ADMINISTRACION DE JUSTICIA

JUZGADO DE PRIMERA INSTANCIA.N.2
SALAMANCA

SENTENCIA: 00006/2025

En Salamanca, a 9 de enero de 2025.

D. JOSÉ LOZANO DÍAZ, Magistrado- Juez del Juzgado de Primera Instancia nº 2 de Salamanca; habiendo visto los presentes autos de juicio verbal nº 1309/ 2023, promovidos a instancia de Dª [redacted], representada por la procuradora Dª María Teresa Domínguez Cidoncha y defendida por el letrado D. Elías Plaza López- Berges, frente a Banco Santander SA, representado por el procurador D. [redacted] y defendido por el letrado D. [redacted] y D. [redacted], sobre contrato bancario y reclamación de cantidad, ha dictado Sentencia, en nombre de S. M. el Rey, con base en los siguientes:

ANTECEDENTES DE HECHO

PRIMERO: La procuradora Dª María Teresa Domínguez Cidoncha en nombre de Dª [redacted] presentó una demanda de juicio verbal frente a Banco Santander SA suplicando que fuese condenado a pagarle la cantidad de 1704.50 euros más los intereses legales desde que se hicieron las disposiciones de dinero y a que comunicase a las empresas o sistemas a los que comunicase en su día la deuda derivada de los hechos de la demanda en virtud del art. 20 de la LO de Protección de Datos 3/2018.

La demanda se basa en los siguientes hechos: la parte demandante es titular de una cuenta corriente en el Banco Santander terminada en 2781 y tiene asociada una tarjeta de débito, terminada en 9505. En los días 14 y 15 de octubre de 2022 sufrió varios cargos en su cuenta que no autorizó. El

ADMINISTRACION DE JUSTICIA

importe de esos cargos asciende a la cantidad reclamada. Esos cargos que ella no autorizó se hicieron pese a que no existía saldo suficiente, pues en la extracción de dinero de 200 euros la cuenta quedó con saldo negativo de 171, 70 euros.

Ya en el 4 de octubre de 2022 la demandante venía detectando situaciones extrañas. Esa fecha el Banco Santander le había bloqueado su Bizum porque alguien desconocido quería acceder a su cuenta. Hecho que volvió a suceder en el 13 de octubre. Por tanto, sin contar con la demandante, el propio banco unilateralmente adoptó medidas para evitar el acceso o el uso fraudulento de su cuenta.

En el 14 de octubre de 2022 la parte demandante recibió una llamada de una persona que se identificó como empleado del Banco de Santander y procedió a comprobar con ella una serie de movimientos en su cuenta que eran reales. Con tal fin esa persona le indicó que le iban a bloquear la tarjeta y le iban a remitir una nueva a su domicilio, el real. Lo que le demostró en ese momento de la legitimidad de la llamada. Es más, las llamadas se hicieron desde el 91 512 31 23 que es el teléfono del Banco Santander y así se hizo constar en el listado de llamadas de su móvil.

Más tarde en el dia 15 de octubre, se puso en contacto con el Banco Santander para preguntarle cuándo le iba a llegar la tarjeta y el banco le respondió que esa llamada no la había hecho. En esa comunicación le informan que desde Lérida alguien ha accedido a su cuenta y le ha sustraído dinero, procediéndose de inmediato a bloquearle la tarjeta y a abrir un expediente de reclamación por fraude.

La parte demandante ha reclamado varias veces la devolución al Banco, pero ha hecho caso omiso y además ha procedido a comunicar a los registros de deudas de ASNEF y de EXPERIAN al estar su cuenta en saldo negativo por importe de 1. 026, 14 euros.

La demandante ha presentado denuncia ante la Policía Nacional.

SEGUNDO: Admitida a trâmite la demanda, se emplazó a la parte demandada para que contestase, lo que hizo alegando: señala que los hechos

ADMINISTRACION DE JUSTICIA

se remontan al 1 de octubre de 2022, fecha en que la demandante recibe un SMS fraudulento. Necesariamente la demandante pulsó el enlace que contenía la comunicación y reveló sus credenciales bancarias. La entidad ha dirigido una campaña de comunicación de prevención del fraude dirigida también a la demandante, advertencias que figuran en los contratos suscritos. Y dice: *Al respecto, tal y como resultará acreditado, en fecha 5 de octubre de 2022, la Sra. García reveló los códigos para autorizar las operativas de alta de registro de dispositivo seguro y visualización del PIN vinculado a su tarjeta *9505. También, el pasado 14 de octubre de 2022, reveló el código para autorizar la configuración de su tarjeta en el servicio de pago móvil ofrecido por la marca APPLE PAY.*

Por ese motivo se produjeron los cargos del 14 y 15 de octubre de 2022 lo que se explica por la negligencia grave de la demandante.

Los pagos se realizaron siguiendo la normativa vigente y con el sistema de doble autenticación y las comunicaciones que el delincuente empleó con la demandante no fue con el canal oficial del Banco Santander, sino con un método fraudulento llamado spoofing, a través del vishing y smishing, por falta de filtros de las compañías telefónicas.

Se dan por reproducidos los argumentos fácticos y jurídicos de la contestación a la demanda, aunque, en síntesis, la oposición se sustenta en que la demandante actuó de forma negligente, fuera de los canales ordinarios del banco, revelando sus credenciales, incluso oralmente, lo que provocó que se hicieran esos cargos fraudulentos.

TERCERO: Seguidamente, se convocó a una vista a las partes, en las que se ratificaron en su demanda.

La prueba practicada fue la documental y el interrogatorio de parte.

Tras conclusiones se declaró el juicio visto para sentencia.

ADMINISTRACION DE JUSTICIA

FUNDAMENTOS DE DERECHO

PRIMERO: La parte demandante pretende que el banco demandado le devuelva el importe total de varios cargos fraudulentos o no consentidos en su cuenta corriente. Señala que días antes de esos cargos, en los días 14 y 15 de octubre de 2022, la entidad ya había bloqueado por dos veces el sistema Bizum, al intentar un tercero entrar en sus cuentas sin autorización. Pese a ello, la parte demandante, conocedora de estas medidas de seguridad, recibió una llamada inserta en el mismo hilo o canal de comunicación con el Banco Santander. Se le identificó una persona como empleada de dicho banco y le reveló detalles de los movimientos de sus cuentas y su domicilio que le inspiró confianza. Por ello procedió a bloquear su tarjeta y a solicitar una nueva. La demandante llamó a su banco para preguntar cuándo le entregarían la tarjeta y la persona que le atendió le dijo que había sido víctima de un engaño y que ellos no habían hecho una llamada, detectándose en ese acto los movimientos no consentidos y los cargos por el importe reclamado, los cuales fueron atendidos por el Banco Santander, pese a que no había saldo, dejando la cuenta en números negativos. Incluso el banco ha procedido a comunicar la deuda en descubierto a las empresas titulares de bases de datos de deudoras, conocidas vulgarmente, como archivos de morosos y ha solicitado que se condene a la entidad a eliminar esos registros.

La entidad bancaria completa los hechos y dice que el 1 de octubre de 2022 la demandante recibió un enlace en su móvil, que lo pulsó y que luego reveló en la web al que se le dirigía sus claves y su usuario, facilitando luego, incluso oralmente, los códigos necesarios para hacer esas operaciones. Es decir, los movimientos fueron ejecutados por el banco porque se recibió las órdenes con las claves y códigos necesarios para ello, confiando su sistema en su legitimidad. La demandante, dicen, actuó con negligencia grave, pues no se puede revelar esos datos personales y bancarios a terceros, hecho advertido en los contratos y en las sucesivas campañas de información que el banco ha remitido, en concreto, a la demandante.

ADMINISTRACION DE JUSTICIA

Ambas partes aplican e interpretan la Ley de servicios de pagos.

Por tanto, el objeto de debate se centra en detallar qué sucedió y si concurre negligencia grave en la demandante, en su caso, y qué incidencia puede tener el hecho de que se haya autorizado gran parte de los cargos sin haber saldo.

SEGUNDO: No es un hecho controvertido el que se hayan realizado las disposiciones de dinero que son objeto de autos, ni que nos encontremos ante un fraude o estafa. El objeto de debate es quién debe pechar con esas consecuencias.

Según el documento 2 de la demanda se realizaron las siguientes operaciones fraudulentas: reintegro de 500 euros en el 14 de octubre de 2022; en la misma fecha, reintegro de 300 euros; reintegro de 200 euros en la misma fecha (que ya dejaba en descubierto la cuenta); pago móvil de dos euros en el 15 de octubre; en esa misma fecha, dos pagos con móvil de 100 euros cada uno; reintegro de dinero en cajero de 502, 50 euros (se entiende que se carga o se suma la comisión); deja el saldo de la cuenta en 876.20 euros.

El documento 3 revela un conjunto de llamadas entrantes y realizadas en el hilo o canal con el Banco Santander. El teléfono es el 915 123 123, que reconoce el propio banco como el suyo de atención al cliente, con lo que en apariencia las llamadas parecen recibirse y dirigirse al banco demandado.

En el documento 10 de la demanda (los anteriores no son relevantes, al ser posteriores al fraude), consta el hilo o canal de mensajes SMS habidos entre la demandante y el banco demandado. En el 1 de octubre consta un mensaje en que se advierte que se ha iniciado una sesión en otro dispositivo. Y se dice que, si no ha sido el cliente el que lo ha hecho, que entre en un enlace (con protocolo https o de seguridad). Por ello, en apariencia ese mensaje lo recie la cliente de su banco y el enlace aparenta ser del banco y con protocolo de transferencia de hipertexto seguro (https).

No hay más mensajes hasta que en el 14 de octubre de 2022 recibe un mensaje en el mismo hilo o canal de su banco, supuestamente, donde le

ADMINISTRACION DE JUSTICIA

dicen que introduzca la clave 379498 para completar su registro en Apple Pay. Luego recibe otro mensaje en el 15 de octubre, fecha de los actos fraudulentos donde le dice que se ha registrado operaciones poco habituales con su tarjeta y que llame al teléfono indicado, el cual, precisamente, es el del banco.

En el interrogatorio de la parte demandante reconoció que su teléfono es el 615 75 02 19. En el documento 1 de la contestación consta un registro de actos con ese móvil: en el 5 de octubre de 2022, entre las 12: 13 y las 16: 06 horas se autorizó un alta de un dispositivo introduciendo incluso el código OTP que se le remitió.

El contrato multicanal aportado como documento 2 de la contestación obliga al cliente a ser cuidadoso con las claves y los móviles o dispositivos que utilice, guardando en estricta confidencialidad las claves, OTP que reciba, la firma electrónica, etc. Se establece un sistema de doble autenticación a través de una clave OTP que deberá introducir el usuario cuando lo reciba en su móvil.

La parte demandada, aparte, ha aportado el contrato de cuenta corriente. En él aparecen los datos personales de la demandante, pero no la dirección de correo electrónico. El listado de mensajes pedagógicos para que el cliente evite ser víctima de una estafa informática, así como el conjunto de esos mensajes con el contenido de cada uno se relacionan con una dirección de email que aparece en el documento 5 de la demanda, sobre apertura de un expediente de reclamación, es decir, es el mismo e-mail que ha usado la demandante para reclamar. Aunque no consta un certificado de tercero de confianza que acredite su recepción, al amparo del art. 326 de la LEC, pues la parte demandante ha negado que hubiese recibido esos mensajes de advertencia. Muchos de estos mensajes (los que tienen contenido, los del documento 4 de la contestación, no el listado de e-mail, que no tienen contenido) no hacen referencia a la modalidad de estafa cometida. Solo el último, que es de 2020, cuando los ciberdelincuentes actuaron en 2022. Adviértase que se ofrece un mensaje de desconfianza, y es precisamente la técnica adecuada la de generar confianza en la víctima.

Como apuntó el letrado de la parte demandante, el contrato aportado son solo las condiciones generales, no se aportan las particulares ni se ha aportado el contrato de tarjeta. Se empleó una tarjeta de débito. Así consta en el documento 1 del acontecimiento 55 del expediente digital. Se aprecia que las operaciones mencionadas, realizadas en los días 14 y 15 de octubre de 2022, fueron debidamente autenticadas y contabilizadas por Redsys y fueron llevadas a cabo con la tarjeta terminada en 9505, la de la parte actora (a través del sistema de Apple Pay y el número *token*).

La parte demandada no ha discutido que esos pagos se hicieran con una tarjeta de débito (no de crédito), ni ha probado que en concreto el contrato de la demandante permita un descubierto en cuenta. El contrato aportado pacta qué es lo que hay que hacer, qué efectos tiene el caso de que se permita un descubierto, pero nada más. De este modo se permitió un descubierto que ni siquiera se ha probado que estuviese pactado de antemano.

En el interrogatorio de parte la demandante negó haber introducido sus claves en el día 4 de octubre de 2022. Dijo que solo las reveló en la llamada previa a los hechos. No consta prueba alguna sobre el bloqueo del Bizum, circunstancia que puede y debe probar el banco, que dispone de todos estos registros.

Además, consta que Orange, operadora de telefonía de la demandante, informó que no consta petición de duplicado de tarjeta, con lo que no se ha hackeado su SIM, si bien, no se ha hecho un estudio del móvil de la demandante para averiguar si tiene o no instalado software malicioso, con lo que esta información no es determinante.

TERCERO: En conclusión, con los datos que obran en las actuaciones, sin que pueda decirse que son completos, como se requeriría en una instrucción penal por estafa, puede concluirse lo siguiente: en el 1 de octubre de 2022 dentro del canal o hilo de SMS legítimo que la demandante mantiene con su banco, recibió y se introdujo un mensaje en que se advertía de una posible conexión de otro dispositivo a su cuenta corriente y que, para

ADMINISTRACION DE JUSTICIA

evitarlo, debía acceder a un enlace, con apariencia del propio Banco Santander. Después, consta en los registros que el teléfono de la demandante recibió un código OTP para vincular otro dispositivo, que fue introducido (sucedió en 5 de octubre de 2022). Posteriormente, en el día 14 se realizó una llamada telefónica en que el estafador se hizo pasar hábilmente por empleado del Banco Santander, generando una confianza legítima en la demandante con la que reveló sus claves, produciéndose operaciones fraudulentas con una tarjeta de débito y dejando su saldo negatiuvo o en descubierto, cuando no se ha probado que el contrato de cuenta corriente lo permita.

Es decir, la demandante fue víctima de una estafa y hábilmente realizada, porque todos los mensajes y llamadas se hace con una apariencia tal que es difícil sospechar en ese momento, sin posibilidad de reflexión, que no se trata del Banco de Santander: los mensajes son en el mismo canal, el teléfono empleado por el estafador es el del Banco Santander (mediante un sistema informático para cometer el fraude), la dirección del enlace goza de una apariencia total como la del Banco, con un código https seguro (precisamente como le aconseja los mensajes que recibió en su e-mail) y la persona que habló con ella, después de recibir mensajes de posible fraude para "trabajarse" a su víctima, le ofrece detalles particulares que solo un empleado de banca legítimo puede tener a su alcance, generándose una confianza completa para que la demandante dé sus claves.

La idea que debe tener siempre un cliente de entidad financiera que emplee este tipo de canales telemáticos para el uso de sus cuentas es que nunca, jamás, el banco pedirá de oficio, por su sola iniciativa, clave o dato personal a su cliente. Los bancos y entidades solo piden las claves a través de los canales previamente pactados y solo y exclusivamente cuando la operación la ha iniciado el propio cliente.

Sin embargo, en los mensajes de consejos o advertencias este mensaje no es tan claro y muchos se remitieron, de los que se conoce contenido, no los del listado, mucho antes de que se produjera el fraude.

ADMINISTRACION DE JUSTICIA

CUARTO: Actualmente las empresas o administraciones públicas trasladan al cliente o administrado las funciones de gestión o administración de datos o dinero, convirtiéndose él, al menos en parte, en la oficina bancaria u órgano administrativo. Al margen de la facilidad que ello pueda proporcionar al cliente o administrado para tales cometidos, lo cierto es que ahorra muchos costes tanto a la administración, como a las entidades de crédito o financieras, pero genera altísimos riesgos, por no ser preciso ya que se relacionen personalmente quien gestiona o administra esos datos o patrimonio, y está obligado a prestar un servicio, y el cliente o administrado. En todo caso, se entiende, como lo hace el banco demandado, que el sistema bancario por internet es seguro y que nos encontramos en casos muy residuales. Pero esa no es la cuestión. La cuestión es si se producen esos casos concretos quién soporta las consecuencias del fraude.

En lo que respecta a los servicios de pago, la norma trata de distribuir la responsabilidad que deriva del uso fraudulento de los canales empleados para dicha gestión a través de internet o móvil. Es decir, la norma disciplina la atribución de las consecuencias de la realización de dichos riesgos.

En especial, la ciberdelincuencia, sabido es, se aprovecha de esas facilidades o flexibilidad y del anonimato de internet para cometer fraudes, suplantando de una forma u otra la identidad del cliente de servicios bancarios, logrando transferencias de dinero a su favor.

Existen tantos fenómenos de fraudes como técnicas pueda emplear los delincuentes para eludir los controles que se establezcan (sin ánimo de ser exhaustivos, pues ahora se pueden añadir los *spoofing, vishing o smishing*):

1°.- *phishing* (derivado del verbo to fish, pescar claves o PIN, si bien es un término que tiene más que ver con la jerga propia de los hackers, o se dice que es un acrónimo de la frase *password havertsting fishing*), y que consiste en que el delincuente envía SMS, correos electrónicos o mensajes de whatsapp ficticios al terminal del cliente (móvil, PC, tableta), muchas veces masivos, provocando que el cliente acceda a un enlace que suele simular la página web de su banco o caja, introduciendo sus claves, que el delincuente copia y utiliza después para el fraude.

ADMINISTRACION DE JUSTICIA

2º.- *pharming*: introducción en el móvil o terminal del cliente de un malware o virus que redirige al cliente a una página web ficticia donde introduce las claves que son copiadas y empleadas por el delincuente.

3º.- *keylogging*: es un *spyware* o programa espía que, a espaldas del cliente o usuario, va registrando las claves que el usuario introduce en la página web legítima de su banco o caja y luego los usa fraudulentamente.

4º.- *sniffing*: consiste en captar del usuario sus datos y claves cuando usa redes públicas, aprovechando su baja seguridad, y luego las usa fraudulentamente.

En todas estas modalidades se observa que el delincuente suplanta la identidad del cliente, consiguiendo el engaño del banco. Identidad que se configura con nombre de usuario o PIN. Antes el ciberdelicuente ha engañado al cliente del banco mediante esas técnicas, obteniendo fraudulentamente las claves y datos que lo legitiman frente al banco.

Para evitar estas actividades ilícitas las entidades de crédito emplean tarjetas de coordenadas, pero también se clonan o captan. Y otras veces se usa un número de un solo uso, que consiste en exigir al usuario o cliente que introduzca una clave que recibe para cada operación en su propio móvil (OTP o PUSH); pero ante esto último los delincuentes han encontrado otra herramienta, pues a través de métodos semejantes a los antes expresados logran una clonación de la tarjeta SIM del móvil del usuario o cliente, de modo que el sistema informático del banco o caja recibe la confirmación de una tarjeta con el mismo número de teléfono de su cliente, accediendo a la operación sin que este se entere. O, como en este caso, logran generar una apariencia tal que inspira confianza en el cliente que da directamente, bien oralmente, o bien introduciéndolas en su dispositivo, sus claves personales.

Una vez que las disposiciones fraudulentas se han realizado, surge la pregunta de quién responde o asume el perjuicio causado, siendo mayoritarios los casos en que es imposible o extremadamente dificultoso identificar al delincuente y recuperar el dinero.

Esta cuestión, como han alegado las partes, está recogida en el Real decreto ley 19/ 2018 de servicio de pago y otras medidas urgentes en

ADMINISTRACION DE JUSTICIA

materia financiera. La mayoría de las Audiencias señalan que este sistema, muy semejante al de la legislación precedente (Ley 16/ 2009), instaura un régimen jurídico cuasi objetivo de responsabilidad patrimonial del proveedor de servicios de pago o de la entidad financiera.

Esta norma instituye un régimen jurídico específico dentro del ámbito del contrato de cuenta corriente, depósito o de tarjeta de crédito, en el que la parte demandada, el banco o entidad de crédito, no solo está obligado a prestar el servicio, sino a ser diligente en la custodia de los fondos. Pero, a su vez, el cliente asume cargas contractuales, como no facilitar datos o claves pues, de lo contrario, dificultaría el cumplimiento de aquella obligación, planteándose un posible supuesto de concurrencia de causas, al menos, sino un caso de culpa exclusiva de la víctima. Pero todo esto depende del régimen jurídico concreto que se está exponiendo en este fundamento.

El art. 44 del Real decreto ley mantiene la inversión de la carga de la prueba del régimen jurídico antecedente: cuando el usuario o cliente de los servicios de pago alegue que no ha autorizado un determinado cargo o disposición, corresponde al operador de servicios de pago, a la entidad financiera, demostrar que la operación ha sido autenticada, registrada y debidamente contabilizada y que no se vio afectada por fallo técnico o deficiencia. No basta, además, con aportar el registro para probar que el cliente ordenó o autorizó la disposición u operación, ni alegar que este ha actuado de forma negligente o fraudulenta.

Es decir, la entidad financiera u operador de servicios de pago, en general, no puede alegar que, como la operación se ha realizado y se ha anotado correctamente se entiende que ha sido autorizada. Ni puede alegar que, aun cuando no conste fehacientemente que ha sido autorizada, pues el cliente lo niega, se debe deducir que ha sido descuidado con sus claves, permitiendo a un tercero suplantar su identidad electrónica.

Al gozar de los beneficios que internet otorga (en redes TCP/IP-internet o WAP, comunicaciones móviles), con reducción de costes empresariales, y al estar obligado a implementar técnicas de seguridad, así como al tener todos los medios de prueba a su alcance, la norma protege al

ADMINISTRACION DE JUSTICIA

cliente o usuario de los servicios de pago. En puridad, bastaría con que el cliente alegase que una determinada operación no la ha autorizado para que la entidad deba desplegar toda actividad probatoria para evitar la obligación de reintegrar su importe.

Incluso podemos afirmar que la responsabilidad se convierte en objetiva, salvo fraude, cuando la entidad financiera o el proveedor de servicios de pago o intermediario no exijan autenticación reforzada (art. 46. 2), que no es el caso, pues hubo códigos de un solo uso o de doble canal, como se ha dicho.

En la SAP de Almería de 31 de enero de 2023 se analiza el régimen jurídico del sistema de doble autenticación, según el 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 y concluye que hay inversión de la carga de la prueba en todo caso, limitándose solo al fraude cuando no consta la exigencia de doble autenticación. Y, aunque conste ese sistema, el régimen jurídico general invierte la carga de la prueba, pudiéndose probar, además del fraude, la negligencia grave.

El hecho de que la inversión de la carga de la prueba permita exonerarse a la entidad de crédito por la existencia de negligencia grave, excluye supuestos de negligencia leve. Ello nos lleva a concluir que ser víctima de esos casos de fraude, antes analizados, no tiene por qué suponer negligencia y atribuir en todo caso las consecuencias negativas de aquel. Así lo expone, por ejemplo, la SAP de Asturias 236/ 2023 o la SAP de Cáceres de 23 de noviembre de 2023 (todas las sentencias pueden consultarse en el Cendoj).

En la SAP de Cuenca de 16 de mayo de 2022 se aplica el mismo principio, transcribiendo e invocando los criterios de la AP de Madrid y de Alicante.

La SAP de Madrid de 13 de enero de 2023, como en la precedente, descartó que ser víctima de un *phishing* sea un supuesto de negligencia que

impida atribuir las consecuencias del fraude al cliente o usuario de los servicios de pago.

La SAP de Madrid de 26 de enero de 2023 (sección novena), llega a conclusiones que no se pueden compartir porque exige que el demandante explique el mecanismo del fraude. Ello no es un requisito impuesto por la ley. De hecho, ni siquiera se exige al propio banco, o proveedor de servicios de pago, alegar, probar o explicar un fraude. Basta con demostrar que o bien la operación fue firmada o autorizada realmente, que no ha existido fraude de un tercero, o bien negligencia o fraude del cliente o los demás supuestos recogidos en la ley. No se causa indefensión por el hecho de que el demandante no describa cómo sucedió (muchas veces no lo sabe), pues basta con alegar que esos movimientos de su cuenta, esas operaciones concretas no las ha autorizado, para que la entidad deba demostrar negligencia, fraude, etc. No obstante, esta sentencia es útil por cuanto recoge una línea doctrinal que cada vez se va abriendo camino a medida que el *phishing* es más conocido y más frecuentes las alarmas, advertencias y avisos entre los usuarios de la banca "online", bien por labor de las entidades financieras, bien de las propias administraciones o de los medios de comunicación.

Esta sentencia identifica concretos casos en que se ha hecho responsable a la víctima de *phishing* por negligencia:

Así, la SAP de La Coruña de 19.10.2022 considera una negligencia grave de la cliente al facilitar la misma su número de tarjeta, pin de acceso a banca móvil y tecleo de 4 números de confirmación remitidos por SMA, ante una mera llamada al teléfono fijo de su domicilio.

La SAP de Zaragoza de 1.7.2022, si bien condenó a la entidad bancaria a reintegrar el importe defraudado (por ausencia de autentificación reforzada en ese tipo de operaciones), valoró el acceso a los datos del cliente mediante la recepción de un correo electrónico con un link al que pinchó aquel facilitando el enrolamiento de la tarjeta al sistema de pago.

ADMINISTRACION DE JUSTICIA

La SAP Barcelona de 23.5.2022 apreció falta de diligencia en lo clientes al contestar a dos emails para descargar una aplicación en el móvil y contratando una tarjeta.

La SAP de Madrid de 20.5.2022 condenó al banco al reintegro de cantidades defraudadas tras estudiar que la víctima fue víctima de un phishing al recibir un SMS al móvil asociado a la tarjeta y contrato de cuenta corriente, haciendo clic en un enlace clonado de la web del banco.

La SAP de Pontevedra de 1.12.2022 desestimó la demanda frente al banco ya que la demanda hacía referencia únicamente al acceso fraudulento al ordenador del demandante, sin referencia alguna a la utilización indebida del móvil del actor, resultando de la pericial practicada la necesidad de disponer del dispositivo móvil para realizar la transferencia.

La SAP Badajoz de 30.12.2021 aprecia negligencia grave de la demandante al responder a un correo irregular y no custodiar debidamente sus claves a fin de garantizar los pagos.

En definitiva, esta sentencia pone de manifiesto las dificultades de prueba que tendría el banco o proveedor de servicios de pago en averiguar la negligencia si no posee dichos datos, es decir, cómo se llegó a realizar el *phishing*, pues esta técnica, así como las otras, de alguna manera exigen la colaboración del cliente, consciente o inconsciente.

Esta conclusión no se puede compartir, pues consta la posibilidad de acudir a los operadores de telefonía y de internet y, dependiendo del tiempo transcurrido, de los propios archivos de la entidad, a los que no se les puede negar valor probatorio por el mero hecho de haber sido emitidos unilateralmente por el propio banco, sin perjuicio de su valoración conjunta.

Y, en todo caso, se insiste en que estamos en un sistema de responsabilidad cuasi objetiva, como se ha dicho, de suerte que exigir a la parte actora alegar en su demanda para probar su propia negligencia no está establecido en la ley.

La SAP de Pontevedra de veintiuno de diciembre de dos mil veintiuno recuerda que la propia Directiva 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado

ADMINISTRACION DE JUSTICIA

interior, precisamente la que se traspone en el Real decreto ley que estamos aplicando. Y señala que la prueba de la negligencia debe siempre considerarse con arreglo a todas las circunstancias del caso concreto. El caso analizado es de phishing cuando una señora, haciendo caso a un SMS que indicaba que se necesitaba pagar 2, 90 euros para que Correos le hiciese un servicio, acabó por introducir su tarjeta, claves, código CVV y el mensaje que luego Abanca realmente le remitió, facilitando que el delincuente dispusiese fraudulentamente más de 4000 euros. Pero la sala concluyó que, con arreglo a todas las circunstancias, como la apariencia del primer código, así como a que no habría probado el banco los sistemas de seguridad implementados, no había negligencia grave.

En la SAP de Zaragoza de 1 de julio de 2022 se estima la demanda de un usuario que víctima de phishing, señalando que los anuncios o avisos de cautela que aportó el banco eran muy genéricos y que no demostró que sus sistemas de seguridad hubiesen funcionado, existiendo una inversión de la carga de la prueba.

Y, por último, la mayoría de las recientes sentencias de las Audiencias sobre el phishing y otras modalidades de fraude vienen asentando el criterio precedente de que ser víctima de una estafa no es un caso de negligencia grave. Así, la SAP de Barcelona de 24 de octubre de 2024, la SAP de Gerona de la misma fecha o la SAP de Cáceres (que se hace eco de la doctrina de la AP de Pontevedra) de 15 de octubre de 2024 (Cendoj). Como ejemplo contrario, la SAP de Valladolid de 10 de octubre de 2024 acepta como negligencia grave aquél caso en que una persona se instala a sabiendas en su ordenador un programa informático al que debe ceder sus claves bancarias y sus datos personales, negando, sin embargo, de forma implícita que no es negligencia grave aquél supuesto de phishing o de estafa similar en que la iniciativa de la operación no parte del cliente, sino que es un engaño apto del estafador.

En definitiva, a través de estas sentencias, las más recientes que se han encontrado en el Cendoj, así como de la lectura de la norma, se puede concluir que ser víctima de un *phishing*, en que el delincuente hace una

puesta en escena, una añagaza, para engañar al cliente bancario y provocar que facilite sus claves, no es sinónimo de negligencia grave, pero que se va abriendo un camino para que, después de la pedagogía de las entidades financieras (cada vez que accede uno a su app de su banco se abre un cartel de aviso y de advertencia) y de las administraciones públicas, se pueda llegar a considerar con el paso del tiempo el *phishing* como grave negligencia del cliente.

Se considera, sin embargo, que en este caso es prematuro: que una entidad bancaria o un profesional de la Justicia conozca el *phishing* es algo natural por ser numerosos los procesos al respecto o abundantes las diligencias previas incoadas para averiguar la identidad del delincuente. Pero no se entiende que este conocimiento sea generalizado en el público o que sea un hecho notorio. No puede suponerse en cualquier persona, con independencia de su edad, que sepa de antemano que puede ser víctima de esta estafa. Aunque hay que decirse, para el futuro, que jamás el banco por su sola iniciativa pide a sus clientes sus datos y hay que desconfiar de mensajes de entidades o de terceros que piden un pago por un servicio que previamente no se ha solicitado.

Ni siquiera con la remisión de mensajes de advertencia en este concreto caso puede eludir ese criterio porque muchos de ellos no se ajustan a lo sucedido y otros no son tan claros como decir simple y llanamente que tu banco nunca te pedirá tus claves a no ser que tú, cliente, inicies la operación.

En estos razonamientos, debe añadirse otro dato muy relevante: que muchas de las operaciones se permitieron en descubierto con una tarjeta de débito, no de crédito, sin que el banco haya probado que esto estaba permitido en el contrato.

QUINTO: Por tanto, la primera pretensión ha de ser estimada y se añaden los intereses legales desde las dos operaciones fraudulentas, según los arts. 1100, 1101 y 1108 del Código civil, de aplicación general, sin perjuicio de los del art. 576 de la LEC, en su caso, y ello por exigirlo el art.

ADMINISTRACION DE JUSTICIA

45 del Real decreto ley 19/2018 de 23 de noviembre, que dice que la devolución del dinero de las operaciones no autorizadas debe devolverse de inmediato.

En cuanto a la segunda de las pretensiones, el documento 12 de la demanda prueba que el banco incluso advirtió a la cliente de ser inscrita en un registro de deudas si no pagaba la que tenía con el banco y que fue fruto de un fraude, del que el banco es responsable, como se ha dicho.

Se desconoce, porque no hay prueba, si al final ha sido o no inscrita. Esto corresponde probarlo a la parte demanda, art. 217 de la LEC, pues no hay motivo para aplicar una inversión de la carga de la prueba, porque se pudo dirigir un oficio a esos registros para averiguar si se había intentado la inscripción, o si esta se había producido realmente y si se mantenía vigente.

Pero ello no quiere decir que esta pretensión no pueda estimarse, ya que, de la lectura del suplico, se desprende la obligación de que el banco comunique que el crédito o deuda es litigioso y que deben abstenerse de su inscripción (art. 20. 1 b) de la LO de Protección de Datos de 2018.

SEXTO: En muchas ocasiones, en casos como el presente, no se imponen las costas al banco por entender que hay serias dudas de hecho en cuanto a la negligencia y a la colaboración del cliente en ser víctima de una estafa informática. Pero en este caso nos encontramos con algo distinto, pues la estafa es más elaborada que en esos otros y se tiene en cuenta que el banco permitió el descubierto, pese a no probar que estuviese pactado, y además advirtió de que la víctima podría ser inscrita en un registro de morosos. Estas circunstancias permiten aplicar sin más el principio de vencimiento objetivo del art. 394 de la LEC y, si se han generado costas, imponérselas al banco.

Vistos los preceptos legales citados y demás de general y pertinente aplicación,

ADMINISTRACION DE JUSTICIA

FALLO

ESTIMO la demanda presentada por Dª María Teresa Domínguez Cidoncha, frente a Banco Santander SA, representado por el procurador D. [redacted], y **DECLARO:**

La responsabilidad de Banco Santander S.A. por incumplimiento contractual y de la Normativa de Servicios de Pago y sus Directivas, relativas al contrato de cuenta corriente suscrito entre doña [redacted] y la entidad bancaria, y el contrato de tarjeta de débito nº 5489 0191 1593 9505 asociada al contrato de cuenta corriente nº [redacted], al haberse cargado una serie de operaciones por importe de 1.704,50 € que no fueron efectuadas ni autorizadas por la demandante.

Que se han ocasionado a la demandante unos daños y perjuicios por importe de 1.704,50 € correspondientes a los cargos en cuenta por las operaciones ejecutadas sin su consentimiento y, en consecuencia:

LE CONDENO pagar a la parte actora 1.704,50 euros más los intereses legales desde la fecha de las operaciones no autorizadas hasta su pago, o consignación para pago, y sin perjuicio, en su caso, de los que se devenguen al amparo del art. 576 de la LEC.

Además, **LE CONDENO** a comunicar a las entidades que mantienen sistemas comunes de información crediticia, a los que hubiese solicitado la inscripción, para que se abstengan de inscribir la deuda derivada de las operaciones fraudulentas que se han analizado en esta sentencia.

Se imponen las **costas** de este proceso a la parte demandada, en el caso de que se hayan causado.

Notifíquese esta resolución a las partes haciéndoles saber que contra la misma no cabe recurso alguno y es firme.

Así lo acuerdo, mando y firmo:

ADMINISTRACION DE JUSTICIA

PUBLICACIÓN: En la misma fecha fue leída y publicada la anterior resolución por el Ilmo. Sr. Magistrado-Juez que la dictó, celebrando Audiencia Pública.