la mencionada regulación, en caso de operaciones no autorizadas, **la responsabilidad de la entidad bancaria es de naturaleza cuasi objetiva** o de riesgo por razón legal (SAP Alicante, s.8, de 12 de marzo de 2018 y SAP de Zaragoza, Sec. 5^a, S. 01-07-2022, nº 804/2022, rec. 1130/2021).

La obligatoria obligación de restitución inmediata al usuario de una operación no autorizada se excepciona al único caso de que haya actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, la obligación de custodiar las claves personales con todas las medidas razonables.

Con el anterior marco de referencia, valorando las pruebas del procedimiento, estimo que la entidad demandada ha incurrido en responsabilidad por los motivos que siguen:

1.- Considero probado por el informe pericial (documento 7-D) y las explicaciones del perito en el acto del juicio que el dispositivo móvil donde se recibieron los SMS fraudulentos resultó infectado desde el 7 de enero de 2023 por un malware con la capacidad de emular el acceso a la banca online de multitud de entidades bancarias, capturando las credenciales y suplantar la identidad del usuario realizando y validando operaciones bancarias no autorizadas. Debo admitir, con todo, que concurren dudas de hecho sobre el mecanismo concreto del fraude porque como dice la entidad bancaria se ha de disponer de la numeración de la tarjeta para poder incluir los datos en cualquier servidor de pago y estos no deberían resultar del dispositivo infectado.

Sin embargo, ante un fraude bancario, el usuario debe interponer una denuncia y posteriormente una reclamación ante su entidad bancaria. La entidad tiene un plazo de quince días para resolver la reclamación (Art. 69 LSP). Esto lo hizo diligentemente el actor llamando a la entidad bancaria el mismo día en que advirtió del movimiento no autorizado, acudiendo al día siguiente a la oficina solicitando la anulación y presentando denuncia ante los Mossos de Esquadra. Esto ya sería suficiente para estimar la responsabilidad del banco porque el movimiento fraudulento se produjo el día 12 de enero, 4 días después de ser advertida la entidad bancaria, y sin que ésta hubiera justificado qué inconveniente tuvo para retrotraer o anular la operación.

2.- Por otra parte, no se puede estimar una negligencia grave del usuario cuando ha sido objeto de una estafa y de un malware informático que controlaba el dispositivo móvil, tal y como ha acreditado el informe pericial aportado con la demanda. La negligencia grave del usuario que exoneraría a la entidad bancaria demandada “*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 (...)*” (SAP de Madrid, Sec. 20^a, nº 184/2022, de fecha 20/5/2022, Rec. 945/2021). Dicho de otra forma, el usuario no incurre en iniciativa ni negligencia grave cuando ha sido víctima de un engaño.

3.- En relación al fraude que comete un tercero, la normativa aplicable tiene en cuenta que las prácticas delictivas son cada vez más sofisticadas y difíciles de detectar más para el usuario que carece de conocimientos informáticos y menos para la entidad bancaria que debe estar constantemente actualizando sus medios de seguridad. En este sentido, la Directiva 2015/2366, sobre Servicios de Pago en el Mercado Interior (DSP2),



Data i hora 14/10/2024 11:52	Signat per Ferrer del Pino, Claudia;
------------------------------------	--------------------------------------



los Considerandos (7), (33), (69), (91) y (95) advierten que, ante el incremento de los riesgos de seguridad debido a la mayor complejidad técnica de los pagos y fraudes, es esencial disponer de servicios de pago fiables y seguros, de forma que los usuarios gocen de la debida protección frente a los riesgos inherentes a estos nuevos medios de pago. Y en particular, **obliga a los proveedores de servicios de pago a realizar controles adecuados para gestionar sus riesgos operativos y de seguridad** (Art. 96 DSP2). En desarrollo de estas obligaciones, el Reglamento Delegado 2018/389, de 27 de noviembre de 2017, que complementa la DSP2 en lo relativo a las normas técnicas para la autenticación reforzada de cliente, establece la **obligación de realizar un análisis de riesgo en tiempo real basado en el análisis de operaciones y en los elementos que caracterizan al usuario en un contexto de uso normal de las credenciales de seguridad**. Ese análisis de riesgo debe tener en cuenta los siguientes factores: **(i) importe de las operaciones, (ii) supuestos conocidos de fraude conocidos, (iii) gastos o pautas de comportamiento anormales en el ordenante, (iv) información inusual sobre el dispositivo o programa informático de acceso del ordenante, (v) infecciones por programas informáticos maliciosos en cualquier sesión del procedimiento de autenticación, (vi) supuestos conocidos de fraude en la prestación de servicios de pago, (vii) una ubicación anormal del ordenante, y (viii) una ubicación de alto riesgo del beneficiario.**

En el presente caso, relacionado con un malware que toma el control del dispositivo móvil del usuario, el perito del actor explicó que la verificación en 2 pasos no es seguro, pues se parte de la convicción de que el SMS se envía correctamente al móvil del cliente bancario, cuando éste no sabe ni conoce que está siendo objeto de un fraude bancario. Siendo esto así, el actor ha demostrado que el movimiento de 4.900 euros conjugado con una disposición de la tarjeta es anormal y extraño a las pautas del usuario tanto en su operativa como en el importe. También ha demostrado que los accesos al servicio de pagos de la entidad bancaria son desde una IP extranjera (Turquía) y la IP española, en el periodo de tiempo analizado, lo que representa una “*ubicación anormal del ordenante*”. Estas circunstancias no han sido discutidas por la demandada y no ha aportado prueba alguna de las medidas de alarma que tenía implementadas para poder gestionar de forma responsable la orden de pago, anormal en relación a su cliente-usuario. Es más, el mismo día 9 de enero recibió la llamada del usuario y al día siguiente se personó en la oficina informando que la operación no estaba autorizada, aportando la denuncia ante la policía, y todo ello cuando el movimiento fraudulento tuvo lugar posteriormente, el día 12 de enero.

Por todo lo expuesto, desestimada la falta de legitimación pasiva relativa a la reclamación de 202,71.-€ y no discutiéndose el resto de la cantidad reclamada, es procedente la condena a la demandada al pago de 5.102,71 € con más los intereses legales desde la reclamación extrajudicial de acuerdo con los art. 1.100 y 1.108 CC, y los del art 576 LEC desde el dictado de esta sentencia.

QUINTO. - costas.

Al ser estimada la demanda, corresponde a la parte demandada hacerse cargo de todas las costas del proceso ex art. 394 LEC.

FALLO



Data i hora 14/10/2024 11:52	Signat per Ferrer del Pino, Claudia;
------------------------------------	--------------------------------------



ESTIMO LA DEMANDA promovida a instancia de [REDACTED] contra BANKINTER S.A., por lo que:

1- Declaro el incumplimiento por el Banco de las obligaciones legales y contractuales que le incumbían y su responsabilidad en la incorrecta custodia y ejecución de las operaciones realizadas contra las cuentas de la parte actora y no autorizadas por la demandante.

2- En consecuencia, condeno a la demandada a abonar a la actora en concepto de daños y perjuicios causados el importe de 5.102,71€ con más los intereses legales desde la reclamación extrajudicial efectuada el 15 de febrero de 2015, así como al pago de las costas causadas.

Notifíquese esta Sentencia a las partes, haciéndoles saber que contra la presente puede interponerse recurso de apelación ante la Audiencia Provincial, en este mismo Juzgado, en un plazo de veinte días a contar desde la notificación de la misma, advirtiéndoles de la necesidad de constitución de depósito en la Cuenta de Depósitos y Consignaciones del Juzgado, en los términos indicados en la Disposición Adicional Decimoquinta de la Ley Orgánica del Poder Judicial.

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

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,



Data i hora 14/10/2024 11:52	Signat per Ferrer del Pino, Claudia;
------------------------------------	--------------------------------------



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.



Data i hora 14/10/2024 11:52	Signat per Ferrer del Pino, Claudia;