Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Facultad de Derecho

MÁSTER EN ABOGACÍA Y PROCURA

TRABAJO FIN DE MÁSTER

PHISHING BANCARIO: NORMATIVA Y JURISPRUDENCIA SOBRE OPERACIONES DE PAGO NO AUTORIZADAS

Alumno: Juan Ramón Díaz García

Convocatoria: Ordinaria Diciembre/Enero

RESUMEN

Este trabajo analiza el régimen de responsabilidad cuasi-objetiva que la Ley de servicios de pago impone a los proveedores de este tipo de servicios en relación con las operaciones no autorizadas por los usuarios. Para ello, se estudian los principales métodos del *phishing* bancario, junto con la regulación a nivel legal de estas operaciones, así como sus aspectos prácticos, destacando especialmente la jurisprudencia dictada por nuestras Audiencias Provinciales.

Del análisis realizado se puede comprobar cómo la presencia de negligencia grave en la conducta del usuario es la cuestión en torno a la cual orbitan las resoluciones judiciales en esta materia, que matizan y complementan la normativa para su aplicación al caso concreto según el tipo de fraude de que se trate.

Por tanto, el objetivo final de este trabajo es abordar este tipo de asuntos desde una perspectiva completa, tratando de abarcar desde el propio fraude hasta su consecuencia final, poniendo el foco especialmente en aquellos elementos que hacen del *phishing* una cuestión de plena actualidad.

ABSTRACT

This paper analyses the quasi-objective liability regime that the Payment Services Act imposes on payment service providers in relation to unauthorised transactions by users. To this end, the main methods of bank phishing are studied, together with the legal regulation of these operations, as well as their practical aspects, with particular emphasis on the case law handed down by our provincial courts.

From the analysis carried out, it can be seen how the presence of gross negligence in the user's conduct is the issue around which the judicial decisions on this matter orbit, which qualify and complement the regulations for their application to the specific case depending on the type of fraud in question.

Therefore, the final objective of this work is to approach this type of matter from a complete perspective, trying to cover from the fraud itself to its final consequence, focusing especially on those elements that make phishing a highly topical issue.

ABREVIATURAS Y ACRÓNIMOS

AEPD ..... Agencia Española de Protección de Datos

art. (s) ..... artículo (s)

AAPP ..... Audiencias Provinciales

AP ..... Audiencia Provincial

BDE ..... Banco de España

BOE ..... Boletín Oficial del Estado

CEO ..... *Chief Executive Officer*

cfr. ..... confróntese

FJ ..... fundamento (s) jurídico (s)

JPI ..... Juzgado de Primera Instancia

INCIBE ..... Instituto Nacional de Ciberseguridad

INE ..... Instituto Nacional de Estadística

LEC ..... Ley de Enjuiciamiento Civil

LSP ..... Ley de Servicios de Pago

núm. (s) ..... número (s)

ob. cit. ..... obra citada

pág. (s) ..... página (s)

RDLey ..... Real Decreto-Ley

rec. ..... recurso

ss. ..... siguientes

SAP ..... Sentencia de la Audiencia Provincial

SJPI ..... Sentencia del Juzgado de Primera Instancia

STJUE ..... Sentencia del Tribunal de Justicia de la Unión Europea

vid. ..... véase

ÍNDICE

1. INTRODUCCIÓN

Este Trabajo Fin de Máster tiene por objeto el estudio de los principales aspectos que caracterizan al *phishing* bancario desde su perspectiva jurídica. A mi parecer, esta es una materia que resulta muy interesante de abordar en un trabajo como este, enfocado a la práctica jurídica en el marco de un máster habilitante para la profesión de la abogacía.

La combinación de elementos jurídicos muy específicos, entroncados con aspectos fundamentales del derecho, y de cuestiones técnicas, dan lugar a que se trate de un tema atractivo para desarrollar en un trabajo de estas características. Además, por supuesto, de la actualidad e importancia que presenta el *phishing* en las resoluciones dictadas por nuestros tribunales.

Y es que este "fenómeno" ha experimentado un enorme crecimiento durante los últimos años, tal y como se refleja en el aumento del número de víctimas afectadas por este tipo de fraudes, quienes ven sustraídos sus fondos depositados en cuentas bancarias.

Siendo esto así, puede afirmarse que esta situación encuentra su origen, en gran medida, en el hecho de que en los últimos años se han generalizado los servicios de banca electrónica, los cuales, si bien tienen muchas ventajas para los usuarios de servicios de pago, también implican un gran riesgo al suponer un aumento de los fraudes a través de estas técnicas de *phishing.*

Estos ciber fraudes se desarrollan mediante una amplia variedad de modalidades defraudatorias que combinan conocimientos de informática y telecomunicaciones con técnicas de ingeniería social mediante las cuales obtener las credenciales y códigos de seguridad de los usuarios.

Frente a este aumento de la cibercriminalidad, se erige la LSP como la norma reguladora en materia de operaciones no autorizadas por los usuarios de servicios de pago, estableciendo una responsabilidad cuasi-objetiva para el proveedor estos servicios, generalmente una entidad bancaria, con respecto a estas operaciones.

Las disposiciones establecidas en la LSP encuentran su plasmación práctica en la reclamación de los fondos sustraídos mediante las operaciones no autorizadas a través de la vía judicial, la cual se ve caracterizada por las particularidades procesales que tienen lugar en este tipo de procedimientos, los cuales versan sobre las reclamaciones de los importes sustraídos consecuencia del fraude en el marco del ejercicio de acciones de responsabilidad.

Junto a la realidad práctica, la normativa es moldeada por la jurisprudencia, que la interpreta y determina los estándares que han de ser tenidos en cuenta para considerar si en la conducta del usuario concurre negligencia grave, así como si el proveedor de servicios ha cumplido con las obligaciones y medidas que la normativa le atribuye.

Mayoritariamente, las resoluciones judiciales son favorables a las peticiones de los usuarios, sin que ello suponga que exista una unanimidad ni un criterio estandarizado que permita resolver este tipo de asuntos de manera genérica.

Así, para realizar el estudio de esta materia se ha seguido la misma estructura que la empleada para elaborar su presentación. Comienzo en primer lugar con la introducción a los conceptos y modalidades del *phishing* para proseguir con el análisis de la normativa reguladora de este tipo de fraudes, poniendo el foco posteriormente en los aspectos procesales más destacados y finalizando el trabajo con el análisis de la jurisprudencia dictada por nuestras AAPP.

A tal fin, se han consultado las obras doctrinales y artículos publicados sobre este tipo de fraudes, así como publicaciones y noticias que se hacen eco de los aspectos característicos del *phishing*, junto al examen de la normativa reguladora y de la jurisprudencia dictada en esta materia, todo ello complementado con la experiencia práctica obtenida a en el curso de las prácticas profesionales enmarcadas dentro de la titulación correspondiente a este trabajo.

2. EL *PHISHING*: ELEMENTOS DEFINITORIOS

El *phishing* es una práctica defraudatoria que en los últimos años ha aumentado exponencialmente, ocasionando un elevadísimo número de fraudes -principalmente en el ámbito bancario- dentro del cual pueden englobarse numerosos aspectos y cuestiones, respondiendo todos ellos a un mismo objetivo: la pesca[1] (*fish*) de datos de la víctima[2].

En cuanto a la definición de este fenómeno, puede servirnos como punto de partida el concepto ya elaborado en 2006 por la AEPD[3], que hoy en día sigue resultando plenamente válido y es recogido por la jurisprudencia para explicar este tipo de fraudes digitales. Así, en la

[1] Pescar se traduce al inglés como *fish*, siendo utilizado el término *phishing* en lugar de una traducción literal al derivar este del *phreaking* (*phone* -teléfono- + *freak* -obsesionado-), una palabra empleada en los ámbitos de la informática y las telecomunicaciones para referirse a quienes se dedican al estudio y aprendizaje sobre estas áreas, y caracterizarse el *phishing* por el empleo de métodos telemáticos.

[2] Vid. SAN MARTINO, A., & PERRAMON, X., "Phishing Secrets: History, Effects, Countermeasures", *International Journey of. Network Security*, nº 11, 2011, págs. 163-171.

[3] Ficha protección de datos y prevención de delitos (fecha de última consulta: 01/02/2025) y Guía de protección de datos y prevención de delitos (fecha de última consulta: 01/02/2025).

SAP de Jaén, Sección 1ª, 546/2024, de 24 de abril de 2024, rec. 1531/2022, se recoge tal definición: "*consiste en la obtención de forma engañosa y fraudulenta de los códigos de usuarios y contraseñas de clientes de Banca Electrónica, al objeto de realizar transferencias no autorizadas*".

Así, la realidad es que el *phishing* consiste en la captación ilícita de datos personales, principalmente relacionados con claves para el acceso a servicios bancarios y financieros a través de correos electrónicos o páginas web que imitan y copian la imagen o apariencia de una entidad bancaria o financiera[4].

Al objeto de obtener datos bancarios y credenciales de seguridad, los *phishers*, autores que perpetran este tipo de fraudes, se valen de variadas técnicas de ingeniería social y de conocimientos expertos en informática y telecomunicaciones mediante cuales logran causar en sus víctimas un grado de engaño tal, que resulta indetectable para un usuario medio de la banca electrónica.

Como se ha puesto de manifiesto, si bien el *phishing* se define como la pesca de datos, el principal fin de esta clase de estafas consiste en obtener un enriquecimiento patrimonial por parte de los ciberdelincuentes, motivo por el cual la mayor parte de fraudes se realizan suplantando la identidad de las entidades bancarias. Para completar su objetivo resulta fundamental conseguir la información bancaria de la víctima, al objeto de sustraer la mayor cantidad de fondos posible de su cuenta mediante compras con tarjeta, emisión de transferencias, suscripción de préstamos, y todas aquellas operaciones que los ciberdelincuentes son capaces de realizar sin el consentimiento, ni el conocimiento, del usuario de servicios de pago -como se verá más adelante-[5].

Llegados a este punto ha de advertirse el cambio que se ha producido en los últimos años con el avance de la tecnología y la implementación de medios telemáticos para realizar operaciones financieras, pasando de ser la banca online o electrónica un complemento de un servicio físico a, prácticamente, un elemento indispensable en la realización de las operativas bancarias más comunes.

[4] Cfr. PIQUERES CASTELLOTE, F. "Conocimientos básicos en Internet y utilización para actividades ilícitas", *Delitos contra y a través de las nuevas tecnologías ¿Cómo reducir su impunidad?*, Consejo General del Poder Judicial, Madrid, 2006, pág.71.

[5] Aunque es un sistema notorio y conocido, puesto que la mayor parte de operaciones se realizan empleando la banca electrónica, se quiere esbozar el método mediante el cual los usuarios de este tipo de banca realizamos operaciones bancarias. Así, y teniendo en cuenta que los métodos varían en función de la entidad bancaria que se trate, lo más común es que para efectuar este tipo de operaciones se introduzcan los datos bancarios del usuario y se confirmen estas mediante el envío de un código OTP (*One Time Password*) recibido por SMS.

Así, en los últimos años se ha incrementado notablemente el número de personas que emplean la banca a través de internet. Esta circunstancia ha sido impulsada por las entidades financieras mediante el cierre de oficinas y sucursales bancarias por todo el territorio nacional, convirtiendo a la banca online en un elemento intrínseco a la realización de transacciones financieras.

Al efecto de explorar con mayor detalle esta nueva realidad bancaria, es necesario poner de manifiesto que el número de entidades ha disminuido a la par que la cantidad de sucursales abiertas al público[6], pudiéndose apreciar mediante una búsqueda a través de la página web del BDE que el número de oficinas abiertas continúa en descenso[7]. Los medios de comunicación se han hecho eco también de esta circunstancia, y es que, como los usuarios prefieren realizar sus gestiones en sedes físicas, el cierre de sucursales se mantiene a la orden del día en las noticias[8].

Así mismo, es posible consultar a través del INE[9] el aumento en el uso de las nuevas tecnologías entre la población española. A los efectos de este trabajo, interesa destacar que el uso de la banca por internet ha aumentado hasta dar lugar a que el 71,5% de la población de 16 a 74 años haya empleado este servicio dentro de los tres meses anteriores a la encuesta referenciada.

Todo ello, unido también al auge de la tecnología, hace que los fraudes a través de internet sean uno de los delitos más denunciados en los últimos años, con un crecimiento exponencial, que puede comprobarse consultando el portal estadístico de criminalidad[10].

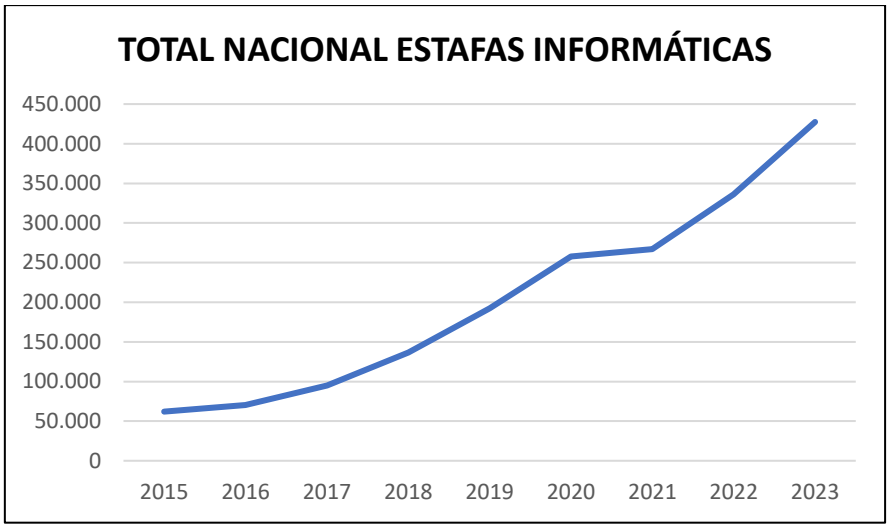
[6] JIMÉNEZ GONZALO, C. Y TEJERO SALA, H.: "Cierre de oficinas bancarias y acceso al efectivo en España", *Revista de Estabilidad Financiera / Banco de España*, nº 34, 2018, pág. 42.

[7] Los datos pueden consultarse en la página web del BDE, Registro de oficinas de entidades supervisadas, dentro del apartado "Variaciones en el número de oficinas por entidad" (fecha de última consulta: 23/01/2025).

[8] Noticia del periódico El País publicada en fecha 2 de agosto de 2024 (fecha de última consulta: 01/02/2025) y Noticia del periódico El Mundo publicada en fecha 7 de diciembre de 2023 (fecha de última consulta: 01/02/2025).

[9] Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares publicada por el INE mediante nota de prensa de fecha 28 de noviembre de 2023 (fecha de última consulta: 01/02/2025).

[10] Portal estadístico de criminalidad, filtrando los datos para obtener el total nacional de estafas informáticas (fecha de última consulta: 23/01/2025).



Fuente: Elaboración propia empleando datos del portal estadístico de criminalidad

A la hora de llevar a cabo el *phishing*, los ciberdelincuentes emplean operativas fabricadas con un gran nivel de detalle, mediante las cuales logran engañar a sus víctimas. Estos fraudes, como se ha manifestado, combinan técnicas de ingeniería social con elementos tecnológicos, como el diseño de páginas web "espejo" que imitan a la perfección los auténticos portales de inicio de sesión propios de las distintas bancas electrónicas, indistinguibles para un usuario medio dada la apariencia de autenticidad que se llega a conseguir (direcciones de internet con protocolos de transferencia de hipertexto seguro "https", mismos logos, colores y textos, etc.). Sin embargo, antes de llegar a este paso, se requiere una aproximación a la víctima, para la cual son empleados diversos métodos. Y ello nos lleva a abordar en el siguiente epígrafe las distintas modalidades empleadas para la obtención de los datos de los usuarios.

3. MODALIDADES EMPLEADAS EN EL *PHISHING*

En un principio, la mayoría de los fraudes cometidos a través del *phishing* se llevaban a cabo mediante el envío de correos electrónicos manipulados en los cuales se suplantaba la identidad de un remitente, la entidad bancaria, advirtiendo sobre algún supuesto problema que motivaba a su receptor a realizar una actuación tendente a solucionarlo con la mayor prontitud posible (por ejemplo, clicando en algún enlace que instalaba en su dispositivo un programa informático malicioso -*malware*-)[11].

Hoy en día, y aunque el *modus operandi* y el objetivo final continúan siendo los mismos, el paso del tiempo y el auge de los medios tecnológicos en la vida diaria de las personas -

[11] Así puede comprobarse, por ejemplo, en el artículo publicado en la página web de la compañía de software "McAfee": Ejemplos de *phishing*: ¿cómo detectar un correo de *phishing*? (fecha de última consulta: 01/02/2025).

principalmente, el teléfono móvil con conexión a internet-, han creado un nuevo ecosistema de métodos, combinables entre sí, destinados a captar de manera ilícita los datos personales de las víctimas.

Entre estos métodos se erigen como más utilizados tres: *smishing*, *vishing* y *SIM swapping* [12]. A continuación, se procederá a explicar en qué consisten las principales técnicas empleadas para cometeré ciber estafas, todas ahora englobadas bajo la definición más común y acertada, *phishing*, pues, como se ha advertido, el fin de esta clase de estafas no es otro que la "pesca" de datos para su uso fraudulento por parte de terceros ciberdelincuentes a la hora de sustraer los fondos depositados en las cuentas de sus víctimas.

3.1. *SMISHING*

El *smishing* consiste en el envío de un SMS a la víctima[13], suplantando la identidad de su banco, o la identidad de organismos públicos u otras empresas -por ejemplo, empresas de paquetería-, y advirtiendo de un aparente problema de seguridad (un acceso no autorizado a su cuenta, un cargo sospechoso empleando su tarjeta, etc.)- para el cual el propio mensaje contiene la solución, un enlace.

Así, los ciberdelincuentes son capaces de enviar un SMS en el que figura como remitente la entidad bancaria, empleando la técnica conocida como *spoofing*[14], y dado que los mensajes son clasificados por el teléfono según su remitente, el mensaje se inserta en el canal

[12] La jurisprudencia también refleja este tipo de técnicas, pudiendo consultarse por ejemplo el Auto dictado por la AP de Barcelona, Sección 9ª, 447/2019, de 19 de julio de 2019, rec. 753/2018 que ilustra las modalidades del *phishing*:

"actividad ilícita enmarcada en lo que se denomina "phishing ",técnica defraudatoria consistente en el envío masivo, fundamentalmente a usuarios de la banca on-line, bien de correos electrónicos, que es lo más habitual, bien de mensajes a través de SMS, -lo que se conoce como Smishing - o incluso a través de llamadas telefónicas - el denominado Vishing-, en que los autores, haciéndose pasar por empresas o fuentes fiables, especialmente entidades bancarias, y alegando supuestas razones de seguridad, les solicitan que faciliten aquellas contraseñas o datos confidenciales necesarias para operar telemáticamente en las webs bancarias, o bien les solicitan que pinchen en algún enlace que les redirecciona a una página idéntica a la oficial de dichas entidades o les introducen virus informáticos capaces de apoderase de sus claves, -el denominado Pharming que puede dirigirse a ordenadores concretos o directamente a los servidores DNS-, de suerte que cuando el usuario opera en dichas páginas clonadas introduciendo su claves de acceso, lo hace en la confianza de se trata de la página original de su entidad bancaria, facilitando de este modo a los autores, sin saberlo, sus claves confidenciales"

[13] Cfr. YEBOAH-BOATENG, E. O. y AMANOR, P.M.: "Phishing, SMiShing & Vishing: an assessment of threats against mobile devices", *Journal of Emerging Trends in Computing and Information Sciences*, 2014, vol. 5, nº 4, pág. 297.

[14] El *spoofing* es una técnica por la cual resulta posible falsificar la identidad (ID) del remitente de un SMS, pudiendo ser falsificado también el emisor de una llamada o una dirección de correo electrónico, entre otros. Existen páginas web que permiten realizar este tipo de falsificaciones, fundamentales a la hora de llevar a cabo los fraudes, pues la apariencia de realidad en la primera aproximación a la víctima marca la actuación posterior de esta ante la comunicación recibida.

habitual que el banco emplea para comunicarse con su cliente (códigos para realizar compras, publicidad, etc.), dando lugar a una total apariencia de realidad.

Normalmente, se realizan campañas de envío de SMS a clientes de una o varias entidades bancarias, suplantando la identidad de estas. Si bien hubo un tiempo en el que los ciberdelincuentes optaban por envíos masivos de SMS –"pesca" de arrastre-, pudiendo los mensajes recibidos resultar sospechosos por no coincidir el remitente con el verdadero banco del receptor del mensaje o contener faltas de ortografía en el texto, en la actualidad los SMS enviados tienen un gran nivel de detalle pues los ciberdelincuentes han perfeccionado su contenido.

Así mismo, les ha resultado posible obtener los datos de los clientes de las entidades bancarias mediante su compra en páginas web destinadas a este tipo de fines o debido a brechas de seguridad del banco. De esta forma, se han conseguido realizar de campañas de envío de SMS totalmente precisas, en las que concuerda la identidad del banco remitente con el banco del destinatario del mensaje.

En otras ocasiones, los SMS no suplantan directamente la identidad del banco, si no que aparentan ser comunicaciones provenientes de instituciones públicas como los -famosos y falsos- SMS de la Dirección General de Tráfico avisando de una multa junto con un enlace para hacer frente a su pago, o los envíos de SMS por parte de empresas de paquetería -de nuevo falsos- que advierten sobre un problema con la entrega del paquete y emplazan a acceder a un *link* a través del cual realizar el pago correspondiente a los gastos necesarios para solucionar el problema.

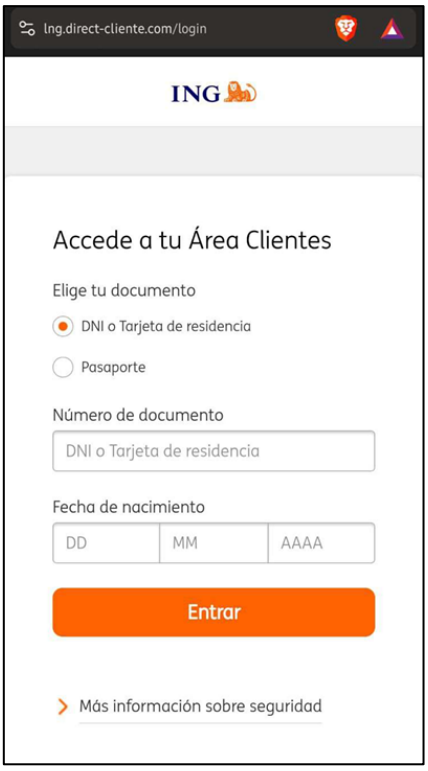
A continuación, se inserta una imagen ilustrativa de este tipo de fraudes que permite ver cómo se insertaría en el canal habitual de comunicaciones un SMS fraudulento que lleva adjunto un enlace[15].

[15] Imagen obtenida de la página web del BDE: Suplantación de SMS y del identificador de llamadas (fecha de última consulta: 01/02/2025).

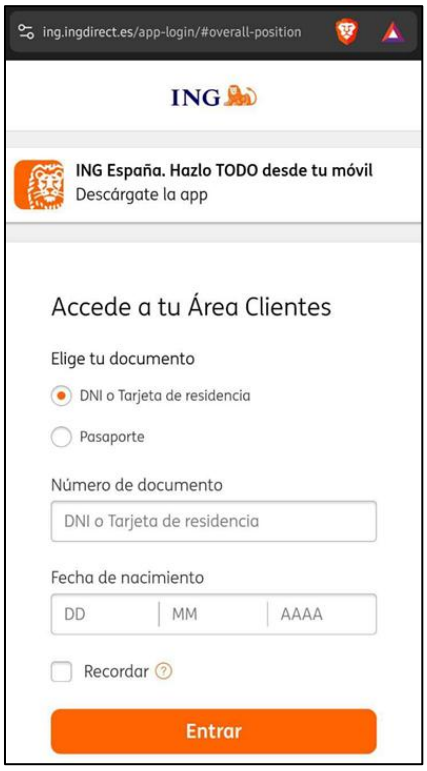
Fuente: Página web del BDE

Si se examina el contenido de este tipo de mensajes, puede comprobarse cómo el enlace enviado tiene todos los visos de ser real, pues la dirección que muestra contiene palabras clave, normalmente precedidas de un protocolo de transferencia de hipertexto seguro (“https”). A pesar de ello, se trata de un enlace fraudulento que en la mayoría de los casos redirige a una página web falsa, la cual imita a la perfección el auténtico portal de banca electrónica de la entidad bancaria, destinada a captar los datos financieros de la víctima.

Con el fin de ilustrar también el tipo de página web al que se hace referencia y su diseño imitando a la banca online de las distintas entidades, se insertan a continuación dos capturas de pantalla, una de la verdadera banca online de la entidad “ING” y otra de la web “espejo” imitando la apariencia de esta. Ambas capturas han sido obtenidas de mi experiencia en la práctica profesional sobre este tipo de fraudes, al haber sido realizadas por una víctima de *phishing* bancario.



Captura de pantalla de la página web falsa



Captura de pantalla de la página web auténtica

Fuente: Práctica profesional

En otras ocasiones, el enlace no redirige a ningún tipo de página web, debido a que tras hacer clic o pulsar sobre el mismo se instala de manera automática un programa malicioso –*malware*- destinado también a captar los datos bancarios del usuario, sin que este pueda percatarse de ello[16].

Además de los mensajes que llevan aparejados algún tipo de enlace, suele ser habitual que los ciberdelincuentes empleen los denominados SMS "de refuerzo" que les permiten ganarse la confianza de los usuarios gracias a comunicaciones remitidas a través del canal habitual que indican, por ejemplo, la supuesta cancelación de una operación sospechosa.

Es a través de este tipo de mensajes como los ciberdelincuentes consiguen ir mellando poco a poco las sospechas que el usuario pueda tener, incidiendo con comunicaciones precisas en la autenticidad de las instrucciones que las víctimas van recibiendo en el transcurso de la operativa defraudatoria.

Por último, ha de mencionarse una variante del *smishing*, el conocido como *wishing* cuyo método es idéntico con la salvedad de que las comunicaciones a la víctima del fraude no

[16] Esta afirmación puede comprobarse en el artículo publicado en la página web de la compañía de software "McAfee": ¿Cuáles son los riesgos de hacer clic en enlaces maliciosos? (fecha de última consulta: 01/02/2025).

se producen mediante el envío de SMS, sino que se llevan a cabo empleando la plataforma de mensajería instantánea "WhatsApp", utilizada a diario por millones de usuarios.

3.1.1. Enrolamiento de tarjetas bancarias en plataformas de pagos para móviles

En este momento, me gustaría detenerme en la vinculación de las tarjetas bancarias de los usuarios en plataformas de pagos para móviles como "Apple Pay", "Google Pay" o "Samsung Pay", por la peligrosidad que presenta este tipo de fraudes para quien es víctima de ellos.

Habitualmente, los códigos de un solo uso que son enviados a los usuarios por SMS tienen por fin la autorización de operaciones de pago, como pueden ser compras con la tarjeta bancaria. Sin embargo, existe una alternativa a la ejecución directa: el código para enrolar su tarjeta en una plataforma de pagos para móviles.

Una vez se vincula la tarjeta en una plataforma de este tipo, el ciberdelincuente tiene a su merced la posibilidad de realizar cuantas operaciones quiera realizar hasta agotar el límite dispuesto en la tarjeta bancaria. Esto es así ya que se entiende realizada la doble autenticación, -que se explicará más adelante- con el envío de un solo código mediante SMS -el cual no informa sobre el dispositivo al que se está vinculando la tarjeta bancaria-, motivo por el cual el ciberdelincuente puede realizar con la tarjeta del usuario un número elevadísimo de operaciones sin que este tenga conocimiento respecto a las mismas, pues ni siquiera llega a recibir las notificaciones correspondientes a las compras realizadas.

3.2. *VISHING*

Pasando ahora a la siguiente modalidad defraudatoria, la técnica del *vishing* (*voice* -voz- + *phishing*) es utilizada por los ciberdelincuentes para así sustraer de la víctima su información personal mediante una llamada telefónica en la cual los estafadores despliegan todo su entrenamiento en técnicas de ingeniería social[17].

El INCIBE la ha definido como *"un tipo de estafa de ingeniería social por teléfono en la que, a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima"*[18].

[17] Información sobre *vishing* disponible en el Portal del Cliente Bancario en la página web del BDE (fecha de última consulta: 01/02/2025).

[18] Consultado a través de la página web del INCIBE, dentro del apartado "Aprende Ciberseguridad", *Vishing* (fecha de última consulta: 01/02/2025).

La operativa más frecuente en la práctica es la combinación de esta técnica con el uso del método defraudatorio *smishing*, antes explicado, de tal forma que, tras el envío de un mensaje fraudulento contenedor de un enlace el ciberdelincuente llama por teléfono a la víctima -algunas veces de inmediato sin esperar siquiera a que el cliente de la entidad bancaria haya introducido sus credenciales de acceso en la falsa página web del banco-[19].

Es preciso en este momento poner de manifiesto que en muchas ocasiones los ciberdelincuentes llevan a cabo el fraude empleando la ya mencionada técnica del *spoofing*, una suplantación de la identidad del banco mediante la cual se consigue que figure en el teléfono de la víctima como emisor de la llamada el nombre de la entidad bancaria.

En este sentido, los estafadores son capaces los estafadores de realizar la llamada suplantando el propio número de teléfono del banco, lo cual evidencia la vulnerabilidad de los canales telefónicos designados por las entidades bancarias como los medios a través de los cuales comunicarse con sus clientes.

Durante la llamada, el ciberdelincuente se hace pasar a la perfección por un empleado de la entidad bancaria -identificándose como asesor bancario, empleado del departamento de ciberseguridad, etc.- e imita los protocolos que los auténticos trabajadores del banco llevan a cabo.

En ocasiones, las llamadas comienzan ya relatando datos personales a sus víctimas -obtenidos mediante el enlace fraudulento en casos de SMS previo o mediante fugas de datos de las entidades financieras[20], que han supuesto para el sector financiero un coste medio de 5,9 millones de dólares en 2023[21]-, desde su nombre o DNI hasta los últimos cargos de su cuenta o los dígitos de su tarjeta, dotando de una apariencia de realidad total a sus comunicaciones.

[19] La realidad es que existen herramientas gratuitas que permiten conocer cuántos usuarios han hecho clic en un enlace, permitiendo saber también el momento y lugar (geolocalización) así como el tipo de dispositivo desde el que han accedido. Estas herramientas están al alcance de cualquier usuario de internet, por lo que solo puede imaginarse la cantidad de datos a los que un ciberdelincuente experto -tal y como es habitual en este tipo de asuntos- puede tener acceso tras haber accedido al enlace fraudulento que se consigue insertar dentro del canal habitual de comunicaciones entre el cliente y la entidad bancaria.

[20] Son múltiples las noticias publicadas en medios de comunicación, disponibles para su consulta mediante una búsqueda a través de internet, que informan de los ciberataques y fugas de datos. Únicamente a efectos ejemplificativos para dejar constancia de que el *phishing* es una problemática en tremendo auge que se produce con carácter generalizado, se insertan algunas de estas noticias: Banco Santander, Deutsche Bank, Unicaja, Caja Rural, EVO BANCO, INVERSIS (fecha de última consulta: 01/02/2025). Así mismo, también las compañías telefónicas son víctimas de este tipo de ciberataques: Telefónica, Vodafone, Orange (fecha de última consulta: 01/02/2025). Con estas noticias lo que se pretende indicar es la fragilidad de los datos personales en internet, así como el hecho de que ciberdelincuentes expertos pueden obtener este tipo de información por múltiples vías.

[21] Cfr. HERNÁNDEZ DE COS, P.: "El ciberriesgo y sus implicaciones para la estabilidad financiera", *Repositorio Institucional Banco de España*, 2024, pág. 2.

Lo habitual es que, tras la imitación de los protocolos del personal del banco, el ciberdelincuente suela lograr que sea el propio usuario de la banca quien le revele los datos asociados a sus credenciales de seguridad -aunque no siempre es así pues, como se ha puesto de manifiesto, los datos bancarios de la víctima pueden obtenerse mediante otro tipo de métodos-, bajo el engaño y la creencia de que se encuentra al teléfono con un empleado de la entidad bancaria que, aparentemente, está realizando las gestiones tendentes a solucionar un problema de seguridad en su cuenta, el cual en realidad no existe.

En otras ocasiones, los ciberdelincuentes consiguen que engañar a la víctima para que sea esta quien realice una transferencia, u otro tipo de envío de dinero, con destino a una cuenta aparentemente segura que el aparente agente bancario había creado con el fin de proteger sus fondos ante una supuesta amenaza en forma de fraude ocasionado por un tercero[22].

Sin ánimo de adelantar cuestiones de la práctica jurídica en este momento, resulta preciso notar que este supuesto de fraude plantea la incógnita de si realmente se trata de operaciones no autorizadas en tanto que se realiza una transferencia cuyos datos introduce en la banca electrónica el propio usuario, siendo lo definitorio de este tipo de asuntos para considerar que falta la autorización el hecho de que las operaciones se realizan bajo el engaño orquestado por un tercero.

3.3. *SIM SWAPPING*

Otra forma de obtener los datos bancarios del usuario de forma fraudulenta consiste en realizar un duplicado de la tarjeta SIM correspondiente a su número de teléfono. Esta práctica recibe el nombre de *SIM Swapping* y ha sido reconocida como tal por la jurisprudencia menor, pudiéndose citar a tal efecto la SAP de La Rioja, Sección 1ª, 185/2024, de 18 de abril de 2024, rec. 149/2023, que define esta modalidad de fraude: *"el "SIM swapping", que consiste en duplicar de forma fraudulenta la tarjeta SIM del teléfono móvil de una persona suplantando su identidad, y después, una vez que la víctima se queda sin servicio telefónico, accede a su información personal y toma el control de su banca digital utilizando los SMS de verificación que llegan al número de teléfono"*.

De esta manera los ciberdelincuentes son capaces de conseguir el "segundo factor" de autenticación enviado al usuario para realizar operaciones. Y es que, tras la entrada en vigor de la normativa PSD2 en el año 2019, el teléfono móvil pasó a ser un elemento fundamental en la

[22] Este supuesto se recoge, por ejemplo, en la reciente SJPI nº7 de las Palmas de Gran Canaria, 508/2024, de 16 de octubre de 2024, rec.1919/2023.

ejecución de las operativas financieras al ser este el medio por el cual se lleva a cabo la autenticación reforzada del cliente (SCA) en los pagos electrónicos[23].

Esta modalidad de fraude es especialmente sangrante para el usuario, en el sentido de que ni siquiera tiene constancia de que se está produciendo una estafa puesto que se queda temporalmente sin cobertura ni línea telefónica, impidiendo que pueda realizar o recibir mensajes ni llamadas.

Así, en estos casos las que deberían ser las comunicaciones del usuario las recibe el tercero ciberdelincuente en el dispositivo de aquel, hasta el momento en que la víctima es notificada del fraude; generalmente porque llama a su compañía telefónica o a su banco, o porque termina recibiendo los avisos de las operaciones no autorizadas por parte de la propia entidad bancaria una vez recupera la cobertura en su teléfono o se conecta a una red wifi.

3.4. *PHARMING*

El *pharming* supone hablar de servidores DNS (*Domain Name System* o Sistema de Nombres de Dominio), "*un conjunto de protocolos y servicios que permite a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas"*[24], es decir, asignar nombres a direcciones IP[25] para que sea más sencilla su búsqueda e identidad.

Así, "*el pharming realiza su ataque sobre estos servidores DNS. Su objetivo es cambiar la correspondencia numérica a todos los usuarios que lo utilicen. Al cambiar esta correspondencia, usted escribe en su navegador cajamadrid.es, pero el DNS le otorga otra correspondencia numérica distinta a la original y real, llevando al usuario a una página idéntica a la de cajamadrid, pero que en realidad ha sido creada por los delincuentes. A partir de aquí, el usuario ve en su navegador que está en www.cajamadrid.es y realiza sus movimientos con total tranquilidad. El delincuente informático tan sólo tiene que utilizar las claves que el usuario escribe"*[26].

---

[23] Cfr. RIBÓN SEISDEDOS, E.: *Fraudes bancarios y defensa del afectado. Nuevas tendencias defraudatorias. Especial referencia al phishing bancario*, Tirant lo Blanch, Valencia, 2024, págs. 43 y 44.

[24] Consultado a través de la página web de la Universidad de Jaén, en su apartado "Servicio de Informática" (fecha de última consulta: 01/02/2025).

[25] "*Una dirección IP es una dirección única que identifica a un dispositivo en Internet o una red local. IP significa «protocolo de Internet», que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o una red local." (https://www.kaspersky.es/resource-center/definitions/what-is-an-ip-address)* (fecha de última consulta: 01/02/2025).

[26] RECOVERY LABS: "Fraude en Internet: Del phishing al pharming", *Laboratorio de Recuperación de Datos Informáticos*, pág. 2.

3.5. *SPEAR PHISHING*

El método conocido como *spear phishing* es una modalidad de ataque dirigido específicamente a suplantar la identidad de un objetivo concreto para, a través del envío de correos electrónicos, obtener la información personal de la víctima[27].

Lo particular de este tipo de fraude en relación con las anteriores técnicas, reside en el estudio previo de la víctima, pues los correos electrónicos mediante los cuales se ejecuta esta modalidad tienen un elevado nivel de detalle y precisión mediante los que se hace parecer ante su destinatario que se trata de comunicaciones reales, sin peligro aparente.

Así, como ya se ha puesto de manifiesto, las técnicas de *phishing* conllevan una preparación detallada del método y un estudio previo de la víctima, tal y como sucede en estos casos, dando lugar a complejas operativas fabricadas con el fin de obtener de la víctima sus datos personales y bancarios a través de los cuales perpetrar las posteriores estafas.

3.6. *WHALING*

Esta técnica, también conocida como *whale phishing*, consiste en *"un tipo de ataque de phishing dirigido a altos cargos de empresas con correos electrónicos, mensajes de texto o llamadas telefónicas fraudulentos. Los mensajes están cuidadosamente redactados para manipular al destinatario con el fin de que divulgue datos corporativos sensibles e información personal o autorice grandes pagos a los ciberdelincuentes"*[28].

3.7. *QRSHING*

A través del *qrshing*, el ciberdelincuente trata de sustraer la información personal de la víctima mediante la simulación de un código QR[29] *"de una supuesta marca o comercio pero que enlaza a un sitio web fraudulento, a través de la creación y pegado de adhesivos para su escaneo en sitios públicos"*[30].

---

[27] Consultado a través de la página web del INCIBE, dentro del apartado "Aprende Ciberseguridad", *Spear Phishing* (fecha de última consulta: 01/02/2025).

[28] Consultado a través de la página web de IBM (fecha de última consulta: 01/02/2025).

[29] Un código QR (*Quick Response* o código de respuesta rápida) almacena información mediante la representación de códigos binarios que se interpretan mediante un lector de códigos QR -como, por ejemplo, un teléfono móvil- para revelar los datos almacenados, pudiendo redirigir estos a una página web. *(https://www.kaspersky.es/resource-center/definitions/what-is-a-qr-code-how-to-scan)* (fecha de última consulta: 01/02/2025).

[30] Consultado a través de los artículos publicados en la página web de Sello Legal Abogados por la abogada del Ilustre Colegio de Abogados de Oviedo, Paloma González Llorente, colegiada ICAO 5611, *(https://sellolegal.com/blog/los-8-tipos-de-ataque-phishing-mas-utilizados/) y* por el abogado del Ilustre Colegio de Abogados de Oviedo, Iñigo Serrano Blanco, colegiado ICAO 5852, *(https://sellolegal.com/blog/qrshing-los-ataques-de-phishing-a-traves-de-codigos-qr-falsos/)* (fecha de última consulta de ambos artículos: 01/02/2025).

3.8. *PHISHING* "DESCONOCIDO"

Así mismo, se quiere hacer referencia a esta modalidad de fraude, la cual resulta especialmente perjudicial para el usuario de la banca electrónica pues le son sustraídos sus fondos sin haber realizado ninguna actuación por su parte. En este sentido, es similar al *SIM swapping* con la salvedad de que se desconoce la manera mediante la cual los ciberdelincuentes consiguen obtener los datos del usuario, de ahí su denominación[31].

Como ya se ha comentado en este trabajo, existen múltiples formas de obtener las credenciales de seguridad de los usuarios de la banca electrónica, desde brechas de seguridad -inherentes al empleo de métodos telemáticos a través de internet- que posibilitan las fugas de datos de los usuarios, de las cuales las entidades bancarias -lógicamente, como cualquier otra persona que emplee internet- no están exentas, hasta ciberataques con programas de *malware* a sus dispositivos.

Así, esta modalidad suele adolecer de un relato que permita explicar su *modus operandi*, ya que, si bien en ocasiones consta una fuga de datos sufrida por la entidad bancaria o un ataque al dispositivo de la víctima, en otros casos no se tiene noticia alguna respecto al modo en que pudo haberse producido el fraude, encontrándose el usuario con la pérdida patrimonial sufrida sin haber tenido posibilidad siquiera de evitarla.

3.9. FRAUDE DEL CEO

Junto las técnicas de fraude ya estudiadas, quiere ponerse de manifiesto el conocido como fraude del CEO o estafa del CEO. Esta modalidad consiste en engañar a un empleado de una empresa que tenga acceso a las cuentas de esta, para que emita una orden de pago -normalmente, una transferencia-, supuestamente siguiendo las instrucciones de su jefe o responsable -de ahí el nombre de la tipología defraudatoria-, a favor de un tercero destinatario de los fondos, el ciberdelincuente, quien retira rápidamente estos de la cuenta para impedir su bloqueo o retroacción[32].

Resulta fundamental en la ejecución de este tipo de estafas el estudio previo de la sociedad de la cual se pretende sustraer los fondos y del empleado de esta, autorizado para

[31] El nombre dado a esta modalidad de *phishing* ha sido acuñado por el abogado del Ilustre Colegio de Abogados de Oviedo, Jorge Grau Fernández, colegiado ICAO 6889, a la hora de enfrentarse a la realidad de este tipo de fraudes.

[32] Cfr. SEISDEDOS RIBÓN, E. ob. cit. pág. 40.

emitir órdenes de pago; de tal manera que la suplantación de identidad llevada a cabo por el tercero defraudador sea totalmente perfecta, sin levantar ningún tipo de sospecha.

3.10. *MAN IN THE MIDDLE*

Como última modalidad defraudatoria a enunciar en este trabajo, se encuentra el *Man in the Middle (MitM),* conocido también como fraude del intermediario.

Este ataque va dirigido principalmente a empresas y consiste en el acceso no autorizado al correo electrónico de un empleado de la mercantil, buscando siempre que se trate de alguien con acceso a las cuentas bancarias y que tenga entre sus funciones la recepción y pago de facturas, al objeto de monitorizar sus comunicaciones, en ocasiones durante largos períodos de tiempo, esperando al momento en que es recibida una factura cuyo importe debe ser abonado[33].

Una vez los ciberdelincuentes tienen noticia de la recepción de este correo -gracias a la monitorización de las comunicaciones y a las herramientas informáticas que permiten detectar palabras clave como "pago", "factura" o "albarán"- interceptan el mismo, y proceden a modificar los datos correspondientes a la cuenta donde deba realizarse el abono, es decir, se modifica el IBAN de la cuenta de destino de los fondos[34].

Tras haber cambiado la información financiera, el correo llega a la bandeja de entrada de la víctima sin ningún viso de falsedad, motivo por el cual el encargado de realizar el pago correspondiente lleva a cabo la operación bajo la creencia de que está abonando al acreedor legítimo el importe de sus servicios, siendo la realidad que está ingresando los fondos en la cuenta designada por el ciberdelincuente.

Como se ve, esta técnica defraudatoria da lugar a que haya una víctima directa, quien realiza el pago, y una indirecta, el acreedor que no obtiene el ingreso correspondiente a los servicios prestados.

Así, el *Man in the Middle* emplea una complejidad en su método de fraude que haría necesario un análisis individual y por separado del resto de modalidades para englobar todos los aspectos que conlleva, tanto técnicos como jurídicos -pago al acreedor aparente del art. 1.164 CC-.

---

[33] Vid. GANGAN, S.: "A review of man-in-the-middle attacks". *arXiv preprint arXiv:1504.02115*, 2015.

La realidad es que los ciberdelincuentes cuentan con herramientas informáticas que permiten monitorizar los correos enviados y recibidos en busca de palabras clave, como pueden ser "pago", "factura" o "albarán".

[34] Cfr. CUAIRÁN GARCÍA, J. y FERNÁNDEZ HUERTAS, P.: "El fraude «man in the middle». Un análisis dual en los órdenes penal y civil", *Diario La Ley*, 2024.

Al fin de aclarar esta última idea, ha de precisarse que pueden existir, derivados de esta técnica, dos litigios diferentes en función de las relaciones entre las partes: la reclamación del importe sustraído basada en la relación mantenida entre acreedor y deudor, y la responsabilidad cuasi-objetiva atribuida al proveedor de servicios de pago en relación con las operaciones no autorizadas.

Finalizando con este apartado, y dado que el objeto de este trabajo es un estudio sobre el *phishing* y la responsabilidad del proveedor de servicios de pago para con las operaciones no autorizadas, a continuación, se estudiará la regulación de esta materia sin perjuicio de discutir esta modalidad defraudatoria al realizar el estudio jurisprudencial sobre este tipo de asuntos.

4. NORMATIVA REGULADORA DE LOS SERVICIOS DE PAGO

Una vez examinadas las principales modalidades del *phishing* y teniendo conocimiento de que su objeto es la obtención de los datos de los usuarios para realizar con ellos todo tipo de fraudes es el turno de analizar la normativa reguladora de las operaciones de pago ejecutadas.

En este sentido, La LSP se erige como el marco regulatorio sobre el que pivota la judicialización de las sustracciones de fondos derivadas del *phishing*, es decir, de aquellas operaciones de pago no autorizadas por los usuarios. Esta norma, que modifica la LSP del año 2009 y transpone el contenido de la Directiva europea PSD2, se complementa con el Reglamento Delegado 2018/319, analizándose ambas a lo largo de este apartado.

4.1. INTRODUCCIÓN A LA LSP

El RDLey 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera sucede a la LSP del año 2009, introducida en nuestro ordenamiento jurídico mediante la transposición de la Directiva 2007/64/CE sobre servicios de pago en el mercado interior, y continúa en sus preceptos con el espíritu sentado por su predecesora.

La actualización de la LSP en 2018 viene motivada también de la Directiva (UE) 2015/2366 sobre servicios de pago en el mercado interior, también conocida como PSD2[35]. Esta

[35] Sobre la implementación de la Directiva PSD2 en el ordenamiento jurídico español, vid. ZUNZUNEGUI PASTOR, F.: "Spain's Implementation of PSD2", Gimigliano, G. y Božina Beroš, M. (editores*), The Payment Services Directive II*, Edward Elgar Publishing Limited, Cheltenham, 2021, págs. 406-424*; y vid. CONESA LAREO, C., GORJÓN RIVAS, S. y RUBIO ORTEGA, G.: "Un nuevo régimen de acceso a las cuentas de pago: la PSD2", *Revista de Estabilidad Financiera / Banco de España*, nº 35, 2018, págs. 81-102.

*Este capítulo también puede consultarse en ZUNZUNEGUI, F.: "Spain's Implementation of PSD2", *Revista de Derecho del Mercado Financiero*, 7/2020, 2020, págs. 1-22 (*https://www.rdmf.es/wp-content/uploads/2020/11/ZUNZUNEGUI-F._Spains-Implementation-of-PSD2_WP_noviembre-2020.pdf*) (fecha de última consulta 01/02/2025).

nueva Directiva encuentra su motivación en el desarrollo tecnológico y la creación de un entorno más seguro para su implementación[36], pues, como se ha puesto de manifiesto con anterioridad, el paso del tiempo, junto con los consiguientes avances tecnológicos, han propiciado tanto la implementación con carácter general de la banca electrónica a nivel usuario como el aumento de la ciberdelincuencia en este ámbito.

A los efectos de centrar el trabajo sobre las cuestiones propias que se discuten en la práctica jurídica -se comprobará del análisis de la jurisprudencia-, la exposición de la norma versará sobre los preceptos correspondientes a la discusión mantenida en torno a si las operaciones bancarias han de considerarse como no autorizadas, así como a la responsabilidad cuasi-objetiva que la LSP establece para el proveedor de servicios de pago con relación a este tipo de operaciones.

4.2. CONCEPTOS Y AUTENTICACIÓN REFORZADA EN LA LSP

4.2.1. Conceptos base de la LSP

Para entender la LSP y no perderse en la terminología empleada por la norma, parte de la cual ya se ha ido adelantando en este trabajo, ha de consultarse su art. 3, el cual establece las definiciones de conceptos clave, necesarios para el posterior análisis de la configuración legal del régimen de responsabilidad sobre las operaciones no autorizadas.

Entre estos términos destacan los conceptos de "instrumento de pago" (por ejemplo: una tarjeta de crédito), "operación de pago" (por ejemplo: una compra con tarjeta o una transferencia), servicio de pago, proveedor de servicios de pago y usuario de servicios de pago.

Junto a estas definiciones más descriptivas resulta de plena relevancia el concepto de autenticación, pues este es el método empleado para verificar las operaciones de pago realizadas por el usuario.

Para comenzar con las definiciones clave de la LSP, ha de entenderse por servicios de pago las actividades reguladas por la LSP en su art. 1.2. Entre ellas se encuentran aquellos servicios que permiten gestionar una cuenta de pago, el ingreso y retirada de efectivo de una cuenta, la ejecución de operaciones de pago -incluidas aquellas que se encuentran cubiertas por una línea

[36] Tal y como indica la propia exposición de motivos del RDLey 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera.

de crédito-, la emisión de instrumentos de pago, el envío de dinero, los servicios de iniciación de pagos[37] y los servicios de información sobre cuentas[38].

Pasando ya a los actores de este este tipo de servicios, la condición de proveedor de servicios de pago, o entidad de pago, se otorga a las entidades contempladas en los arts. 5, 14 y 15 LSP, y puede definirse en un sentido práctico como aquellas personas jurídicas *"a las que el Banco de España ha otorgado una autorización administrativa para prestar y ejecutar uno o varios de los servicios de pago"*[39].

La contraparte del proveedor de servicios es el usuario de servicios de pago. Este término responde a una definición totalmente lógica, pues se trata de la persona física o jurídica que utiliza el servicio de pago -ordenante, beneficiario o ambos-[40].

Finalmente, la autenticación es el proceso por el cual el proveedor de servicios comprueba y verifica la identidad del usuario o la validez de la utilización del instrumento de pago, incluida la utilización de las credenciales de seguridad del usuario[41]. Este proceso es imprescindible en la realización de las operaciones de pago, habiendo resultado el refuerzo en la autenticación uno de los aspectos más destacados de la nueva regulación normativa sobre estas operaciones.

4.2.2. Autenticación reforzada (SCA)

La Directiva 2015/2366 introdujo un concepto novedoso, hoy imprescindible, que supuso un paso más respecto del proceso de autenticación: la autenticación reforzada o SCA (*Strong Customer Authentication*)[42]. Este nuevo proceso dota de mayores garantías de seguridad a la ejecución de operaciones de pago a través de un sistema caracterizado por la independencia en los elementos empleados para la verificación de identidad del usuario.

Este nuevo sistema encuentra su definición en la propia LSP: "*la autenticación basada en la utilización de dos o más elementos categorizados como conocimiento (algo que solo conoce el usuario), posesión (algo que solo posee el usuario) e inherencia (algo que es el usuario),*

[37] *"El servicio de iniciación de pagos te permite pagar las compras que hagas por Internet sin tener un medio de pago, por ejemplo una tarjeta, en el momento de la compra."* Página web del BDE (fecha de última consulta 01/02/2025).

[38] *"El servicio de información sobre cuentas, también conocido como «servicio de agregación de cuentas», es prestado por los «agregadores de información» y te permite acceder, en cualquier momento y desde una única aplicación informática, a la información agregada de todas tus cuentas de pago (de ahí su nombre) que sean accesibles en línea."* Página web del BDE (fecha de última consulta 01/02/2025).

[39] Cfr. ESTANCONA PÉREZ, A.A.: "Responsabilidad de las entidades financieras ante el hackeo de cuentas bancarias. En particular, casos de "phishing"", *Actualidad jurídica iberoamericana*, nº 18, 2023, págs. 1590-1617.

[40] Art. 3 LSP, apartado 46.

[41] Art. 3 LSP, apartado 4.

[42] Cfr. ALVARADO HERRERA, L.: "Autenticación reforzada de cliente y responsabilidad en la segunda directiva de servicios de pago", *Revista de Derecho del Sistema Financiero*, nº 5, 2023, págs. 69-112.

que son independientes –es decir, que la vulneración de uno no compromete la fiabilidad de los demás–, y concebida de manera que se proteja la confidencialidad de los datos de identificación"[43].

Para ejemplificar esta definición, por conocimiento puede entenderse una clave de firma, por posesión un teléfono móvil -al cual enviar códigos OTP por SMS o notificaciones dentro de la aplicación bancaria[44] - y por inherencia un rasgo biométrico -huella dactilar, reconocimiento facial, etc.-. Una vez dos de estos tres elementos se introducen para ejecutar una operación de pago, se entiende verificada la identidad del cliente y se autoriza la operación.

Como se ha dicho, la autenticación reforzada es un proceso indispensable que debe realizar el proveedor de servicios de pago del usuario *"que accede a la cuenta o inicia la orden de pago; es decir, el PSP que emite las credenciales de seguridad personalizadas"*[45], sin cuya utilización no puede entenderse como autorizada una operación de pago, salvo contadas excepciones.

Estas excepciones se encuentran recogidas en la propia LSP, art. 68.6, que redirige al art. 98.1.b) de la Directiva 2015/2366. A su vez, este apartado emplaza a consultar el art. 98.3 de la Directiva, donde se encuentran los criterios que han de seguirse para determinar si resulta posible aplicar una exención a la autenticación reforzada: el nivel de riesgo, el importe y la frecuencia con que se repite la operación y el canal de pago empleado[46].

A pesar de la aplicación de la autenticación reforzada, la realidad es que los ciberdelincuentes son capaces de obtener las credenciales del usuario y autorizar las operaciones, o engañar a la víctima para que las verifique, y sustraer así los fondos de su cuenta.

4.3. RÉGIMEN DE RESPONSABILIDAD EN TORNO A LAS OPERACIONES DE PAGO

Una vez se produce el fraude bancario empleando los métodos de *phishing* entra en juego el principal debate en torno a este fenómeno: la consideración de las operaciones como autorizadas o no autorizadas. En los arts. 36 a 49 LSP reside el principal debate jurídico en torno al *phishing* bancario, para cuyo análisis se estudiarán los preceptos más relevantes.

[43] Art. 3, apartado 5 LSP.
[44] Sistemas *Out of Band* (OoB).
[45] Cfr. ALVARADO HERRERA, L., ob. cit., pág. 85.
[46] Es por estos criterios por los que, en ocasiones, como usuarios de servicios de pago nos encontramos con que al realizar una operación de pago no se nos aplica la autenticación reforzada, como sucede por ejemplo al realizar una compra por un pequeño importe en nuestro supermercado habitual.

Para comenzar con este estudio, ha de ponerse de manifiesto la definición de operación autorizada o no autorizada recogida en el art. 36.1 LSP bajo la -eficaz- premisa de que la operación se considera autorizada si concurre el consentimiento del usuario para su ejecución, y, en sentido contrario, cuando no existe este consentimiento la operación se entiende como no autorizada.

La aparente sencillez del precepto anterior lleva consigo aparejada un debate que la jurisprudencia trata de resolver, pues, tal y como se estudiará más adelante, las operaciones de pago ejecutadas correctamente desde el punto de vista técnico -en su mayoría introduciendo los datos del instrumento de pago más el código recibido por SMS- no siempre equivalen a la autorización pues puede faltar el consentimiento del usuario o la certificación de la identidad del ordenante[47].

Continuando con el orden del articulado de la LSP, los arts. 41 y 42 establecen las obligaciones que el usuario y el proveedor, respectivamente, han de cumplir en relación con los instrumentos de pago. La actuación conforme a estas obligaciones es fundamental para determinar quién ha de responder de los fondos sustraídos en casos de *phishing* bancario mediante la realización de operaciones no autorizadas.

El primero de estos artículos, 41.a) LSP, determina para el usuario las imposiciones de utilizar el instrumento de pago conforme a las condiciones que regulen su emisión, debiendo tomar "*todas las medidas razonables a fin de proteger sus credenciales de seguridad"*. Como se verá, la protección de las claves de seguridad es fundamental a la hora de valorar la posible negligencia grave en la conducta del usuario.

Además de la protección de sus credenciales, el apartado b) del art. 41 LSP impone al usuario la obligación de comunicar sin demora indebida al proveedor de servicios cualquier extravío, sustracción o utilización no autorizada del instrumento de pago, tan pronto se percate de alguna de estas circunstancias, contando para ello con un plazo máximo de trece meses[48]. Se trata esta de la otra obligación fundamental e imprescindible de cumplir para el usuario a la

[47] Esta falta de certificación de la identidad del ordenante ha sido recogida por la jurisprudencia, siendo posible citar, entre otras, la SAP A Coruña, Sección 3ª, 364/2023, de 5 de octubre de 2023, rec. 87/2023, FJ 3º: *"La operación habrá sido "autenticada" en términos de la LSP (que tampoco es así, porque no consta el factor de posesión, como hemos dejado sentado anteriormente), pero lo que es elemento nuclear de este litigio es la "falsedad" de tal autenticación, en términos del art. 44 LSP (negación por el usuario de haber sido él quien ha autorizado la operación), escenario en el que recae la carga de la prueba en la entidad proveedora del sistema de pago. Pues bien, habiéndose constatado que la parte demandante ha sido víctima de "phishing", resulta claro que la operación no se encuentra completamente "autenticada" en términos de la LSP, porque falta la certificación de la identidad del usuario ordenante de la operación"*.

[48] Art. 43.1 LSP.

hora de determinar sobre quién ha de pesar la responsabilidad respecto a las operaciones no autorizadas.

Como contraparte del precepto anterior se encuentra el art. 42 LSP, que establece las obligaciones para el proveedor de servicios de pago. Este artículo, más extenso que el anterior, impone al proveedor de servicios las obligaciones de cerciorarse de que las credenciales de seguridad solo sean accesibles para el usuario, de no enviar más instrumentos de pago que los solicitados -salvo en caso de sustitución-, de garantizar que siempre estén disponibles para el usuario medios adecuados y gratuitos mediante los cuales efectuar una notificación con respecto al art. 41.1.b) LSP, y de impedir el uso del instrumento de pago tras haberse efectuado la notificación por parte del usuario.

Así mismo, tal y como se recoge en el art. 42.1 LSP, el proveedor de servicios ha de responder de los riesgos acaecidos en relación con el envío del instrumento de pago o de las credenciales de seguridad de este.

Por último, antes de tratar los conceptos de responsabilidad cuasi-objetiva y negligencia grave, ha de ponerse de manifiesto la obligación que el art. 43 LSP establece a favor del usuario de servicios de pago en tanto que este habrá de obtener la rectificación de las operaciones de pago no autorizadas, o ejecutadas incorrectamente, por parte del proveedor de servicios una vez lo haya puesto en su conocimiento, para lo cual se estipula un plazo máximo de trece meses a contar desde la fecha del adeudo.

4.3.1. Responsabilidad cuasi-objetiva para las operaciones no autorizadas

Es preciso en este momento tratar el art. 45 LSP, adelantando un artículo el contenido de la ley. Este precepto establece la responsabilidad cuasi-objetiva en relación con las operaciones no autorizadas, siendo sus únicas excepciones que el usuario haya actuado de manera fraudulenta o con negligencia grave.

Así, el apartado primero de este precepto impone al proveedor de servicios la obligación de reintegrar al ordenante de la operación no autorizada su importe de inmediato, junto con la obligación de restituir la cuenta de pago al estado anterior a haber tenido lugar esta operación.

Resulta preciso poner de manifiesto que la responsabilidad cuasi-objetiva encuentra su excepción en aquellos casos en los que el proveedor considera que ha mediado fraude, estando obligado a comunicar tal situación al BDE. En este sentido, corresponde también al proveedor cumplir con la obligación de probar la correcta ejecución de la operación, tal y como se estudiará más adelante.

En caso de tener lugar alguna de las excepciones mencionadas -fraude o negligencia grave- la responsabilidad recaerá en el ordenante de las operaciones, conforme a lo establecido en el art. 46 LSP.

Sin embargo, no resulta tan sencillo como pudiera parecer atribuir tal responsabilidad, pues frente a la excepción existen nuevas excepciones, que descartan la responsabilidad del ordenante en aquellos casos en los que no hubiera podido detectar la pérdida, sustracción o apropiación indebida del instrumento de pago, o cuando estas circunstancias hubieran tenido su origen en el propio proveedor de servicios.

Junto a lo anterior, se descarta también la responsabilidad del ordenante en aquellos casos en que las operaciones que no se reconocen como autorizadas se hubieran realizado empleando únicamente los datos impresos en el instrumento de pago -siempre y cuando no medie fraude ni negligencia grave en relación con las obligaciones de custodia propias del art. 41.b) LSP-.

Por último, ha de recogerse que únicamente respondería el ordenante de las operaciones no autorizadas en caso de haber actuado fraudulentamente en las ocasiones en que no se hubiera aplicado la autenticación reforzada, las operaciones se hubieran ejecutado con posterioridad a la notificación al proveedor de servicios o cuando este proveedor no dispusiese de medios adecuados para notificar las circunstancias recogidas en el art. 41.1.b) LSP[49].

4.3.2. Prueba de la autenticación de las operaciones. Fraude y negligencia grave

Conforme al art. 44.1 LSP, el proveedor de servicios está obligado a probar que la operación discutida como autorizada o no autorizada *"fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado"*.

El propio precepto descarta la posibilidad de que el registro por parte del proveedor de servicios de la utilización del instrumento de pago sea suficiente motivo como para demostrar que la operación fue autorizada por el ordenante. Igualmente, tampoco basta este registro para demostrar que el usuario actuó mediando fraude o negligencia grave.

Resulta preciso detenerse a comentar estos dos supuestos, pues la propia LSP en su art. 44.3 establece la obligación para el proveedor de probar que la actuación del usuario se caracterizó por haber tenido lugar alguna de las circunstancias anteriores.

[49] Art. 46.2, 3 y 4 LSP.

Y es que el mayor debate a la hora de dictaminar si una operación de pago es autorizada o no, pasa por descifrar si en el comportamiento del usuario de servicios de pago hubo fraude o negligencia grave -principalmente, el debate orbita en torno a este último parámetro-. Para dilucidar si un comportamiento ha de considerarse gravemente negligente, la propia Directiva establece en su considerando 72 que la negligencia grave ha de ir más allá de la mera diligencia, ejemplificando una conducta de este tipo con el hecho de guardar las claves de seguridad junto al instrumento de pago[50].

Como se pondrá de manifiesto con el posterior análisis de la jurisprudencia dictada en este tipo de asuntos, la negligencia y la actuación del usuario de servicios de pago marcan el devenir de la restitución de los fondos sustraídos mediante fraudes en los que se emplean los métodos y técnicas de *phishing*. Para su reintegro, además, es necesario que se cumplan las obligaciones expuestas en los artículos anteriores, pero puede afirmarse que el elemento definitorio que determina los veredictos judiciales en esta materia es la negligencia grave.

4.4. REGLAMENTO DELEGADO (UE) 2018/389 DE LA COMISIÓN, DE 27 DE NOVIEMBRE DE 2017

Conforme se había anunciado, la LSP encuentra su complemento en el Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, el cual establece las normas técnicas respecto de la autenticación reforzada que caracteriza a la LSP.

Así, el considerando 2 del Reglamento ya avanza la realidad -y uno de los principales rasgos- de las operativas estudiadas en este trabajo con la siguiente manifestación: *"Como los métodos de fraude cambian constantemente, los requisitos de autenticación reforzada de clientes deben permitir la innovación en las soluciones técnicas con objeto de hacer frente a la aparición de nuevas amenazas a la seguridad de los pagos electrónicos"*[51].

Retomando lo ya comentado en este trabajo, existen numerosos métodos mediante los que perpetrar los fraudes que han dado lugar a las cifras tan elevadas sobre estafas informáticas ya

[50] Considerando 72 Directiva 2015/2366: *"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."*

[51] Considerando 2 del 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.

vistas. En concordancia con la realidad, la normativa técnica ha de adaptarse e innovar, implementando nuevos mecanismos de autenticación reforzada que aminoren los riesgos intrínsecos a la utilización de la banca electrónica, y al mismo tiempo, protejan a los usuarios de servicios de pago y permitan a los proveedores ofrecer servicios más seguros y eficaces.

Además de los mecanismos propios de autenticación reforzada en sentido estricto, el Reglamento establece dos elementos para vigilar y controlar las operaciones de pago[52]: la supervisión de las operaciones efectuadas por los usuarios -pauta de gasto- y la trazabilidad de estas. Sin derivar el objeto de este trabajo hacia el punto de vista técnico, resulta necesario denotar que estos dos elementos son fundamentales a la hora de dilucidar la consideración de las operaciones como no autorizadas.

Sobre la pauta de gasto, este concepto se recoge en el art. 2 del Reglamento, estableciendo la obligación para los proveedores de servicios de disponer de mecanismos de supervisión al fin de detectar operaciones no autorizadas basándose en el uso común de sus credenciales por parte del usuario de servicios de pago.

La supervisión de operaciones también se ha puesto de manifiesto por la jurisprudencia, pudiéndose citar a modo de ejemplo la reciente SAP de Asturias, 324/2024, de 17 de abril de 2024, en cuyo FJ 4º se recoge la comparación entre las operaciones habituales y las no autorizadas, destacando la anomalía que suponen estas últimas en atención a su concatenación, importe y lugar desde el que fueron efectuadas.

Para finalizar con este apartado, respecto a la trazabilidad de las operaciones el art. 29 del Reglamento impone a los proveedores de servicios la obligación de disponer de procesos que posibiliten identificar aspectos cruciales sobre cada operación que se realice, como son el origen, la fecha y hora, el importe, el comercio, el instrumento de pago empleado o el método de autenticación reforzada, entre otras[53].

[52] Sobre este aspecto, es preciso notar que el art. 40.2 LSP faculta al proveedor de servicios para bloquear un instrumento de pago por causas justificadas relacionadas con la seguridad del propio instrumento.

[53] Este artículo ha de ponerse en relación con el art. 44 LSP, en referencia a la obligación para el proveedor de servicios de pago correspondiente a demostrar la correcta autenticación técnica de las operaciones.

5. ASPECTOS PRÁCTICOS DEL *PHISHING* BANCARIO Y SU RECLAMACIÓN JUDICIAL

5.1. PLANTEAMIENTO

A la hora de valorar la práctica jurídica sobre el *phishing* bancario, han de tenerse varios aspectos en cuenta, desde las respuestas emitidas por las entidades bancarias hasta los aspectos jurídicos más frecuentes no comentados anteriormente. Previamente a estudiar estos aspectos, resulta preciso ejemplificar el procedimiento habitual que tiene lugar en un fraude cometido empleando técnicas de *phishing* y que termina por ser resuelto ante los tribunales.

Así, el supuesto más común es que el origen de la estafa venga motivado por alguna de las técnicas vistas anteriormente -un SMS fraudulento, una llamada, etc.-. A continuación, el usuario respondería a la iniciativa del tercero defraudador mediante algún tipo de acción -clicar en el enlace contenido en el SMS, facilitar telefónicamente el código OTP para verificar la operación, o similares-.

Una vez tiene lugar la sustracción de los fondos, el usuario se percataría, en ese mismo momento o con posterioridad de la misma. Tras darse cuenta de la estafa, rápidamente contactaría con su banco[54] y desde la entidad se procedería a bloquear su cuenta e instrumentos de pago -aunque puede intentarse, muchas veces resulta imposible retroceder las operaciones al haberse efectuado estas mediante mandatos de pago inmediatos e irrevocables-. Tras ello, se emplazaría al usuario a presentar una denuncia, que sería posteriormente remitida al banco.

Además de la denuncia -vía penal-, los usuarios intentan recuperar los fondos sustraídos mediante reclamaciones extrajudiciales al banco formalizadas a través de los servicios de atención al cliente. Si se analizan las respuestas emitidas por las entidades bancarias frente a este tipo de reclamaciones, puede comprobarse cómo estas suelen ser negativas, tomando como principal referencia la correcta autenticación de las operaciones en referencia al art. 44 LSP.

En caso de que la respuesta de la entidad bancaria sea desfavorable, el usuario tiene a su disposición la posibilidad de acudir al BDE presentando una nueva reclamación. Las respuestas emitidas por este organismo analizan la conducta de la entidad bancaria y valoran la actuación del proveedor de servicios verificando la correcta autenticación de las operaciones de pago. Sin embargo, para el caso de que el usuario haya resultado víctima de un engaño o estafa mediante

[54] Como se ha visto, esta es una obligación impuesta por la propia LSP en su art. 41.1.b) y como tal se recoge en la jurisprudencia, pudiendo citarse, entre otras, la SAP Zaragoza, Sección 4ª, 215/2013, de 14 de mayo de 2013, rec. 116/2013.

phishing el BDE no tiene competencias para valorar el grado de negligencia ni tampoco para atribuir responsabilidad al proveedor de servicios conforme a la LSP.

De esta manera, al usuario de servicios de pago le resta la opción de acudir a los tribunales de justicia. Para ello, dispone de dos vías: la vía penal -abierta con la denuncia presentada- y la vía civil -ejercitando una acción de reclamación de cantidad frente al proveedor de servicios en virtud del articulado de la LSP-. A los efectos de este trabajo, se estudian a continuación dos de los aspectos procesales más característicos de la vía civil en esta materia.

5.2. PARTICULARIDADES DE LAS RECLAMACIONES POR FRAUDES DE *PHISHING* BANCARIO

En este apartado se observará como el hecho de que la acción ejercitada por medio de la LSP encuentre su origen en la actuación defraudatoria de un tercero da lugar a que en los procedimientos judiciales sobre esta materia se planteen con frecuencia dos cuestiones, usualmente aducidas por los proveedores de servicios de pago: la prejudicialidad penal y la falta de legitimación pasiva.

Así, en primer lugar, ha de ponerse de manifiesto que la excepción de prejudicialidad penal es habitual en los procedimientos judiciales relativos al *phishing* bancario[55]. Lógicamente, el fraude es cometido por un ciberdelincuente y responde a un ilícito penal cuya investigación se origina mediante la presentación de una denuncia por parte del usuario.

Sin embargo, la investigación se ve dificultada y ralentizada por la propia actuación del ciberdelincuente. Y es que, normalmente, los fondos sustraídos son transferidos a cuentas abiertas por "mulas" o aperturadas a nombre de un tercero a quien le hubieron sustraído sus datos personales con anterioridad a la estafa, sin que el dinero permanezca por mucho tiempo en estas cuentas, puesto que rápidamente el destinatario -ciberdelincuente- dispone del mismo y lo retira de la cuenta de destino.

También suele ser habitual en la práctica que los ciberdelincuentes empleen los fondos en la compra de criptomonedas, cuya facilidad de movimiento y anonimato resulta muy adecuada al fin de mover los fondos rápidamente -además, es preciso notar que en ocasiones los importes sustraídos tienen por destino comercios y cuentas extranjeras, por lo cual la Policía suele archivar la denuncia ante la imposibilidad de realizar acción al respecto-.

[55] Cfr. SEISDEDOS RIBÓN, E. ob. cit. págs. 206-216.

Siendo esto así, las víctimas suelen optar por una reclamación al proveedor de servicios en atención a la responsabilidad cuasi-objetiva establecida por la LSP. Esta acción civil no supone que se descarte la vía penal, motivo por el cual es común que se plantee la necesidad de acoger o no la excepción que se analiza en este apartado.

En este sentido, los tribunales han tenido ocasión de pronunciarse sobre este aspecto y de la propia práctica jurídica puede afirmarse que comúnmente no se acoge la excepción por entender que no concurren los requisitos establecidos para ello en el art. 40.2 LEC, aunque puede demorarse la decisión judicial -por ejemplo, por estar a la espera de informes por parte del Ministerio Fiscal o de oficios a la Policía o Guardia Civil para conocer el estado en que se encuentra la denuncia presentada-, sino que se rechaza la prejudicialidad razonando que se trata del ejercicio de dos acciones distintas, las cuales, a pesar de tener su origen en el mismo hecho, persiguen finalidades diferentes.

Un ejemplo de estas decisiones judiciales puede encontrarse en el Auto 308/2024 dictado por la Sección 10ª de la AP de Madrid en fecha 15 de julio de 2024. En esta resolución se revoca la decisión de acoger la excepción tomada por el JPI en aplicación del art. 40.4 LEC, en un caso en el cual ya se habían abierto diligencias previas.

Así, en el FJ 2º de esta resolución, la Audiencia fundamenta su decisión en la necesidad de que para acoger la prejudicialidad penal debe existir *"una íntima conexión entre el objeto del pleito civil y la cuestión penal bien porque el objeto del pleito civil esté inserto en el penal, bien porque la decisión que haya de adoptarse en el pleito civil dependa directamente de la decisión que adopte la jurisdicción penal sobre un determinado hecho que, sin ser debatido en aquel, tiene una influencia determinante o decisiva en el fallo, que no puede dictarse sin aquélla"* .

De acuerdo con este razonamiento, aplicándolo al caso concreto de *phishing*, la AP razona que la acción civil se ejercita en base a la LSP y a la relación jurídica del usuario con el proveedor de servicios, sin que el fraude de un tercero investigado en el pleito penal afecte a la acción civil.

Otro ejemplo del rechazo al acogimiento de la prejudicialidad penal se encuentra en el Auto 71/2023 dictado por la Sección 5ª de la AP de Vizcaya en fecha 21 de septiembre de 2023, en este caso relativo a un asunto en el que únicamente constaba la presentación de una denuncia por la víctima del fraude. La AP descarta la prejudicialidad bajo la fundamentación jurídica de que la mera formalización de una denuncia no implica que exista una causa criminal en curso.

Junto a la prejudicialidad penal, la alegación de falta de legitimación pasiva es otra cuestión habitual en este tipo de asuntos. Ello es así por dos motivos principales: el hecho de que es un tercero quien realiza las actuaciones materiales que dan lugar al fraude y la división de las carteras de negocios por parte de las entidades bancarias, proveedoras de servicios de pago.

El primero de estos motivos no tiene, a mi modo de ver, un especial recorrido jurídico como excepción, entroncando directamente con la prejudicialidad penal para el caso de que, si se decide que la responsabilidad ha de atribuirse al tercero defraudador, esta tenga que perseguirse en el citado orden.

Es evidente la legitimación que ostenta el proveedor de servicios en una acción de reclamación de cantidad en virtud de lo establecido por la LSP, quedando la relación de las partes acreditada por la titularidad de la cuenta o del instrumento de pago y la responsabilidad cuasi-objetiva que la LSP establece para los proveedores de servicios.

Pasando a citar un ejemplo jurisprudencial, respecto de la legitimación del proveedor de servicios de pago sobre las operaciones no autorizadas puede consultarse el FJ 2º de la SAP Valencia, Sección 8ª, 308/2023, de 5 de julio de 2023, rec. 536/2022, que estudia la posible prescripción de la acción en un asunto de *phishing*. Para ello, analiza el contrato de cuenta corriente como instrumento regulador de la responsabilidad contractual entre las partes y el deber de la entidad depositaria de los fondos de actuar conforme a los estándares de un comerciante experto, terminando por resolver la plena legitimación del proveedor de servicios en este tipo de asuntos.

A diferencia del anterior, más recorrido judicial tiene el segundo motivo, la división de las carteras de negocios en entidades bancarias, que dan lugar a que existan sociedades mercantiles con denominaciones similares y aparentemente dedicadas al mismo negocio.

Este tipo de excepciones procesales suele rechazarse por motivos varios, como el hecho de que la cuenta a la que está asociada la tarjeta bancaria empleada para cometer el fraude pertenece a la entidad demandada -depositaria de los fondos- o también el hecho de que sea la entidad demandada la que conteste a la reclamación extrajudicial previa a la demanda -acto propio-.

Un ejemplo de la opinión jurisprudencial en esta materia puede encontrarse en la Sentencia 597/2024 dictada por la Audiencia Provincial de Barcelona en fecha 12 de septiembre, en cuyo FJ 3º se analiza la excepción procesal y recopila la jurisprudencia reciente en esta materia para terminar desestimando la petición del proveedor de servicios de pago en base a los argumentos

antes indicados, los cuales se consolidan en las resoluciones judiciales como destacados en esta materia.

5.3. DILIGENCIA EXIGIBLE AL PROVEEDOR DE SERVICIOS DE PAGO

A la hora de atribuir la responsabilidad por las operaciones de pago no autorizadas, además de la concurrencia de negligencia grave en la actuación del usuario, tratada en el apartado cuarto de este trabajo, ha de analizarse la diligencia exigible al proveedor de servicios de pago. En este sentido, la diligencia va más allá de la que puede exigirse al usuario, la mayoría de las ocasiones consumidor, al ser el proveedor de servicios una entidad bancaria que debe responder más allá del estándar de un buen padre de familia.

Esta diligencia entronca directamente con el cumplimiento de las obligaciones que la LSP impone, debiendo responder la conducta del proveedor con el estándar de un comerciante experto[56]. Además de la diligencia exigible a un comerciante experto, la jurisprudencia ha asociado la conducta del proveedor de servicios de pago con la diligencia del leal y honorable banquero caracterizado por el santo temor al déficit y el respeto absoluto por el dinero ajeno, encontrándose tal estándar de diligencia en, entre otras, la SAP de Madrid, Sección 14ª, 386-2017, de 21 de diciembre de 2017, rec. 498/2017.

Resulta evidente, entonces, que la diligencia exigible al proveedor de servicios marca un estándar de conducta mayor que el fijado por la diligencia del buen padre de familia al llevar a cabo *"una actividad que se aleja de los parámetros generales"*[57], motivo por el cual las entidades bancarias han de tomar las medidas y precauciones necesarias para salvaguardar los fondos de los usuarios de aquellos intentos de sustracción ejecutados por parte de los ciberdelincuentes.

La diligencia conforme al estándar del *bonus argentarius*[58] queda patente respecto a todas las modalidades de *phishing* bancario, existiendo en la jurisprudencia mayor o menor unanimidad en torno a un criterio específico según el tipo de fraude que se trate.

[56] Vid. HERRANZ RAMOS, I.: "El estándar mercantil de diligencia: el ordenado empresario", *Anuario de derecho civil*, nº 1, 2006, pág. 200.

[57] Cfr. HERRANZ RAMOS, I. ob. cit., pág. 200.

[58] Vid. PEÑALOSA TOMÉ, C.: "Man in the middle. El error en la transferencia. Interposición delictiva de tercero. Responsabilidad civil bancaria", *Diario La Ley*, nº 10467, 2024.

6. EL *PHISHING* BANCARIO EN LA JURISPRUDENCIA MENOR

A lo largo de este trabajo se ha hecho referencia a la jurisprudencia dictada en este tipo asuntos, para así introducir y conectar la realidad de la práctica jurídica con los conceptos teóricos que posibilitan esta última.

Llegado este punto, resulta necesario efectuar un examen más detallado de las resoluciones judiciales dictadas por nuestros tribunales al objeto de indicar la interpretación llevada a cabo por estos respecto de los conceptos analizados en los apartados previos.

En aras de esclarecer la postura de los jueces y tribunales que enjuician estas cuestiones y a divulgar el conocimiento en materia jurisprudencial, se adjunta a este trabajo como Anexo I un listado resumen que muestra 184 sentencias dictadas por nuestras AAPP. Para la elaboración de este listado, se han buscado y clasificado las resoluciones judiciales dictadas en el marco de procedimientos civiles en materia de *phishing* y operaciones no autorizadas.

Tal y como se puede comprobar del Anexo I, la mayoría de AAPP entienden que la conducta de los usuarios víctimas de esta clase de fraudes no puede considerarse como negligencia grave, requisito indispensable -como ya se ha manifestado- para considerar que el proveedor de servicios no deba hacer frente a las operaciones no autorizadas por el usuario, imputando a este la responsabilidad sobre las operaciones.

Así mismo, es evidente el auge en este tipo de ciberdelitos dado el gran número de sentencias dictadas en los últimos años, y cómo las resoluciones judiciales han tendido a una mayor protección de los usuarios que han visto sustraídos sus fondos por terceros defraudadores.

Sin perjuicio de que la información jurisprudencial analizada pueda consultarse en el Anexo I, a efectos del desarrollo del trabajo y para efectuar un resumen de la jurisprudencia dictada en esta materia, resulta adecuado comenzar destacando -por su relevancia- la sentencia dictada por la AP de Alicante, Sección 8ª, 107/2018, de 12 de marzo de 2018, rec. 622/2017, cuya argumentación ha sido traída a colación en muchas de las sentencias dictadas con posterioridad a esta.

La sentencia analiza la responsabilidad cuasi-objetiva de la entidad bancaria junto a la carga de probar que la operación de pago fue ordenada correctamente sin haber sido afectada por ningún fallo técnico ni otro tipo de deficiencia, la cual le corresponde como proveedor de servicios de pago.

Así, la SAP de Alicante declara la responsabilidad del proveedor de servicios entendiendo que los sistemas de autenticación dispuestos por la entidad son responsabilidad de esta, dando lugar a una responsabilidad por *culpa in vigilando*, sin poder achacar su mal funcionamiento al usuario que ve sustraídos los fondos de su cuenta.

Además de los sistemas de autenticación, la sentencia descarta la concurrencia de negligencia grave en la actuación del usuario, posibilitando la aplicación de la responsabilidad cuasi-objetiva dispuesta por la LSP.

En un sentido similar se pronuncia la SAP de Madrid, Sección 10ª, 24/2023, de 13 de enero de 2023, rec. 918/2022, al resolver que el *phishing* se trata de una modalidad de fraude muy específica de la cual es fácil ser víctima dada la ejecución de esta, sin que ello signifique que el usuario hubo actuado con negligencia grave.

Así mismo, resultan destacado en la jurisprudencia el hecho que el fraude surja por iniciativa de un tercero defraudador y no por la iniciativa del usuario víctima, recogiéndose esto en sentencias como la dictada por la AP de Pontevedra, Sección 3ª, 177/2023, de 23 de marzo de 2023, rec. 634/2022, comúnmente citada en asuntos de *phishing*[59].

Junto a la iniciativa de tercero, la jurisprudencia ha descartado la presencia de negligencia grave bajo el concepto de "error excusable" para explicar aquellos casos en los cuales el usuario víctima del fraude facilita códigos consecuencia de la acción defraudatoria de un tercero. Así se ha reflejado en la SAP de Asturias, Sección 1ª, 502/2024, de 25 de junio de 2024, rec. 508/2024, que define este error como *"aquel en que puede incurrirse pese al empleo de una diligencia media o regular, y pese a ello, sufre un error que vicia su consentimiento"*.

Para finalizar este apartado, ha de destacarse la reciente SAP de Barcelona, Sección 4ª, 735/2024, de 24 de octubre de 2024, rec. 696/2023, puesto que contiene un pronunciamiento muy interesante en tanto que valora la presencia o no de negligencia grave en un fraude cometido a través de un *vishing* en el cual el interlocutor de la llamada se hizo pasar por un

[59] *"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-".*

empleado de “Microsoft” para engañar a la víctima y que esta se descargase un programa *malware* en su ordenador para así obtener mediante transferencias y compras con tarjeta varios miles de euros.

Pues bien, en este caso la AP de Barcelona entiende que no puede considerarse negligencia grave la conducta del usuario de servicios de pago, en atención a que esta gravedad ha de equipararse a *“la falta de la más elemental diligencia”*, presente en engaños burdos o grotescos, no bastando con que el usuario haya actuado con falta de diligencia al descargarse un programa que permitió al tercero defraudador acceder a su ordenador y con él a las contraseñas que tenía almacenadas en el mismo, pues el uso de un equipo informático se presume *“estrictamente personal”*.

A continuación, quisiera destacar en apartados individuales las resoluciones judiciales dictadas en asuntos de tres tipologías distintas: los fraudes ejecutados a través del enrolamiento de la tarjeta bancaria en plataformas de pago para móviles, los fraudes mediante el duplicado de la tarjeta SIM y las resoluciones que entienden como negligentemente grave la conducta del usuario de servicios de pago.

6.1. JURISPRUDENCIA EN MATERIA DE VINCULACIÓN DE LOS INSTRUMENTOS DE PAGO EN PLATAFORMAS DE PAGOS PARA MÓVILES

Como se ha dicho, en este trabajo se han recogido los distintos métodos empleados en la realización de los fraudes de *phishing*. Vistos estos métodos, así como el contenido de la exposición, interesa ahora destacar la jurisprudencia dictada en materia de técnicas defraudatorias concretas utilizadas para llevar a cabo la sustracción de los fondos de los usuarios.

Así, para comenzar con el análisis jurisprudencial individualizado en este tipo de técnicas de *phishing*, interesa destacar un método empleado por los ciberdelincuentes mediante el que se consigue la vinculación del instrumento de pago en una plataforma de pagos para móviles (“Apple Pay”, “Google Pay”, “Samsung Pay”).

En este caso, no se trata tanto de una modalidad en sí, pues su origen suele estar en un *smishing* o un *vishing*, sino más bien en la forma mediante la que se ejecuta la sustracción de fondos. Y es que, como ya se ha indicado, normalmente, los códigos y claves que se obtienen mediante el *phishing* son empleados para realizar las operaciones directamente, sin embargo,

en este tipo de fraudes el ciberdelincuente obtiene de su víctima el código necesario para vincular su tarjeta bancaria a una plataforma de pagos para móviles.

Siendo esto así, interesa destacar este tipo de fraude puesto que únicamente se envía un solo código a través de SMS -sabemos de su vulnerabilidad- para vincular el instrumento de pago a una plataforma. Una vez vinculada la tarjeta, se entiende realizada la doble autenticación, sin cerciorarse de que realmente sea el usuario quien realiza las posteriores operaciones de pago, las cuales no tienen un número límite puesto que la tarjeta bancaria se encuentra vinculada a la plataforma.

La jurisprudencia ha tenido ocasión de pronunciarse respecto a este tipo de fraudes, entendiendo mayormente las AAPP que la responsabilidad en este tipo de asuntos ha de atribuirse al proveedor de servicios, dada la inexistencia de negligencia grave en la conducta del usuario[60].

Detallando un poco más el contenido de estas resoluciones, se pueden destacar argumentos similares a los encontrados en aquellos casos de fraudes con origen en un SMS o en una llamada telefónica -inexistencia de negligencia grave, responsabilidad cuasi-objetiva, etc.- complementados con otros más específicos como, por ejemplo, el recogido en la SAP de Baleares 132/2023 de 17 de febrero de 2023, que enjuicia un supuesto en el que fue enrolada la tarjeta en la plataforma de pagos "Apple Pay" sin que el usuario de servicios dispusiese de dispositivos con sistema operativo "Apple".

6.2. JURISPRUDENCIA EN MATERIA DE *SIM SWAPPING*

Pasando al siguiente supuesto, los casos de *Sim Swapping*, ha de ponerse de manifiesto que, al igual que el anterior, este tipo de fraudes resultan particulares en cuanto a su ejecución práctica. En este caso, puesto que el usuario no recibe ningún tipo de comunicación que le permita tener constancia de que se esté produciendo un fraude, toda vez que el ciberdelincuente consigue realizar un duplicado de su tarjeta SIM para así ser este quien recepcione las comunicaciones que el usuario debería estar recibiendo.

[60] Al respecto pueden citarse las siguientes sentencias: SAP de Asturias, Sección 5ª, 48/2024, de 4 de julio de 2024, rec. 347/2024; SAP de Asturias, Sección 6ª, 79/2024, de 22 de mayo de 2024, rec. 272/2024; SAP de Málaga, Sección 5ª, 192/2024, de 19 de marzo de 2024, rec. 2625/2023; SAP de Ciudad Real, Sección 1ª, 58/2024, de 22 de febrero de 2024, rec. 210/2022; SAP de Asturias, Sección 7ª, 353/2023, de 30 de junio de 2023, rec. 593/2021; SAP de A Coruña, Sección 6ª, 86/2023, de 29 de marzo de 2023, rec. 391/2022; SAP de Baleares, Sección 5ª, 132/2023, de 17 de febrero de 2023, rec. 925/2022; SAP de Badajoz, Sección 3ª, 159/2022, de 16 de junio de 2022, rec. 233/2022; SAP de Pontevedra, Sección 6ª, 539/2021, de 21 de diciembre de 2021, rec. 346/2021.

En este tipo de asuntos, la jurisprudencia tiende a una mayor unanimidad en cuanto a descartar la concurrencia de negligencia grave en la conducta del usuario y a atribuir al proveedor de los servicios la responsabilidad respecto de las operaciones no autorizadas.

A tal efecto puede destacarse por su argumentación la SAP de Zaragoza, Sección 5ª, 996/2022, de 17 de noviembre de 2022, rec. 20/2022, que descarta la presencia de negligencia grave en la actuación del usuario, quien únicamente vio duplicada su tarjeta SIM sin haber realizado ningún tipo de actuación imputable a su conducta que posibilitase el fraude en tanto que esta modalidad puede tener su origen en numerosas circunstancias, como puede ser un supuesto de *pharming* o una falta de diligencia por parte de la compañía telefónica al permitir la realización de un duplicado de tarjeta SIM a un tercero ajeno a la línea móvil contratada.

Entroncando con lo anterior, interesa dejar recogida en este trabajo la SAP de Almería, Sección 1ª, 216/2023, de 1 de marzo de 2023, rec. 1555/2022, que condena a la compañía telefónica que prestaba servicio al usuario al momento de tener lugar el fraude, calificando el duplicado de tarjeta como "*un eslabon mas de la 'cadena defraudadora' sin el cual no es posible completar la apropiación económica" en cuanto permite acceder a los datos útiles incluido DNI, y cometer el fraude"*.

6.3. JURISPRUDENCIA QUE APRECIA NEGLIGENCIA GRAVE EN LA CONDUCTA DEL USUARIO DE SERVICIOS DE PAGO

Hasta el momento, todas las sentencias a las que se ha hecho referencia resultaban favorables al usuario de servicios de pago. Si bien es cierto que la mayor parte de nuestra jurisprudencia se pronuncia descartando la presencia de negligencia grave en su actuación y, por consiguiente, declarando la responsabilidad del proveedor de servicios, no existe unanimidad al respecto.

Esta afirmación puede parecer evidente en tanto que decidir respecto a si concurre, o no, negligencia grave supone realizar un ejercicio de valoración de un elemento subjetivo, debiendo emplear para ello los estándares de diligencia exigibles recogidos en la normativa[61] y en la jurisprudencia[62].

Así, nuestros tribunales se han pronunciado también respecto a asuntos de *phishing* optando por afirmar que el usuario incurrió en negligencia grave en su actuación. Ya en el año

[61] Vid. art. 1.104 CC, considerando 72 de la Directiva 2015/2366, y demás estándares que se recogen en este trabajo.

[62] Vid. Anexo I.

2012, desechaban la posibilidad de que el banco tuviese que hacer frente a los importes sustraídos debido a fraudes de *phishing*.

En este sentido se pronuncia la Sentencia dictada por la AP de Las Palmas, Sección 5ª, 586/2012, de 20 de diciembre de 2012, rec., 1057/2011, dictada estando en vigor la LSP del año 2009, y que tiene en cuenta para efectuar su valoración la ausencia de responsabilidad contractual por parte de la entidad bancaria al facilitar el usuario, víctima de un fraude *phishing*, sus datos bancarios, junto con los avisos publicados en medios de comunicación alertando de los peligros de los sistemas de banca electrónica.

Avanzando en el tiempo más de diez años, puede observarse cómo cada caso de *phishing* resulta particular, pues la SAP de Sevilla, Sección 8ª, 425/2023, de 12 de diciembre de 2023, rec. 9410/2022, se pronuncia respecto a la conducta empleada por la víctima del fraude entendiendo que había obrado con la falta de diligencia suficiente como para desestimar el recurso interpuesto.

Esta falta de diligencia se traduce en el hecho de no haber detectado las anomalías contenidas en el correo electrónico recibido como origen del fraude. Además, junto a lo burdo del engaño, la SAP destaca los avisos realizados por el banco a los usuarios respecto a las técnicas de *phishing*. Y, finalmente, para imputar al usuario la responsabilidad respecto a las operaciones de pago se recoge la tardanza en comunicar el fraude y llevar a cabo las actuaciones tendentes a paliar sus consecuencias.

De manera similar ha resuelto, tan solo hace unos meses, la Sección 1ª de la AP de Valladolid en su sentencia 509/2024, de 2 de septiembre de 2024, rec. 782/2022. En esta resolución, el tribunal entiende como no "*palmaria y no disculpable*" la conducta del usuario de servicios de pago al haber facilitado las claves de acceso y códigos de seguridad, dando lugar al incumplimiento de sus deberes de custodia respecto a estos.

Por último, antes de poner fin a este apartado, interesa destacar de entre todas las sentencias consultadas -por el enfoque dado al concepto de negligencia grave- la SAP de A Coruña, Sección 3ª, de 25 de enero de 2023, que efectúa una valoración de la negligencia grave dividiendo por etapas la actuación del usuario respecto al fraude.

Así, la AP entiende que no se trata de una única negligencia, sino que son tres, cuya excusabilidad disminuye según avanza el fraude: *"No es una negligencia, son tres. Y si la primera aún pudiera ser más o menos comprensible (pinchar en un enlace), la segunda ya es*

grave (facilitar usuario y contraseña), y la tercera es totalmente temeraria (informar de la confirmación)".

6.4. ESPECIAL REFERENCIA A LOS ASUNTOS *MAN IN THE MIDDLE*

Para finalizar con el análisis jurisprudencial, quiere ponerse de relieve las decisiones que nuestros tribunales toman en los asuntos de fraudes *Man in the Middle*. Como ya se ha advertido al estudiar esta modalidad, se trata de estafas muy particulares en las cuales el tercero defraudador extrae el correo electrónico en el que se envía una factura para modificar el IBAN de la cuenta destino de los fondos y sustraer así el importe correspondiente al pago de la comunicación interceptada.

Es en esta clase de fraudes en los que la jurisprudencia encuentra una mayor división, decantándose principalmente por una de dos posturas, bien el proveedor de servicios no ha de hacerse cargo de las operaciones no autorizadas puesto que la LSP establece en su art. 59 la correcta ejecución de la orden de pago en caso de haberse efectuado con arreglo al identificador único (IBAN de la cuenta de destino), bien el proveedor sí ha de hacerse cargo en base a la falta de diligencia en su actuación y en virtud de la responsabilidad cuasi-objetiva establecida por la ley.

Antes de realizar el análisis jurisprudencial, ha de manifestarse que en este tipo de supuestos las reclamaciones efectuadas por el usuario-víctima se dirigen frente al banco de destino de los fondos, en lugar de reclamar al banco emisor de las operaciones, por haber incurrido este en una falta de diligencia, pues como se ha dejado recogido con anterioridad al tratar la diligencia exigible, esta ha de ser la correspondiente a un comerciante experto.

Como ejemplo de la primera corriente jurisprudencial, se encuentran varias sentencias. En primer lugar, ha de destacarse la STJUE de 21 de marzo de 2019 dictada en el asunto C-245/18 con origen en la petición de decisión prejudicial planteada por el Tribunal Ordinario de Udine, Italia.

En esta resolución, el tribunal europeo se pronuncia estableciendo que el art. 74 de la Directiva 2077/64/CE -la cual dio origen a la LSP del año 2009- ha de interpretarse de tal manera que *"cuando una orden de pago se ejecute de acuerdo con el identificador único facilitado por el usuario de servicios de pago y tal identificador no corresponda al nombre del beneficiario indicado por ese mismo usuario, la limitación de la responsabilidad del proveedor*

de servicios de pago establecida en esta disposición se aplicará tanto al proveedor de servicios de pago del ordenante como al proveedor de servicios de pago del beneficiario".

Este pronunciamiento ha sido recogido por nuestra jurisprudencia. Así, la SAP de Madrid, Sección 10ª, 336/2024, de 17 de julio de 2024, rec. 139/2024 rechaza que la entidad destinataria de los fondos haya de asumir ningún tipo de responsabilidad al recibir una transferencia con identificador único cuando no coincidan el beneficiario indicado en la orden de pago con el titular de la cuenta. De igual manera, la SAP de Baleares, Sección 5ª, 347/2023, de 2 de mayo de 2023, rec. 891/2022 recoge la STJUE y descarta la responsabilidad del proveedor de servicios de pago en base a la argumentación ya manifestada.

Por el contrario, existen sentencias que sí estiman la responsabilidad del proveedor de servicios de pago del destinatario respecto a transferencias no autorizadas consecuencia de fraudes del tipo *Man in the Middle*.

Entre estas resoluciones, puede destacarse la SAP de Salamanca Sección 1ª, 311/2024, de 10 de junio de 2024, rec. 466/2023, que declara la responsabilidad del proveedor de servicios en base al articulado de la LSP y a la jurisprudencia dictada por nuestras AAPP en esta materia, resaltando especialmente el siguiente pronunciamiento: *"se efectuó pagos a una cuenta que al estar abierta en su entidad debió de tener constancia de que los estaba realizando a favor de un tercero distinto de aquel a quien iban dirigidos los pagos (...) todo ello sin ninguna comprobación adicional ni advertencia e incluso al ordenante de los pagos. Permitió la operatividad y circulación en el tráfico mercantil de una cuenta bancaria a nombre de una identidad inexistente y de persona a quien no le constaba ningún tipo de actividad económica, (...) Autorizó el acceso libre sin ningún control, ni previo ni posterior, de los delincuentes, al sistema de banca electrónica lo que les permitió, como también se acredita con la investigación efectuada por la policía, disponer de los fondos de manera inmediata y de hacerlos desaparecer prácticamente nada más recibirlos en la cuenta, impidiendo con ello su recuperación una vez detectado diligentemente el fraude y solicitada la retroacción de las operaciones"*.

Junto a la anterior sentencia, resulta muy interesante el pronunciamiento recogido en la SAP de Valencia, Sección 6ª, 343/2021, de 19 de julio de 2021, rec. 68/2021, en tanto que se entiende necesaria la comprobación de los datos de la transferencia por parte del banco ordenante, no siendo suficiente como única comprobación la del identificador único (IBAN)[63].

[63] *"TERCERO.- Esta última interpretación nos parece más acorde con la protección debida al usuario de los servicios bancarios, y a las obligaciones propias de las entidades que ofrecen los servicios telemáticos, que son conocedoras de las crecientes actuaciones ilícitas o estafas que proliferan aprovechando las nuevas*

Esta interpretación respecto a la comprobación de los datos de la transferencia concuerda con lo recogido en la propuesta de la próxima Directiva de Servicios de Pago y servicios de dinero electrónico en el mercado interior (PSD3), que sustituirá a la actual PSD2[64].

Finalmente, para terminar con el análisis jurisprudencial en esta materia ha de dejarse recogido que la casuística de este tipo de fraudes ha dado lugar a pronunciamientos de nuestras AAPP que estudian las reclamaciones a la mercantil en lugar de al proveedor de servicios de pago. Entre estas sentencias pueden destacarse la SAP de La Rioja Sección 1ª, 223/2024, de 10 de mayo de 2024, rec. 150/2023 o la SAP de Cantabria, Sección 2ª, 609/2023, de 24 de noviembre de 2023, rec. 358/2022, que estudian el concepto del pago liberatorio a tercero recogido en el art. 1.164 CC.

7. CONCLUSIONES

I. A lo largo de este trabajo se han puesto de manifiesto las ideas clave que ahora moldean mis conclusiones. Una vez estudiado el *phishing* bancario, mi opinión concuerda con la mayoría de las sentencias dictadas en nuestro país acerca de esta materia. Si bien es cierto que las operaciones se realizan de forma correcta desde el punto de vista técnico, y que puede encontrarse una similar técnica defraudatoria si se presta atención a las ciberestafas que tienen lugar en nuestro país, cada caso es único, puesto que el grado de engaño y los datos facilitados varían, al igual que sucede con el importe sustraído o las operaciones de pago empleadas para ello (compras con tarjeta, transferencias, …), motivo por el cual no puede considerarse una operación de pago como autorizada por su mero registro.

II. Comparto así los argumentos esgrimidos por la jurisprudencia, tales como el hecho de que las operaciones se realizan bajo engaño bastante, el cual no surge por iniciativa del usuario sino de un tercero especialista en este tipo de fraudes, o la realidad del número de afectados,

---

tecnologías, y que desarrollan mecanismos técnicos con el fin de ofrecer un sistema lo más seguro posible para el usuario, como parte igualmente de su oferta de servicios. Y en el caso concreto que se nos somete, y debido a una conducta fraudulenta de tercero, se identificó un determinado número de IBAN, el facilitado por el tercero, si bien con discordancia con el destinatario (conocido y expresado) al que se quería efectuar pago por relaciones comerciales, a través de las dos transferencias. Una alerta acerca de la discordancia entre los datos facilitados en la orden de transferencia hubiera sido suficiente para, o bien no realizarlas, o antes comunicar tal circunstancia de falta de coincidencia al ordenante. Ello, entendemos, concuerda también con el texto del Reglamento Europeo (Reglamento UE nº 260/2012) que invoca la propia parte recurrente, no excluye su responsabilidad, pues si bien es posible una transferencia cuando se efectúe con un número de identificador único, no impide, sino autoriza, a reseñar la identidad del destinatario, lo que sucedió claramente en las dos transferencias que son origen de las presentes actuaciones, y, por ello, no es suficiente, a criterio de la Sala, que escudándose la entidad apelante, en que tan sólo sería necesario el número de IBAN, no necesitaría comprobar ningún otro dato que se facilitara, aunque de esa comprobación, que puede ser efectuada automáticamente, aparezcan divergencias o contracciones en la orden emitida por el ordenante de la transferencia".

[64] Página web de la Unión Europea, propuesta de la Directiva PSD3 (fecha de última consulta: 01/02/2025).

que pone de manifiesto el hecho de que no bastan avisos genéricos por parte del proveedor de servicios, siendo necesarias comunicaciones más precisas y eficientes que tengan por fin concienciar y educar a los usuarios en materia de ciber fraudes. Y es que puede que se haya implementado con demasiada rapidez en nuestras vidas la banca electrónica y la ejecución de operaciones de pago a través de internet.

III. Resulta imprescindible implementar soluciones técnicas, tanto en materia de banca electrónica como de telecomunicaciones, para evitar la suplantación de mensajes y llamadas aparentemente realizadas por los canales oficiales de comunicación designados por el banco. Mientras no se produzca la mejora técnica, los usuarios estamos a merced de la habilidad de los ciberdelincuentes a la hora de ejecutar el fraude.

IV. No pretendo con estas conclusiones tratar de objetivar la responsabilidad en materia de operaciones no autorizadas pues es evidente que existen casos en los que el usuario actúa de manera gravemente negligente. Sin embargo, sí considero que mientras la nueva realidad en materia de operaciones bancarias se consolida y se implementan las medidas *anti phishing* que estimo necesarias, han de ser los proveedores de servicios quienes respondan de las operaciones no autorizadas en cuya realización no concurra ni fraude ni negligencia grave del usuario, siendo estos la gran mayoría de los casos.

V. Por último, personalmente considero el *phishing* bancario un "fenómeno" jurídicamente interesantísimo, que combina elementos técnicos y tecnológicos con cuestiones jurídicas muy especializadas, aunque siempre fundamentado en aspectos elementales del derecho. Se trata de un área de campo a través de la cual se puede adquirir mucho conocimiento, pero ello no debe nunca dejar de lado la realidad, la cual no es otra que el elevado número de víctimas que ha sufrido la sustracción de los fondos de sus cuentas consecuencia de la acción defraudatoria de un tercero.

8. FUENTES DE INFORMACIÓN

8.1. BIBLIOGRAFÍA

ALVARADO HERRERA, L.: "Autenticación reforzada de cliente y responsabilidad en la segunda directiva de servicios de pago", *Revista de Derecho del Sistema Financiero,* nº 5, 2023, págs. 69-112.

CONESA LAREO, C., GORJÓN RIVAS, S. y RUBIO ORTEGA, G.: "Un nuevo régimen de acceso a las cuentas de pago: la PSD2", *Revista de Estabilidad Financiera / Banco de España*, nº 35, 2018, págs. 81-102.

CUAIRÁN GARCÍA, J. y FERNÁNDEZ HUERTAS, P.: "El fraude «man in the middle». Un análisis dual en los órdenes penal y civil", *Diario La Ley*, nº 81, 2024.

ESTANCONA PÉREZ, A.A.: "Responsabilidad de las entidades financieras ante el hackeo de cuentas bancarias. En particular, casos de "phishing"", *Actualidad jurídica iberoamericana*, nº 18, 2023, págs. 1590-1617.

HERRANZ RAMOS, I.: "El estándar mercantil de diligencia: el ordenado empresario", *Anuario de derecho civil*, nº 1, 2006, págs. 195-226.

HERNÁNDEZ DE COS, P.: "El ciberriesgo y sus implicaciones para la estabilidad financiera", *Repositorio Institucional Banco de España*, 2024, pág. 2.

JIMÉNEZ GONZALO, C. y TEJERO SALA, H.: "Cierre de oficinas bancarias y acceso al efectivo en España", *Revista de Estabilidad Financiera / Banco de España*, nº 34, 2018, pág. 42.

PEÑALOSA TOMÉ, C.: "Man in the middle. El error en la transferencia. Interposición delictiva de tercero. Responsabilidad civil bancaria", *Diario La Ley*, nº 10467, 2024.

PIQUERES CASTELLOTE, F. "Conocimientos básicos en Internet y utilización para actividades ilícitas", *Delitos contra y a través de las nuevas tecnologías ¿Cómo reducir su impunidad?, Consejo General del Poder Judicial*, Madrid, 2006, pág. 71.

RIBÓN SEISDEDOS, E.: F*raudes bancarios y defensa del afectado. Nuevas tendencias defraudatorias. Especial referencia al phishing bancario*, Tirant lo Blanch, Valencia, 2024, págs. 43 y 44.

SAN MARTINO, A. y PERRAMON, X., "Phishing Secrets: History, Effects, Countermeasures", *International Journey of. Network Security*, nº 11, 2011, págs. 163-171.

YEBOAH-BOATENG, E. O. y AMANOR, P.M.: "Phishing, SMiShing & Vishing: an assessment of threats against mobile devices", *Journal of Emerging Trends in Computing and Information Sciences*, 2014, vol. 5, nº 4, pág. 297.

ZUNZUNEGUI PASTOR, F.: "Spain's Implementation of PSD2", Gimigliano, G. y Božina Beroš, M. (editores*), The Payment Services Directive II,* Edward Elgar Publishing Limited, Cheltenham, 2021, págs. 406-424.

8.2. RECURSOS ELECTRÓNICOS

AEPD (Ficha protección de datos y prevención de delitos y Guía de protección de datos y prevención de delitos).

BDE (Información sobre "vishing" disponible en el Portal del Cliente Bancario en la página web del BDE, Página web del BDE y Página web del BDE).

Consejo General del Poder Judicial.

INCIBE (Aprende Ciberseguridad y "Spear Phishing").

"Kaspersky" (*https://www.kaspersky.es/resource-center/definitions/what-is-an-ip-address* y *https://www.kaspersky.es/resource-center/definitions/what-is-a-qr-code-how-to-scan*)

"Mcafee" (¿Cuáles son los riesgos de hacer clic en enlaces maliciosos? y Ejemplos de *phishing*: cómo detectar un correo de *phishing*).

Sello Legal Abogados (*https://sellolegal.com/blog/los-8-tipos-de-ataque-phishing-mas-utilizados/* y *https://sellolegal.com/blog/qrshing-los-ataques-de-phishing-a-traves-de-codigos-qr-falsos/*).

Servicio de Informática de la Universidad de Jaén (Servicio de Informática).

Unión Europea, El acceso al Derecho de la Unión Europea (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0366).

8.3. OTRAS FUENTES DE INFORMACIÓN

BDE (Suplantación de SMS y del identificador de llamadas y Variaciones en el número de oficinas por entidad).

GANGAN, S.: "A review of man-in-the-middle attacks". *arXiv preprint arXiv:1504.02115*, 2015.

INE (Nota de prensa de fecha 28 de noviembre de 2023).

Noticia del periódico 20 Minutos (Deutsche Bank y Vodafone).

Noticia del periódico El Confidencial (Caja Rural y Telefónica).

Noticia del periódico El País (Noticia del periódico El País publicada en fecha 2 de agosto de 2024 y Orange).

Noticia del periódico El Mundo (Noticia del periódico El Mundo publicada en fecha 7 de diciembre de 2023).

Noticia del periódico El Independiente (Banco Santander).

Noticia del periódico Escudo Digital (EVO BANCO).

Noticia del periódico Expansión (INVERSIS).

Portal estadístico de criminalidad (Portal estadístico de criminalidad, filtrando los datos para obtener el total nacional de estafas informáticas).

RECOVERY LABS: "Fraude en Internet: Del phishing al pharming", *Laboratorio de Recuperación de Datos Informáticos*, pág. 2.

9. RELACIÓN DE LAS RESOLUCIONES JUDICIALES CITADAS

STJUE de 21 de marzo de 2019 dictada en el asunto C-245/18.

SAP de Barcelona, Sección 4ª, 735/2024, de 24 de octubre de 2024, rec. 696/2023.

SAP de Barcelona, Sección 17ª, 597/2024, de 12 de septiembre de 2024, rec. 65/2024.

SAP de Valladolid, Sección 1ª, 509/2024, de 2 de septiembre de 2024, rec. 782/2022.

SAP de Madrid, Sección 10ª, 336/2024, de 17 de julio de 2024, rec. 139/2024.

SAP de Asturias, Sección 1ª, 502/2024, de 25 de junio de 2024, rec. 508/2024.

SAP de Salamanca Sección 1ª, 311/2024, de 10 de junio de 2024, rec. 466/2023.

SAP de La Rioja Sección 1ª, 223/2024, de 10 de mayo de 2024, rec. 150/2023.

SAP de Jaén, Sección 1ª, 546/2024, de 24 de abril de 2024, rec. 1531/2022.

SAP de La Rioja, Sección 1ª, 185/2024, de 18 de abril de 2024, rec. 149/2023.

SAP de Asturias Sección 1ª, 324/2024, de 17 de abril de 2024, rec. 255/2024.

SAP de Sevilla, Sección 8ª, 425/2023, de 12 de diciembre de 2023, rec. 9410/2022.

SAP de Cantabria, Sección 2ª, 609/2023, de 24 de noviembre de 2023, rec. 358/2022.

SAP de A Coruña, Sección 3ª, 364/2023, de 5 de octubre de 2023, rec. 87/2023.

SAP de Valencia, Sección 8ª, 308/2023, de 5 de julio de 2023, rec. 536/2022.

SAP de Baleares, Sección 5ª, 347/2023, de 2 de mayo de 2023, rec. 891/2022.

SAP de Pontevedra, Sección 3ª, 177/2023, de 23 de marzo de 2023, rec. 634/2022.

SAP de Almería, Sección 1ª, 216/2023, de 1 de marzo de 2023, rec. 1555/2022.

SAP de A Coruña, Sección 3ª, 17/2023, de 25 de enero de 2023, rec. 757/2022.

SAP de Madrid, Sección 10ª, 24/2023, de 13 de enero de 2023, rec. 918/2022.

SAP de Zaragoza, Sección 5ª, 996/2022, de 17 de noviembre de 2022, rec. 20/2022.

SAP de Valencia, Sección 6ª, 343/2021, de 19 de julio de 2021, rec. 68/2021.

SAP de Alicante, Sección 8ª, 107/2018, de 12 de marzo de 2018, rec. 622/2017.

SAP de Zaragoza, Sección 4ª, 215/2013, de 14 de mayo de 2013, rec. 116/2013.

SAP de Las Palmas, Sección 5ª, 586/2012, de 20 de diciembre de 2012, rec. 1057/2011.

AAP Madrid, Sección 10ª, 308/2024 de 15 de julio de 2024, rec. 78/2024.

AAP Vizcaya, Sección 5ª, 71/2023, de 21 de septiembre de 2023, rec. 189/2022.

AAP Barcelona, Sección 9ª, 447/2019, de 19 de julio de 2019, rec. 753/2018.

SJPI nº7 de Las Palmas de Gran Canaria, 508/2024, de 16 de octubre de 2024, rec. 1919/2023.

ANEXO I. RELACIÓN DE TODAS LAS RESOLUCIONES JUDICIALES CONSULTADAS

COMUNIDAD AUTÓNOMA	PROVINCIA	SECCIÓN	SENTENCIA	AÑO PUBLICACIÓN	FALLO (En relación al usuario)	RESUMEN
ANDALUCÍA	ALMERÍA	PRIMERA	SAP ALMERÍA, Sección 1ª, 216/2023, de 01-03-2023, rec. 1555-2022	2023	FAVORABLE/ESTIMACIÓN PARCIAL (Sin costas recurso apelación)	SIM Swapping, condena a VODAFONE, responsabilidad solidaria empresas proveedoras de servicios sin perjuicio de las acciones que correspondan entre ellas, 1.600 euros de daños morales por zozobra, angustia e inquietud padecida pues teléfono móvil es instrumento esencial, tuvo línea móvil bloqueada y terceros tuvieron acceso a su información personal.
		PRIMERA	SAP ALMERÍA, Sección 1ª, 99/2023, de 31-01-2023, rec. 2117-2021	2023	FAVORABLE	Inexistencia negligencia grave, demandante actitud diligente tratando de contactar con el banco, banco no adoptó las medidas de seguridad precisas para evitar o minorar las consecuencias para el cliente de haber sufrido un fraude en red.
ANDALUCÍA	CÁDIZ	SEGUNDA	SAP CÁDIZ, Sección 2ª, 473-2023, de 23-11-2023, rec. 542-2023	2023	FAVORABLE	Carga de la prueba banco, certificado Rural Servicios Informáticos, S.L. no es un informe pericial sino un documento privado de parte elaborado por una entidad del mismo grupo empresarial que la demandada (CAJA RURAL DEL SUR), este certificado no refleja soporte factor doble autenticación, inexistencia negligencia grave cliente, aunque introdujera DNI no consta activación firma biométrica.
		SEGUNDA	SAP CÁDIZ, Sección 2ª, 474-2023, de 23-11-2023, rec. 582-2023	2023	FAVORABLE	Inexistencia negligencia grave, carga prueba banco, no consta acreditados mensajes necesarios para autenticar operaciones se recibieran en el teléfono de la cliente, "fallaron los procesos reforzados para la autenticación de las operaciones".
ANDALUCÍA	CÓRDOBA	PRIMERA	SAP CÓRDOBA, Sección 1ª, 685/2024, de 08-07-2024, rec. 667-2023	2024	NO ES SOBRE PHISHING	No es sobre phishing, pero lo menciona. SMS enviados a través del dispositivo de un particular tras interactuar con un enlace de un SMS fraudulento.
ANDALUCÍA	GRANADA	CUARTA	SAP GRANADA, Sección 4ª, 173/2023, de 10-05-2023, rec. 523-2022	2023	FAVORABLE	Virus informático instalado en el ordenador de la empresa, inexistencia negligencia grave, no queda acreditado CAJA RURAL DE GRANADA comunicase al Banco de España sospecha de fraude artículo 45.1 LSP.
		CUARTA	SAP GRANADA, Sección 4ª, 164/2023, de 04-05-2023, rec. 456-2022	2023	FAVORABLE	Banco no prueba autorización de las operaciones por el cliente, inexistencia negligencia grave, SMS no recibidos dispositivo del cliente, operaciones sospechosas pauta de gasto.
		CUARTA	SAP GRANADA, Sección 4ª, 93/2023, de 09-03-2023, rec. 652-2022	2023	FAVORABLE	Clienta reconoce facilitó credenciales bancarias, autenticación Out of Band (OoB) correcta, pero banco no lo usó en este caso, sino que aplicó "CLIENTE AUTENTICADO MEDIANTE SPA EN COMERCIO ELECTRÓNICO" y se desestima porque se desconoce en qué consiste este sistema así como que si tiene las dos fases de autenticación como el sistema OoB.
		QUINTA	SAP GRANADA, Sección 5ª, 212-/2022, de 20-06-2022, rec. 85-2022	2022	FAVORABLE	Error excusable el hecho de facilitar sus datos personales y claves de confirmación o firma electrónica en virtud de la acción defraudatoria de terceros.
ANDALUCÍA	HUELVA	SEGUNDA	SAP HUELVA, Sección 2ª, 142/2024, de 08-02-2024, rec. 97-2024	2024	FAVORABLE/ESTIMACIÓN PARCIAL (se quitan las costas de primera instancia)	Legitimación pasiva CAIXABANK, responsabilidad cuasi-objetiva, riesgo propio del sistema de pagos, pauta de gasto.
		SEGUNDA	SAP HUELVA, Sección 2ª, 643/2023, de 16-10-2024, rec. 872-2023	2023	FAVORABLE	Inexistencia negligencia grave, para negligencia grave iniciativa propio usuario, phishing hace necesario aumentar medias de seguridad específicas, banco no acredita IP desde la que se efectúa la transferencia.
ANDALUCÍA	JAÉN	PRIMERA	SAP JAÉN, Sección 1ª, 546/2024 de 24-04-2024, rec. 1531-2022	2024	FAVORABLE	Falsedad de la autenticación (víctima phishing = operación no autenticada en términos LSP), banco tiene obligación de prestar banca telemática segura, REDSYS acredita correcta autenticación técnica pero no prueba identidad ordenante. Rapidez del cliente en denunciar y en comunicar al banco el fraude.
		PRIMERA	SAP JAÉN, Sección 1ª, 290/2024, de 29-02-2024, rec. 296-2023	2024	FAVORABLE	Responsabilidad cuasi-objetiva, avisos genéricos bancos no suficientes, inexistencia negligencia grave.
		PRIMERA	SAP JAÉN, Sección 1ª, 1355-2022, de 14-12-2022, rec. 1621-2022	2022	FAVORABLE	Inexistencia negligencia grave, error excusable, operaciones inusuales, banco debe adoptar medidas tecnológicas adecuadas y no solamente medidas genéricas de protección o avisos, entidades bancarias deben asumir los riesgos del sistema, incumplimiento contractual del banco.
ANDALUCÍA	MÁLAGA	QUINTA	SAP MÁLAGA, Sección 5ª, 192/2024 de 19-03-2024, rec. 625-2023	2024	FAVORABLE	Enrolamiento tarjeta en "Apple Pay". Explicación responsabilidad contractual y extracontractual. Responsabilidad cuasi-objetiva y sin que conste prueba de que el banco exigiese método complementario de verificación para realizar las operaciones.
		QUINTA	SAP MÁLAGA, Sección 5ª, 340/2023, de 23-05-2023, rec. 340-2023	2023	FAVORABLE	Inexistencia negligencia grave, para negligencia grave iniciativa propio usuario, banco debió implementar mecanismo tecnológico para evitar phishing, conducta activa y no simplemente informativa o divulgativa, banco no informó cliente sobre las operaciones.
ANDALUCÍA	SEVILLA	OCTAVA	SAP SEVILLA, Sección 8ª, 425/2023, de 12-12-2023, rec. 9410-2022	2023	DESFAVORABLE	Correo electrónico, demandante obró con falta diligencia al no detectar señal de peligro en el anómalo correo electrónico, datos facilitados por la actora, REDSYS acredita operaciones correctamente autenticadas, phishing ampliamente conocido por usuarios de servicios online (técnica delictiva muy frecuente), fácilmente detectables y reconocibles, pasividad en comunicar al banco e interponer denuncia.
		SEXTA	SAP SEVILLA, Sección 6ª, 285/2018, de 04-10-2018, rec. 8228-2017	2018	FAVORABLE	Inexistencia negligencia grave, responsabilidad cuasi-objetiva.
		QUINTA	SAP SEVILLA, Sección 5ª, 319/2014, de 26-05-2014 rec. 10433-2012	2014	DESFAVORABLE/ESTIMACIÓN PARCIAL (quita las costas en primera instancia y no condena a las de apelación)	Grave imprudencia prescindir de la advertencia que salía durante ocho años en que clientes operaron con banca online y accediesen a página web fraudulenta introduciendo usuario y contraseña y facilitasen las 60 o 100 claves de su tarjeta de coordenadas, rellenando una tras otra todas esas claves en el formulario correspondiente. Ley de Servicios de Pago 16/2009.
ARAGÓN	HUESCA	PRIMERA	SAP HUESCA, Sección 1ª, 230/2024, de 30-06-2024, rec. 502-2021	2024	FAVORABLE	No es exigible al cliente medio un conocimiento informático técnicas apropiación datos personales, las entidades bancarias se benefician de la banca online, la diligencia exigible es la de un comerciante experto, las advertencias en la página web no son suficientes, no es responsabilidad contractual sino responsabilidad legal.

ARAGÓN	TERUEL	PRIMERA	SAP TERUEL, Sección 1ª, 74/2023, de 30-06-2023, rec. 56-2023	2023	FAVORABLE	SIM SWAPPING. Inexistencia negligencia grave, no fue el usuario quien realizó las operaciones sino los ciberdelincuentes a través del duplicado de la tarjeta SIM, responsabilidad cuasi-objetiva, el usuario comunicó a la entidad y presentó denuncia tan pronto como tuvo conocimiento de las operaciones no autorizadas.
		QUINTA	SAP ZARAGOZA, Sección 5ª, 621/2024, de 11-10-2024, rec. 169-2024	2024	FAVORABLE	Usuario fue engañado, proveedor de servicios no empleó la diligencia exigible, "el automatismo de la operativa (bajo los criterios del sistema informático de la entidad) no puede justificar irresponsabilidad", condición de experto en la materia para detectar el fraude, no bastan avisos genéricos sobre el fraude.
		SEGUNDA	SAP ZARAGOZA, Sección 2ª, 238/2024, de 12-06-2024, rec. 443-2023	2024	DESFAVORABLE	Negligencia grave porque cualquier persona de tipo medio habría distinguido que se trataba de un correo no enviado por su entidad bancaria, en julio de 2020 era de general conocimiento el hecho de que los bancos no pedían datos personales por correo electrónico, falsedad evidente y no sofisticada, art. 306 Código Comercio frente a la responsabilidad del depositario en un depósito mercantil.
		CUARTA	SAP ZARAGOZA, Sección 4ª, 117/2023, de 10-03-2023, rec. 321-2022	2023	FAVORABLE	Enrolamiento tarjeta en "Samsung Pay". Altísimo grado de vulnerabilidad del sistema, el fraude se proyecta sobre el terminal del cliente (la pieza más vulnerable del sistema), sin disponer dispositivo Samsung, se traslada el riesgo al proveedor de servicios, error identificación del cliente, pauta de gasto.
ARAGÓN	ZARAGOZA	CUARTA	SAP ZARAGOZA, Sección 4ª, 55/2023, de 17-02-2023, rec. 412-2022	2023	FAVORABLE	Se traslada el riesgo al proveedor de servicios, el sistema de pago es bidireccional y cualquier fraude lo es a todo el sistema, los prestadores de servicios no han logrado crear canales seguros de comunicación.
		QUINTA	SAP ZARAGOZA, Sección 5ª, 996/2022, de 17-11-2022, rec. 20-2022	2022	FAVORABLE	SIM Swapping, el banco reintegró parcialmente la cantidad defraudada, pauta de gasto, el cliente había alertado en su sucursal de los mensajes de transferencias recibidos.
		CUARTA	SAP ZARAGOZA, Sección 4ª, 265/2022, de 14-09-2022, rec. 162-2022	2022	FAVORABLE	Cliente no recibió SMS sobre las transferencias, entidad bancaria no prueba negligencia grave.
		QUINTA	SAP ZARAGOZA, Sección 5ª, 804/2022, de 01-07-2022, rec. 1130-2021	2022	FAVORABLE	No consta advertencia al cliente sobre los riesgos de la banca online, aunque la página pueda considerarse poco sofisticada hay que valorar la condición del cliente y las advertencias de quien comercializa un producto que tiene riesgos evidentes, banco carecía de medidas de seguridad exigibles razonablemente, ausencia de autenticación reforzada de ese tipo de operaciones.
		CUARTA	SAP ZARAGOZA, Sección 4ª, 215/2023, de 14-05-2013, rec. 116-2013	2013	FAVORABLE	Salvo una tardanza injustificada del usuario en comunicar la irregularidad de las operaciones, será el banco quien le deba devolver de inmediato el importe de la operación no autorizada.
		SÉPTIMA	SAP ASTURIAS, Sección 7ª, 507/2024, de 24-10-2024, rec. 265-2024	2024	FAVORABLE	Inexistencia negligencia grave, método delictivo complejo.
		QUINTA	SAP ASTURIAS, Sección 5ª, 468/2024, de 10-10-2024, rec. 308/2024	2024	FAVORABLE	Inexistencia negligencia grave, SMS spoofing, la entidad bancaria envía SMS con enlace.
		CUARTA	SAP ASTURIAS, Sección 4ª, 422/2024, de 09-10-2024, rec. 419/2024	2024	FAVORABLE	Inexistencia negligencia grave, SMS spoofing, usuario introduce códigos para vincular otro dispositivo, el engaño proviene del SMS, usuario procedió como haría gran parte de la población.
		QUINTA	SAP ASTURIAS, Sección 5ª, 460/2024, de 07-10-2024, rec. 266/2024	2024	FAVORABLE	Inexistencia negligencia grave, SMS + llamada.
		CUARTA	SAP ASTURIAS, Sección 4ª, 415/2024, de 03-10-2024, rec. 412/2024	2024	FAVORABLE	Inexistencia negligencia grave, SMS spoofing, el engaño viene ya del primer SMS, las operativas poco usuales deberían haber permitido al banco detectar que se trataba de un fraude.
		QUINTA	SAP ASTURIAS, Sección 5ª, 443/2024, de 02-10-2024, rec. 125/2024	2024	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa del usuario, en caso de no aportar SMS ha de tenerse en cuenta que, al contestar la reclamación, la entidad bancaria no cuestionó la operativa del fraude, la entidad bancaria no puede invertir la carga de la prueba.
		CUARTA	SAP ASTURIAS, Sección 4ª, 403/2024, de 25-09-2024, rec. 384/2024	2024	FAVORABLE	Inexistencia negligencia grave, SMS spoofing, el mensaje con la clave de seguridad no advertía de que se trataba de vincular un dispositivo distinto, el segundo paso del fraude viene motivado por el engaño consumado con el primer SMS, el banco no adoptó las medidas necesarias para evitar que se produjeran fraudes de esta naturaleza.
		QUINTA	SAP ASTURIAS, Sección 5ª, 419/2024, de 20-09-2024, rec. 222-2024	2024	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa usuario, responsabilidad cuasi-objetiva, falsedad de la autenticación.
		QUINTA	SAP ASTURIAS, Sección 5ª, 404/2024, de 17-09-2024, rec. 245-2024	2024	FAVORABLE	Inexistencia negligencia grave, responsabilidad cuasi-objetiva, carga de la prueba para la entidad bancaria.
		SEXTA	SAP ASTURIAS, Sección 6ª, 429/2024, de 17-09-2024, rec. 217-2024	2024	FAVORABLE	Descartado fraude, examen negligencia grave, no puede exigirse a quien resultó engañada mayor precaución que a quien debía poner los medios necesarios para evitar el engaño.
		SEXTA	SAP ASTURIAS, Sección 6ª, 368/2024, de 09-07-2024, rec. 152-2024	2024	FAVORABLE	SMS vincula otro dispositivo pero especifica qué dispositivo por lo que podría entenderse que es el propio dispositivo del cliente.
		QUINTA	SAP ASTURIAS, Sección 5ª, 347/2024, de 04-07-2024, rec. 48-2024	2024	FAVORABLE	Enrolamiento tarjeta en "Google Pay". Facilita segundo código autenticación, pero solo tras la llamada como proveniente de su oficina y en base a la confianza previa generada.
		PRIMERA	SAP ASTURIAS, Sección 1ª, 502/2024, de 25-06-2024, rec. 508-2024	2024	FAVORABLE	Error excusable consecuencia de la actitud defraudatoria de un tercero, "aquel en que puede incurrirse pese al empleo de una diligencia media o regular y, pese a ello, sufre un error que vicia su consentimiento, no imputable al interesado, en el sentido de causado por él -o personas de su círculo jurídico-, en sintonía con un elemental postulado de buena fe (Arts. 7.1 y 1258 del Código Civil) a efectos de impedir que se proteja a quien no merece dicha protección por su conducta negligente", el banco no adoptó todas las medidas para proteger a su cliente.
		QUINTA	SAP ASTURIAS, Sección 5ª, 320/2024, de 21-06-2024, rec. 37-2024	2024	FAVORABLE	Inexistencia negligencia grave, la carga de la prueba corresponde al proveedor servicios de pago.
		QUINTA	SAP ASTURIAS, Sección 5ª, 319/2024, de 21-06-2024, rec. 40-2024	2024	FAVORABLE	Inexistencia negligencia grave, la carga de la prueba corresponde al proveedor servicios de pago.
		SÉPTIMA	SAP ASTURIAS, Sección 7ª, 387/2024, de 22-05-2024, rec. 276-2024	2024	FAVORABLE	Inexistencia negligencia grave, SMS apariencia autenticidad, spoofing llamada, el cliente trata de contactar con su banco, pero no lo consigue y solamente tras no conseguirlo accede al enlace.
		CUARTA	SAP ASTURIAS, Sección 4ª, 229/2024, de 15-05-2024, rec. 142-2024	2024	FAVORABLE	Inexistencia negligencia grave, engaño consumado con los SMS recibidos, clienta guiada por el ánimo de evitar una actuación fraudulenta.
		SÉPTIMA	SAP ASTURIAS, Sección 7ª, 252/2024, de 15-05-2024, rec. 621-2023	2024	FAVORABLE	Inexistencia negligencia grave, la iniciativa no parte del cliente, supuesto retraso en la denuncia resulta irrelevante si no se produjeron más operaciones fraudulentas tras formalizarla.
		SÉPTIMA	SAP ASTURIAS, Sección 7ª, 251/2024, de 15-05-2024, rec. 641-2023	2024	FAVORABLE	Inexistencia negligencia grave, el contenido del SMS no hace sospechar que esté autorizando la transferencia y no anulándola, "ni la premura del caso permite exigirle una actuación sosegada".
		QUINTA	SAP ASTURIAS, Sección 5ª, 236/2024, de 10-05-2024, rec. 90-2024	2024	FAVORABLE	El usuario no proporcionó segundo código de autorización, sino que con el primero el defraudador pudo cambiar terminal asociado a la cuenta perdiendo el usuario el control de las operaciones de la misma.
		QUINTA	SAP ASTURIAS, Sección 5ª, 215/2024, de 02-05-2024, rec. 58-2024	2024	FAVORABLE (no impone costas apelación)	Inexistencia negligencia grave, spoofing llamada, cliente facilitó segundo código de autenticación que sería negligencia grave, pero acudió a la oficina y no le fue bloqueada su cuenta ni tampoco se informó a cliente de las pautas que suelen seguir los defraudadores tras el primer paso inicial.

ASTURIAS	ASTURIAS	SÉPTIMA	SAP ASTURIAS, Sección 7ª, 235/2024, de 30-04-2024, rec. 918-2022	2024	FAVORABLE	Inexistencia negligencia grave, responsabilidad cuasi-objetiva, inversión carga de la prueba, no bastan avisos genéricos por parte del banco en su web, la entidad bancaria debe adoptar medidas adecuadas para la banca online.
		QUINTA	SAP ASTURIAS, Sección 5ª, 207/2024, de 26-04-2024, rec. 456-2023	2024	FAVORABLE	Inexistencia negligencia grave, SMS UNICAJA.
		PRIMERA	SAP ASTURIAS, Sección 1ª, 342/2024, de 17-04-2024, rec. 255-2024	2024	FAVORABLE	Pauta de gasto, las operaciones son totalmente anómalas y llamativas, habría bastado una llamada de comprobación del banco antes de permitirlas definitivamente, el proveedor debe garantizar la seguridad en los medios de pago electrónicos que pone a disposición de sus clientes, los sistemas dispuestos por el banco no son eficientes
		CUARTA	SAP ASTURIAS, Sección 4ª, 163/2024, de 11-04-2024, rec. 113-2023	2024	FAVORABLE	Inexistencia negligencia grave, negligencia grave no surge por iniciativa de tercero, pauta de gasto.
		CUARTA	SAP ASTURIAS, Sección 4ª, 166/2024, de 10-04-2024, rec. 84-2024	2024	FAVORABLE	Inexistencia negligencia grave, spoofing, informe pericial demandante, web espejo, pauta de gasto.
		CUARTA	SAP ASTURIAS, Sección 4ª, 154/2024, de 03-04-2024, rec. 111-2024	2024	FAVORABLE	Inexistencia negligencia grave, spoofing llamada, clienta introdujo claves que le iban siendo requeridas para autorizar las operaciones motivada por el engaño ya consumado con la primera llamada, estado nerviosismo y precipitación creyendo que estaba solucionando un supuesto fraude, usuario actuó conforme habría hecho la mayoría de la población.
		CUARTA	SAP ASTURIAS, Sección 4ª, 142/2024, de 21-03-2024, rec. 89-2024	2024	FAVORABLE	Inexistencia negligencia grave, SMS spoofing, numerosas denuncias policiales en las mismas fechas del fraude (fusión UNICAJA), contenido SMS remitido por el banco advertía de la vinculación de un dispositivo a la banca digital pero no especificaba que se tratase de un dispositivo distinto, segundo paso del fraude viene precedido y motivado por el engaño sufrido mediante la remisión del SMS spoofing, gran número de estafas evidencia la falta de medidas por parte de la entidad bancaria, usuario actuó conforme habría hecho la mayoría de la población.
		QUINTA	SAP ASTURIAS, Sección 5ª, 141/2024, de 21-03-2024, rec. 401-2023	2024	FAVORABLE/ESTIMACIÓN PARCIAL (revoca nulidad préstamo sin costas de ninguna instancia)	Existencia de negligencia grave, phishing a través de llamada haciéndose pasar por compañía telefónica (TELECABLE) y clienta facilita datos tarjeta, códigos OTP y fotografías DNI, cara, datos de la marca y modelo de su teléfono móvil, ciberdelincuente le pide que no responda llamadas, solicita préstamo que es nulo y por ello se estima parcialmente el recurso.
		QUINTA	SAP ASTURIAS, Sección 5ª, 124/2024, de 13-03-2024, rec. 597-2023	2024	FAVORABLE	Inexistencia negligencia grave, spoofing llamada, facilitó segundo código de autenticación, pero precedido de engaño.
		QUINTA	SAP ASTURIAS, Sección 5ª, 120/2024, de 08-03-2024, rec. 589-2023	2024	FAVORABLE	Inexistencia negligencia grave, negligencia grave aquella que surge por iniciativa del usuario, no se verifica la identidad del ordenante de la operación, SMS consta enviado, pero no identifica el número al que se remitió no constando entonces "prueba demostrativa de la activación de la compra por la parte demandante", operación autenticada por el doble refuerzo instaurado por la entidad (sin demostrar factor posesión), falsedad de la autenticación, carga de la prueba corresponde al banco.
		QUINTA	SAP ASTURIAS, Sección 5ª, 39/2024, de 30-01-2024, rec. 507-2023	2024	FAVORABLE	Inexistencia negligencia grave, negligencia grave aquella que surge por iniciativa del usuario, no se verifica la identidad del ordenante de la operación, SMS consta enviado, pero no identifica el número al que se remitió no constando entonces "prueba demostrativa de la activación de la compra por la parte demandante", operación autenticada por el doble refuerzo instaurado por la entidad (sin demostrar factor posesión), falsedad de la autenticación, carga de la prueba corresponde al banco.
		SÉPTIMA	SAP ASTURIAS, Sección 7ª, 353/2023, de 30-06-2023, rec. 593-2021	2023	FAVORABLE	Enrolamiento tarjeta. Inexistencia negligencia grave, ciberdelincuentes pueden obtener datos teléfono cliente de múltiples formas.
		QUINTA	SAP ASTURIAS, Sección 5ª, 236/2023, de 22-06-2023, rec. 755-2022	2023	FAVORABLE (sin costas segunda instancia)	Inexistencia negligencia grave, cliente confió en SMS recibido en el canal habitual.
		SÉPTIMA	SAP ASTURIAS, Sección 7ª, 285/2023, de 12-05-2023, rec. 787-2022	2023	FAVORABLE	Inexistencia negligencia grave, se instaló la aplicación de RURALVÍA en otro dispositivo con sistema operativo distinto al del cliente, cliente pudo pensar que la iniciativa provenía por parte de su entidad bancaria e introdujo el código para activar biometría creyendo que se trataba de un sistema de seguridad para ella, necesario implementar tecnología anti phishing, conducta activa y no simplemente divulgativa.
		QUINTA	SAP ASTURIAS, Sección 5ª, 170/2023, de 20-04-2023, rec. 582-2022	2023	FAVORABLE	SIM Swapping, la pérdida de cobertura puede deberse a múltiples factores, no existiendo conocimiento generalizado de asegurar que no se está siendo objeto de un fraude bancario, no hay tardanza en comunicar el fraude al banco, sobre la condena en costas las dudas han de ser ""serias", objetivas y suponer un plus de incertidumbre al que normalmente se suscita en toda contienda judicial".
		PRIMERA	SAP ASTURIAS, Sección 1ª, 351/2022, de 18-09-2012, rec. 594-2011	2012	FAVORABLE	Inexistencia negligencia grave, no se discute que las operaciones se realizasen desde la dirección IP del cliente, mandatario custodiante de las cuentas (banco) ha sido engañado y debe responder pues se disponen los fondos de su ordenante sin haber actuado este con dolo o negligencia grave.
BALEARES	BALEARES	TERCERA	SAP BALEARES, Sección 3ª, 577/2024, de 17 -09-2024, rec. 408/2024	2024	FAVORABLE	Inexistencia negligencia grave, el usuario recibe SMS en el canal habitual, no es fácil detectar que el SMS es fraudulento, sí falta de diligencia, pero no negligencia grave.
		CUARTA	SAP BALEARES, Sección 4ª, 361/2024, de 31-07-2024, rec. 1088-2022	2024	FAVORABLE	Enrolamiento tarjeta "Google Pay". SMS + Llamada (spoofing), inexistencia negligencia grave facilitar el código para el enrolamiento tarjeta al defraudador (considerando 72 Directiva, TS 30 enero 2003 conecta la diligencia grave con la falta de diligencia inexcusable, CAIXABANK no aporta datos que prueben realizó actuaciones necesarias para evitar fraudes ni tampoco aporta advertencias hechas al cliente.
		CUARTA	SAP BALEARES, Sección 4ª, 221/2024, de 16-05-2024, rec. 821-2023	2024	FAVORABLE	Enrolamiento tarjeta "Google Pay". Inexistencia negligencia grave, SMS, no se niega que haya falta de diligencia o exceso de confianza, pero ello no puede considerarse negligencia grave.
		QUINTA	SAP BALEARES, Sección 5ª, 132/2023, de 17-02-2023, rec. 132-2023	2023	FAVORABLE	Enrolamiento tarjeta "Apple Pay". Inexistencia negligencia grave, no constan en el dispositivo del actor los mensajes para activar la tarjeta en "Apple Pay" pero sí los de tarjeta activada, el cliente no tiene dispositivo Apple el proveedor de servicios de facilitar los medios de seguridad oportunos para evitar el fraude, el propio sistema llega a bloquear la tarjeta preventivamente.
CANARIAS	LAS PALMAS	QUINTA	SAP LAS PALMAS, Sección 5ª, 343/2023, de 05-05-2023, rec. 972-2022	2023	DESFAVORABLE	La transferencia se realiza desde la misma IP de la empresa, para lo cual es necesario conocer las claves de acceso.
		QUINTA	SAP LAS PALMAS, Sección 5ª, 568/2012, de 20-12-2012, rec. 1057-2011	2012	DESFAVORABLE	No se puede imputar al banco responsabilidad contractual por un error cometido por el cliente provocado por un tercero, en los medios de comunicación y en la misma red se informaba sobre los peligros de la banca electrónica.

CANARIAS	SANTA CRUZ DE TENERIFE	TERCERA	SAP SANTA CRUZ DE TENERIFE, Sección 3ª, 177/2024, de 23-04-2024, rec. 980-2022	2024	FAVORABLE	Inexistencia negligencia grave, esta debe ser cercana al concepto de falta de diligencia inexcusable, responsabilidad cuasi-objetiva, inversión de la carga de la prueba, incumplimiento contractual del banco por la ausencia de control sobre las operaciones ejecutadas por el cliente totalmente anómalas (pauta de gasto), según testigo este tipo de prácticas se efectúan los viernes a medio día, llamada proveniente operador telefonía (Jazztel), el cliente aprecia que los códigos SMS son remitidos por BANCO SANTANDER.
		TERCERA	SAP SANTA CRUZ DE TENERIFE, Sección 3ª, 173-2024, de 22-04-2024, rec. 890-2022	2024	FAVORABLE	Hechos compatibles con virus troyano en teléfono cliente.
CANTABRIA	CANTABRIA	CUARTA	SAP CANTABRIA, Sección 4ª, 458/2024, de 12-07-2024, rec. 788-2023	2024	FAVORABLE	Inexistencia negligencia grave, la negligencia grave es la que surge por iniciativa del usuario, el hecho de acceder a un enlace que le redirige a una web espejo no es negligencia grave ni tampoco lo es introducir el código para vincular un dispositivo pues el cliente pensaba que debía introducirlo para vincular su dispositivo, "la entidad bancaria debió activar un mayor sistema mayor de seguridad al acreditarse que en la fecha del fraude sufrido por la actora, se produjo el proceso de Fusión de Liberbank con Unicaja".
		CUARTA	SAP CANTABRIA, Sección 4ª, 457/2024, de 12-07-2024, rec. 703-2023	2024	FAVORABLE	Inexistencia negligencia grave, la negligencia grave es la que surge por iniciativa del usuario, "la entidad bancaria debió activar un mayor sistema de seguridad al ver que el día 16 de junio de 2022 se habían intentado realizar diversas operaciones sin doble canal de protección y otras con firma OTP por SMS, todas ellas de importe 0 Euros".
		CUARTA	SAP CANTABRIA, Sección 4ª, 392/2024, de 01-07-2024, rec. 778-2023	2024	FAVORABLE	Inexistencia negligencia grave, SMS+ spoofing llamada, es intrascendente que exista divergencia entre los hechos denunciados y los que componen la demanda, lo relevante es que la versión de los hechos en la demanda tiene apoyo documental.
		CUARTA	SAP CANTABRIA, Sección 4ª, 356/2024, de 31-05-2024, rec. 642-2023	2024	FAVORABLE	Inexistencia negligencia grave, la negligencia grave es la que surge por iniciativa del usuario, las transferencias no se completaron con la necesaria introducción de las claves que la entidad suministra al titular para cada operación a fin de obtener la identidad del ordenante.
		SEGUNDA	SAP CANTABRIA, Sección 2ª, 189/2024, de 13-03-2024, rec. 766-2022	2024	FAVORABLE	Inexistencia negligencia grave, la negligencia grave es la que surge por iniciativa del usuario, phishing "hace exigible aumentar las medidas de seguridad específicas", "riesgo que el propio sistema de pagos conlleva".
		SEGUNDA	SAP CANTABRIA, Sección 2ª, 609/2023, de 24-11-2023, rec. 358-2022	2023	NO ES CONTRA EL BANCO	Man in the Middle, modificación de factura por correo electrónico. Se dirigió la demanda contra la empresa que realizó el pago y se estima el recurso interpuesto por esta empresa sin costas primera instancia. Pago liberatorio realizado a tercero, jurisprudencia que analiza acerca del pago liberatorio, firma digital, "el grado de sofisticación alcanzado por esta clase de fraudes, y la enorme dificultad de la recurrente para poderse detectar la firma digital de las facturas recibidas había resultado manipulada y que, por tanto, no eran las originales, determinan que no puede exigírsele una diligencia mayor y distinta en el marco de la confianza que ha de presidir las relaciones comerciales, de forma que la diligencia desplegada es suficiente para integrar la buena fe objetiva que confiere efecto liberatorio al pago efectuado al tercero".
		SEGUNDA	SAP CANTABRIA, Sección 2ª, 497/2023, de 10-10-2023, rec. 206-2022	2023	DESFAVORABLE (con costas apelación)	Código dentro de la app de BBVA, cliente anota el código de forma refleja sin leer el mensaje, desde la propia app se decía que se estaba llevando a cabo la actualización del módulo de seguridad y podrían requerirse informaciones, pero una información no puede equipararse a una autorización, "negligencia grave que viene determinada por el hecho de no haber observado la diligencia mínima de leer el mensaje de autorización recibido, cuyo conducido y datos no eran susceptibles de inducir a error", "de nada sirve que las entidades bancarias implementen medidas de seguridad para las operaciones realizadas a través de su app o su Web, como la solicitud del código de autorización de la operación, si el usuario realiza las autorizaciones de modo automático lo cual supone ignorar la medida de seguridad", cliente comunica el fraude al banco ese mismo día, cita SAP Madrid 13 enero 2023, cita SAP Alicante 12 marzo 2018.
		SEGUNDA	SAP CANTABRIA, Sección 2ª, 500/2023, de 10-10-2023, rec. 58-2022	2023	FAVORABLE	Inexistencia de negligencia grave, propio banco asume que la clienta fue víctima de fraude en su respuesta a la reclamación de la clienta, pauta de gasto, banco incumple las medidas de seguridad en los medios de pago, cita SAP Madrid 13 enero 2023, cita SAP Alicante 12 marzo 2018.
		CUARTA	SAP CANTABRIA, Sección 4ª, 552/2023, de 02-10-2023, rec. 322-2022	2023	FAVORABLE	Inexistencia negligencia grave, la negligencia grave es la que surge por iniciativa del usuario, el concepto de la transferencia no autorizada es muy extraño, en la fecha del fraude hubo brecha de seguridad en la demandada.
CASTILLA-LA MANCHA	ALBACETE	PRIMERA	SAP ALBACETE, Sección 1ª, 454/2024, de 21-11-2024, rec. 271-2023	2024	DESFAVORABLE	Llamada "Microsoft", acceso remoto y facilita números y CVV de las tarjetas, usuario actuó con negligencia grave.
CASTILLA-LA MANCHA	CIUDAD REAL	CUARTA	SAP CIUDAD REAL, Sección 4ª, 58/2024, de 22-02-2024, rec. 210-2022	2024	FAVORABLE	Enrolamiento tarjeta. Inexistencia negligencia grave, pauta de gasto, sofisticación del fraude, dificultad a la hora de distinguir la web espejo de la auténtica.
CASTILLA-LA MANCHA	CUENCA	PRIMERA	SAP CUENCA, Sección 1ª, 125/2023, de 16-05-2023, rec. 125-2023	2023	FAVORABLE	Inexistencia negligencia grave, la falsedad de la transferencia es un riesgo a cargo del banco (SAP Alicante 12 de marzo de 2018), el banco no actúa con diligencia al no disponer de métodos anti phishing ni medios adecuados.
CASTILLA-LA MANCHA	GUADALAJARA	PRIMERA	SAP GUADALAJARA, Sección 1ª, 72-2021, de 09-03-2021, rec. 370-2019	2021	FAVORABLE	Sustracción tarjeta física. Inexistencia negligencia grave ni en teclear el número secreto ni en la custodia de su tarjeta, tercero observa PIN y sustrae tarjeta física del bolso de la cliente en un descuido y en ejecución de un plan preconcebido, el banco no procedió a identificar al ordenante de las operaciones.
CASTILLA-LA MANCHA	TOLEDO	SEGUNDA	SAP TOLEDO, Sección 2ª, 221/2020, de 30-11-2020, rec. 377-2019	2020	FAVORABLE	Incumplimiento entidad bancaria por falta de habilitación en el ordenante de las transferencias, STS 16 diciembre 2011: "La disposición de fondos depositados en una cuenta corriente o de depósito bancaria por parte de una persona que no podía hacerlo por no ser la titular ni estar autorizada por ésta supone un incumplimiento contractual".

CASTILLA Y LEÓN	ÁVILA					
CASTILLA Y LEÓN	BURGOS	TERCERA	SAP BURGOS, Sección 3ª, 321/2024, de 13-11-2023, rec. 229-2023	2024	ESTIMACIÓN PARCIAL	Condena cliente a devolver principal préstamo y banco a devolver transferencias menos la última y el importe cobrado por el principal más los intereses, sin costas en ninguna instancia. Transferencias y solicitud de préstamo personal, carga de la prueba: "la carga de la prueba de que ha existido una operación de pago no autorizada corresponde al usuario. Al proveedor de servicios de pago le corresponde la carga de la prueba de que, por su parte, se ha actuado siguiendo el protocolo de seguridad previsto para cada operación. Y es el usuario quien debe acreditar que, a pesar de ello, su identidad ha sido suplantada", pauta de gasto, se considera operación autorizada pues se da el consentimiento introduciendo usuario y contraseña y recibiendo el código alfanumérico en el teléfono móvil conforme al artículo 64.2 de la Directiva, se minora la cuantía porque el banco no debe responder de la última transferencia realizada en tanto que la cliente tardó en poner en conocimiento de la entidad el fraude y operó con su banca en el tiempo transcurrido pudiendo haber advertido las transferencias fraudulentas emitidas.
		TERCERA	SAP BURGOS, Sección 3ª, 482/2022, de 05-12-2022, rec. 340-2022	2022	FAVORABLE	Malware. Descarga malware en dispositivo tras clicar enlace empresa paquetería (Fedex). Inexistencia negligencia grave, IBERCAJA no actuó de manera diligente pues no puso a disposición del usuario medios adecuados para notificar la sustracción ni tampoco bloqueó las cuentas en el momento en que llamó el usuario.
CASTILLA Y LEÓN	LEÓN	PRIMERA	SAP LEÓN, Sección 1ª, 716/2024, de 12-11-2024, rec. 646-2024	2024	FAVORABLE	Inexistencia negligencia grave, la advertencia del contenido del SMS era irrelevante puesto que la actora actuaba bajo la creencia de que estaba comunicándose con su banco, no bastan avisos genéricos.
		PRIMERA	SAP LEÓN, Sección 1ª, 700/2024, de 06-11-2024, rec. 699-2024	2024	FAVORABLE	Inexistencia negligencia grave, falta de especiales advertencias sobre delitos o riesgos por parte del banco.
CASTILLA Y LEÓN	PALENCIA					
CASTILLA Y LEÓN	SALAMANCA	PRIMERA	SAP SALAMANCA, Sección 1ª, 311/2024, de 10-06-2024, rec. 466-2023	2024	FAVORABLE	Man in the Middle. Es la entidad bancaria quien dispone de los medios técnicos para la verificación del cliente, artículo 36 LSP, correos idénticos a los que remitía la mercantil.
		PRIMERA	SAP SALAMANCA, Sección 1ª, 193/2024, de 18-04-2024, rec. 108-2023	2024	FAVORABLE	Inexistencia negligencia grave, aquella surge por la iniciativa del propio usuario, de la prueba que obra en autos se desconoce cómo se activó la firma electrónica, la cliente siempre ordenaba las transferencias vía telefónica y luego las confirmaba por correo electrónico, cliente no usaba habitualmente la banca online.
		PRIMERA	SAP SALAMANCA, Sección 1ª, 719/2022, de 04-11-2022, rec. 390-2022	2022	NO ES CONTRA EL BANCO (es contra la mercantil)	Man in the Middle. Sin costas pues dudas de hecho.
CASTILLA Y LEÓN	SEGOVIA	PRIMERA	SAP SEGOVIA, Sección 1ª, 268/2024, de 29-10-2024, rec. 224-2024	2024	FAVORABLE	Ventana emergente dentro de la página web del banco, usuario facilitó clave SMS, no puede concluirse que el sistema del banco no fallara, falta de acreditación de la negligencia grave del usuario.
CASTILLA Y LEÓN	SORIA					
CASTILLA Y LEÓN	VALLADOLID	TERCERA	SAP VALLADOLID, Sección 3ª, 675/2024, de 28-10-2024, rec. 61-2024	2024	FAVORABLE	Inexistencia negligencia grave, muchos clientes de la entidad habían sufrido fraude en fechas similares.
		PRIMERA	SAP VALLADOLID, Sección 1ª, 581/2024, de 10-10-2024, rec. 272-2024	2024	DESFAVORABLE	Conducta imprudente del usuario al facilitar clave de acceso, el banco cumplió con sus obligaciones, el usuario facilitó la instalación de un programa en su ordenador y en su móvil mediante el cual el ciberdelincuente se hizo con sus claves y controló la operatividad total de su cuenta y de su tarjeta.
		PRIMERA	SAP VALLADOLID, Sección 1ª, 509/2024, de 02-09-2024, rec. 782-2022	2024	DESFAVORABLE	Usuario cede sus claves de acceso, advertencias del banco sobre la no cesión de claves, el correo electrónico fraudulento se recibe en la bandeja de correos no deseados, "El uso de una tarjeta en virtud de su contratación no se trata de un producto financiero complejo que escape de las posibilidades de comprensión normal de un ciudadano medio", son notorios los avisos sobre el fraude online, usuario autoriza operaciones una vez enviados los SMS de seguridad a su teléfono.
		PRIMERA	SAP VALLADOLID, Sección 1ª, 405/2023, de 23-10-2023, rec. 134-2023	2023	FAVORABLE	Inexistencia negligencia grave, SMS, deber de aumentar las medidas de protección, no bastan avisos genéricos del banco.
		PRIMERA	SAP VALLADOLID, Sección 1ª, 74/2010, de 10-03-2009, rec. 280-2009	2009	FAVORABLE/ESTIMACIÓN PARCIAL	Acciones y transferencias.
CASTILLA Y LEÓN	ZAMORA	PRIMERA	SAP ZAMORA, Sección 1ª, 235/2024, de 04-09-2024, rec. 134-2023	2024	FAVORABLE	Recurso de ING. Inexistencia negligencia grave, aquella surge por iniciativa del propio usuario, no puede considerarse como gravemente negligente no haber dado la trascendencia necesaria a que el dispositivo que se indicaba en el SMS para vincular no era el suyo, el banco no actuó de manera diligente por la pauta de gasto y por no haber realizado actuación respecto a la paralización de las transferencias hasta que la demandante puso bajo su conocimiento el fraude.
		CUARTA	SAP BARCELONA, Sección 4ª, 735/2024, de 24-10-2024, rec. 696-2023	2024	FAVORABLE	Llamada "Microsoft", descarga programa malware, avisos SMS por parte del banco, inexistencia negligencia grave, esta debe surgir por iniciativa del usuario.
		DECIMOSÉPTIMA	SAP BARCELONA, Sección 17ª, 630/2024, de 23-09-2024, rec. 205-2024	2024	FAVORABLE	El banco no prueba la negligencia grave del usuario, enumeración requisitos autenticación Reglamento, phishing fácil ser víctima.
		DECIMOSÉPTIMA	SAP BARCELONA, Sección 17ª, 597/2024, de 12-09-2024, rec. 65-2024	2024	FAVORABLE	Desestima falta legitimación pasiva CAIXABANK. Inexistencia negligencia grave, aquella surge por iniciativa usuario, responsabilidad cuasi-objetiva, el banco no consigue impedir el fraude cuando tenía obligación de custodiar el dinero (arts. 306 y 307 Código Comercio), a pesar de la trazabilidad de las operaciones no consta que operaciones tan anómalas extrañaran al banco.
		DECIMOSÉPTIMA	SAP BARCELONA, Sección 17ª, 501/2024, de 26-06-2024, rec. 987-2022	2024	FAVORABLE	Inexistencia negligencia grave, transferencias IP Varsovia, cuentas "mula", cita SAP Asturias 20 marzo 2024 entre otras.
		PRIMERA	SAP BARCELONA, Sección 1ª, 269/2023, de 07-06-2023, rec. 310-2022	2023	FAVORABLE	Malware. Inexistencia negligencia grave, aquella surge por iniciativa propio usuario.

		DECIMOSEXTA	SAP BARCELONA, Sección 16ª, 249/2022, de 23-05-2022, rec. 138-2020	2022	DESFAVORABLE	Hipótesis de la demanda inciertas, al perito demandante no se le facilitaron los SMS para recogerlos en su informe, Ley de Servicios de Pago de 2009.
CATALUÑA	BARCELONA	UNDÉCIMA	SAP BARCELONA, Sección 11ª, 292/2021, de 30-04-2021, rec. 292-2021	2021	DESFAVORABLE/ESTIMACIÓN PARCIAL DEMANDA	783.475'75 €. Privalia envía carta a BANCO SANTANDER avisando de que habían sufrido un ciberataque y que no se debían autorizar transferencias por correo electrónico pero sí aquellas por carta adjunta en la que la beneficiaria fuera otra empresa del grupo, se estima parcialmente el recurso por el F.J. sexto y es que el fraude no se produce por una suplantación de identidad sino por el engaño a la persona que ordena las transferencias.
		DECIMOSEXTA	SAP BARCELONA, Sección 16ª, 11/2019, de 22-01-2019, rec. 227-2017	2019	FAVORABLE	Analiza la legitimación pasiva desde el punto de vista de la relación contractual, negligencia en la actuación del proveedor de servicios de pago por autorizar las órdenes de pago sin efectuar las comprobaciones necesarias.
		UNDÉCIMA	SAP BARCELONA, Sección 11ª, 214/2015, de 23-07-2015, rec. 832-2013	2015	FAVORABLE	Ley de Servicios de Pago de 2009. Cliente inexperto en temas de seguridad informática cree que está colaborando con el banco para solucionar el fraude.
		DECIMOCUARTA	SAP BARCELONA, Sección 14ª, 151/2013, de 07-03-2013, rec. 150-2012	2013	FAVORABLE	Entidad demandada no adoptó las medidas de seguridad pactadas en cuanto a límites de disposición, "tampoco ha aportado prueba de la adopción de medidas concretas de seguridad para dicho tipo de fraude conocido del pushing siendo obligación de la entidad conforme la Condición General 3 del contrato que Caixa Catalunya puede establecer filtros adicionales de seguridad, no constando el mismo para el pushing".
		DECIMOSEXTA	SAP BARCELONA, Sección 16ª, 510/2011, de 15-09-2011, rec. 923-2009	2011	DESFAVORABLE/ESTIMACIÓN PARCIAL DEMANDA	Incumplimiento contractual BANCO SANTANDER, "el fraude pudo consumarse porque resultaba posible copiar con verosimilitud la página web de la entidad bancaria permitiendo que se capturaran las claves de los usuarios al responder a un correo spam, página cuya defensa y protección sólo a Banco de Santander incumbía", liente incurrió en indiscutible negligencia respecto a la custodia de sus claves.
CATALUÑA	GIRONA	PRIMERA	SAP GIRONA, Sección 1ª, 808/2024, de 24-10-2024, rec. 773-2024	2024	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa usuario, el phishing actúa como un vicio de la voluntad.
		PRIMERA	SAP GIRONA, Sección 1ª, 276/2024, de 17-04-2024, rec. 905-2023	2024	FAVORABLE	Legitimación pasiva CAIXABANK. Inexistencia negligencia grave, aquella surge por iniciativa propio usuario, IP diferente, la entidad debió advertir estas circunstancias y efectuar una "comprobación directa sobre el consentimiento para ejecutar esas operaciones".
		SEGUNDA	SAP GIRONA, Sección 2ª, 62/2024, de 31-01-2024, rec. 724-2023	2024	FAVORABLE	Malware. Inexistencia negligencia grave, aquella surge por iniciativa del propio usuario.
		SEGUNDA	SAP GIRONA, Sección 2ª, 164/2014, de 28-05-2014, rec. 164-2014	2014	FAVORABLE	Ley de Servicios de Pago de 2009. La prueba de que la operación se realizó a causa de negligencia grave del cliente corresponde a la entidad financiera.
CATALUÑA	LLEIDA	SEGUNDA	SAP LLEIDA, Sección 2ª, 575/2024, de 30-07-2024, rec. 1164-2022	2024	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa propio usuario la carga de la prueba sobre la negligencia grave del usuario recae en el banco, hipótesis malware, cita SAP Oviedo 11 de abril entre otras.
		SEGUNDA	SAP LLEIDA, Sección 2ª, 303/2024, de 19-04-2024, rec. 1305-2022	2024	FAVORABLE	Malware. Descarga malware en dispositivo tras clicar enlace empresa paquetería (Fedex). Inexistencia negligencia grave, fija hechos probados pauta de gasto e IP distinta a la habitual, STS 141/2021, de 15 marzo 2021 (Caso Uralita), seguro responsabilidad civil profesional art. 16 LSP, bancos beneficiados por la banca online mientras que clientes solo tienen un "interés difuso por el ahorro de tiempo en desplazamientos presenciales a la sucursal", "uno de los troyanos más sofisticados y peligrosos de la historia de Android", cliente introduce sus datos en la verdadera banca online pero es espiado por el ciberdelincuente.
CATALUÑA	TARRAGONA	TERCERA	SAP TARRAGONA, Sección 3ª, 278/2024, de 09-05-2024, rec. 634-2022	2024	FAVORABLE	La falta de consulta regular del histórico de movimientos no supone negligencia grave del cliente, pues no está obligado a ello.
CEUTA	CEUTA					
COMUNIDAD VALENCIANA	ALICANTE	NOVENA	SAP ALICANTE, Sección 9ª, 45/2024, de 29-01-2024, rec. 457-2023	2024	FAVORABLE	Phishing "desconocido". Banco tiene la responsabilidad de asegurar el buen funcionamiento y seguridad del sistema de banca electrónica, banco no prueba negligencia grave en el cliente, inexistencia negligencia grave, aquella surge por iniciativa del propio usuario.
		NOVENA	SAP ALICANTE, Sección 9ª, 371/2023, de 23-06-2023, rec. 172-2023	2023	FAVORABLE	En principio habría negligencia grave al facilitar credenciales y códigos de autenticación reforzada, explica los tipos de transferencia SEPA (estándar e inmediata), la inicial negligencia de las usuarias habría podido ser subsanada con una actitud diligente de la sucursal, doctrina jurisprudencial que mantiene que el criterio de la prohibición de regreso que justifica negar la imputación del resultado dañoso, tendrá lugar cuando en el proceso causal que desembocó en aquél, puesto en marcha por el posible responsable, se ha incardinado de forma sobrevenida la conducta dolosa o gravemente imprudente de un tercero.
		OCTAVA	SAP ALICANTE, Sección 8ª, 107/2018, de 12-03-2018, rec. 622-2017	2018	FAVORABLE	Carga de la prueba corresponde al proveedor de servicios de pago, inexistencia negligencia grave, responsabilidad cuasi-objetiva, banco debe proveer de un sistema seguro la banca electrónica.
COMUNIDAD VALENCIANA	CASTELLÓN	TERCERA	SAP CASTELLÓN, Sección 3ª, 196/2024, de 12-04-2024, rec. 240-2022	2024	FAVORABLE	Inexistencia de negligencia grave, supuesta llamada de operador de telefonía (Vodafone), no se acredita cliente facilitase más datos que el código recibido por SMS, al no pedirse intereses legales desde la reclamación extrajudicial se conceden desde la interposición de la demanda.
		TERCERA	SAP CASTELLÓN, Sección 3ª, 493/2013, de 19-12-2013, rec. 485-2013	2013	FAVORABLE	No acoge excepción prejudicialidad penal, inexistencia negligencia grave, responsabilidad cuasi-objetiva.
COMUNIDAD VALENCIANA	VALENCIA	SÉPTIMA	SAP VALENCIA, Sección 7ª, 434/2024, de 26-07-2024, rec. 699-2024	2024	FAVORABLE	El usuario actuó de manera diligente comunicando el fraude, el proveedor de servicios no puede invertir la carga de la prueba en base al correcto registro técnico de las operaciones, debe implementar las medidas de seguridad para evitar fraudes a través de la banca digital que potencia entre sus clientes.
		SEXTA	SAP VALENCIA, Sección 6ª, 254/2022, de 13-06-2022, rec. 254-2022	2022	FAVORABLE	Inexistencia negligencia grave, no se activó a tiempo el protocolo antifraude, clienta avanzada edad con hija como autorizada para ayudarla en la banca online.
		SEXTA	SAP VALENCIA, Sección 6ª, 343/2021, de 19-07-2021, rec. 343-2021	2021	FAVORABLE	Man in the Middle. Habría bastado una alerta sobre la discordancia en los datos facilitados en la orden de transferencia para no efectuar la transferencia, no basta solamente con comprobar el IBAN.

		NOVENA	SAP VALENCIA, Sección 9ª, 130/2013, de 23-04-2013, rec. 53-2013	2013	FAVORABLE/ESTIMACIÓN PARCIAL	La operativa por internet supone un ahorro de costes y a la vez mayor comodidad para el cliente, suplantación de la página del banco, incongruencia extra petita, costas en estimación parcial.
		SÉPTIMA	SAP VALENCIA, Sección 7ª, 631/2012, de 31-01-2013, rec. 43-2013	2012	DESFAVORABLE	Contrato cuenta corriente lo redacta el banco por lo que el usuario sigue las medidas de seguridad que el banco ha fijado y al banco le corresponde probar que las ha cumplido como ha demostrado en este caso, negligencia por haber facilitado claves.
		TERCERA	SAP BADAJOZ, Sección 3ª, 109/2024, de 12-04-2024, rec. 173-2024	2024	FAVORABLE	SMS + app espejo, inexistencia negligencia grave, el banco no dotó de las medidas anti phishing oportunas la banca online.
EXTREMADURA	BADAJOZ	SEGUNDA	SAP BADAJOZ, Sección 2ª, 204/2024, de 06-03-2024, rec. 1291-2023	2024	FAVORABLE	Inexistencia negligencia grave, inversión de la carga de la prueba, es difícil detectar el fraude para los consumidores y más para los que sufren la brecha digital, no se puede poner en el mismo plano a los consumidores y a los bancos, las entidades bancarias tienen la condición de depositarias y de generadoras del riesgo, abandono cada vez mayor de la presencialidad, "hacen falta comunicaciones seguras, más formación a los clientes, más inversión en seguridad para evitar la clonación de las páginas y, si es necesario, bloquear las cuentas para la mejor protección de los clientes. No podemos olvidar que el depositante tiene derecho a la indemnidad de sus ahorros", en general nadie tiene culpa del engaño salvo que sea patente o burdo.
		TERCERA	SAP BADAJOZ, Sección 3ª, 159/2022, de 16-06-2022, rec. 233-2022	2022	FAVORABLE	Enrolamiento tarjeta en "Apple Pay". Inexistencia negligencia grave, el banco cumple con su obligación de acreditar "que la operación de pago fue autenticada, sido registrada con exactitud y contabilizada y que no se vio afectada por un fallo técnico", el banco no dotó de la tecnología anti phishing necesaria, no cabe observar negligencia grave por utilizar el instrumento de pago y dirigirse a un enlace simulado.
		PRIMERA	SAP CÁCERES, Sección 1ª, 588/2024, de 15-10-2024, rec. 292-2024	2024	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa del usuario, el banco ha de adoptar las medidas de seguridad necesarias al ofrecer el sistema de banca online, es necesario ser un experto en la materia para detectar que el SMS se trata de una estafa, el banco asume en su contestación que el usuario fue víctima de un phishing.
		PRIMERA	SAP CÁCERES, Sección 1ª, 378/2024, de 03-09-2024, rec. 461-2023	2024	FAVORABLE	Inexistencia negligencia grave, habría que ser un experto en la materia para reconocer que el SMS se trata de un fraude, el banco admite en su contestación que el cliente fue víctima de un phishing, reconociendo así que no había implementado todas las medidas o mecanismos necesarios para proteger a su cliente.
		PRIMERA	SAP CÁCERES, Sección 1ª, 351/2024, de 25-07-2024, rec. 168-2023	2024	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa del usuario, los bancos deben tener sus propios sistemas de alarma para detectar fraudes.
		PRIMERA	SAP CÁCERES, Sección 1ª, 267/2024, de 01-07-2024, rec. 46-2024	2024	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa del usuario, responsabilidad cuasi-objetiva.
		PRIMERA	SAP CÁCERES, Sección 1ª, 182/2024, de 03-05-2024, rec. 3-2024	2024	FAVORABLE	Demandante una empresa y la trabajadora de la empresa reintegra el dinero, esto son relaciones laborales entre empresa y trabajador que no tienen que ver con el perjuicio sufrido, la entidad financiera corresponde acreditar la falta de diligencia del usuario.
		PRIMERA	SAP CÁCERES, Sección 1ª, 64/2024, de 20-02-2024, rec. 835-2023	2024	FAVORABLE	Inexistencia negligencia grave, cliente recibe llamada telefónica de alguien que se identifica como trabajador del banco quien le avisa de que le va a enviar unos códigos a su teléfono, el banco no había implementado los mecanismos anti phishing necesarios.
EXTREMADURA	CÁCERES	PRIMERA	SAP CÁCERES, Sección 1ª, 570/2023, de 22-12-2023, rec. 570-2023	2023	FAVORABLE	Inexistencia negligencia grave, carga de la prueba al banco le corresponde acreditar la negligencia grave del usuario.
		PRIMERA	SAP CÁCERES, Sección 1ª, 555/2023, de 18-12-2023, rec. 714-2023	2023	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa del usuario, responsabilidad cuasi-objetiva, spoofing llamada, la responsabilidad del banco no queda exenta con avisos genéricos en su página web.
		PRIMERA	SAP CÁCERES, Sección 1ª, 531/2023, de 28-11-2023, rec. 563-2023	2023	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa del usuario.
		PRIMERA	SAP CÁCERES, Sección 1ª, 132/2022, de 16-02-2022, rec. 1371-2021	2022	FAVORABLE	Inexistencia negligencia grave, el demandante observó toda la diligencia exigible cuando comprobó que las operaciones eran fraudulentas "como son, fundamentalmente, las siguientes actuaciones: la denuncia de los hechos ante la Guardia Civil y la comunicación de las disposiciones de efectivo a la entidad bancaria", inversión carga de la prueba, lo único que puede exigirse al usuario es que el dispositivo tenga un mantenimiento de seguridad, condición de consumidor y protección reforzada, "cláusula de imputación de responsabilidad que ha sido calificada como abusiva por el Tribunal Supremo en su Sentencia núm.792/2009 de 16 de diciembre, al entender que "La exclusión de responsabilidad en todo caso para la entidad bancaria por las utilizaciones de tarjeta o de libreta -consistentes en extracciones en efectivo u otras operaciones con cargo a la cuenta bancaria-, con anterioridad a la comunicación de la sustracción o extravío (o evento similar) es desproporcionada, y abusiva.", a la entidad bancaria le corresponde asumir los riesgos de las operaciones con tarjeta porque se lleva los beneficios (comisiones de uso, mantenimiento, …).
		SEXTA	SAP A CORUÑA, Sección 6ª, 286/2024, de 10-10-2024, rec. 441-2023	2024	FAVORABLE	Inexistencia negligencia grave, SMS + llamada a nombre de la entidad bancaria, la cual ha incumplido sus obligaciones al permitir la realización de las operaciones fraudulentas.
		CUARTA	SAP A CORUÑA, Sección 4ª, 303/2024, de 22-05-2024, rec. 37-2023	2024	FAVORABLE	SMS + llamada ABANCA + vinculación banca online en un nuevo dispositivo. Inexistencia negligencia grave, el relato fáctico de la demanda es inexacto e incompleto, toma en cuenta el relato de la demanda y de la reclamación al banco, la actitud del cliente es negligente pues facilitó el código para que se vinculase la banca online en un nuevo dispositivo, aunque casos similares han tenido valoraciones diversas (SAP A Coruña Sección 3ª no es una negligencia, son tres) en este caso el elemento diferencial es la llamada recibida desde el número oficial de ABANCA, "y así las cosas la valoración que merece la conducta del usuario, sin duda negligente, no alcanza el grado de gravedad exigible cuando, bajo engaño, facilita sus datos y los códigos de confirmación a la persona que le llama desde un número de teléfono de ABANCA y que simula ser un empleado de la entidad que está tratando de arreglar un problema relativo a su cuenta", una concurrencia de culpas supondría asignar al usuario responsabilidad parcial aún sin negligencia grave, incumpliendo la legalidad.

GALICIA	A CORUÑA	TERCERA	SAP A CORUÑA, Sección 3ª, 191/2024, de 19-04-2024, rec. 149-2024	2024	FAVORABLE/ESTIMACIÓN PARCIAL (cada parte abonará costas causadas a su instancia y las comunes por mitad primera instancia)	Concurrencia de culpas (60% clienta – 40 % entidad bancaria) al ser negligentemente grave la conducta del usuario y haber incumplido el proveedor su obligación de autenticación reforzada, conducta clienta poco diligente, al banco le corresponde acreditar su propia actitud diligente, testigo-perito banco, "aunque la entidad bancaria hubiera remitido un primer código OTP de implantación de la banca online, que la usuaria al introducirlo, conllevó que la banca electrónica se implantará en otro terminal, resulta que los defraudadores podían realizar operaciones de transferencias de dinero sin necesidad de introducir ningún otro código OTP, esto conlleva, a que se estaría incumpliendo por la entidad bancaria las medidas de seguridad de un procedimiento de autenticación reforzada, lo que conllevaría a una plena disponibilidad de los fondos sin mayores medidas de seguridad para intentar dificultar la disponibilidad por los defraudadores", no consta que el banco haya generado el código OTP para la realización de la transferencia fraudulenta efectuada.
		TERCERA	SAP A CORUÑA, Sección 3ª, 364/2023, de 05-10-2023, rec. 87-2023	2023	FAVORABLE	Inexistencia negligencia grave, el certificado REDSYS no verifica la identidad del usuario ordenante de la operación, negligencia grave surge por iniciativa del usuario, en este caso la cliente actuó de manera diligente comunicando al banco el fraude y denunciando los hechos el mismo día.
		TERCERA	SAP A CORUÑA, Sección 3ª, 17/2023, de 25-01-2023, rec. 757-2022	2023	DESFAVORABLE	Negligencia grave, "no es una negligencia, son tres. Y si la primera aún pudiera ser más o menos comprensible (pinchar en un enlace), la segunda ya es grave (facilitar usuario y contraseña), y la tercera es totalmente temeraria (informar de la confirmación)", SMS + llamada procedente de ABANCA donde su interlocutor se identifica como ABANCA y el cliente le facilita códigos, transferencia inmediata, es incuestionable que el usuario fue víctima de un engaño, nadie puede alegar su propia torpeza, medidas de protección especiales solo pueden aplicarse a traspasos de un determinado importe pero no para cuantías pequeñas porque supondría paralizar el sistema.
		TERCERA	SAP A CORUÑA, Sección 3ª, 398/2022, de 19-10-2022, rec. 443-2022	2022	DESFAVORABLE	Llamada telefónica ajena al banco y facilita datos de la tarjeta junto a su número móvil y se descargó una aplicación que daba acceso a su teléfono siguiendo instrucciones de su interlocutor. Negligencia grave, la entidad bancaria no puede negar los cargos o incumpliría el contrato con el suministrador.
GALICIA	LUGO	PRIMERA	SAP LUGO, Sección 1ª, 307/2024, de 10-09-2024, rec. 1043-2022	2024	FAVORABLE (sin costas apelación)	Inexistencia negligencia grave, aquella surge por iniciativa usuario, responsabilidad cuasi-objetiva, oficio a compañía telefónica (Telefónica) y no consta alta de MULTISIM ni duplicado de ICC, SAP Baleares de 17-02-2023 y SAP Navarra de 27-05-2024.
		PRIMERA	SAP LUGO, Sección 1ª, 232/2024, de 25-06-2024, rec. 964-2022	2024	FAVORABLE	Venta online de un producto (Wallapop, etc.). Inexistencia negligencia grave, artículo 68 LSP autenticación reforzada, visto el año en que se produjo la operación, no fue suficiente por parte del cliente llamar al teléfono del banco, en ninguno de los SMS enviado se avisaba sobre el peligro de la operación que estaba realizando el particular al vincular un dispositivo, incumpliéndose así el requisito de "código de refuerzo" de la autenticación del artículo 68 LSP.
GALICIA	OURENSE	PRIMERA	SAP OURENSE, Sección 1ª, 393/2024, de 27-05-2024, rec. 295-2022	2024	FAVORABLE	SMS + enlace + llamada desde número oficial. Inexistencia negligencia grave, clienta cumplió con su obligación del artículo 41 LSP al comunicarse de inmediato con el banco, la entidad bancaria incumple el artículo 42 LSP pues una vez contactada por la clienta debió impedir el uso fraudulento de la tarjeta, son los bancos quienes fomentan la utilización de la banca online por lo que sería injusto "hacer pechar al usuario con las nocivas consecuencias derivadas de los riesgos de utilización de un servicio facilitado por la entidad, en buena medida, en su propio beneficio", el SMS fue recibido en el canal habitual.
		PRIMERA	SAP OURENSE, Sección 1ª, 369/2023, de 09-06-2023, rec. 1047-2022	2023	FAVORABLE	Préstamo concedido junto a más operaciones no autorizadas, conversación por WhatsApp con el ciberdelincuente, venta online de un producto (Milanuncios). Inexistencia negligencia grave, es el banco quien dispone de los medios técnicos para identificar al ordenante y mejorar el sistema de banca electrónica por lo que no se puede pretender cargar con los fallos del sistema al usuario normalmente consumidor, la carga de la prueba corresponde al proveedor de servicios, la práctica precomercial de concesión de concesión de préstamos aumentó el riesgo, STJUE de 17 de mayo de 2022 modera la aplicación de la normativa procesal de un Estado miembro cuando se oponga a la efectividad del Derecho de la Unión.
		PRIMERA	SAP OURENSE, Sección 1ª, 311/2023, de 12-05-2023, rec. 737-2022	2023	FAVORABLE	Inexistencia negligencia grave, el banco tiene la carga de la prueba, el banco no comprobó la identidad del ordenante de las operaciones.
		SEXTA	SAP PONTEVEDRA, Sección 6ª, 650/2024, de 17-10-2024, rec. 673-2024	2024	FAVORABLE	Inexistencia negligencia grave, usuario actúo con diligencia comunicando el fraude al banco, sistemas de prevención de fraude son de bajo nivel ya que no se detectaron las operaciones fraudulentas.
		SEXTA	SAP PONTEVEDRA, Sección 6ª, 302/2024, de 20-05-2024, rec. 166-2022	2024	FAVORABLE	Banco no prueba negligencia grave cliente, informe pericial BBVA no ha sido ratificado ni se toma en consideración por no concordar sus datos con los que manifiesta el testigo (responsable de gestión de tarjetas de BBVA), no es posible tratar la demora en la comunicación al banco del fraude por no haberse mencionado en la primera instancia.
		SEXTA	SAP PONTEVEDRA, Sección 6ª, 244/2024, de 02-05-2024, rec. 985-2023	2024	FAVORABLE	Inexistencia negligencia grave, es el banco sobre quien recae la carga de la prueba y no puede alegarse que haya de ser la cliente (actora) quien pruebe cómo un tercero pudo haberse hecho con sus claves, exigir a la actora que pruebe que NO recibió un SMS supondría incurrir en prueba diabólica, para imputar negligencia grava al usuario no es suficiente con efectuar una presunción, banco no prueba el método por el que se enviaron los códigos de verificación de las operaciones ni si estos códigos llegaron únicamente al cliente, no se acredita de ningún modo que las operaciones fueran autorizadas por el cliente.

		SEXTA	SAP PONTEVEDRA, Sección 6ª, 50/2024, de 05-02-2024, rec. 762-2023	2024	DESFAVORABLE	SMS + Llamada oficial ABANCA. Negligencia grave, el actor facilitó todos los códigos a su interlocutor, el SMS enviado por ABANCA avisando de la vinculación en un nuevo dispositivo le alertaba de cuál era ese nuevo dispositivo dándole la opción de bloquear si no había sido él, considerando 72 Directiva se deben considerar nulas las cláusulas contractuales que aumenten la carga de la prueba sobre el consumidor y se reduzca esta sobre el emisor de los instrumentos de pago, el engaño y la apariencia de que era ABANCA quien estaba llamando al usuario pueden justificar la vinculación de la banca online en un nuevo dispositivo pero no es esta vinculación la que causa un perjuicio económico al usuario, hubo un fallo en los sistemas de comunicación de ABANCA pero el banco informó al cliente de cada actuación mediante la autenticación reforzada, se desestima el recurso por la negligencia grave al facilitar códigos para la compra.
GALICIA	PONTEVEDRA	SEXTA	SAP PONTEVEDRA, Sección 6ª, 426/2023, de 19-09-2023, rec. 545-2022	2023	FAVORABLE	Malware. Inexistencia negligencia grave, virus informático en el software del ordenador, "de ahí que tampoco podamos aceptar que el acceso a la Web de Banco Santander que figura en el listado de resultados de Google signifique una actuación negligente o incorrecta, pues si la entidad considera que esa forma de acceso no es segura, es ella la que tiene el deber de adoptar las medidas correspondientes, bien, como indica el apelado, poniendo los medios para que su página de acceso no sea localizable de esa forma o estableciendo medios de garantía más seguros", cantidad operación superior al límite y no fue controlada por el banco.
		TERCERA	SAP PONTEVEDRA, Sección 3ª, 177/2023, de 23-03-2023, rec. 634-2022	2023	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa del usuario, diligencias previas no hacen posible estimar argumento prejudicialidad penal, complejo y bien disfrazado comportamiento fraudulento, se reconoce daño moral.
		TERCERA	SAP PONTEVEDRA, Sección 3ª, 623/2022, de 01-12-2022, rec. 375-2022	2022	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa del usuario.
		SEXTA	SAP PONTEVEDRA, Sección 6ª, 539/2021, de 21-12-2021, rec. 346-2021	2021	FAVORABLE	Enrolamiento tarjeta en "Samsung Pay". Correo electrónico empresa de paquetería "Correos". Inexistencia negligencia grave, la negligencia para que el cliente responda ha de ser grave, cliente introduce códigos en web espejo, han de tenerse en cuenta las circunstancias que llevan a la toma de decisiones por los clientes, quienes actúan por el engaño premeditado de un tercero para ganarse su confianza, el banco no podía desconocer que se había solicitado la activación del servicio en un dispositivo distinto a los que aparecían registrados por la clienta, banco no ha implementado los mecanismos anti phishing para proteger a sus clientes ni puso en conocimiento del usuario que se trataba de vincular el servicio en un dispositivo distinto al suyo, la clienta únicamente se percata del fraude tras haber examinado los movimientos de su cuenta bancaria.
		SEXTA	SAP PONTEVEDRA, Sección 6ª, 113/2021, de 07-04-2021, rec. 587-2020	2021	FAVORABLE	Inexistencia negligencia grave, aunque no haya agotado la diligencia debida, los SMS enviados por el banco revelan que este conocía la vinculación a la banca online producida y no realizó ninguna investigación al respecto en los tres días que pasaron entre esta vinculación y el cargo efectuado, si el banco quien cuenta con los medios para detectar el fraude no lo detecta no se puede pretender que sea la conducta del cliente la negligentemente grave, y la transferencia excede del límite máximo autorizado.
		PRIMERA	SAP LA RIOJA, Sección 1ª, 253/2024, de 30-05-2024, rec. 217-2023	2024	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa usuario, la carga de la prueba corresponde al banco, no hubo tardanza injustificada en comunicar al banco el fraude.
		PRIMERA	SAP LA RIOJA, Sección 1ª, 223/2024, de 10-05-2024, rec. 150-2023	2024	NO ES CONTRA EL BANCO, SE DIRIGE CONTRA LA MERCANTIL (sin costas de apelación)	Man in the Middle. La cuestión está en determinar si el pago realizado es liberatorio de la deuda, no se practicó ninguna pericial, el hecho de que un equipo tenga activados sistemas básicos a nivel usuario no impide ser víctima de un ciberataque más sofisticado, diligencia exigible exige un plus superior respecto de la exigible al padre de familia, no consta ningún documento que acredite el intento de cancelar la transferencia, el artículo 1164 CC exige a quien lo invoca probar que ha actuado con la diligencia debida en sentido objetivo, en este caso no consta que la demandada (una mercantil acostumbrada a operar en el tráfico jurídico y transacciones electrónicas) haya probado la debida protección de su cuenta de correo electrónico ni que haya sido el sistema electrónico de la actora el que haya sufrido el ciberataque.
LA RIOJA	LA RIOJA	PRIMERA	SAP LA RIOJA, Sección 1ª, 185/2024, de 18-04-2024, rec. 149-2023	2024	FAVORABLE	SIM Swapping. Inexistencia negligencia grave, demanda comunidad de propietarios, el riesgo lo asume el proveedor del servicio, no cabe indicar el incumplimiento por el cliente de lo fijado en las condiciones generales por el prestador del servicio y menos cuando ello conlleve una alteración del régimen legal de responsabilidades, "sistema de seguridad para verificar y autentificar la identidad del emisor y el receptor en las transmisiones efectuadas, con un sistema de seguridad que indica el banco reforzado consistente en envió de un código sms al teléfono móvil del cliente, sin considerar el rango de seguridad de dicho dispositivo, fue deficiente, lo que dio lugar a la realización por terceras personas de transferencias no autorizadas por el cliente, sin que conste un actuar doloso ni gravemente negligente del cliente".
		PRIMERA	SAP LA RIOJA, Sección 1ª, 49/2023, de 17-02-2023, rec. 11-2023	2023	FAVORABLE	Inexistencia negligencia grave, no se duda que la clienta respondiese al SMS, pero no se ha probado cómo lo hizo, art. 36 en relación con art. 44 LSP, banco devuelve los cargos en un primer momento bajo la creencia de que se trata de un posible fraude, la banca es quien principalmente se ha beneficiado de las nuevas tecnologías y debe asumir el riesgo, los bancos publicitan la banca online mediante la creación de sus propias "apps" y las publicitan insistentemente entre sus clientes, no bastan los avisos predispuestos y vacíos de contenido por parte del banco, el aumento de límite de disposición no hizo activarse ninguna alarma.
		DÉCIMA	SAP MADRID, Sección 10ª, 462/2024, de 07-11-2024, rec. 368-2024	2024	FAVORABLE	Inexistencia grave, responsabilidad cuasi-objetiva, SIM Swapping según Guardia Civil.

DÉCIMA	SAP MADRID, Sección 10ª, 349/2024, de 18-07-2024, rec. 158-2024	2024	FAVORABLE	Llamada y el cliente facilita códigos que le llegaban por SMS. Inexistencia negligencia grave, responsabilidad cuasi-objetiva, la carga de la prueba corresponde al proveedor de servicios de pago, fraude del que es fácil ser víctima dado lo bien articulado que está en su ejecución, actuación negligente de la entidad bancaria, el informe REDSYS dispone "Dispositivo o entidad que autentifica al cliente no identificado", banco no cumplió con la doble autenticación y el no devolver de inmediato los fondos supone un nuevo incumplimiento.
VIGÉSIMOQUINTA	SAP MADRID, Sección 25ª, 133/2024, de 15-03-2024, rec. 42-2023	2024	FAVORABLE	Inexistencia negligencia grave, desestimación de la excepción procesal de falta de legitimación pasiva CAIXABANK y pluspetición en primera instancia, desestimación falta legitimación pasiva CAIXABANK porque esta indujo a error a la cliente y la excepción planteada debe considerarse contraria a la buena fe, prueba pericial es de apreciación libre y no tasada susceptible de ser valorada por el tribunal según su prudente arbitrio (reglas de la sana crítica único criterio legal), no se ha identificado al ordenante de la operación por lo que no se cumplen las características del PS2D de comercio electrónico seguro (no se ha utilizado la tarjeta de manera física, no se ha identificado el móvil del cliente, SMS enviado al número que no es el del cliente).
DÉCIMA	SAP MADRID, Sección 10ª, 24/2023, de 13-01-2023, rec. 918-2022	2024	FAVORABLE	Inexistencia negligencia grave, clienta trató de acceder a banca online pero no se le remitió el código a su teléfono para acceder, SMS web espejo facilita credenciales y códigos, se elevó el límite máximo pactado de disposición cita SAP Alicante 2018, responsabilidad cuasi-objetiva, carga de la prueba corresponde al banco, no bastan los avisos genéricos advirtiendo del comportamiento de seguridad que deba tener el cliente en la banca electrónica.
VIGÉSIMA	SAP MADRID, Sección 20ª, 249/2022, de 01-07-2022, rec. 75-2022	2022	DESFAVORABLE	La devolución parcial por CAIXABANK fue consecuencia de la cooperación entre entidades y del dinero que constaba en la cuenta de destino, la sustracción de la mochila del usuario un año antes no tiene relación causal con el fraude sufrido pues no se especifica en la denuncia a qué información bancaria tuvo acceso quien la robó, usuario acude al banco tras el robo y le cambian las claves de acceso y nueva tarjeta coordenadas, el fraude tuvo que haberse cometido empleando las nuevas credenciales de acceso y tarjeta de coordenadas, no pudiendo establecer el nexo causal el fraude únicamente pudo haberse producido por el descuido o ausencia de adopción de las medidas exigibles al usuario a fin de proteger sus claves, no se puede tratar de atribuir responsabilidad en base a las conclusiones del Banco de España que manifiestan que la actitud de la entidad fue contraria a las buenas prácticas y usos financieros por no haber aportado el banco el consentimiento del usuario para la operación, pero "la forma de prestar el cliente el consentimiento es facilitando los datos y claves de acceso personal que sólo conoce el cliente, o quien las tenga por habérselas facilitado voluntariamente éste o las haya obtenido por descuido o falta de diligencia o bien por sustracción o engaño, y en el caso presente, las claves se suministraron correctamente, luego existía el "consentimiento preciso" para materializarlas y no consta acreditado que el mismo se prestara viciadamente".
VIGÉSIMA	SAP MADRID, Sección 20ª, 184/2022, de 20-05-2022, rec. 945-2021	2022	FAVORABLE	SMS + enlace a web espejo sin haber recibido SMS alertando de la primera operación. Inexistencia negligencia grave, un error gramatical ("lo" cuando debería decir "le") no puede hacer pesar sobre el usuario el hecho de que debía haber detectado el fraude, es preciso ser un experto en la materia para detectarlo, dicho comportamiento no puede considerarse diligente pero para que el usuario soporte las consecuencias -aun parcialmente- es preciso apreciar una negligencia grave, la responsabilidad del banco es la de adoptar medidas de seguridad y dotarse de mecanismos de supervisión que permitan detectar operaciones fraudulentas, la entidad bancaria ha de adoptar medidas anti phishing que le permitan detectar las páginas clonadas de las propias web oficiales sin que sea suficiente realizar avisos genéricos en su página web, para quedar exonerado el proveedor de servicios de su responsabilidad no basta con que el usuario no tuviese activado el sistema de alarma en su tarjeta puesto que ha de ser el proveedor quien debe adoptar una actitud activa para su implantación no solo poniéndolo a disposición del cliente, el banco debía saber que se había vinculado la tarjeta en un dispositivo distinto al habitual del usuario, no se ha acreditado que la demandada cumpliese con los deberes de diligencia en la autenticación ni de implementación de mecanismos anti phishing de protección de los usuarios.

MADRID	MADRID	UNDÉCIMA	SAP MADRID, Sección 11ª, 74/2022, de 28-02-2022, rec. 35-2021	2022	FAVORABLE	Man in the Middle. Las transferencias se realizan siguiendo un protocolo no habitual en la mercantil ordenante, BBVA puso sobre aviso de que esas transferencias se trataban de realizar por alguien que no estaba apoderada ni autorizada y aun así cedió a las pretensiones de esta persona y autorizó las transferencias, pauta de gasto: las transferencias se dirigen a Hong Kong -paraíso fiscal- adonde la empresa nunca había efectuado transferencias, en primera instancia se desestima la demanda aplicando la regla de prohibición de regreso según la cual no cabe imputar el daño a quien puso en marcha el curso causal que inició o condujo al resultado dañoso y tampoco el incumplimiento de la ley de blanqueo de capitales por resultar de aplicación la doctrina del factor notorio (factor notorio = alguien que, aunque carece de ese poder registrado, está claramente relacionado con la empresa de manera ampliamente conocida), en el contrato entre mercantil y banco consta acreditado que el apoderado era la mercantil y no la persona física ordenante de las transferencias, la responsabilidad es cuasi-objetiva, cita SAP Alicante 2018 y SAP Zaragoza 2013, mala praxis de BBVA al ejecutar la transferencia porque quien se comunicaba con la entidad no era apoderada, no se autorizó la segunda transferencia porque el secretismo con el que se efectuaba la misma hizo sospechar al banco pero la primera transferencia tiene el mismo correo y sí se autorizó, incumplimiento contractual del banco, no sirven los avisos genéricos del banco consistentes en avisar a la mercantil sobre este tipo de fraudes porque después es el propio banco quien no respeta los parámetros marcados por el contrato permitiendo que se realice el fraude, la firma de la presidenta que figuraba en el documento unido al correo enviado al banco era un corta pega (ratificado informe pericial informático) y el banco no cotejó la misma ni examinó la falsedad por falta de diligencia en su actuación, el procedimiento de emisión de transferencia no tenía nada que ver con el habitual (la emisión de transferencias mediante correo electrónico era excepcional y en este caso no se puso en copia a nadie), BBVA no cumplió el protocolo pactado con la mercantil para la emisión de las transferencias pues únicamente se dirigió al correo y teléfono personales de la empleada, analizar la causa que ocasionó la estafa es cuestión penal y en este caso lo que hay que analizar es la posibilidad o no de aceptar una transferencia bancaria por persona no autorizada y el cumplimiento de la entidad bancaria del protocolo para su emisión, la entidad bancaria actuó sin tomar las medidas de diligencia necesarias.
		DECIMOCUARTA	SAP MADRID, Sección 14ª, 386/2017, de 21-12-2017, rec. 498-2017	2017	DESFAVORABLE	Man in the Middle. BANCO SANTANDER recibió un correo electrónico desde el correo de la mercantil ordenando una transferencia, el banco solicitó confirmación por escrito junto con firma y le fue enviada, y solicitó también la confirmación telefónica siendo de nuevo confirmada. Discusión de consumidor o empresario, el empresario que habitualmente ordena transferencias desde su cuenta personal o de empresa para fines empresariales no es consumidor. La carga de la prueba es del banco pero el banco ha probado que cumplió con sus obligaciones, el comportamiento del banco fue "exquisito y enormemente diligente", el banco debe responder de sus sistemas de seguridad pero no puede responder de los fallos de seguridad ni de la vulnerabilidad de los sistemas informáticos de sus clientes ni tiene obligación de investigar si han sido usurpados por terceros (hackeado o crackeado), la diligencia que debe emplear el banco no es la de un buen padre de familia sino la de un honorable banquero caracterizado por el respeto absoluto por el dinero ajeno, no parece que pueda exigírsele al banco que se comporte como un grafólogo para examinar la firma y menos aún cuando realizar transferencias es habitual en el emisor, no es creíble el defecto de información por parte del banco quien diligentemente pide la confirmación dos veces, además el banco realizó gestiones de recuperación ante el banco destinatario de la transferencia (sin éxito), sobre la testifical lo recogido en la denuncia suele ser más veraz por estar aún en shock por lo ocurrido y en este caso en la denuncia se dice que la firma se debió escanear de algún otro documento y en reclamaciones posteriores así como en la demanda y el recurso se niega la firma.
		NOVENA	SAP MADRID, Sección 9ª, 178/2015, de 04-05-2015, rec. 661-2013	2015	FAVORABLE	El banco no ha acreditado la negligencia grave del usuario, tampoco el banco ha acreditado fehacientemente la cesión de claves a un tercero pese a contar con los sistemas de seguridad elevados que dice tener, en aquel momento temporal CAJAMAR sufrió numerosos casos de phishing, los sistemas de seguridad no eran tan eficaces como alega el banco, el banco no actuó de manera diligente pues no detectó el fraude sufrido a pesar de que los ciberdelincuentes emplearon el modus operandi habitual para llevar a cabo el fraude informático y, además se había superado el límite diario para las transferencias.
		VIGÉSIMOPRIMERA	SAP MADRID, Sección 21ª, 302/2012, de 29-11-2012, rec. 279-2012	2012	NO ES PHISHING. FAVORABLE	Recurre operador telefonía ("TELEFÓNICA") contra mercantil. El operador bloqueó el acceso a la página web de la mercantil por la denuncia de un usuario por phishing. Se desestima la falta de legitimación pasiva por parte de TELEFÓNICA porque se genera confusión cuando se acude a la utilización de diversos entes societarios con práctica entidad nominal y se pretende que para reclamar distintos servicios se deba acudir a otra sociedad a pesar de que se compartan nombres, direcciones y páginas web y todo ello cuando se responde a las reclamaciones desde la matriz, SAP Cáceres Sección 1ª, 13 de julio de 2001, se desestima el recurso por los perjuicios causados por el bloqueo además de que la operadora no tenía autorización administrativa ni judicial para bloquear la página web de la mercantil.
MELILLA	MELILLA					
MURCIA	MURCIA	PRIMERA	SAP MURCIA, Sección 1ª, 414/2022, de 19-12-2022, rec. 852-2022	2022	FAVORABLE	Inexistencia negligencia grave, la debe probar el banco, responsabilidad cuasi-objetiva, el riesgo operacional lo debe asumir el banco "por su posición de garante al ser una pieza clave para evitar la comisión de fraudes", el banco no ha probado la remisión de los mensajes al usuario para autorizar las compras, tampoco ha probado el incumplimiento de los deberes del usuario del artículo 41 LSP sobre el resguardo de las credenciales de seguridad, el usuario comunica al banco de inmediato, el banco no ha probado haber cumplido con el artículo 68 autenticación, gsi se retrocede una operativa de las tres que tuvieron lugar por idéntico modo no tiene sentido discutir que las otras dos operativas fueron autorizadas por el usuario.

		PRIMERA	SAP MURCIA, Sección 1ª, 398/2012, de 30-07-2013, rec. 252-2012	2012	FAVORABLE	El banco no cambió el sistema de autenticación a pesar de conocer que se venían produciendo ataques a sus usuarios, no se puede imputar imprudencia en la actitud del usuario por haber respondido a través del canal por el que el banco se comunicaba con ella un mensaje aparentemente del banco y haber facilitado sus claves, más aún cuando al día siguiente acude a la oficina y le dicen solamente que denuncie.
		TERCERA	SAP NAVARRA, Sección 3ª, 796-2024, de 21-06-2024, rec. 525-2022	2024	FAVORABLE	Inexistencia negligencia grave, se bloquea la aplicación de CAJA RURAL y el usuario lo comunica al banco, no es falta de diligencia no haber revisado su ordenador por el usuario ni tampoco no haberse percatado de la transferencia efectuada hasta dos días después pues el servicio de banca se había bloqueado en otras ocasiones sin que se produjese ninguna operación no autorizada, el informe pericial aportado por el banco no es suficiente para acreditar la negligencia grave ni tampoco que un tercero hubiese utilizado malware para emitir operaciones como si las estuviera realizando desde la IP del usuario.
NAVARRA	NAVARRA	TERCERA	SAP NAVARRA, Sección 3ª, 702/2024, de 27-05-2024, rec. 1473-2023	2024	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa propio usuario, grave sería la negligencia de quien toma la iniciativa para desproteger sus credenciales, no consta acreditado por el banco que se enviase el mensaje "push" para autorizar la operación al número del usuario, el informe REDSYS no sirve para corroborar la identidad del usuario ordenante de la operación.
		TERCERA	SAP NAVARRA, Sección 3ª, 223/2023, de 09-03-2023, rec. 1465-2022	2023	FAVORABLE	Inexistencia negligencia grave, aquella surge por iniciativa propio usuario, el riesgo de identificación errónea del ordenante recae sobre el proveedor de servicios de pago, porque el deudor solo se libera pagando al verdadero acreedor por lo que si el banco cumple una orden falsa habrá de reintegrar las cantidades salvo que haya sido el usuario quien haya creado o aumentado injustificadamente el riesgo, artículo 36 LSP, REDSYS no basta para acreditar que la operación fue real y se ejecutó con doble autenticación del cliente (no identifica el número de teléfono al que se envió el SMS), la operación no se encuentra autenticada porque falta la "certificación de la identidad del usuario ordenante de la operación", el usuario facilitó claves bajo la creencia en todo momento de que no era un tercero a quien se las estaba facilitando, corresponde al proveedor de servicios adoptar las medidas necesarias para garantizar la plena autenticación de la operación.
PAÍS VASCO	ÁLAVA					
PAÍS VASCO	GUIPÚZCOA					
		TERCERA	SAP VIZCAYA, Sección 3ª, 27/2024, de 24-01-2024, rec. 447-2022	2024	FAVORABLE	Control remoto de su ordenador supuesto servicio técnico "MICROSOFT". Suscripción de un seguro, de un crédito y dos transferencias bancarias. Los bancos conocen la existencia de los fraudes y por ello la responsabilidad del sistema de banca online se les viene imponiendo legislativamente en protección de los clientes, el uso de sistemas de autenticación reforzada no supone de manera automática considerar que las operaciones son autorizadas, inexistencia negligencia grave, hay un exceso de confianza del usuario pero no tiene la gravedad suficiente para que el banco eluda su responsabilidad, a través del control remoto del ordenador no se podía acceder a sus claves pues no estaban tales datos en el ordenador, no es el usuario quien introduce las claves en el teléfono móvil para autorizar cada operación ni es consciente de estas, por tanto no cede de forma voluntaria a un tercero sus credenciales de entrada a la banca online ni OTP para autenticar operaciones.
PAÍS VASCO	VIZCAYA	TERCERA	SAP VIZCAYA, Sección 3ª, 429/2016, de 10-11-2016, rec. 386-2016	2016	FAVORABLE	Inexistencia negligencia grave, el banco no acredita negligencia grave usuario ni tampoco que sus sistemas sean seguros, el phishing es una modalidad muy extendida y el banco debe contar con sistemas seguros, el sistema de seguridad quiebra, se superó el límite pactado, el dinero en las cuentas de destino fue dispuesto muy rápidamente para evitar el retroceso, el sistema de banca electrónico se publicita siendo seguro por contar con sistemas para detectar el fraude cuando no es así.