ADMINISTRACION DE JUSTICIA

JDO. PRIMERA INSTANCIA N. 4
GIJON

SENTENCIA: 00245/2024

JDO. PRIMERA INSTANCIA N. 4 DE GIJON

[redacted] 3, [redacted] DE VISTAS 9 // CIF: [redacted]
Teléfono: 985-175583/84-159997, Fax: [redacted]
Correo electrónico:

Equipo/usuario: GE2
Modelo: [redacted]

N.I.G.: 33024 42 1 2023 0003771
ORD PROCEDIMIENTO ORDINARIO 0000363 /2023
Procedimiento origen: /
Sobre OTRAS MATERIAS
DEMANDANTE D/ña. UNION DE CONSUMIDORES DE ASTURIAS
Procurador/a Sr/a. [redacted] DE [redacted]
Abogado/a Sr/a. JOSE ANTONIO BALLESTEROS GARRIDO
DEMANDADO D/ña. UNICAJA BANCO,S.A.
Procurador/a Sr/a. [redacted] LARROQUE
Abogado/a Sr/a.

SENTENCIA

En Gijón, a 22 de julio de 2024.

Vistos por mí, Doña Diana Corredera Bermúdez, Jueza en sustitución en el Juzgado de Primera Instancia nº 4 de Gijón, los presentes autos de **Juicio Ordinario nº 363/2023**, seguidos ante este Juzgado a instancia de la "UNIÓN DE CONSUMIDORES DE ASTURIAS" (actuando también en representación de su socio Don [redacted] legalmente representada por la Procuradora de los Tribunales Doña [redacted] de [redacted] y asistida del Letrado Don [redacted] Antonio Ballesteros Garrido, contra la entidad "UNICAJA BANCO, S.A.", legalmente representada por el Procurador Don [redacted] Larroque y asistida por la Letrada Doña [redacted] sobre reclamación de cantidad, y con los siguientes

ANTECEDENTES DE HECHO

PRIMERO.- En fecha 17 de marzo de 2023 por la representación de la parte actora se interpuso demanda de juicio ordinario cuyo conocimiento, por turno de reparto, correspondió a este Juzgado, en la que con fundamento en las alegaciones fácticas y fundamentos de derecho que estimó de aplicación, concluía suplicando se dicte "sentencia estimando la demanda y condenando al demandado a reembolsar a [redacted] los 39.600 euros que les fueron defraudados, con sus intereses legales desde su primera reclamación, el 17 de junio de 2022 (Documento 15); y al pago de las costas".

SEGUNDO.- Admitida a trámite la demanda por Decreto de 28 de junio de 2023, se dio traslado de ella a la parte demandada, para que formulase contestación en el plazo de 20 días hábiles. El 29 de septiembre de 2023 se formuló contestación por dicha parte oponiéndose a la demanda, en base a los hechos y fundamentos de derecho que expone, y solicitando "se dicte Sentencia desestimatoria con expresa imposición de costas a la parte actora".

TERCERO.- Por Diligencia de Ordenación de 16 de noviembre de 2023 se convocó a las partes para la celebración de la audiencia previa, que tuvo lugar en la sede de este Juzgado el día 7 de febrero de 2024, a cuya conclusión las partes quedaron citadas para la práctica de la prueba y conclusiones para el día 19 de junio de 2024.

CUARTO.- En el acto del juicio, se practicó la prueba declarada pertinente que consistió en: Testifical de Don [redacted] y Pericial de Don [redacted] Tras manifestar las partes sus conclusiones, se dio por terminado el acto, quedando los autos

PRINCIPADO DE ASTURIAS

ADMINISTRACION DE JUSTICIA

conclusos para dictar sentencia. El juicio se registró en documento electrónico que queda bajo la custodia de la Sra. Letrada de la Administración de Justicia y en grabación videográfica.

FUNDAMENTOS DE DERECHO

PRIMERO.- La parte actora ejercita, a través del cauce procesal del juicio ordinario, acción de reclamación de cantidad frente a la entidad "UNICAJA BANCO" por importe total de 39.600 euros, con base en los artículos 44 y 45 del Real Decreto-Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, y en la jurisprudencia aplicable, alegando, en síntesis, que los días 11 y 12 de junio de 2022 se produjeron cuatro cargos en la cuenta corriente de Don [redacted] al haber sido víctima de una operación fraudulenta, tras haber recibido su hijo Don [redacted] SMS que tenían apariencia de ser auténticos, puesto que aparecían como remitidos por Unicaja, que le llevaron a una web que tiene apariencia de ser la de Unicaja, era un clon de la real; Don [redacted] comprobó que efectivamente se había producido un intento de acceso a su web, lo que reforzaba la apariencia de veracidad del origen del mensaje y de su contenido. Tras ello recibió llamadas del número de atención de urgencias de Unicaja, procediendo Don [redacted] a comprobar que era el teléfono que aparece en la página web antes de contestar a una segunda llamada. A raíz de la segunda llamada, introdujo las claves, que permitieron realizar las transferencias fraudulentas. Considera la parte actora que Unicaja no dispone de medidas de seguridad adecuadas para evitar tales operaciones fraudulentas, no apreciándose negligencia por parte del cliente, por lo que interesa se condene a la entidad bancaria al reembolso de las cantidades defraudadas.

Por su parte, la demandada se opone a los pedimentos de la contraparte, aduciendo una negligencia grave por parte del cliente, al haber introducido las claves (usuario y contraseña) que permitieron la vinculación del dispositivo y el acceso de los estafadores a la banca digital del actor.

Conviene puntualizar que, por medio de Otrosí Segundo Digo, la parte demandada interesaba en su escrito de contestación la suspensión del procedimiento por prejudicialidad penal, cuestión que fue resuelta en sentido desestimatorio en el acto de la audiencia previa por las razones allí expuestas, que, en aras de la brevedad, se dan aquí por reproducidas.

SEGUNDO.- Nos encontramos ante una acción de reclamación de cantidad derivada de un fraude informático, que comportó cuatro transferencias cargadas en la cuenta corriente titularidad de Don [redacted] Supuestos como el que nos ocupa han sido resueltos por nuestra Audiencia Provincial. Entre otras, cabe citar la Sentencia núm. 142/2024, de fecha 21 de marzo de 2024, de la Audiencia Provincial de Asturias, Sección Cuarta, que establece que "Se está ante un tipo de estafa informática cometida mediante la captación de datos bancarios, induciendo a error a la víctima tras hacerse pasar por la propia entidad bancaria, a la que suplantan a través de correos electrónicos (técnica conocida como "phishing") o bien a través de SMS fraudulentos como en este caso ("smishing"), con el objetivo final de que los clientes proporcionen sus datos de carácter personal y claves bancarias para acceder así a sus cuentas de forma fraudulenta. La excusa frecuentemente utilizada, como sucedió en este caso, es la de informar sobre un acceso no autorizado a las cuentas on line, de tal modo que los clientes alertados ante esa circunstancia, intentan comunicar con el Banco cuando en realidad lo que hacen es facilitar sus datos bancarios al defraudador".

Añade la referida Sentencia que "Como decíamos en sentencia de 13 de diciembre de 2023, al abordar un caso similar "El marco normativo que sirve para dar respuesta a la controversia se contiene en la actualidad en el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que sustituyó a la precedente Ley 16/2009, de 13 de noviembre, de servicios de pago, y en el que, por lo que aquí importa, se recogen las obligaciones esenciales que incumben al usuario de servicios de pago y a las entidades que los prestan.

Así, y por lo que concierne al primero, el usuario está obligado (artículo 41 a) a utilizar el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del mismo, y, en particular, "tomará todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas". En tanto el proveedor de esos servicios está obligado (artículo 42.1 a) a cerciorarse que de que "las credenciales de seguridad personalizadas del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento...".

A su vez, y en relación a los supuestos de operaciones no autorizadas o ejecutadas incorrectamente, el usuario está obligado (artículo 43.1) a comunicar su existencia "sin demora injustificada, en cuanto tenga conocimiento de cualquiera de dichas operaciones...". Y está llamado, además, a soportar (artículo 46.1.3º) "todas las pérdidas derivadas de operaciones de pago no autorizadas si ... ha incurrido en tales pérdidas por haber actuado de manera fraudulenta o por haber incumplido, deliberadamente o por negligencia grave, una o varias de las obligaciones que establece el artículo 41".

[redacted] DE ASTURIAS

ADMINISTRACION DE JUSTICIA

Fuera de esos supuestos -ausencia de comunicación en tiempo de las operaciones, actuación fraudulenta del usuario, o negligencia grave- la proveedora del servicio está obligada a realizar la rectificación del cargo (artículo 43.1) y devolución del importe (artículo 45.1), bajo la premisa de que, ante la negación por el usuario de haber autorizado la operación o la afirmación de que la misma fue realizada de manera incorrecta, corresponde a aquella (artículo 44.1º) "demostrar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado...", al igual que tiene la carga de acreditar (artículo 44.3º) "que el usuario del servicio de pago cometió fraude o negligencia grave", sin que, a la par, el registro de la utilización del instrumento por el proveedor baste por sí solo y necesariamente para demostrar que "la operación de pago fue autorizada por el ordenante, ni que éste ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones..." (artículo 44.2º).

Y esa responsabilidad se acentúa aún más cuando el proveedor no exige "autenticación reforzada" del cliente, supuesto en que éste último únicamente responde de haber actuado de forma fraudulenta (artículo 46.2º). Concepto ese que se corresponde con (artículo 2.5) "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), 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".

Con todo, pues, lo que resulta de esas previsiones es el establecimiento a cargo de la proveedora de los servicios de pago de un riguroso régimen de responsabilidad ante disposiciones no autorizadas, que solo cede con la demostración de la actuación fraudulenta o gravemente negligente del usuario. Régimen sin duda inspirado en la idea de que los beneficios que comporta (tanto para el tráfico económico, como para la actividad del proveedor de los servicios) el avance tecnológico en los instrumentos de pago, debe estar justamente compensado con la protección reforzada de quien los emplea y se ve expuesto a actuaciones fraudulentas como la que hubo en el caso de autos. Con razón dice, por ello, la sentencia de instancia que se trata de una responsabilidad cuasiobjetiva, que es la calificación que le otorgan, además de las resoluciones que en ella se citan, otras del mismo sentido como las sentencias de las Audiencias Provinciales de Lleida, Sección 2ª, de 29 de junio de 2023 ; La Rioja, Sección 1ª, de 17 de febrero de 2023 ; Almería, Sección 1ª, de 31 de enero de 2023 ; o Madrid, Sección 10ª, de 13 de enero de 2023, además de cuantas en ellas se mencionan, en las que, con las variaciones propias de cada caso, se abordan supuestos de fraude similares al que nos ocupa. Al igual que lo hace también la Sentencia de la Sección 5ª de esta Audiencia de 22 de junio de 2023".

Partiendo de las anteriores premisas, llega la citada Sentencia a la siguiente conclusión: "el recurso debe ser desestimado, por cuanto el Banco no solo no ha demostrado que el cliente hubiera incurrido en negligencia grave en el proceso que desembocó en la estafa, sino que todo apunta a un déficit del sistema de seguridad de la propia entidad bancaria para evitar esta clase de ataques informáticos. Y así:

1º) Ya se ha dicho que ni siquiera el apelante califica de negligencia grave la primera actuación del demandante, al clicar sobre el enlace que aparecía en el primer mensaje. Y que ello es así se desprende sin lugar a dudas por la imposibilidad para el cliente, o para su terminal telefónico, de percibir que se estaba ante un SMS fraudulento, dada la técnica utilizada de SPOOFING, pues el estafador utilizaba el propio ID de la entidad bancaria. Actuación la del cliente, por lo demás lógica ante la alerta, que se suponía enviada por el Banco, de que alguien no autorizado había entrado en su cuenta online.

2º) En coherencia con lo anterior, introdujo a continuación la clave de seguridad que le fue facilitada por el Banco con el fin de "finalizar con la vinculación de dispositivo a Banca Digital". No se advertía entonces, como pretende la apelante, de que se trataba de vincular otro dispositivo distinto, circunstancia que podría haber generado desconfianza en el cliente, sino que se hablaba solo de dispositivo, sin indicar cual fuera, de tal modo que lo que hubo de presumir éste es que se trataba del propio, que había que vincular de nuevo dado el acceso no autorizado del que había sido informado. No es cierto, en consecuencia, que el demandante hubiera introducido la clave OTP necesaria para llevar a cabo la concreta operación, la transferencia indicada, sino que, una vez vinculado el dispositivo que utilizaba el ciberdelincuente, a éste le serían remitidas las claves necesarias para las nuevas operaciones que deseara realizar, y no a quien aquí acciona.

[redacted] DE ASTURIAS

En definitiva, este segundo paso venía precedido y motivado por el engaño ya consumado con el primer SMS, y estaba sin duda guiado por el ánimo de evitar lo que, desgraciadamente, se perseguía con él, por lo que esa actuación no puede calificarse de temeraria ni gravemente negligente, sin que, como decíamos en la sentencia citada de 13 de diciembre de 2023, "pueda exigirse a quien resultó engañada mayor precaución que a quien debía poner los medios necesarios para evitar el engaño". Y

ADMINISTRACION DE JUSTICIA

3°) Concurren, además, otros datos que apuntan a la responsabilidad de la demandada en lo sucedido. Ella misma señala en el escrito de contestación que seis meses antes, el 11 de enero de 2022, el Banco de España se había hecho eco de esta clase de delitos, informando de las nuevas modalidades de smishing y spoofing. Y, sin embargo, no adoptó las técnicas o medidas de seguridad que fueran suficientes para evitar que se produjeran esta clase de fraudes en su ámbito de actuación, al menos hasta que sucedieron los hechos controvertidos, como lo demuestra que siguieran teniendo lugar. Es más, el gran número de estafas cometidas por este medio en pocos días con relación a esta misma entidad bancaria evidencia la falta de medidas o la quiebra de las que pudiera haber tomado, pues difícilmente puede sostenerse que un gran número de usuarios hubieran incidido casi simultáneamente en una conducta gravemente negligente en sus interacciones con el Banco.

Incluso las particularidades del caso (transferencia con carácter inmediato, por importe de relativa importancia, desde un nuevo dispositivo que acaba de vincularse a la banca digital, a favor de una financiera extranjera de dinero electrónico), tan poco usuales en la práctica, debía haber permitido al Banco detectar que se estaba ante un posible fraude.

En resumen, como también señalábamos en la repetida sentencia de 13 de diciembre de 2023, el usuario procedió como con "toda probabilidad habría realizado gran parte de la población, por más que sea usuaria de esos canales tecnológicos, en los que el refinamiento en el desarrollo de la actividad delictiva parece ir un paso por delante de las barreras que se ponen para evitarla, pese a que, sin duda, es a la entidad a quien corresponde implementar todos los medios precisos para anticiparse a esa actividad, que es de lo que, sin embargo, aquí no hay prueba alguna".

En el mismo sentido, cabe citar, entre otras, la Sentencia núm. 166/2024, de fecha 10 de abril de 2024, dictada por la misma Sección Cuarta de nuestra Audiencia Provincial.

TERCERO.- Aplicando la anterior doctrina al caso que nos ocupa, la demanda ha de ser estimada. La fundamentación jurídica señalada en los párrafos anteriores es plenamente aplicable al presente supuesto, resultando acreditado el acceso irregular a la banca digital del demandante, sin que pueda apreciarse negligencia grave en su actuación, atendida la testifical practicada en el acto del juicio. No ha conseguido probar la demandada que cuenta con medidas de seguridad adecuadas, pretendiendo imputar al cliente tales operaciones fraudulentas, que, sin duda resultan indetectables si no eres experto informático.

Además, obra en autos informe pericial, aportado por la parte actora en fecha 20 de octubre de 2023, que concluye que "el usuario de banca electrónica común no es capaz de reconocer que está inmerso en un fraude electrónico por las siguientes razones: 1ª) Los mensajes SMS fraudulentos que inician el fraude se agrupan automáticamente con los legítimos siendo imposible diferenciarlos entre sí; 2ª) El envío de mensajes SMS con enlaces hacia páginas Web es una práctica habitual que se ha venido realizando tanto por entidades bancarias como por otros organismos públicos y privados. En muchas ocasiones, estos enlaces son total o parcialmente opacos; 3ª) Que el enlace enviado en los mensajes SMS lleva a páginas que se sirven bajo un protocolo seguro y visualmente similares a las originales de la entidad financiera; 4ª) El descubrimiento del fraude a partir del análisis de las direcciones contenidas en los mensajes requiere de habilidades técnicas especializadas; y 5ª) La operativa para la realización del ciberataque es similar a la operativa convencional del banco". Añade "que Unicaja envía a sus clientes mensajes SMS y correos electrónicos que incluyen enlaces hacia portales Web donde se les acaba requiriendo su usuario y contraseña"; que la entidad bancaria "utiliza para su sistema de autenticación reforzada mensajes SMS que como bien indica el Banco de España es un medio inseguro; que este canal de comunicación ya no es utilizado por la mayoría de los bancos por sus problemas de suplantación"; y "que las estafas no habrían podido ser realizadas, de haber tenido las medidas de seguridad que el banco asegura tener implantadas en la actualidad". Se remite esta Juzgadora a las oportunas explicaciones ofrecidas por el perito autor del informe en el acto de la vista, debiendo destacarse que fue tajante al afirmar que el sistema de SMS no es seguro ni adecuado y el Banco debe cambiar de operativa.

Por lo expuesto, procede la estimación integra de la demanda.

CUARTO.- Corresponde imponer a la demandada, el pago de los intereses fijados en los artículos 1100 y 1108 del Código Civil, desde la fecha de la reclamación extrajudicial (17 de junio de 2022, conforme al Documento número 15 de la demanda), que se incrementará en dos puntos desde la fecha de la presente resolución (artículo 576 de la Ley de Enjuiciamiento Civil).

QUINTO.- En cuanto a las costas, y de conformidad con el artículo 394 de la Ley de Enjuiciamiento Civil, procede imponerlas a la parte demandada al haberse rechazado todas sus pretensiones.

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

[redacted] DE ASTURIAS

ADMINISTRACION DE JUSTICIA

FALLO

Que ESTIMANDO ÍNTEGRAMENTE la demanda formulada por la Procuradora Sra. [redacted] de [redacted] en nombre y representación de "UNIÓN DE CONSUMIDORES DE ASTURIAS", en representación de su socio Don [redacted] contra la entidad "UNICAJA BANCO, S.A.", DEBO CONDENAR Y CONDENO a la demandada a abonar a la parte actora la cantidad de 39.600 euros. Todo ello más los intereses legales correspondientes, conforme a lo establecido en el Fundamento Jurídico Cuarto de la presente resolución.

Con imposición de costas a la parte demandada.

Notifíquese la presente resolución a todas las partes, haciéndoles saber que la misma no es firme y contra ella cabe interponer recurso de APELACIÓN ante este Juzgado, dentro de los VEINTE días siguientes a aquel en que se produzca su notificación, para su conocimiento por la Ilma. Audiencia Provincial de Asturias (artículo 458.1 de la LEC, tras la reforma operada por la Ley 37/2011, de 10 de octubre, de medidas de agilización procesal). Para interponer el recurso será necesaria la constitución de depósito, conforme a lo dispuesto por la Disposición Adicional 15ª de la LOPJ (tras la reforma por LO 1/2009, de 3 de noviembre), sin cuyo requisito no será admitido a trámite.

Así por esta mi Sentencia, lo acuerdo, mando y firmo.

[redacted] DE ASTURIAS