



JUZGADO DE 1ª INSTANCIA N° 04 DE ALCALÁ DE HENARES

C/ Colegios, 4 y 6 , Planta 1 - 28801

Tfno: 918839486

Fax: 918839485

alcala_instancia4@madrid.org

42020306

NIG: ~

Procedimiento: Juicio Verbal 762/2023

Materia: Obligaciones

NEGOCIADO 2

Demandante: D./Dña. [REDACTED]

PROCURADOR D./Dña. [REDACTED]

Demandado: BANCO SANTANDER SA

PROCURADOR D./Dña. [REDACTED]

SENTENCIA N° 82/2024

MAGISTRADO- JUEZ:

D. CARLOS JAVIER GARZÓN INIGO

Lugar: Alcalá de Henares

Fecha: trece de marzo de dos mil veinticuatro

El Sr. **D. Carlos Javier Garzón Inigo**, **MAGISTRADO-JUEZ** del Juzgado de 1ª instancia nº 4 de Alcalá de Henares y su Partido, habiendo visto los presentes autos de JUICIO VERBAL siendo parte actora Dª. [REDACTED] y como demandado BANCO SANTANDER SA.

ANTECEDENTES DE HECHO

PRIMERO.- Por el Procurador de la parte actora en virtud de la representación conferida se formuló demanda con arreglo a las prescripciones legales, en la cual tras la alegación de los hechos y fundamentos jurídicos que tuvo por convenientes terminó suplicando que se dictara Sentencia conforme a lo solicitado en el suplico de su demanda.

SEGUNDO.- Siendo competente este Juzgado para el conocimiento del procedimiento, se admitió a trámite la demanda disponiéndose el emplazamiento del demandado para que contestara a la demanda y se personara en el término improrrogable de 10 días, lo cual se verificó por el demandado oponiéndose a la demanda.

TERCERO.- habiéndose solicitado la celebración de vista, han comparecido las partes, ratificando sus posiciones iniciales, practicándose la prueba que, propuesta ha sido declarada pertinente, tras lo cual, las partes han realizado alegaciones finales, quedando de todo ello constancia en autos.



Madrid

FUNDAMENTOS DE DERECHO

PRIMERO.- Por la parte actora se ha ejercitado acción de reclamación de cantidad en concepto del perjuicio sufrido por la misma, como consecuencia de que fueron distraídas de su cuenta la cantidad de 4.845,83 euros, que es la cantidad reclamada en la demanda, frente a lo cual, la parte demandada esgrime que ninguna negligencia se ha producido por su parte, que deba llevar a la reparación del perjuicio causado, considerando que han sido los propios actos de la actora lo que ha llevado a la pérdida patrimonial sufrida.

SEGUNDO.- Es hecho acreditado que la actora tenía contratadas con la entidad Banco Santander un contrato de cuenta corriente con nº IBAN:

4776 (Documento nº 1 de la demanda); asimismo existe un contrato de tarjeta de débito, y en virtud del mismo le fue entregada una tarjeta de débito con el número

..... (Documento nº 2 de la demanda), siendo que la actora tenía concertado el sistema o servicio de Banca “on line”, dando de alta tanto un portátil como un dispositivo móvil. Así las cosas, señala que en la fecha 28 de julio de 2022 a las 17,53.-horas un ciberdelincuente, tras haberse adueñado a través de un ataque informático de las credenciales de usuario y contraseña de acceso a la banca on line de la actora, inició sobre éste un ciberataque, con aplicación de una técnica de ingeniería social, mediante el envío a su dispositivo móvil de un mensaje SMS al que dio la apariencia de haber sido remitido por BANCO SANTANDER, entremezclándolo dentro del hilo de mensajes SMS auténticos provenientes de la referida entidad bancaria. Señala la actora que creyendo que tal mensaje provenía realmente de su entidad bancaria al constatar que venía entremezclado dentro del hilo de mensajes de BANCO SANTANDER, junto a mensajes auténticos de tal entidad, y visualizando la leyenda “SANTANDER PARTICULARES, en la confianza de que se pretendía protegerle frente a una utilización fraudulenta de su tarjeta de pago, pulsó dicho enlace, que le redirigió a través de la web internet a un dominio de internet que a su vez aparentaba la página web de BANCO SANTANDER. Consecuencia de todo lo anterior, no volvió a tener más noticias sobre irregularidad alguna, hasta que, sorpresivamente, en fecha 1 de agosto a las 14,11 horas recibió un SMS proveniente de BANCO SANTANDER en el cual se le comunicaba que se habían registrado operaciones “poco habituales” con su tarjeta, instándole a que llamará al teléfono del Servicio de Atención al

Cliente. Argumenta la actora que ante tal mensaje, y en esa misma fecha 1 de agosto de 2022, mi mandante efectuó de forma inmediata una comprobación en su plataforma de banca on line, pudiendo constatar con estupor cómo se habían producido dos compras presenciales con utilización de los datos de su tarjeta de tarjeta de débito en el comercio “El Corte Inglés”, por importes respectivos de 1.866,83 Euros y 2.979 Euros (Documentos 14 y 15 de la demanda). Considera la actora que no ha incurrido en negligencia grave, sino más al contrario ha sido la demandada quien no obstante disponer de registros de trazabilidad que le permitían detectar las irregularidades que se estaban produciendo, permitió que se produjese una brecha objetiva de seguridad en su sistema de autenticación, por lo que reclama en concepto de indemnización la suma de 4.845,83 Euros por las disposiciones efectuadas.

TERCERO.- Por su parte la entidad bancaria esgrime como fundamento de su oposición que la actora fue víctima de un caso de “*phishing*” que, en esencia, consiste en una actividad

delictiva cuyo objeto es dar la apariencia frente a la víctima de ser un tercero, valiéndose incluso de emblemas y/o marcas comerciales similares, con ánimo de obtener datos personales y de seguridad provocando en la víctima un perjuicio patrimonial. Señala que la actora en ningún momento expone cómo fue posible que unos terceros accedieran a sus credenciales de seguridad para llevar a cabo las operaciones fraudulentas, de forma que el origen del problema no está en ningún fallo en el sistema de seguridad, sino en el acceso que tuvieron unos terceros a las credenciales de seguridad de la demandante. Al respecto señala que los mecanismos de seguridad de Banco Santander, funcionaron, lo que implica necesariamente que, o bien los movimientos los realizó la propia demandante, o bien, que los movimientos los realizó un tercero a quien la demandante entregó sus credenciales de seguridad. Argumenta que la demandada en todo momento ha cumplido con la normativa de aplicación en materia de servicios de pago, a cuyo efecto, alude a los certificados de la entidad REDSYS, considerando en definitiva que existe falta de diligencia de la parte actora, lo que debe eximir de responsabilidad a la entidad bancaria, por cuanto que no ha existido ninguna omisión en los sistemas de seguridad que le sean imputables, considerando que no se han podido constatar que mensajes o contestaciones dio la actora que permitan verificar su falta de diligencia.

CUARTO.- Es hecho acreditado que como consecuencia de la relación contractual existente entre las partes, existía un contrato de cuenta corriente con nº IBAN:

, así como un contrato de tarjeta de débito, y en virtud del mismo le fue entregada una tarjeta de débito con el número . No hay tampoco duda ni litigio respecto de las sustracciones realizadas a la parte actora de su cuenta, con motivo de las dos disposiciones de compras efectuadas. Así las cosas, hemos de decir que la jurisprudencia en este tipo de supuestos señala que la responsabilidad será del Banco salvo que la actora haya actuado con negligencia grave. Conforme al Real Decreto Ley 19/2018, las operaciones de pago se considerarán autorizadas cuando el ordenante haya dado consentimiento para su ejecución. A falta de consentimiento la operación de pago se considerara no autorizada. En este sentido, se considera que puede existir negligencia grave cuando existe una tardanza injustificada del usuario del servicio de banca en comunicar las irregularidades de la operación. Quiere ello decir que en supuestos como el presente, se establece un sistema de responsabilidad cuasi objetiva de la entidad bancaria, de forma que hay inversión de la carga de la prueba al presumirse la falta de autorización de la orden de pago si el cliente lo niega. De este modo el deber del cliente es comunicar de forma inmediata al proveedor del servicio la posible pérdida o extravío. Alega la parte demandada que la actora omitió el cómo pudieron obtener los estafadores los datos de sus claves, más como hemos visto, lo que existe es una presunción de que no ha habido autorización de esa orden de pago por la actora, presunción que puede ser rota por prueba en contrario, lo que implica que ante la negativa expuesta en la demanda por la actora de que ella diese autorización para las operaciones fraudulentas, corresponde a la demandada acreditar esa autorización.

QUINTO.- Se han practicado en autos diversas pruebas, tendentes a verificar los extremos discutidos, y lo cierto es que lo que consta acreditado es que la actora recibió un aviso de posibles conductas u operaciones no habituales, siendo ese el momento en que la actora constata las sustracciones habidas. No basta con acreditar el hecho de que se pueda haber facilitado de forma involuntaria las claves, siendo necesario una negligencia grave en la

omisión de la lectura atenta de correos o mensajes recibidos, o de aceptaciones. No olvidemos que en los casos de *phising*, suele ser mecanismo habitual el empleo de técnicas de ingeniería social para ganarse la confianza del usuario del instrumento de pago y aprovecharse así de una interpretación errónea en la toma de decisiones por parte del usuario. En definitiva, queda acreditado que terceras personas consiguieron la sustracción del dinero de la cuenta de la actora, mediante el acceso ilícito de algún modo a las claves informáticas del titular de la cuenta, con motivo de la operativa realizada por los estafadores, mediante la suplantación de signos e imágenes que hacen creer a la actora que realmente se está comunicando con la entidad bancaria, pues no consta autorización de la actora, autorización que sí podría implicar una negligencia, siendo que la actora en su demanda niega haber otorgado la autorización, correspondiente entonces a la parte demandada probar la negligencia grave de la actora. Recordemos que el Tribunal Supremo encuadra estas conductas de *phishing* bancario como hechos delictivos en el artículo 248.2 a) del Código Penal y señala que la conducta básica que encarna este tipo de delitos consiste en el envío de emails fraudulentos desde direcciones supuestamente de entidades bancarias a la dirección de correo electrónico de la víctima, reclamando datos personales de contenido económico, como regla general datos de acceso a las cuentas (usuario y contraseña) que la víctima o víctimas tengan abiertas en la entidad o mediante enlaces a una web casi idéntica o muy similar a la de la entidad bancaria, produciendo así engaño en los usuarios con la finalidad de obtener un beneficio económico ilícito mediante la realización de transferencias a la cuenta del autor o autores del delito. Resulta claro que estamos ante supuestos de fraudes informáticos que afectan a los usuarios de banca, siendo que la negligencia grave que debe imperar para eximir de responsabilidad a la entidad bancaria, ha de concurrir acreditada de forma precisa. Genera ello, a juicio del T. Supremo, un sistema de cuasi-responsabilidad civil objetiva de las entidades bancarias sobre la base de una falta de diligencia del Banco por no contar con medidas de protección suficientes del servicio de banca online. Por tanto, el Tribunal Supremo considera que, como regla general, no se le puede exigir a la víctima del delito mecanismos de autoprotección en orden a evitar la comisión del hecho delictivo, pues por la propia complejidad de las conductas delictivas que configuran este delito de estafa informática es muy difícil que la víctima pueda darse cuenta y en consecuencia evitar que se consumen dichas conductas delictivas, sino que es la entidad bancaria la que debe adoptar los mecanismos de precaución necesarios para evitar dichas conductas delictivas. No se ha acreditado en el presente caso, cual es la negligencia grave de la actora, que hubiese provocado el error, siendo que la responsabilidad cuasi objetiva, conlleva la inversión de la carga de la prueba, recayendo en el Banco probar una conducta negligente que no ha sido acreditada. Lo anterior, debe llevar por tanto a la estimación de la demanda, y por ende, condenar a la parte demandada a abonar al actor la cantidad de 6.900 Euros, más los intereses legales desde la reclamación extrajudicial.

SEXTO.- Por lo que a las costas del procedimiento se refiere, y de acuerdo con el principio del vencimiento establecido en el artículo 394 de la LEC, estas se imponen a la parte demandada, al haberse estimado la demanda.

FALLO

Que estimando la demanda formulada por la Procuradora D^a. _____, en nombre y representación de D^a. _____, debo condenar a la

demandada. BANCO SANTANDER SA, a abonar al actor la cantidad de 4.845,83 Euros, más los intereses legales desde la reclamación extrajudicial, todo ello con imposición al demandado de las costas del procedimiento.

Notifíquese esta resolución a las partes, haciéndoles saber que la misma no es firme y que contra ella puede interponerse recurso de Apelación para ante la Iltma. Audiencia Provincial de MADRID, recurso que deberá prepararse ante este órgano judicial en el término de VEINTE DÍAS contados a partir de su notificación.

Así por esta mi Sentencia, de la que se expedirá testimonio para su unión a las actuaciones, juzgando en primera instancia, la pronuncio, mando y firmo.

El Magistrado/a Juez

PUBLICACIÓN.- Leída y publicada fue la anterior Sentencia por el/la **MAGISTRADO-JUEZ** que la dictó, estando celebrando audiencia pública en el mismo día de su fecha. Doy fe.

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

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