Juzgado de Primera Instancia de Barcelona que por turno corresponda

Demandante: ELVIRA [redacted]
Demandada: [redacted], S.A.

Objeto del escrito: Demanda de procedimiento ordinario en el ejercicio de acción de reclamación de daños y perjuicios

Fecha del escrito: 2 de marzo de 2023

AL JUZGADO

Dña. **INÉS CASADO GÜELL**, Procuradora de los Tribunales y de Dña. **ELVIRA** [redacted], según designa apud acta que se verificará ante la presencia judicial, **COMPAREZCO** y **DIGO**:

Que, por medio del presente escrito, interpongo **DEMANDA DE PROCEDIMIENTO ORDINARIO EN EL EJERCICIO DE ACCIÓN DE RECLAMACIÓN DE DAÑOS Y PERJUICIOS** contra la sociedad [redacted], con establecimiento abierto al público en [redacted], Barcelona (08003), sobre la base de los siguientes:

HECHOS

PREVIO. - Partes y objeto de la presente *litis*.

Mi mandante, **<u>parte actora</u>** en este procedimiento, es Dña. **ELVIRA** [redacted] cliente y usuaria de [redacted], que actúa en calidad de perjudicada por ser víctima de una estafa denominada phishing.

La **<u>parte demandada</u>**, el [redacted], más conocido por las siglas [redacted], es un banco español con sede en [redacted]

En fecha 3 de agosto de 2021 mi representada, Dña. [redacted], y la mercantil aquí demandada, [redacted], firmaron un contrato de tarjeta denominado “Aqua Debito”, concretamente firmaron el contrato N.º 0182 - 3077 - 0616 – 00000040595373, a través de la oficina N.º 3077, en virtud del cual se emitía una tarjeta con carácter personal e intransferible a mi representada. Es importante destacar que la actora es “cliente” y no se le presume conocimiento ni experiencia en la contratación de productos de inversión. Por ello, el nivel de protección debe ser el máximo.

[Se adjunta como **Documento N.º 1** el contrato de Tarjeta Aqua Debito firmado el 3 de agosto de 2021, la respectiva información precontractual y la política de protección de datos].

El objeto de la presente demanda es que se **declare la responsabilidad de la entidad por los hechos acaecidos,** que expondremos a continuación, **y reclamar el importe de 10.679,57 €,** importe que fue estafado a la parte actora por la falta de diligencia de BBVA.

PRIMERO. – La operación.

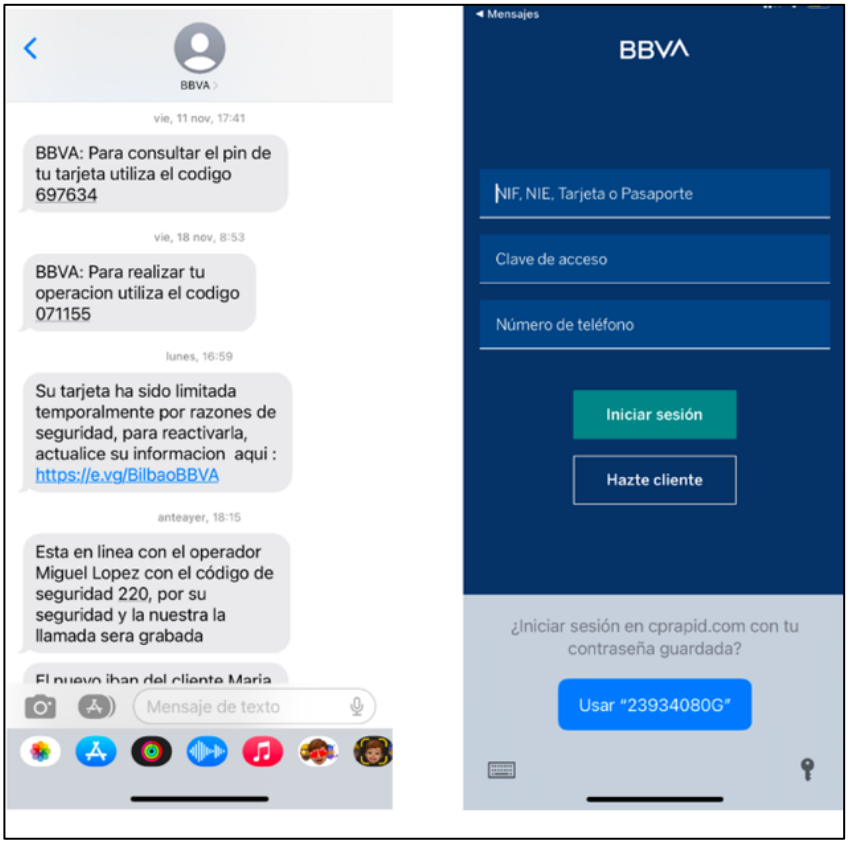
A fin de centrar el objeto del presente procedimiento, resulta necesario relatar brevemente los siguientes **antecedentes fácticos**:

A) El día 28 de noviembre de 2022, mi representada recibió una serie de comunicaciones por SMS, supuestamente del banco BBVA, informando que su cuenta, [redacted], había sido limitada por motivos de seguridad y que se debía reactivar mediante un enlace web. Mi representada introdujo los correspondientes datos.

B) Seguidamente, el día 29 de noviembre de 2022 recibe una llamada, supuestamente del Departamento de fraude de BBVA, dónde le dicen que le han bloqueado la cuenta y que van a crear una de nueva dónde tiene que transferir la cantidad total de la que disponía, esta es de **10.679'57 Euros**.

   Dado que la persona que le llama conoce sus datos personales y la cantidad de la que dispone, se genera una situación de confianza y mi mandante procede a realizar dicha transferencia. Una vez realiza la trasferencia, se le facilita un nuevo número de cuenta al que no puede acceder con la contraseña facilitada y es ahí donde detecta que ha sido víctima de una estafa.

C) Como se puede ver en las capturas de los SMS que adjuntamos a continuación, **tanto las comunicaciones del estafador como el código para autorizar la transferencia del propio banco, se reciben a través del mismo remitente y en la misma cadena de mensajes, BBVA**. Es decir, **alguien había suplantado la identidad de BBVA y había accedido a los datos personales de mi cliente**, creando de este modo una situación que induce a error a Dña. ELVIRA:



[Se adjunta como **Documento N.º 2** las capturas de los SMS recibidos tanto por el estafador como por BBVA en el mismo hilo de conversación].

D) Desde la apertura de dicha cuenta corriente, esto es en diciembre de 2021, cuyo extracto al que actualmente se puede acceder vía web acompañamos, podemos comprobar que es una cuenta de ahorro, con pocos movimientos y que no se ha utilizado nunca para realizar transferencias superiores a 249 Euros. **Es evidente que la entidad bancaria, cuando cursó la orden, debió constatar la irregularidad que esta conllevaba y valorar el posible fraude, teniendo en cuenta que, mediante dicha transferencia, se descapitalizó totalmente la cuenta de mi representada**, pues debemos tener en cuenta que las entidades bancarias **deben guardar una diligencia cualificada en sus operaciones habida cuenta de su condición de expertas que custodian el dinero de los ciudadanos.**

[Se adjunta como **Documento N.º 3** el extracto de los movimientos realizados desde la apertura de la cuenta bancaria].

E) **En fecha 1 de diciembre, mi mandante interpone la denuncia ante el cuerpo de los "Mossos d'Esquadra" en relación con lo sucedido**. Se ha mantenido informada a la entidad, en todo momento y de forma inmediata del fraude, de la denuncia interpuesta ante los "Mossos d'Esquadra", así como de las reclamaciones realizadas a la entidad bancaria.

[Se adjunta como **Documento N.º 4** la denuncia interpuesta ante el agente del Cuerpo de "Mossos d'Esquadra" con el TIP 22414].

SEGUNDO. – De las reclamaciones previas a [redacted] y la desestimación de las peticiones.

Seguidamente, la parte actora interpuso el día 2 de diciembre, la primera reclamación en la oficina BBVA al SAC (Servicio de atención al cliente de BBVA), con el expediente N.º 9550645, mediante el formulario de reclamaciones que fue facilitado por la propia entidad reclamando la devolución del importe total sustraído.

[Se adjunta como **Documento N.º 5** el formulario de la reclamación presentado el 2 de diciembre de 2022].

El día 14 de diciembre de 2022, se interpuso la segunda reclamación al SAC reclamación que fue desestimada el día el 23 de diciembre de 2022 mediante la resolución N.º 9550645. Dicha respuesta argumenta que la transferencia ha estado validada por un doble factor y que por ello, no pueden atender la petición realizada. Es importante remarcar que **para la autorización de la transferencia se envió un SMS en la cadena de mensajes que habitualmente era utilizada por la entidad bancaria, que fue la misma en la que se**

estaba comunicando el estafador como se puede acreditar en el Documento N.º 2, aportado anteriormente.

> [Se adjunta como **Documento N.º 6** la segunda reclamación realizada al SAC el día 14 de diciembre de 2022].
> [Se adjunta como **Documento N.º 7** la respuesta del SAC del día 23 de diciembre de 2022].

El día 23 de diciembre de 2022, se remitió la correspondiente reclamación al Defensor del Cliente de BBVA, manifestando la inconformidad con la resolución emitida por el SAC y solicitando su revisión, reclamación que fue nuevamente desestimada el día 19 de enero mediante la resolución N.º 9618617. La desestimación se fundamenta en imputar negligencia grave a mi representada.

> [Se adjunta como **Documento N.º 8** la reclamación realizada al Defensor del Cliente de BBVA].
> [Se adjunta como **Documento N.º 9** la respuesta del Defensor del Cliente de BBVA].

TERCERO. - La inexistencia de negligencia grave por parte de mi mandante.

En relación con la respuesta del Defensor del Cliente de [redacted], es importante destacar que elude su responsabilidad alegando que existe negligencia grave por parte de mi mandante.

Pues bien, esto se contradice con la siguiente afirmación que la propia entidad, concretamente en la respuesta del Defensor del Cliente, hace en la pág.9:

> Estamos ante un caso típico de Smshing combinado con Vishing en el que terceras personas, a través de un SMS y una llamada telefónica, suplantan la identidad de una empresa conocida, en este caso BBVA, y con técnicas de ingeniería social para engañar, logran obtener información delicada, personal y sensible para acceder a su cuenta bancaria o realizar operaciones bancarias.

La cuestión es la siguiente: **¿Puede la entidad bancaria determinar que existe negligencia grave por parte de mi mandante cuando esta ha sido suplantada?**

La Audiencia Provincial de Pontevedra en su **Sentencia nº 539/2021, de 21 de diciembre de 2021**, por la que se revoca la Sentencia dictada en primera instancia y se condena a ABANCA a reintegrar a la víctima de un delito de phising las cantidades sustraídas pues, según se afirma, que **el banco no habría conseguido acreditar el cumplimiento de las**

obligaciones de diligencia exigibles tanto para la autentificación de las operaciones de pago como para disponer de la tecnología *antiphishing* precisa para detectar las páginas clonadas de las oficiales propias y cerrarlas o eliminarlas. Correlativamente, aprecia el tribunal que **no puede atribuirse negligencia al usuario que introduce sus claves de acceso en una página idéntica a la oficial de la entidad bancaria, ni siquiera cuando el mensaje contenga pequeños indicadores de su origen fraudulento tales como faltas de ortografía o falta de concreción de la operación auténtica a la que supuestamente se refiere.**

Esta postura judicial se desarrolla con más extensión en los Fundamentos de Derecho.

La jurisprudencia no da lugar a error. Los bancos tienen una responsabilidad cuasi objetiva con los datos de sus clientes. **Solo sería responsabilidad de la víctima en el caso de que existiera negligencia grave**. **Ahora bien, entregar sus credenciales bajo engaños no se considera una negligencia grave según la jurisprudencia actual**. Por ello, el **Tribunal Supremo establece que el phishing es un "engaño bastante" y este tipo de engaños no comprenden la negligencia grave**. Por lo tanto, se considera que el phisher estafa al usuario, que entrega sus claves sin ser consciente de que lo hace a un tercero no autorizado. El banco está obligado a custodiar correctamente las claves, las credenciales y los depósitos de sus clientes y es por ello que en este tipo de estafas denominadas phishing, son los bancos los que están obligados a devolver todo el dinero robado a las víctimas.

Para poder considerar que existe negligencia grave, y atendiendo a la Directiva 2015/2366 expuesta en los Fundamentos de Derecho, en un caso de denuncia por phishing contra la entidad bancaria, se tendrían que dar unas circunstancias similares a las siguientes:

a) Que el cliente pierda los datos personales y de la cuenta bancaria con las credenciales anotadas al lado.

b) Que el diseño de la página web creada por los estafadores sea tan burdo que resulte muy evidente que no se trata de la entidad bancaria.

En el presente caso, nos encontramos con que la entidad ha sido suplantada, que los SMS del estafador le llegaron en la misma cadena de mensajes a través de la cual la entidad [redacted] se comunicaba con su clienta y que, además, la persona que le llamó haciéndose pasar por el Departamento de fraude de [redacted] conocía **datos personales y sensibles de mi mandante. Por todo lo expuesto, no cabe duda que no podemos imputar negligencia grave a Dña. ELVIRA.**

CUARTO. - Falta de diligencia por parte de la entidad.

Conforme al relato fáctico contenido en los anteriores apartados, entendemos que no puede haber lugar a dudas de la responsabilidad y la falta de prevención de la entidad bancaria, [redacted], única causante de que la estafa pudiera conseguir su propósito.

Es así como en la cláusula 5.3 de las Condiciones Generales aplicables a los servicios de pago de [redacted] (Anexo del Documento N. º1) se indica:

> "[redacted] *dispone de sistemas de detección de fraude para la identificación eficaz y rápida de operaciones sospechosas o fraudulentas. En el caso de que estos sistemas detecten una operación que pueda resultar sospechosa de fraude real o de amenazas para la seguridad,* [redacted] ***se pondrá en contacto con el Cliente bien telefónicamente y/o de forma telemática para confirmar la veracidad o el consentimiento real del cliente a la operación concreta y sospechosa.*** *Además,* [redacted] ***podrá enviar al Cliente notificaciones a modo informativo de operaciones de especial relevancia por su cuantía****, o que excedan los límites de la operativa habitual del cliente, etc.*"

Pues bien, el banco no exigió autenticación reforzada de cliente en una operación que por su importe y método debió solicitar, tal y como dispone el articulo 68 del Real Decreto-ley de servicios de pago y otras medidas urgentes en materia financiera. **En este caso, no se llamó telefónicamente para autentificar la operación que suponía la transferencia de la totalidad del dinero existente en la cuenta y además, los SMS para autentificar el pago, le llegaron a mi mandante a través de la misma cadena de mensajes en los que se estaba comunicando el estafador, creando un consentimiento totalmente viciado en mi representada.**

También se alega por parte de BBVA que se envió un correo electrónico, de tipo informativo, a ELVIRA de que se iba a realizar una transferencia de alto importe:

Es así, como podemos corroborar que pese a que la entidad era conocedora de que se realizaba una transferencia de alto importe, no realizó ni una sola llamada para autentificar la operación por otro medio y meramente envió un mensaje informativo.

A todo esto [redacted] le llama: autentificación reforzada.

Así las cosas, la Sentencia número 269/2016, razona que **la entidad es la responsable de velar por la seguridad del acceso al sistema de pago electrónico, ya que era quien *"tenía y disponía de los medios necesarios para detectar y evitar"* los ataques informáticos contra las cuentas de sus clientes.** En un mismo sentido se pronuncia la *Sentencia 107/2018, de 12 de marzo, de la Audiencia Provincial de Alicante* que establece que **la responsabilidad en la banca online es cuasi-objetiva** y **es la entidad bancaria la responsable de implementar las medidas de seguridad oportunas para evitar el fraude y debe responder de las consecuencias de los fallos de seguridad de su sistema.**

Es por ello, que la falta de diligencia por parte de la entidad bancaria no es un perjuicio que tenga que soportar Dña. ELVIRA. **No basta con un comunicado genérico como intenta hacer valer la parte demandada en su respuesta del Defensor del cliente, que obviamente pasa desapercibido, a la hora de introducir el usuario y contraseña al entrar en la aplicación.**

Es importante destacar **la reciente Sentencia 32/2022, de 2 de febrero de 2022**, del Juzgado de Primera instancia de Oviedo, pues se trata de un caso prácticamente idéntico al que nos ocupa y que manifiesta lo siguiente:

> "*Consta acreditado que el actor recibió un SMS en la línea de mensajes del propio Banco, siendo éste el medio de comunicación elegido por la propia demandada para comunicar claves de operaciones. Esto constituye ya, en sí mismo, una clara falta de seguridad de la banca on-line de la demandada puesto que,* ***sin ningún tipo de complicación un tercero no autorizado consiguió introducir un mensaje que derivaba al usuario a una página web en la que debía de introducir unas claves si no quería ver bloqueada su cuenta. La página web a la que se le derivaba era prácticamente idéntica a la de la demandada sin que puede apreciarse ninguna responsabilidad en el actor que, al recibir un mensaje en la forma habitual decidió seguir las instrucciones que allí se le daban para no ver bloqueada su cuenta*****".**

Esta postura judicial se desarrolla con más extensión en los Fundamentos de Derecho.

Es de destacar, además, para valorar la falta de diligencia de la entidad, que la transferencia realizada por mi cliente se realizó a otra persona que la entidad ha podido localizar, nombre que aparece en la respuesta del Defensor del cliente (ya aportada como Documento 8)**,** y

dado que la estafa se comunicó a la entidad de forma inmediata, daba a la entidad un margen de tiempo para retrotraerla y no lo hizo.

Con ello, **deberá ser [redacted] la que, asumiendo su responsabilidad por la falta de diligencia, abone a mi representada la cantidad total de 10.679,57 €.**

A los anteriores hechos, les son de aplicación los siguientes

FUNDAMENTOS DE DERECHO

I.- Capacidad. Ambos litigantes tienen la capacidad procesal suficiente a tenor de lo que disponen los artículos 6 y siguientes de la Ley de Enjuiciamiento Civil (LEC).

II.- Representación. Mi mandante está representado por la Procuradora que suscribe, conforme a lo establecido en el artículo 23 de la LEC.

III.- Jurisdicción. Es competente la jurisdicción civil, conforme a lo dispuesto en el artículo 21.1 de la Ley Orgánica del Poder Judicial y 9 de la LEC.

IV.- Competencia. El Art. 51 de la LEC dispone la competencia de los juzgados de primera instancia del domicilio del demandado cuando se éste es persona jurídica. Concretamente, en este supuesto se formula la demanda ante el Juzgado de primera instancia de Barcelona al ser el lugar donde ha nacido la relación jurídica y surte efectos, al tener la demandada establecimiento abierto al público.

VI.- Legitimación activa. Corresponde a la parte actora por cuanto le corresponde ejercer la reclamación que se postula con esta demanda.

VII.- Legitimación pasiva. Corresponde a la parte demandada.

VIII.- Juicio por el que debe sustanciarse la demanda. El procedimiento se ajustará a los trámites del Juicio Ordinario por reclamarse una cuantía superior a 6.000,00.-€, conforme dispone el artículo 249.2 de la LEC.

IX.- Materiales. En cuanto al fondo del asunto, las partes no discuten la estafa ni el importe de la misma, centrándose la cuestión debatida en la posible responsabilidad de la demandada y del actor en los hechos.

Se ejercita **acción de reclamación de daños y perjuicios,** conforme a los **artículos 41 y ss. del RD Ley-19/2018de 23 de noviembre de servicios de pago y otras medidas urgentes en materia financiera.**

Para analizar si hay negligencia grave por parte de mi representada debemos atender a la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior (LA LEY 20018/2015), en su apartado (72), hace referencia a lo siguiente:

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

Asimismo, la Audiencia Provincial de Pontevedra en su **Sentencia nº 539/2021, de 21 de diciembre de 2021**, se establece que no puede atribuirse negligencia al usuario que introduce sus claves de acceso en una página idéntica a la oficial de la entidad bancaria, pues afirma el tribunal con acierto:

> *"En el phising se usan técnicas de ingeniería social para ganarse la confianza del usuario del instrumento de pago y aprovecharse de los sesgos cognitivos en la toma de decisiones, lo que, en el caso se habría concretado en la simulación del envío a nombre de una entidad de confianza para la usuaria (Correos y Telégrafos), y en el aprovechamiento del sesgo de confirmación por el cual se tiende a favorecer la información que confirma las opiniones que ya se tenían o que resulta consistente con los hechos ya conocidos".*

Asimismo, confirma la **Audiencia Provincial de Alicante en su Sentencia de 12 de marzo de 2018** aclarando que:

> *"1º.) El proveedor de los servicios de pago (la Entidad Bancaria) "debe implementar las medidas necesarias para asegurar la autenticación e identidad del ordenante a la hora de prestar su consentimiento. Por ello y para su ejecución, el banco debe comprobar en todo caso la autenticidad de la orden;*
>
> *2º.) La falsedad de la transferencia (es decir, que el ordenante no sea el titular de la cuenta) es un riesgo a cargo del banco porque, en principio, el deudor sólo se libera pagando al verdadero acreedor por lo que, si el banco cumple una orden falsa, habrá de reintegrar en la cuenta correspondiente las cantidades cargadas.*
>
> *3º.) La responsabilidad en estos supuestos no puede atribuirse directamente al supuesto ordenante de la transferencia por entenderse ésta autorizada al haberse realizado de acuerdo con los sistemas de autenticación del banco. Los sistemas de autenticación se establecen por los proveedores de servicios de pago y si un banco no ha sido capaz de limitar el acceso al canal de banca electrónica no puede pretender que el presunto ordenante víctima de esta práctica fraudulenta sea el único responsable, pues es el banco quien tiene responsabilidad respecto del buen funcionamiento y la seguridad del mismo.*
>
> *4º.) Las medidas de seguridad no solamente están destinadas a proteger la seguridad de las órdenes de pago emitidas por los clientes, sino que su eficacia exonera a las entidades de crédito de su responsabilidad frente a las órdenes de pago no emitidas por sus clientes de tal forma que el incumplimiento de este específico deber de vigilancia da lugar a una responsabilidad por "culpa invigilando" o responsabilidad objetiva por el mal funcionamiento de los servicios de banca electrónica".*

La jurisprudencia es unánime al entender que es el banco quien debe restituir las cantidades sustraídas, como es el caso de la reciente **Sentencia de la Audiencia Provincial de Pontevedra – Sección 6 Vigo, de fecha 7 de abril de 2021**, donde se condena a [redacted], S.A. a que pague a la actora recurrente la suma de 19.632 euros, en un caso muy parecido al presente.

La Sentencia de la Audiencia Provincial de Madrid de 4 de mayo de 2015, **en un caso similar al que nos ocupa, condenó a Cajamar a abonar a la víctima la cantidad de 17.390'35€ a pesar de que ésta había facilitado sus claves, dado que lo hizo a través de una página web clonada que simulaba ser la del banco.** La sentencia razona que el artículo 31 de la Ley 16/09 de 13 de noviembre de Servicios de Pago establece un sistema de responsabilidad cuasi objetiva de la entidad proveedora del servicio de pago con inversión de la carga

probatoria y que **no se ha acreditado que el sistema fuese seguro, puesto que, de hecho, terceros ajenos, consiguieron introducir un mensaje en la línea habitual de SMS con los que el banco se comunicaba con el cliente**.

Reiterada jurisprudencia, como hemos podido ver, confirma que es la prestadora de los servicios de pago quien tiene la obligación de facilitar un sistema de banca telemática segura, y **no son sus clientes los que deben prevenir ni averiguar las modalidades de riesgos que el sistema conlleva, ni prevenir con un asesoramiento experto los mismos, ni objetar que el usuario debía conocer aspectos técnicos tales como identificar una web como falsa, cuando además esta no consta que fuera burda y por tanto, evidente de toda falsedad.**

X.- Cuantía. La cuantía del procedimiento se fija en la cantidad de **DIEZ MIL SEISCIENTOS SETENTA Y NUEVE (10.679,57) EUROS.**

XI.- Costas. Es de aplicación el artículo 394 de la LEC, en cuanto a la condena en costas en primera instancia y la mala fe procesal.

XII.- Cuantos otros resulten de aplicación en virtud de los aforismos "*Iura Novit Curia*" y "*Narra mihi factum, dabo tibi ius"*, actualmente positivizados en el artículo 218.1, segundo párrafo, de la LEC.

En su virtud,

AL JUZGADO SE SOLICITA: Tenga por presentado este escrito, junto con los documentos acompañados, los admita, y tenga por interpuesta, en nombre de **ELVIRA** [redacted], demanda de **JUICIO ORDINARIO** contra la parte demandada referida en el encabezamiento de este escrito, la emplace al objeto de que comparezca si a su derecho conviene y tras los trámites correspondientes, dicte Sentencia por la que:

1) **Se condene al pago a** [redacted], por los daños y perjuicios sufridos por mi representada, de la cantidad de **DIEZ MIL SEISCIENTOS SETENTA Y NUEVE CON CINCUENTA Y SIETE (10.679,57) EUROS**, en concepto de principal, más intereses y costas.

Barcelona, a 2 de marzo de 2023.

Mònica [redacted]
ICAB N.º 46689

Inés Casado Güell
Procuradora de los Tribunales