ADMINISTRACION DE JUSTICIA

ADMINISTRACION DE XUSTIZA

XDO. PRIMEIRA INSTANCIA N. 1
LUGO

SENTENZA: 00151/2023

-

C/ ARMANDO DURAN S/N - LUGO
Teléfono: 982294693- 982294694, Fax: 982294691
Correo electrónico: instancia1.lugo@xustiza.gal

Equipo/usuario: EP
Modelo: N04390

N.I.G.: 27028 42 1 2022 0000109
ORD PROCEDIMIENTO ORDINARIO 0000007 /2022
Procedimiento origen: /
Sobre RECLAMACION DE CANTIDAD
DEMANDANTE D/ña. [redacted]
Procurador/a Sr/a. ANA MARIA FERNANDEZ SANTOS
Abogado/a Sr/a. XOSE MANUEL FERNANDEZ VARELA
DEMANDADO D/ña. [redacted]
Procurador/a Sr/a. ALVARO ANTONIO MARTIN BUITRAGO CALVET
Abogado/a Sr/a. LUIS PIÑEIRO SANTOS

XULGADO DE PRIMEIRA INSTANCIA NÚMERO 1

7-2022

SENTENZA

Xuíz: Eladio Prieto Bellas

Lugar: Lugo.

Data: 2-5-2023

Demandante: don [redacted] (representado por dona Ana María Fernández Santos e asistido por don Xosé Manuel Fernández Varela).

Demandada: [redacted] (representada por don Álvaro Martín Buitrago Calvet e asistida por don Luis Piñeiro Santos).

ANTECEDENTES DE FEITO

PRIMEIRO.- Dona Ana María Fernández Santos, en representación de don [redacted], presentou demanda (folios 6 a 13).

SEGUNDO.- Don Álvaro Martín Buitrago Calvet, en representación de [redacted], presentou escrito de contestación (folios 39 a 45).

TERCEIRO.- Tivo lugar audiencia previa e xuízo.

FUNDAMENTOS DE DEREITO

PRIMEIRO.- O demandante solicitou (folio 13) condena da demandada a abonar ao demandante o importe de 185349,15 euros, cos seus xuros legais dende o día 11-8-2021 ou, subsidiariamente, dende a reclamación extraxudicial do 20-10-2021 e custas.

A demandada solicitou a desestimación da demanda con imposición de custas ao demandante (folio 45).

O demandante estableceu como fundamento das súas pretensións: 1) o demandante é xubilado, de 77 anos de idade, sen coñecementos específicos sobre produtos bancarios ou novas tecnoloxías; pasou a xubilación o 10-7-2009 e traballou como funcionario do Corpo de Xestión da Xunta de Galicia; desde que precisou servizos bancarios dunha entidade financieira foi cliente da demandada [redacted], antes [redacted] o demandante era, no momento no que tiveron lugar os feitos, titular de conta corrente 2080016237304001l695, titular da conta de aforro 2080010495300001O169, titular da tarxeta de crédito 4339543011996007; 2) o demandante, na actualidade e nos últimos anos, mantén unha operativa, nos seus produtos bancarios, propia dunha persoa da súa idade e condición; as únicas operacións efectuadas son as que se corresponden co pagamento dos gastos habituais da familia, cargos habituais de consumo de servizos se subministracións tales como auga, electricidade, comunidade de propietarios, compra de roupa, comida e demais do fogar, así como pequenas subscricións e doazóns; así se deduce claramente da atenta lectura dos cargos e ingresos bancarios (éstes procedentes da pensión mensual); os límites da operativa estaban prefixados contractualmente (uso individual mensual 12000 euros, caixeiros diario crédito 600, débito 600, mensual crédito 12000, débito 999999,99, oficinas diario 600, mensual 12000, compras en tpv diario 12000, mensual 12000, compras en internet diario 12000, mensual 12000); 3) o 11-8-2021 persoa ou persoas descoñecidas puideron acceder, de xeito clandestino e fraudulento, mediante medios telemáticos, ás contas bancarias do actor, extraendo das súas contas corrente e de aforro, para o seu ingreso na da tarxeta, diversas cantidades (dende a conta de aforro 8000 e 8000, da conta corrente 10000, 12000, 11000, 20000, 30000, 50000, 50000 e 10000) que suman 193000 euros; seguidamente o autor ou autores deses feitos provocaron disposicións simulando supostas e inexistentes compras con cargo á tarxeta; en total os cargos na conta da tarxeta supuxeron 183249,15 euros, a maior parte dos aforros do actor e esposa froito do traballo de toda a súa vida; coetáneamente tivo lugar outro movemento por importe de 6000 euros conceptuado como transferencia a dona [redacted]; descoñécese quen pode

ADMINISTRACION DE JUSTICIA

ADMINISTRACIÓN DE XUSTIZA

ser dona [redacted]; en relación con esta operación, sen explicación de ningún tipo, produciuse a devolución de 3400 euros o 17-8-2021; deste xeito, os importes ilicitamente detraídos dos depósitos bancarios do demandante suman 185849,15 euros (183249,15-6000-3400); a demandada non desprego nin o máis mínimo dispositivo de seguridade pra protexer ao seu cliente fronte a tal fraude; 4) o demandante foi informado sobre o día 16 ou 17 de que se producira unha entrada ilegal nas súas contas por medios telemáticos, con manipulación delas, coa finalidade de apropiarse ilicitamente dos seus fondos; foi entón cando o demandante puido sospeitar dunah conversa do día 11 cunha persoa que dicía pertencer a empresa informática e que lle prometía mellorar o rendemento dos seus equipos podendo, ao longo da conversación, acceder mediante argucia informática aos seus datos persoais e bancarios; o demandante formulou reclamación ante a demandada sen obter, ao tempo de elaborar a demanda, resposta nin explicación; 5) foi necesario interpoñer demanda; 6) existe responsabilidade contractual e extracontractual da demandada; incumpriuse o Decreto Lei 19-2018, do 23 de novembro.

A demandada estableceu como fundamento da súa posición: 1) néganse os feitos afirmados na demanda en canto non sexan aceptados expresamente na contestación; non existe responsabilidade contractual nin extracontractual da demandada; o fraude ou engano provén de circuntancias totalmente alleas á demandada; as disposicións foron realizadas mediante banca móvil que o demandante tiña previa e debidamente instalada no seu móvil e a través de pagamentos en comercio seguro coa dirección IP de conexión habitual utilizada polo cliente, co pin da banca electrónica que só o cliente pode ter e coa cvv (dato presente só no plástico da propia tarxeta en poder do cliente) e sen constancia de incidencia operativa imputable á demandada; o demandante non actuou coa dilixencia debida no uso, garda e custodia do pin asignado para o uso da banca electrónica, da súa tarxeta e códigos de seguridade; 2) o demandante é unha persoa con aptitudes (ten experiencia de vida profesional para comprender o alcance do tratado no proceso) e con actitudes (contratou banca electrónica e é usuario dela); a demandada formula campañas de concienciación cos clientes, realiza avisos de seguridade na web; 3 e 4) foi o demandante quen facilitou os seus datos; existiu falta de dilixencia por parte do demandante; 5) o demandante incumpriu obrigas descritas no contrato de servizo de banca electrónica e obrigas contidas no contrato de tarxeta de crédito do 6-6-2017; non custodiou debidamente o instrumento de pagamento.

O demandante propuxo, como medios de proba, documentos.

A demandada propuxo, como medios de proba, documentos e declaración da testemuña don [redacted]

Todos os medios de proba propostos foron admitidos.

O demandante achegou: 1) fotocopia de DNI (folio 14); 2) informe de vida de traballo (folios 15 e 16); 3) contrato de conta en libreta de aforro á vista do 6-2-1992 (folio 17); 4) solicitude-contrato tarxeta de crédito (folios 18 a 21); 5) extracto de movementos (folios 22 a 24); 6) extracto de conta (folio 25); 7) extracto de conta (folios 26 a 28); 8) burofax (folios 29 e 30).

A demandada achegou: 1) escritura de poder; 2) testemuño parcial da fusión e cambio da denominación social (folio 47); 3) informe de oficina de prevención de perdas e fraude de Abanca do 17-2-2022 (folios 56 e seguintes); 4) contrato de tarxeta; 5) denuncia (folios 48 a 52); 6) contrato de servizo de banca electrónica (folios 53 a 55).

Don [redacted] declarou ser empregado de [redacted] dende setembro do 2007, que o declarante fixo un informe, que se ratificaba na demanda, que non se pode acceder a [redacted] sen nome de usuario e pin, que non existiu ningún tipo de incidencia, que as alertas saltan cando as operacións se fan en comercio non seguro, que moitos clientes esquecen o pin e todos os días moitos clientes teñen problemas co pin, que todo indicaba que o propio cliente era o que facía as operacións, que existiron campañas de concienciación, que nunha vez o cliente pulsou en "máis información" nunha campaña de información, que é o xeito no que mandan a operación determina se o comercio é seguro ou non, que os límites dos contratos de banca electrónica son límites pero poden modificarse, que un usuario pode modificar on line os límites, que o declarante non coñece a operativa previa do cliente, que non sabe por que se devolveron 4000 euros de 6000 euros, que se basean na información de propio demandante, que o declarante non sabe se a denuncia se fixo acompañado o cliente por empregada de Abanca que o atendía habitualmente.

SEGUNDO.- Considero que procede estimar a demanda.

En relación con un caso substancialmente similar a Ilma. Audiencia Provincial de Pontevedra, en sentenza do 1-12-2022, invocada pola demandante, afirmou:

"PRIMERO.- La sentencia apelada estimó la demanda de juicio verbal interpuesta por Bernardino, en ejercicio de acción de responsabilidad contractual en relación a alegada falta de autenticación de transferencia efectuada el 24.8.2021 desde su cuenta bancaria, frente a la entidad ABANCA CORPORACIÓN BANCARIA,

S.A., condenando a la anterior al abono de 4.891 euros más intereses legales, interpretando arts. 1.091, concordantes CC, 217 LEC, 147 y 148 LGDCU y normativa asociada a Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior.

Recurre en apelación la entidad bancaria, argumentando que aunque el reclamante fue víctima de fraude, incurrió en negligencia grave al facilitar credenciales personalizadas a tercero desconocido, debiendo ser exonerada de responsabilidad en aplicación de arts. 41 y 46 del RDL 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (LPS).

SEGUNDO.- Se debate con carácter principal la existencia de autorización en transferencia ejecutada el 24.8.2021 en cuenta demandante a través de sistema de banca electrónica de la entidad bancaria interpelada, en orden a concluir la correcta o incorrecta aplicación de sistema de autenticación reforzada por el proveedor del servicio y el proceder diligente o negligente del usuario.

Constituye marco legal aplicable el Reglamento Delegado (UE) 2018/389 de la Comisión de 27.11.2017 que completa Directiva (UE) 2015/2366 sobre normas técnicas de regulación para la autenticación reforzada, el RDL 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera (LSP), y los arts. 147 y 148 LGDCU.

El RDL 19/2018 establece en el art. 44.1 la carga probatoria del proveedor sobre la autenticación de la operación ante negativa del usuario, sentando la responsabilidad del usuario que actúe de modo fraudulento o con negligencia grave (arts. 44.3 y 46.1) y fijando como obligaciones esenciales del citado usuario la protección de sus credenciales de seguridad personales y la comunicación sin de mora al proveedor del servicio en casos de extravío, sustracción o utilización no autorizada (art. 41). Por su parte, el prestador del servicio deberá garantizar el control técnico adecuado y debidos niveles de seguridad en la operativa, respondiendo por daños y perjuicios en caso de incumplimiento (arts. 148 y 147 LGDCU).

A la hora de estudiar la concurrencia de negligencia grave del usuario del servicio de pago on line, partiendo del admitido criterio de responsabilidad cuasi-objetiva de la entidad en la prestación del servicio de banda virtual respecto a operaciones de pago como la transferencia, reiterada jurisprudencia considera que dicha negligencia debe ser grave en atención a las circunstancias demostradas del caso, atribuyéndose en todo caso la carga probatoria de la misma al proveedor del servicio con arreglo a art. 217 LEC. ***En interpretación de directiva 2015/2366, la negligencia que 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 haya podido ser inducido por un delincuente profesional. Como parámetro del actuar negligente también cabrá acudir al art. 1.104 CC, que exige la diligencia asociada a la naturaleza de la obligación y a las circunstancias personales, de tiempo y lugar. Ello destacándose la complejidad y grado de perfección que presenta en la actualidad el método de "phishing" de difícil detección por persona de formación media, así como el deber de la proveedora, del servicio de dotarse de tecnología suficiente y adecuada con exigencia de medidas implantadoras activas, sin entenderse suficientes avisos generales o en página web de mero carácter informativo o divulgativo -por todas, SS. AP Pontevedra (Secc. 6ª) 21.12.21 y Madrid (20ª) 20.5.2022, en la línea de lo razonado en SS. AP Valencia (6ª) 13.6.2022, Granada (5ª) 20.6.2022 y Badajoz (3ª) 21.6.2022-."***

Do mesmo modo, a sentenza da Ilma. Audiencia Provincial de Madrid do 20-5-2022, invocada pola demandante, afirmou:

"PRIMERO.- En la demanda que dio inicio a las presentes actuaciones, el demandante titular de una tarjeta de débito asociada a una cuenta corriente que tiene abierta en el BANCO DE SANTANDER, ejercita una acción en reclamación de 6.090 € en que cuantifica los daños y perjuicios que se le causaron como consecuencia de las 6 disposiciones que por un tercero desconocido, se hicieron con cargo a la cuenta de la que era titular al haber sido víctima de un uso fraudulento de la tarjeta, mediante la actuación fraudulenta denominada "phising" de la que fue víctima, cuando el recibió un SMS en móvil asociado a la tarjeta y contrato de cuenta corriente, en el que se le invitaba a hacer un clic en un enlace clonado de la página web del Banco demandado, realizando las operaciones que se le requirieron, sin que por el Banco se le hubiera advertido previamente sobre posibles fraudes o incidencias de suplantación de identidad, procediendo a continuación a descargar la aplicación que

ADMINISTRACIÓN DE JUSTICIA

ADMINISTRACIÓN DE XUSTIZA

se le ofrecía en su móvil, comprobando al día siguiente que entre los días 12 y 13 de julio se habían realizado 6 reintegros consecutivos de efectivo con su tarjeta de débito por importes de 1.000 € cada uno de ellos. Atribuye a la demandada haber incurrido en el incumplimiento que contractual y legalmente le corresponden, al no haberle alertado cuando se efectuó la primera extracción, enviándole un aviso vía SMS al teléfono móvil adherido a la tarjeta, lo que le hubiera permitido bloquearla cuando se efectuó la primera extracción y podido bloquear la tarjeta.

Invoca al respecto las obligaciones que imponen a la entidad bancaria el Real Decreto ley 19/2018 de 23 de noviembre de Servicios de Pago, la Directiva (UE) 2915/2366 del Parlamento y del Consejo, de 25 de noviembre sobre servicios de pago en el mercado interior y el Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017.

La entidad demandada se opuso a las pretensiones formuladas en su contra. Sostiene que la pérdida patrimonial sufrida por el demandante se debe a la actuación delictiva de un tercero y niega haber incurrido en los incumplimientos que se le atribuyen, en cuanto en su página web da continuas instrucciones sobre cómo prevenir el fraude e identificar el phisning, no obstante lo cual y a pesar de que del texto del correo recibido por el demandante se podía cuando menos, sospechar de que el mismo no era remitido por la entidad bancaria, el demandante, voluntariamente cliqueó el enlace y facilitó los datos que permitieron efectuar las disposiciones, que se encontraban dentro del límite autorizado y por tanto no le imponían avisar al cliente, negando que éste tuviera concertado el servicio de alerta para la tarjeta a través de la que se hicieron las disposiciones.

Frente a dicha resolución interpuso recurso de apelación la entidad demandada articulando el mismo en un único motivo de impugnación, mediante el que sostiene haberse efectuado una incorrecta valoración probatoria e incurrido en infracción de los artículos 41 y 46 del RDL 19/2018.

El demandante se opuso al recurso e impugnó la sentencia en los pronunciamientos que le resultan desfavorable, centrando su discrepancia en la negligencia que se le atribuye en la sentencia,

en cuanto insiste que conforme a la normativa nacional y comunitaria aplicable, para que el usuario quede obligado a soportar las pérdidas ha de acreditarse por la entidad demandada que el cliente actuó con negligencia grave y ésta no se puede apreciar al haber sido víctima de un delito de estafa y haber facilitado los datos personales motivado por el error a que se le indujo. Niega por otro lado, que el Banco adoptara las medidas de seguridad que le eran exigibles.

SEGUNDO.- Centrada la discrepancia en si el comportamiento adoptado por las partes aquí enfrentadas debe ser calificado como negligente, en el cumplimiento de las obligaciones que para cada uno de ellos se deriva del contrato de tarjeta de débito que les vincula y las consecuencias a extraer de todo ello, para el análisis del cumplimiento que cada una de las partes ha hecho de las obligaciones que les corresponde como titular y usuario de la tarjeta el demandante y como prestadora del servicio de pago la demandada, el marco normativo de que debe partirse viene constituido por el RDL 19/2018, que derogó la Ley 16/2009 a la que se remite la sentencia de primera instancia. La Directiva 2015/2366 y el Reglamento delegado 2018/389 de la Comisión, interpretado todo ello conforme a las reglas y principios básicos establecidos en el cc, respecto de las obligaciones y contratos y ello a la vista de todas las circunstancias concurrentes en el supuesto de hecho enjuiciado. Como se indica en la sentencia nº 539/2021 de 21 de diciembre de la Sec. 6ª (Sede Vigo) de la Audiencia provincial de Pontevedra,(ponente el Ilmo Sr. José Ferrer González), en la que se analiza un supuesto de hecho similar al presente, el marco nopr,matrivo del que debe partirse es el siguiente:

" Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015 , sobre servicios de pago en el mercado interior

Considerando:

(72) A la hora de evaluar la posible negligencia o la negligencia grave del usuario de servicios de pago, deben tomarse en consideración todas las circunstancias. Las pruebas de una presunta negligencia, y el grado de esta, deben evaluarse con arreglo a la normativa nacional. No obstante, si el concepto de negligencia

supone un incumplimiento del deber de diligencia, la negligencia grave tiene que significar algo más que la mera negligencia, lo que entraña una conducta caracterizada por un grado significativo de falta de diligencia. Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros. Se deben considerar nulas las cláusulas contractuales y las condiciones de prestación y utilización de instrumentos de pago mediante las cuales aumente la carga de la prueba sobre el consumidor o se reduzca la carga de la prueba sobre el emisor. Además, en situaciones específicas y, más concretamente, cuando el instrumento de pago no esté presente en el punto de venta, como en el caso de los pagos en línea, resulta oportuno que el proveedor de servicios aporte pruebas de la presunta negligencia, puesto que los medios a disposición del ordenante son limitados en esos casos.

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 . En vigor desde el 14 de septiembre de 2019 (artículo 38)

Artículo 1 Objeto

El presente Reglamento establece los requisitos que deben cumplir los proveedores de servicios de pago a efectos de la aplicación de medidas de seguridad que les permitan hacer lo siguiente:

a) aplicar el procedimiento de autenticación reforzada de clientes, de conformidad con el artículo 97 de la Directiva (UE) 2015/2366 ;

b) eximir de la aplicación de los requisitos de seguridad de la autenticación reforzada de clientes, bajo determinadas condiciones limitadas y basadas en el nivel de riesgo, el importe de la operación de pago y la frecuencia con que se repite, y el canal de pago empleado para la ejecución de dicha operación;

c) proteger la confidencialidad y la integridad de las credenciales de seguridad personalizadas del usuario de servicios de pago;

d) establecer estándares abiertos comunes y seguros para la comunicación entre los proveedores de servicios de pago gestores de cuenta, los proveedores de servicios de iniciación de pagos, los proveedores de servicios de información sobre cuentas, los ordenantes, los beneficiarios y otros proveedores de servicios de pago en relación con la provisión y la utilización de servicios de pago en aplicación del título IV de la Directiva (UE) 2015/2366 .

Artículo 2 Requisitos generales de autenticación .

1. Los proveedores de servicios de pago dispondrán de mecanismos de supervisión de las operaciones que les permitan detectar operaciones de pago no autorizadas o fraudulentas a efectos de la aplicación de las medidas de seguridad a que se hace referencia en el artículo 1, letras a) y b).

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.

Artículo 3 Revisión de las medidas de seguridad

ADMINISTRACION DE JUSTICIA

ADMINISTRACIÓN DE XUSTIZA

1.La aplicación de las medidas de seguridad a que se refiere el artículo 1 deberá documentarse, probarse periódicamente, evaluarse y auditarse de conformidad con el marco jurídico aplicable al proveedor de servicios de pago por auditores con experiencia en el ámbito de la seguridad y los pagos informáticos y funcionalmente independientes, ya pertenezcan al organigrama del propio proveedor de servicios de pago o sean externos a él.

.....

12. El RDL 19/2018 derogó la ley 16/2009 de 13 de noviembre de servicios de pago (disposición derogatoria única) y dispuso, en cuanto al régimen transitorio, que los contratos de servicios de pago suscritos con anterioridad a su entrada en vigor seguirían siendo válidos pero en todo caso habría de aplicarse las disposiciones de carácter imperativo que resulte más favorables para los consumidores y microempresas (Disposición Transitoria quinta). La Disposición Final 13ª estableció un régimen de entrada en vigor de la norma de manera escalonada que, partiendo de la general vigencia desde el día 25 de noviembre de 2018 (el siguiente a la fecha de publicación de la norma en el BOE, DF 13ª.1) culminó el 14 de septiembre de 2019 (18 meses desde la entrada en vigor del Reglamento Delegado (UE) 2018/389 de la Comisión de 27 de noviembre de 2017, DF 13ª2.b) fecha desde la que habrían de aplicarse los artículos 37, 38, 39 y 68.

13. De las normas que en la legislación vigente regulan las obligaciones del proveedor y del usuario de los servicios de pago y el régimen de responsabilidad importa a efectos de este proceso considerar:

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.

.....

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) el 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 concurran 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 .

TERCERO . Responsabilidad por operaciones de pago fraudulentas.

14. El proveedor de servicios de pago se encuentra sujeto al cumplimiento de específicas obligaciones de protección en la emisión de los instrumentos de pago y en los procesos de autenticación de las operaciones de pago cuya finalidad es minimizar la probabilidad de ejecución de operaciones no autorizadas.

15. En relación con los instrumentos de pago ha de cumplir con las obligaciones sobre emisión y uso seguro que se establecen en el artículo 42.1 RDL 19/2018 .

16. Los procesos o mecanismos de autenticación de las operaciones de pago deben cumplir con los requisitos que establece el Reglamento Delegado 2018/389 , lo que exige:

- a) Implementar las medidas de seguridad previstas en el artículo 1, que han de incluir el procedimiento de autenticación reforzada de clientes, con las salvedades específicamente señaladas.

- b)Incluir mecanismos de supervisión de las operaciones que permitan al proveedor de servicios de pago detectar operaciones de

pago no autorizadas o fraudulentas. A tal efecto el proveedor de servicios de pago ha de tener en cuenta la totalidad de los factores de riesgo enumerados en el artículo 2, y, entre ellos, los supuestos de fraude conocidos en la prestación de servicios de pago.

- c) Auditar las medidas, en las condiciones del artículo 3.

17. El usuario de los servicios de pago deberá cumplir con las obligaciones que se establecen en el artículo 41 RDL 19/2018 : a) Usar del instrumento de pago conforme a lo pactado y tomar las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas; b) En cuanto tenga conocimiento de haber perdido la posesión del instrumento de pago o de haber sido este utilizado sin su autorización, lo notificará sin demora indebida al proveedor de servicios de pago.

18. El régimen de la responsabilidad por las pérdidas derivadas de operaciones de pago por uso fraudulento de un instrumento de pago por un tercero se determina interpretando de manera integrada las previsiones del artículo 46 con la regulación general de las pérdidas por operaciones de pago no autorizadas del artículo 45 y con el régimen de la carga probatoria que se establece en el artículo 44 (todos del RDL 19/2018).

19. Será el proveedor de los servicios de pago quien habrá de responder de las pérdidas de importe superior a 50 euros por las operaciones de pago resultantes del uso fraudulento del instrumento de pago por un tercero; responderá de la totalidad de la pérdida cuando al ordenante no le hubiera sido posible detectar el posible uso fraudulento antes de que éste se hubiese materializado o cuando la pérdida se debiera a la acción u omisión de cualquier persona de la que el proveedor de servicios hubiera de responder.

20. El ordenante será quien soporte la totalidad de las pérdidas cuando concurran dos requisitos: a) La operación de pago fue autenticada y registrada con exactitud y no se vio afectada por ninguna deficiencia del servicio prestado por el proveedor de servicios de pago; b) El ordenante actuó de manera fraudulenta, o incumpliendo deliberadamente o por negligencia grave alguna de las obligaciones recogidas en el artículo 41 RDL 19/2018 .

ADMINISTRACIÓN DE JUSTICIA

ADMINISTRACIÓN DE JUSTICIA

21. Al proveedor de servicios de pago le corresponde la carga procesal de acreditar tanto su propio comportamiento diligente en la autenticación de la operación de pago como el fraude o la negligencia grave del ordenante. La prueba de la diligencia en el procedimiento de autenticación deberá realizarse en relación a las exigencias del Reglamento Delegado 2018/389 . La prueba del fraude del ordenante requerirá de la acreditación de hechos de los que pudiera llegar a inferirse que aquel actuó con engaño para beneficiarse de la operación de pago. La prueba de la negligencia grave del ordenante requerirá de la acreditación de las circunstancias concurrentes en la operación de pago de las que quepa inferir que la misma pudo realizarse porque aquel obró con una significativa falta de diligencia al usar del instrumento de pago o al proteger sus credenciales.

22. Cuando el proveedor de servicios de pago no acredite el cumplimiento de los deberes de diligencia propios en la autenticación habrá de responder de la pérdida resultante del uso fraudulento del instrumento de pago por un tercero salvo que concurra el fraude del ordenante."

TERCERO.- La aplicación de la normativa anteriormente indicada al caso presente, nos lleva a estimar la impugnación formulada por el demandante en cuanto, no discutiéndose la forma en que se llegaron a materializar las 6 retiradas de efectivo por un importe total de 6.000 €, iniciadas por una actuación fraudulenta de tercero, no cabe apreciar en el demandante un comportamiento negligente de la gravedad y entidad para con base en el mismo hacerle responsable, ni siquiera de la primera disposición de efectivo realizada con la tarjeta usada de manera fraudulenta por un tercero. ***Como se indica 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. Tampoco puede calificarse como grave dicho comportamiento conforme a la normativa del código civil, pues siendo exigible al demandante la diligencia que exija la naturaleza de la obligación y correspondan a las circunstancias de las personas, tiempo y lugar (art. 1.104 del cc), el método fraudulento empleado - phishing- es de una complejidad y grado de perfección, dificilmente detectable por un cliente de las características del***

demandante, sin que la forma en que se denominaba al Banco en el SMS recibido o el error gramatical al emplear la palabro "lo" en lugar de "le", sean errores de entidad suficiente para detectar con base en ellos el fraude de que estaba siendo objeto. En esas circunstancias, era preciso ser un experto en la materia para poder detectar que la comunicación obedecía a una estafa o fraude. Es cierto que dicho comportamiento no puede considerarse diligente, pero para hacer soportar al cliente las consecuencias, aún parciales como se concluye en la sentencia apelada, es preciso apreciar en él una negligencia y que además sea grave, que en la normativa europea antes referida se equipara a la comisión de un fraude, actuación en la que no se ha acreditado incurriese el demandante, por el hecho de haber pinchado el link que se le ofrecía y facilitar los datos y clave de la tarjeta

*CUARTO.- **Por el contrario, la responsabilidad exigida a la entidad demandada, como proveedora del servicio, es la que se deriva de la naturaleza de tal prestación y de la posición contractual en la que se encuentran las partes, lo que le obliga a adoptar una serie de medidas de seguridad y dotarse de mecanismos de supervisión que permitieran detectar operaciones fraudulentas en la prestación de servicios de pago, tal como señala el artículo 2 del Reglamento Delegado 2018/389**, pues como se indica también en la sentencia citada de la Audiencia de Pontevedra, incluyendo la técnica del phishing, la creación y puesta en la red de páginas que clonan las del sitio oficial de las entidades emisoras de instrumentos de pago, el deber de diligencia de la entidad demandada exigía dotarse de la tecnología antiphishing precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas, lo que, de producirse, impediría que el defraudador pudiera hacerse con las credenciales del usuario del instrumento de pago por ella emitido, pues la rotura del enlace del correo electrónico haría ya ineficaz cualquier conducta que frente al mismo pudiera observar el usuario receptor. Dicha actuación diligente no puede considerarse acreditada por las información que se facilita a los clientes a través de su página web, en cuanto la efectividad de esas obligaciones preventivas, lo que requerían era implementar en el sistema informático el mecanismo tecnológico adecuado para evitarlo; es decir mediante una con una conducta activa y no simplemente informativa o divulgativa.*

De dicha omisión, no puede quedar exonerada por el hecho de que el cliente no tuviera activado el sistema de alarma en la tarjeta utilizada fraudulentamente, pues siendo obligación suya adoptar las

medidas de seguridad adecuadas, esa obligación no puede entenderse cumplida con la simple puesta a disposición del cliente, sino que es ella quien debe adoptar una actitud activa para su implantación, no solo ponerla a disposición del cliente.

En consecuencia, la demandada incurrió en un incumplimiento de los deberes de diligencia en la prevención del fraude mediante phising, que le hace ser responsable del perjuicio total sufrido por el demandante, pues no podía la entidad desconocer que frecuentemente mediante esa técnica el tercero defraudador utiliza los datos de la tarjeta para activarla en una aplicación de pago de la que tiene dominio, por lo que debiendo conocer que el teléfono desde el que se le había solicitado la activación no se encontraría entre los que hubiera registrado su nombre el demandante en su ficha de cliente, la comunicación del número de terminal telefónico devenía exigible para que aquélla pudiera conocer que era un tercero quien podría disponer de los datos de la tarjeta mediante la aplicación de pago que se activaría.

No habiendo quedado acreditado que la entidad demandada cumplió en la forma que le es exigible los deberes de diligencia en la autenticación de las operaciones de pago, pues ni habría probado haber implementado un mecanismo antiphising de protección de los usuarios de los instrumentos de pago por ella emitidos frente al uso fraudulento por un tercero de páginas imitativas de las propias para hacerse con las credenciales del instrumento, ni habría puesto en conocimiento del usuario los datos necesarios para que este conociera que se trataba de instalar su tarjeta en una aplicación de pago de un terminal de un tercero y no apreciándose que el demandante incurrió en negligencia grave en el cumplimiento de sus deberes de custodia y uso de la tarjeta, ha de declararse la responsabilidad de la entidad demandada como proveedora de los servicios de pago usados de manera fraudulenta por un tercero y por tanto es quién debe responder de las pérdidas sufridas por el demandante con tales operaciones, responsabilidad que se hace extensible a la totalidad de la pérdida, pues en momento alguno anterior a que se realizase la última de las operaciones fraudulentas de pago, la entidad demandada había informado a la demandante del número del terminal telefónico desde el que se estaban realizando las órdenes de pago fraudulentas, ni de circunstancia alguna que hubiera permitido conocer al demandante tal uso fraudulento."

En cambio, a sentenza de 1lma. Audiencia Provincial de Pontevedra do 1-12-2020, invocada pola demandada, afirmou:

"Sobre la responsabilidad por la transferencia desde la cuenta bancaria del demandante.

13 Estima el recurrente que debía haberse apreciado la responsabilidad de la entidad bancaria como proveedora del servicio de pago alegando, en esencia, que resulta evidente que, en el caso, hubo un incumplimiento contractual del banco al ejecutar una orden de pago sin comprobar su legitimidad es decir, que provenía efectivamente del titular (o autorizado) de la cuenta, no disponer de un sistema adecuado de seguridad que previera tal tipo de órdenes fraudulentas y sobre todo, al no revertir la orden realizada fraudulentamente por los estafadores cuando toma conocimiento de una situación operativa anormal.

14 En la sentencia de primera instancia se estima probado que por los registros de la operación litigiosa ésta se realizó desde el dispositivo móvil del demandante, asociado al contrato de banca electrónica, desde su dirección IP y con marcado correcto del PIN que es elemento de seguridad, por lo que resulta ahora suficiente con indicar que tal apreciación encontraba fundamento en el contenido del informe de fraude CE 1036/2019 sobre la operación de pago que se había aportado con la contestación a la demanda (en el que tras recogerse el registro de instalación de la aplicación de banca móvil que se había realizado por el hoy demandante el día 4 de diciembre de 2018, y el registro de la operación de transferencia realizada el 3 de octubre de 2019, se concluye que la dirección IP de conexión desde la que se hizo la presunta operación fraudulenta es la habitual utilizada por el cliente; además el dispositivo móvil desde el que se hizo la operación, Huawei ATU L21 con sistema operativo Android, es también el mismo que el cliente venía utilizando de forma masiva desde diciembre de 2018, pues la única consideración que en el recurso se realizan sobre la realización de la transferencia desde la aplicación del teléfono móvil del demandante (señalando que resulta cronológicamente imposible hacer la transferencia (día tres) antes de la llamada-estafa (día cuatro) e instalación) carece de atendibilidad lógica pues aparece realizada tomando en consideración únicamente el día del mes sin tener en cuenta la diferencia en el mes y el año y el diferente tipo de operación a los que ambas datas se refieren (una a la instalación de

la banca móvil en el teléfono del demandante, y otra a la operación de pago disculida).

19 La relevancia de la cuestión atinente al dispositivo desde el que se habría realizado la operación de transferencia se evidencia si consideramos que en la demanda únicamente se refería el acceso fraudulento de un tercero al ordenador del demandante para realizar una limpieza de virus, sin referencia alguna a la utilización indebida del teléfono móvil del demandante, y que, como resulta de las explicaciones dadas en el acto de juicio por don Ricardo Rodríguez Gómez, autor del informe de fraude aportado, para la realización de la transferencia era necesario disponer físicamente del dispositivo móvil, acceder a la aplicación de banca electrónica, introducir el PIN y teclear la operación. Tampoco en el recurso se llega siquiera alegar que el teléfono móvil del demandante hubiera sido indebidamente utilizado por un tercero para realizar la transferencia En tales circunstancias fácticas de realización de la transferencia desde el teléfono móvil del demandante del que ni siquiera se alega uso indebido por un tercero necesariamente habrá de considerarse que la operación se realizó encontrándose en su poder tanto el dispositivo desde el que se accedió a la aplicación usada para la operación como las credenciales personales de seguridad que permitieron autenticarla, por lo que carecían ya de relevancia las alegaciones del recurso sobre las operaciones de comprobación de la legitimidad de la orden de pago que se dice debía haber realizado la entidad bancaria en atención al destino o importe de la transferencia.

16 En el desarrollo de la segunda de las razones por las que en el recurso se estima que debía haberse apreciado la responsabilidad de la entidad bancaria (no revertir la orden realizada fraudulentamente por los estafadores cuando toma conocimiento de una situación operativa anormal) se comienza con la cita del artículo 43 del RDL 19/2018 por lo que importa considerar que la citada norma regula el derecho del usuario de servicios de pago de obtener del proveedor de tales servicios la rectificación de aquellas operaciones no autorizadas o ejecutadas incorrectamente siempre que la petición se comunique sin demora injustificada . La rectificación o anulación de la orden de pago supone que el banco deberá proceder, de forma inmediata a recibir la petición del usuario, a realizar las labores oportunas para dejarla sin efecto lo que supondrá, en el caso de que la petición del usuario se hubiese realizado cuando todavía el dinero se encontrara en la cuenta bancaria a la ausencia de realización del movimiento solicitado en su día, o, en el caso en

que la comunicación del usuario fuese realizada cuando los fondos ya se hubiesen transferido a a la cuenta bancaria del beneficiario, a iniciar el procedimiento de retrocesión, solicitando, también sin demora, de la entidad bancaria en la que ésta se encuentre abierta la devolucion de la cantidad transferida.

17 En la sentencia de primera se señala que tampoco se ha justificado irregularidad alguna en la ejecución por Abanca de la revocación de la transferencia; en el informe que se aporta con la contestación a la demanda se indica que tal comunicación se hizo el día 4 , día siguiente la ejecución de la transferencia, declarando el testigo que esa orden se gestiona por un proceso interbancario y que en este caso no se pudo recuperar la transferencia porque ya no había fondos en la cuenta de destino como es habitual en estos casos. De tal apreciación el recurrente únicamente discrepa de la fecha en que habría realizado la comunicación señalando que llamó por teléfono de forma inmediata -el día 3 no el día 4- para anular la transferencia realizada

18 Contrariamente a lo que se afirma en el recurso ni en la denuncia policial (folios 13 y 14), ni en la posterior reclamación al banco (folio 15) se concreta el día y hora en que el usuario hubiese llamado al banco solicitando la anulación de la transferencia. Tampoco se señala con claridad tal datación en el escrito de demanda, por lo que la ausencia de referencia al mismo en el escrito de contestación de la demandada carecería de toda virtualidad a efectos probatorios, máxime si se considera que con la misma se aportaba el informe de fraude en el que se sitúa cronológicamente la llamada en el día 4 de octubre de 2019. En todo caso, la acreditación de la fecha de comunicación de la petición de rectificación de la transferencia que se estima la sentencia primera instancia aparece acreditada por la copia del registro de gestión de devolución de transferencias que aparece inserta en el informe de fraude ya referido (folio 40 vuelto) en el que consta como fecha de la solicitud de devolución de la de 4 de octubre de 2019 y hora 00.44.06.

19 Alega el recurrente que el entidad bancaria a pesar de esta llamada-reiteramos, inmediata-no revoca la transferencia ello supone la clara infracción del artículo 45 RDL 19/2018 .

20 El artículo 45 del RDL 19/2018 regula el régimen de la responsabilidad del proveedor de servicios de pago cuando se realicen operaciones de pago no autorizadas, por lo que su interpretación sólo puede realizarse de manera conjunta con el artículo 46 en el que se regula la responsabilidad del ordenante en los mismos supuestos de operaciones de pago no autorizadas, siendo aplicable al caso lo previsto en el párrafo segundo del número 1 de este último artículo en el que se dispone: 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."

CUARTO.- **Considero que o presente caso é similar ao analizado nas dúas primeiras sentenzas expostas no fundamento de dereito anterior. Considero que os razoamentos dados nas dúas primeiras sentenzas expostas no fundamento anterior son plenamente aplicables ao presente caso no que non consta neglixencia grave do demandante, non consta que os feitos se teñan producido pola súa iniciativa. Considero que o demandante (funcionario xubilado) non actuou con neglixencia grave, non consta que tomase a iniciativa e é difícil de detectar a posta en escena dos autores da defraudación que logran dotar dunha apariencia de seriedade as súas operacións para obter os datos das persoas coas que contactan. O feito de que o demandante fose funcionario na súa vida profesional non impide que poida caer fácilmente nos enganos desta clase especial de defraudadores.**

En cambio, considero que si existiu un relevante incorrecto modo de proceder da demandada. Consta nos folios 22 e 23 que as cuantías das que se dispoñía coa tarxeta eran pequenas (a cantidade maior fora de 600 euros) e, en cambio, o 11 de agosto do 2021, nun só día, aparecen cantidades elevadas (8000, 8000, 10000, 12000, 11000, 20000, 30000, 50000, 50000, 10000). Considero que a demandada, se tivese establecido mecanismos de control adecuados, podería ter fácilmente detectado o que resulta claro para calquer persoa media, que a realización de operacións nun só día (o 11-8-2021) polas cuantías expresadas non se correspondía co modo normal de actuar do demandante (un funcionario xubilado que só realizaba coas tarxetas as operacións normais que se espera que un funcionario xubilado faga cunha tarxeta, pequenos gastos da vida diaria de calquer persoa ou familia) **e que, detrás deses actos, estaba unha actividade ilícita dun terceiro, un defraudadador que ilícitamente tivera acceso aos datos do demandante para poder realizar esas operacións. Considero que, en definitiva, procede estimar a demanda.**

Considero que o criterio mantido na sentenza da Ilma. Audiencia Provincial de Pontevedra do 1-12-2020 non é aplicable no presente proceso porque neste caso é claro que se a demandada tivese actuado cunhas adecuadas medidas de precaución podería ter detectado moi fácilmente que non era o demandante o autor dunhas disposicións de diñeiro que excedían moi amplamente das que ususlmente realizaba o actor, sen corresponderse con ningunha das operacións que normalmente levaba a cabo o demandante. **Considero que a demandada, actuando coa debida dilixencia, debe establecer un mecanismo que impida a consumación dunha transferencia (sen confirmación a través do consentimento prestado persoalmente en oficina bancaria polo cliente da demandada) cando a transferencia exceda notablemente da cuantía das operacións que o cliente realiza habitualmente ou non se corresponda coas operacións que normalmente leva a cabo o cliente.**

Como resume, considero que procede estimar a demandada por incumprimento do art. 1902 do Código Civil en relación con Reglamento Delegado (UE) 2018/389 da Comisión de 27.11.2017 que completa Directiva (UE) 2015/2366 sobre normas técnicas de regulación para a autenticación reforzada, o RDL 19/2018, de 23 de novembro, de servizos de pagamento e outras medidas urxentes en materia financieira (LSP) e os arts. 147 e 148 LXDCU.

QUINTO.- En materia de xuros considero que, se ben os feitos tiveron lugar o 11-8-2021, a recta aplicación do art. 1100 do Código Civil determina que a condena ao pagamento de xuros só sexa a partir do 20-10-2021, data da primeira reclamación extraxudicial (folio 30).

SEXTO.- En materia de custas procesuais, examinado o art. 394 LAC, sendo a sentenza estimatoria, procede condenar á demandada ao pagamento das custas procesuais orixinadas no presente proceso.

DECIDO

Estimo a demanda.

Condeno á demandada a abonar ao demandante o importe de 185849,15 euros, cos seus xuros legais dende o dia 20-10-2021.

Condeno á demandada ao pagamento das custas procesuais orixinadas no presente proceso.

Contra esta sentenza cabe recurso de apelación, a interpoñer no prazo de 20 días a partir da súa notificación, ante este Xulgado, para posterior resolución pola Ilma. Audiencia Provincial de Lugo.

Notifíquese ás partes.