DEFENSOR DEL CLIENTE
[redacted]

[redacted] 61- 8º Dcha.
28003 Madrid
Teléfono [redacted] Fax [redacted]
Email: [redacted]
[redacted] 28080 Madrid

Madrid, 8 de febrero de 2023

Sra. Dª. [redacted]
[redacted] BARCELONA

N/ Ref.: [redacted]/22

Muy Sra. mía:

En relación con la reclamación que tiene interpuesta contra Bankinter, en el escrito que motivó la apertura del expediente de referencia, cúmpleme manifestarle lo siguiente:

Expone que, el día 05.09.2022, recibió en su móvil un mensaje sms, desde un numero perteneciente a Bankinter, informándole de una compra de 986,45€ efectuada con su tarjeta de crédito e indicándole que si no había realizado la misma accediera a un enlace que se le adjuntaba para anularla.

Indica que, al acceder al enlace, le resultó sospechosa la página a la que se le dirigió, dada la naturaleza de los datos que le solicitaba, por lo que salió de la misma sin facilitar ningún dato, entrándole en eses mismo momento una llamada desde otro número perteneciente a la banca telefónica de Bankinter, para indicarle que había sospechas de un posible fraude en su tarjeta por importe de 6.900€ motivada por una compra de criptomonedas. Ante tal información, respondió Vd. que no había efectuado tal compra y que le explicara como anular tal operación, para lo cual le pidió que se identificara siguiendo el protocolo, con su número de DNI su código de acceso a Banca telefónica, indicándole que debía acceder a la aplicación móvil para poder hacer la anulación (lo que efectuó por identificación facial), cortándose en ese momento la llamada.

Llamó Vd. al mismo número de teléfono y explicó lo acontecido a la persona que le atendió, que le informó que Bankinter no había realizado la llamada y que efectivamente aparecía una compra de 6900€ (la tarjeta tiene un crédito de 7000€, por lo que las personas que cometieron la estafa sabían el límite disponible de la tarjeta, ya que en ese momento estaba dispuesta en 90€).

Solicita la intercesión de este Defensor del Cliente para que la Entidad la retroceda la totalidad de la cantidad defraudada, entregándole así mismo la documentación mercantil bancaria acreditativa del autor o autores de los hechos y del modus operandi utilizado para apoderarse de su dinero.

Recabada la preceptiva información de la Entidad reclamada, por su departamento de Servicio de Atención al Cliente se emite informe que, entre otros particulares, manifiesta lo siguiente:

"Por lo que se refiere al asunto que nos ocupa cabe señalar en primer término que en fecha 6 de julio de 2006 la Sra. [redacted] suscribió con Bankinter Consumer Finance una tarjeta de crédito Siempre, sin que exista discrepancia entre las partes sobre esta cuestión.

Dado que nos encontramos ante un contrato de duración indefinida, en virtud de las facultades que les son otorgadas por la normativa actualmente vigente a las entidades financieras, y con el fin de adaptarse a lo establecido por la actual normativa sobre servicios de pago, en fecha febrero de 2021, Bankinter remitió a la hoy reclamante un aviso de cambio de condiciones y una modificación de condiciones del contrato , que acompañamos, siendo éste el que le es de aplicación a las operaciones que ahora constituyen el objeto de su reclamación.

Si examinamos el movimiento reclamado con la autorización del cargo proporcionado por la empresa Redsys (pasarela de pagos de las entidades de crédito, que adjuntamos, observamos que efectivamente el día 5 de septiembre de 2022 fue efectuado un cargo por importe de 6.900 euros, del que resultó beneficiario el comercio VOL/SAFECURRENCY.COM, habiendo bloqueado nuestro cliente su tarjeta día 5 de septiembre de 2022 a las 12:51:18 horas tal como se acredita mediante la captura de pantalla que aportamos.

Por lo que se refiere a las obligaciones de nuestro cliente, manifestamos que éstas han de regirse por lo establecido en la actual normativa sobre servicios de pago, constituida por el Real Decreto Ley 19/2018 de 23 de noviembre.

Del análisis de la normativa es importante recordar que el artículo 41 del referido texto legal impone al cliente un deber de custodia de su tarjeta y de confidencialidad de las credenciales personalizadas de la misma (número PAN, caducidad, CVV y código PIN), estableciendo el artículo 46 .1 que el usuario de servicios de pago responderá de la

totalidad de los cargos efectuados si actúa con negligencia grave, siendo esta obligación también recogida en las condiciones de la tarjeta en vigor que han sido aportadas.

Así pues, para delimitar cual debe ser la responsabilidad soportada por cada una de las partes, se hace necesario analizar las circunstancias particulares del caso concreto de la Sra [redacted].

De la lectura del escrito de Denuncia de reclamación de nuestra cliente observamos que la propia Sra. [redacted], manifiesta que el día 5 de septiembre de 2022, recibió en su teléfono móvil un sms de Bankinter, informándole que se había realizado una compra por importe de 986,45 euros y que si no había sido ella la autora que entrase en un enlace para cancelarla, que el sms lo recibe desde un número de teléfono donde la entidad le ha mandado anteriormente un sms de confirmación de compra, que recibe una llamada del teléfono [redacted], y que el operador que le contestó le dio todos los datos de ella correctos por lo que no sospecho que seria un fraude.

De la narración de los hechos, resulta evidente la Sra. [redacted] actuó de manera negligente dado que proporcionó todos los datos de su tarjeta y también ejecutó, por ello, consideramos que se cumplen los requisitos establecidos en el contrato mencionado para que nuestro cliente se haga responsable de la totalidad del cargo objeto de su reclamación.

En cuanto al hecho que nos indica que recibió una llamada de una persona que se hizo pasar por empleado de Bankinter y desde un teléfono de Bankinter, informamos a ese Defensor que nuestra entidad se ha puesto en contacto con las principales compañías telefónicas que operan en España, respecto a esta situación, habiéndonos sido comunicado que ellas no pueden hacer nada, tanto en lo que se refiere al envio de mensajes, como en llamadas recibidas supuestamente desde números que pertenecen a nuestra entidad. Asimismo, es importante destacar que el número del teléfono indicado por la reclamante, desde el que afirma que recibió la llamada telefónica, es un número de Bankinter que únicamente está habilitado para recibir llamadas, pero no para emitirlas.

Recordar por otra parte que, tal y como está recogido en la web, en Bankinter nunca le solicitaremos sus claves de acceso o de firma de operaciones, o cualquier otro dato que ya poseamos en nuestro conocimiento, ni por correo ni por otra vía. Ante cualquier duda al respecto debe comunicarse inmediatamente en contacto con Banca Telefónica, bloquear sus tarjetas de crédito/débito a través de nuestra web/app en el apartado de tarjetas.

*Por otra parte, en lo que se refiere al deber de autenticación reforzada que es exigido a las entidades financieras por la normativa sobre servicios de pago actualmente vigente, si analizamos la información contenida en el epígrafe "punto de servicio" presente en el documento de autorizaciones aportado, observamos que la operación no se llevó a cabo marcando el PIN de la tarjeta, sino a través de la denominada **firma biométrica**, que se realiza mediante la introducción de la huella dactilar o del reconocimiento facial en el terminal móvil del cliente (identificación que, de las propias manifestaciones de la reclamante, reconoce la misma haber efectuado).*

Así las cosas, por lo que se refiere a este caso concreto, y según se acredita mediante los documentos denominados huella digital y movilidad que adjuntamos, Bankinter le remitió a su teléfono móvil [redacted] que es el mismo que ella indica como suyo en su denuncia, el enlace para acceder a la pasarela de pagos de nuestra entidad. Tras acceder al mismo, la cliente se le solicitó que introdujese en su terminal su firma biométrica (huella dactilar o reconocimiento facial) para autenticar la operación, cosa que ésta hizo, procediendo con ello a confirmar la operación, habiendo cumplido nuestra entidad el deber de autenticación reforzada mencionado."

Pues bien, expuestas las alegaciones de ambas partes, con carácter previo debo indicar a las mismas que los elementos fácticos que este Defensor tiene que tomar en consideración para emitir su resolución son, únicamente, los acreditados por medios probatorios fehacientes y/o documentales, carácter que no tienen las meras manifestaciones de las partes, salvo que las mismas fueran reconocidas por una de ellas en lo que le afecta, o los hechos fueran ratificados por ambas.

En este sentido se ha manifestado en reiteradas ocasiones el Banco de España, a través de su Departamento de Conducta de Mercado y Reclamaciones (DCMR), al manifestar en la pág. 116 de la Memoria del año 2009, así como en otras posteriores, lo siguiente:

*"...Este Servicio, cuando atiende las reclamaciones que sobre materias de su competencia le presentan los clientes de las entidades sujetas a la supervisión del Banco de España, estudia el asunto que se expone, recaba información al respecto de la entidad objeto de la reclamación, y **emite un informe al reclamante ciñéndose exclusivamente a la documentación aportada al expediente**. En consecuencia, cuando ambas partes mantienen versiones distintas acerca de lo sucedido, sin respaldo documental suficiente, este Servicio de Reclamaciones no puede hacer prevalecer una versión en detrimento de la otra, debiendo los interesados someter su controversia, en su caso y de estimarlo oportuno, a conocimiento y resolución de los tribunales de justicia, únicos que, mediante la práctica de las pruebas que estimen oportunas, pueden determinar, sin ningún género de duda, cómo acaecieron los hechos y establecer las consecuencias que de los mismos deban derivarse para los interesados."*

Expuesto cuanto antecede, cabe indicar a la reclamante que el ámbito competencial de este Defensor, se restringe exclusivamente a examinar si la Entidad reclamada ajustó o no su actuación a

las previsiones previstas en el contrato de tarjeta y en la normativa de servicios de pago, constituida por el Real Decreto-ley 19/2018, de 23 de noviembre (RDLSP).

Por tanto, no le corresponde a este Defensor del Cliente constatar cómo acontecieron realmente los hechos (es decir, el procedimiento utilizado por los defraudadores), entendiendo que, la determinación indubitada de tales hechos excede del ámbito competencial de este Instituto, correspondiendo su indagación o averiguación a las autoridades policiales.

Establece el art. 44.1 del mencionado Real Decreto-ley, lo siguiente:

*"1. Cuando un usuario de servicios de pago niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, **corresponderá al proveedor de servicios de pago 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 por el proveedor de servicios de pago."*

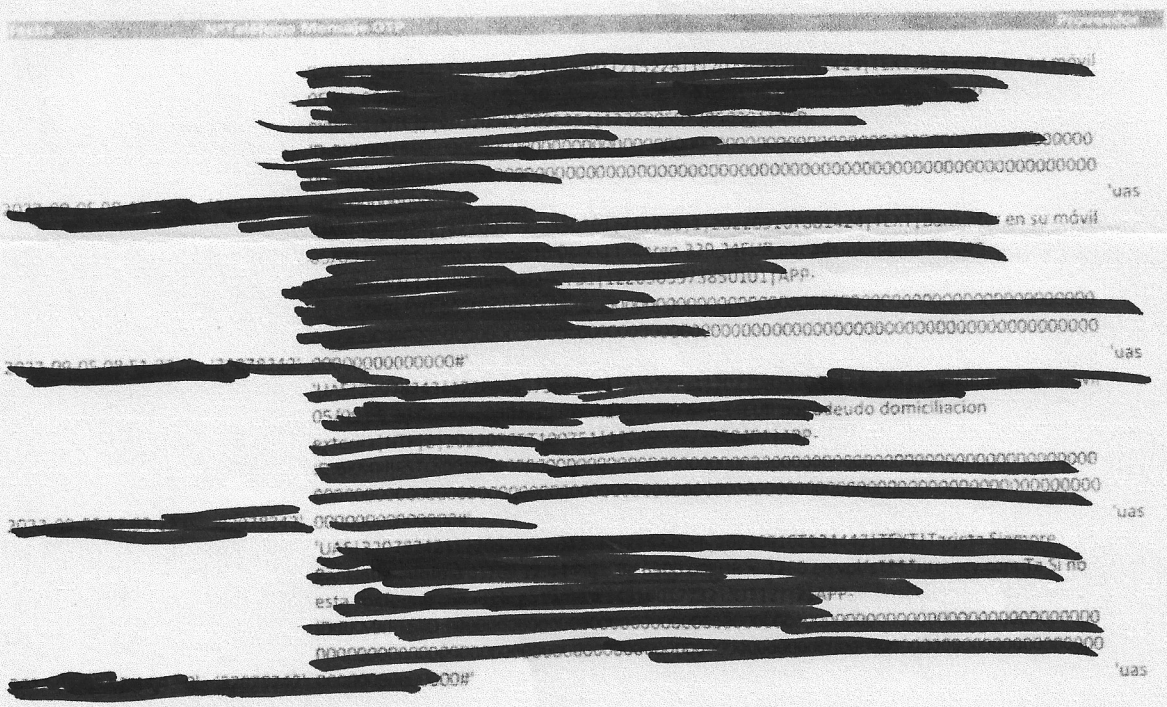
En consecuencia, pesa sobre la Entidad reclamada la carga de probar que la operación de pago impugnada fue autenticada (en este caso, la autenticación debe ser reforzada), registrada con exactitud y contabilizada.

Define el art. 3.5 del RDLSP, la autenticación reforzada de la siguiente forma:

"5. Autenticación reforzada de cliente: 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."

A tal efecto, indica la Entidad que cuando se solicitó efectuar la transacción que se reclama, una vez comprobada por la Entidad que la tarjeta pertenecía a la reclamante (tarjeta[redacted]) y que tenía límite disponible para llevarla a cabo, procedió a remitir al teléfono móvil de la Sra[redacted] un mensaje sms, en el cual le comunicaba la necesidad de autorizar la operación a través de la web de la Entidad.

En apoyo de lo indicado, aporta la Entidad documentación denominada "movilidad" que se reproduce a continuación:



BANCOS ADHERIDOS:
Bankinter, Credit Suisse, Deutsche Bank, Gespensión Caminos, March, Open Bank, Sabadell, Santander, Santander Consumer, UBS

DEFENSOR DEL CLIENTE

[redacted]

[redacted] Madrid

[redacted] 28080 Madrid

El examen del documento reproducido, en el cual la Entidad fundamenta haber efectuado la autenticación reforzada de la reclamante y de la operación reclamada, pone de manifiesto lo siguiente:

1) A tenor de la documentación aportada por Redsys (pasarela de pagos de la Entidad reclamada), la fecha de grabación de la operación fue el 05.09.2022 a las 12:44 horas.autorización a la operación.

2) Del documento denominado "movilidad" antes reproducido, se desprende:

a) Que no consta que el "Mensaje OTP" que el Banco manifiesta haber enviado a la reclamante (*con anterioridad* a la transacción), se efectuara al móvil de la misma.

Como consta en la denuncia policial de los hechos y en la última versión del contrato de tarjeta aportada por la Entidad, el teléfono móvil de la reclamante era el [redacted]. Sin embargo, en el documento reproducido se indica que el móvil al que se remitió el sms era el [redacted] (numero éste que, a juicio de este Defensor, no se corresponde con un "móvil" ni tampoco coincide con el de la Sra. [redacted]

b) El mensaje fue remitido a las 12:44 hs., coincidente con la indicada en el ordinal 1 anterior. El examen del documento pone de manifiesto que el sms anterior fue remitido a las 08:53hs., no guardando relación alguna con el presente incidente. Y con posterioridad a las 12:44 hs. no consta enviado ningún mensaje, posiblemente porque la tarjeta se canceló a las 12:51hs (según pantallazo aportado).

c) Que el mensaje supuestamente remitido a la reclamante (según afirmaciones de Bankinter), indicaba lo siguiente: *"Tarjeta Siempre Bankinter informa 05/09 12:44* ***Pago*** *de 6900,00EUR n. 1280 en vol/s***urrency.com Ta* (1280 son los 4 últimos dígitos de la tarjeta; vol/safecurrency es el comercio; Ta (Tallín-Estonia). ***Si no está conforme con el cargo*** *llame a [redacted]".*

Claramente se infiere del mensaje que se comunicaba un pago ya realizado con cargo a la tarjeta y que NO se solicitaba a la reclamante su previa autorización al mismo, manifestándole simplemente que de no estar de acuerdo con el cargo (efectuado ya en la tarjeta) lo manifestara a determinado telefono.

Por tanto, a la vista de la propia documentación aportada por la Entidad, no ha quedado acreditado lo manifestado por la misma en su informe cuando afirma que *"Bankinter le remitió a su teléfono móvil [redacted] que es el mismo que ella indica como suyo en su denuncia, el enlace para acceder a la pasarela de pagos de nuestra entidad. Tras acceder al mismo, la cliente se le solicitó que introdujese en su terminal su firma biométrica…"*

En consecuencia, al no quedar acreditada la autenticación reforzada de la transacción impugnada, **procede acoger la presente reclamación, debiendo la Entidad retroceder a la reclamante, a la mayor brevedad, los 6.900€ reclamados.**

Le saluda atentamente.