



**JDO. 1A.INST.E INSTRUCCION N. 4
PALENCIA**

SENTENCIA: 00005/2023

UNIDAD PROCESAL DE APOYO DIRECTO

PLAZA DE LOS JUZGADOS, S/N
Teléfono: 979168732, Fax:
Correo electrónico:

Equipo/usuario: MSG
Modelo: N04390

N.I.G.: 34120 41 1 2022 0002664
JVB JUICIO VERBAL 00 /2022

Procedimiento origen: /
Sobre **RECLAMACION DE CANTIDAD**
DEMANDANTE D/ña. _____
Procurador/a Sr/a. _____
Abogado/a Sr/a. SOLEDAD FERNANDEZ SIMON
DEMANDADO D/ña. IBERCAJA BANCO
Procurador/a Sr/a. _____
Abogado/a Sr/a. _____

S E N T E N C I A

En Palencia, a 27 de febrero de 2023

SS^a. Ilma. Doña M^a Jesús Serna Gallardo, Magistrada Titular del Juzgado de Primera Instancia e Instrucción 4 de Palencia y su partido judicial, ha visto los presentes autos de Juicio Verbal, número 00005/2022 en ejercicio de acción de reclamación de cantidad, promovidos a instancia de don _____, asistido por la letrada doña Soledad Fernández Simón, frente a IBERCAJA, S.A., representado por don _____ y asistido por el letrado doña _____.

ANTECEDENTES DE HECHO

PRIMERO.- Por la representación procesal de don _____ se formuló el demanda de juicio verbal en ejercicio de acción de reclamación de cantidad turnada a este Juzgado, en la que solicitaba que se dictare sentencia en su día, previa la tramitación del juicio, condenando a la parte demandada a todos



y cada uno de los puntos recogidos en el suplico, así como al pago de las costas causadas.

SEGUNDO.- Admitida a trámite la demanda por Decreto de 30 de septiembre de 2022 se dio traslado a la demandada que contestó el 29 de noviembre de 2022 oponiéndose a las pretensiones de la parte actora.

TERCERO.- Se celebró vista el 27 de febrero de 2022. El día del juicio comparecieron ambas partes debidamente asistidas por sus letrados. Solicitado que fue, se recibió el pleito a prueba, proponiéndose la prueba, la testifical de doña y la documental unida a las actuaciones. Las partes formularon las conclusiones que tuvieron por oportuno, siendo declarados los autos conclusos para sentencia.

CUARTO.- En la tramitación de este Juicio se han observado las formalidades legales.

FUNDAMENTOS DE DERECHO

PRIMERO.- OBJETO DEL LITIGIO: Por la parte actora, titular de la tarjeta de crédito vinculada a la cuenta número se ejercita acción de reclamación de cantidad por responsabilidad contractual de IBERCAJA BANCO, S.A, en calidad de depositaria, solicitando que se condene a la entidad demandada al pago de cantidad a la que asciende el coste de las dos operaciones bancarias que suponen cargos en dicha cuenta el 24 de febrero de 2022, así como al pago de las costas del presente procedimiento. Dicha pretensión la fundamenta en los artículos 306 del CCom y 1769 del CC, así como en los artículos 44.1, 2 y 3 del Real-Decreto-Ley 19/2018 de 23 de noviembre, de servicios de pago y otras medidas urgentes. Alega que impetra la acción de la justicia porque tras interponer la correspondiente denuncia el de febrero de 2022 por estafa, formuló reclamación a la entidad el de febrero de 2023 recibiendo contestación negativa a su pretensión de reintegro de los cargos el 8 de marzo de 2023 y posterior reclamación al servicio de atención al cliente que fue resuelto de idéntica manera a 30 de marzo de 2023. Planteó igualmente la reclamación al departamento de Conducta del Banco de España, que contestó en el sentido de no tener facultades para resolver sobre le reintegro interesado

La entidad demandada explica que en el contrato suscrito con el actor el 11 de septiembre de 2019 se recogía en un teléfono móvil operativo del titular

por si quisiera registrarse en la plataforma de pagos Samsung pay. Que el proceso de registro en la operación de pago con móvil se realizó el mismo día del fraude a las 22.23 horas. Las operaciones de pago cuestionadas se realizaron con posterioridad, a las 23.16 y las 23.17 horas. Para darse de alta en la plataforma de pagos se remitió un código por sms al móvil facilitado al momento de la contratación en 2019. Cuando se realizaron los movimientos en el cajero a través del dispositivo móvil, por ser importes superiores a 100 euros también se remitió el correspondiente mensaje.

SEGUNDO.- HECHOS PROBADOS: de lo manifestado pro la propia testigo, que es coincidente con las distintas operaciones bancarias que se van registrando resulta lo siguiente;

- 1) don recibió en su teléfono móvil el siguiente sms: “ESP.IBERCAJA.S.A, A partir del 24/02/2022, No puede utilizar su tarjeta. Tienes que activar el nuevo sistema de seguridad web: <https://tiny.one/Ibercaja>.” La URL <https://tiny.one/Ibercaja>. No es de la entidad demandada.
- 2) Don, alertado por el contenido del mensaje recibido solicita el auxilio de su hija, doña, que explicó en el acto del juicio como pinchó el enlace e introdujo en la pagina a la que accedió, en la creencia de que se trataba de la página de Ibercaja, el usuario y contraseña de acceso de su padre a la banca on line.
- 3) Recibió con posterioridad en el teléfono móvil el código de activación 812818, reconociendo que el contenido del mensaje decía expresamente que el código era para añadir a la tarjeta visa finalizada en en la plataforma Samsung Pay manifestando que desconocía que era Samsung Pay. Aun así, introdujo el código en la página que simulaba ser de IBERCAJA y el número de la tarjeta bancaria, la fecha de caducidad de dicha tarjeta y la clave CVV.
- 4) Al rato, a las 23.17 y a las 23.18 horas recibió dos mensajes de los cargos realizados poniéndose de inmediato con atención al cliente, por lo que cabe concluir que con todos los datos facilitados el defraudador completó la instalación de la tarjeta en la aplicación Samsung de su terminal.
- 5) Según el documento octavo de los aportados con la contestación a la demanda el 24 de febrero de 2022 a las 23.35 horas queda bloqueada la tarjeta.

TERCERO.- NORMATIVA APLICABLE: La normativa aplicable al caso concreto es Real-Decreto-Ley 19/2018 de 23 de noviembre, de servicios de pago y otras medidas urgentes, en concreto los siguientes artículos:

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

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

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

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

.....

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

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

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

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

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

c) Garantizará que en todo momento estén disponibles medios adecuados y gratuitos que permitan al usuario de servicios de pago efectuar una notificación en virtud del artículo 41.b), o solicitar un desbloqueo con arreglo a

lo dispuesto en el artículo 40.4. A este respecto, el proveedor de servicios de pago facilitará, también gratuitamente, al usuario de dichos servicios, cuando éste se lo requiera, medios tales que le permitan demostrar que ha efectuado dicha comunicación, durante los 18 meses siguientes a la misma.

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

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

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

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

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

Si el usuario de servicios de pago inicia la operación de pago a través de un proveedor de servicios de iniciación de pagos, corresponderá a éste demostrar que, dentro de su ámbito de competencia, la operación de pago fue autenticada y registrada con exactitud y no se vio afectada por un fallo técnico u otras deficiencias vinculadas al servicio de pago del que es responsable.

2. A los efectos de lo establecido en el apartado anterior, el registro por el proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, de la utilización del instrumento de pago no bastará, necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que éste ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones con arreglo al artículo 41.

3. *Corresponderá al proveedor de servicios de pago, incluido, en su caso, el proveedor de servicios de iniciación de pagos, probar que el usuario del servicio de pago cometió fraude o negligencia grave.*

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

1. *Sin perjuicio del artículo 43 de este Real decreto-ley, en caso de que se ejecute una operación de pago no autorizada, el proveedor de servicios de pago del ordenante devolverá a éste el importe de la operación no autorizada de inmediato y, en cualquier caso, a más tardar al final del día hábil siguiente a aquel en el que haya observado o se le haya notificado la operación, salvo cuando el proveedor de servicios de pago del ordenante tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España, en la forma y con el contenido y plazos que éste determine. En su caso, el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada.*

.....

el artículo 45 establece que cuando se ejecute una orden de pago no autorizada, el banco debe devolver al cliente el importe de la operación: "el proveedor de servicios de pago del ordenante restituirá la cuenta de pago en la cual se haya efectuado el adeudo al estado en el que se habría encontrado de no haberse efectuado la operación no autorizada".

.....

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

1. *No obstante lo dispuesto en el artículo 45, el ordenante podrá quedar obligado a soportar, hasta un máximo de 50 euros, las pérdidas derivadas de operaciones de pago no autorizadas resultantes de la utilización de un instrumento de pago extraviado, sustraído o apropiado indebidamente por un tercero, salvo que:*

a) *al ordenante no le resultara posible detectar la pérdida, la sustracción o la apropiación indebida de un instrumento de pago antes de un pago, salvo cuando el propio ordenante haya actuado fraudulentamente, o*

b) la pérdida se debiera a la acción o inacción de empleados o de cualquier agente, sucursal o entidad de un proveedor de servicios de pago al que se hayan externalizado actividades.

El ordenante soportará todas las pérdidas derivadas de operaciones de pago no autorizadas si el ordenante ha incurrido en tales pérdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 41. En esos casos, no será de aplicación el importe máximo contemplado en el párrafo primero.

En todo caso, el ordenante quedará exento de toda responsabilidad en caso de sustracción, extravío o apropiación indebida de un instrumento de pago cuando las operaciones se hayan efectuado de forma no presencial utilizando únicamente los datos de pago impresos en el propio instrumento, siempre que no se haya producido fraude o negligencia grave por su parte en el cumplimiento de sus obligaciones de custodia del instrumento de pago y las credenciales de seguridad y haya notificado dicha circunstancia sin demora.

2. Si el proveedor de servicios de pago del ordenante no exige autenticación reforzada de cliente, el ordenante solo soportará las posibles consecuencias económicas en caso de haber actuado de forma fraudulenta. En el supuesto de que el beneficiario o el proveedor de servicios de pago del beneficiario no acepten la autenticación reforzada del cliente, deberán reembolsar el importe del perjuicio financiero causado al proveedor de servicios de pago del ordenante.

3. Salvo en caso de actuación fraudulenta, el ordenante no soportará consecuencia económica alguna por la utilización, con posterioridad a la notificación a que se refiere el artículo 41.b), de un instrumento de pago extraviado o sustraído.

4. Si el proveedor de servicios de pago no tiene disponibles medios adecuados para que pueda notificarse en todo momento el extravío o la sustracción de un instrumento de pago, según lo dispuesto en el artículo 42.1.c), el ordenante no será responsable de las consecuencias económicas que se deriven de la utilización de dicho instrumento de pago, salvo en caso de que haya actuado de manera fraudulenta.

.....

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

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

.....

Artículo 68. Autenticación.

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

- a) acceda a su cuenta de pago en línea;*
- b) inicie una operación de pago electrónico;*
- c) realice por un canal remoto cualquier acción que pueda entrañar un riesgo de fraude en el pago u otros abusos.*

.....

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

CUARTO.- VALORACIÓN PROBATORIA: No es controvertido que el actor sufrió un ataque de los que se denominan phishing. La hija de éste explicó que recibió un sms con unas instrucciones que siguió en la creencia de que le iban a bloquear la tarjeta. Consta acreditado por la entidad bancaria que el código de seguridad para autorizar el enrolamiento al servicio Samsung pay sí fue remitido al número de teléfono indicado en el contrato, por lo que todo apunta a que fue doña _____, a través la página inicialmente abierta quien autorizó la operación, facilitando además otros datos que permitieron hacer uso de la aplicación Samsung desde otro terminal en la localidad de Murcia. Es obvio que en el presente caso la operativa fraudulenta contó para su perfeccionamiento y consumación, con la conducta de la hija del actor, pues sin su cooperación no se hubiera producido la estafa.

Hay que examinar dos extremos, por un lado, si el banco implementó el doble control o autenticación reforzada como establece el Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes y por otro lado, si cabe apreciar en la demandante un comportamiento negligente de la gravedad y entidad para con base en el mismo hacerle responsable.

Los bancos, en cuanto facilitadores de medios de pago electrónicos, están obligados a implementar la doble autenticación o autenticación reforzada. Sin embargo, en el presente caso las dos operaciones fraudulentas no se realizaron a través de un comercio electrónico seguro. Lo que sí se realizó "on line" fue el enrolamiento a la plataforma de pago móvil que certifica que se produjo la autenticación reforzada (Las mismas fueron autorizadas bajo las claves de seguridad del cliente y con los códigos OTP mandados a través de mensajes SMS al teléfono del propio cliente) constando certificado con la traza del mensaje enviado al teléfono del cliente, por lo que la citada operación fue autorizada, registrada con exactitud y contabilizada y no se vio afectada por un fallo técnico o cualquier otra deficiencia. Cuestión distinta es que un tercero, en posesión de las claves facilitadas por la propia [redacted], luego las haya utilizado para realizar dos reintegros en cajeros automáticos.

En relación con la conducta de don [redacted], en la Directiva 2015/2036 la negligencia que le hace responder al cliente, es la que se deriva de una conducta caracterizada por un grado significativo de falta de diligencia, lo que supone que la misma surge o se produce por iniciativa del usuario, no como consecuencia del engaño al que ha sido inducido por un delincuente profesional. En el presente caso, y pese a que mediante carta remitida a 11 de febrero de 2020 la entidad bancaria advertía a sus clientes de este tipo de fraudes, es la hija del actor la que sin ningún tipo de cautela introduce todos los datos que le van demandando, por lo que no cabe duda de que existió una conducta negligente, queda por determinar en que grado se produce esa negligencia. En presente caso no podemos determinar si el enlace llevaba a una página que aparentaba ser el sitio oficial de la entidad de crédito pero sí que el mensaje recibido tiene la apariencia de ser remitido por Ibercaja. Entendemos que el pinchar en el enlace no se puede considerar una negligencia grave. Tampoco introducir los datos en una página que clona las del sitio oficial de la entidad emisora, pues corresponde a la entidad dotar de la tecnología antiphishing precisa para detectar las páginas clonadas de las oficiales propias. Más dudas presenta el no advertir que en el mensaje remitido con el código de actuación se hacía constar que la operación que se autorizaba consistía en vincular la tarjeta visa finalizada en [redacted] a la plataforma Samsung pay. Si hubiera realizado una lectura más atenta hubiera

consultado con carácter previo en qué consistía la citada plataforma sin dar por hecho de que se trataba del nuevo sistema de seguridad de la tarjeta, pero aun así no podemos estimar que concurre una negligencia grave en la obtención de los datos personales y de seguridad por los defraudadores, toda vez que la entidad también pudo haber constatado que el terminal en el que se instaló la aplicación de pago tenía distinto número que el terminal facilitado por el cliente al que se remitió el código de activación.

Tampoco en la obligación de comunicación sin demora, pues notificó la situación inmediatamente y por teléfono a la entidad bancaria que la cuenta se bloqueó minutos después de la realización de los cargos bancarios.

Por todo lo expuesto, debe prosperar la demanda interpuesta.

QUINTO.- INTERESES: Deberán abonarse los dejados de percibir por los [redacted] desde que se efectuaron las transferencias fraudulentas, el 24 de febrero de 2022, que se incrementarán en dos puntos desde el dictado de la sentencia hasta su completo abono.

SEXTO.- COSTAS. La estimación de la demanda determina que, de conformidad con lo dispuesto en el artículo 394 de la Ley de Enjuiciamiento Civil, proceda hacer expresa imposición de costas a la parte demandada.

FALLO

Que ESTIMO la demanda interpuesta por la representación de don [redacted] frente a IBERCAJA BANCO, S.A, condenando a IBERCAJA BANCO SA al abono a la parte actora de [redacted] y los intereses legales de dicha cantidad en la forma establecida en el fundamento de derecho quinto, a todo ello con expresa imposición de costas a la parte demandada.

Advierto a las partes que contra esta sentencia no cabe interponer recurso alguno.

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

EL/LA MAGISTRADO/JUEZ



La difusión del texto de esta resolución a partes no interesadas en el proceso en el que ha sido dictada sólo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contuvieran y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutelar o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda.

Los datos personales incluidos en esta resolución no podrán ser cedidos, ni comunicados con fines contrarios a las leyes.