

- Expediente N.º: EXP202203918

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes:

HECHOS

PRIMERO: Con fecha 3 de marzo de 2022, se presentó reclamación ante la Agencia Española de Protección de Datos contra BANCO BILBAO VIZCAYA ARGENTARIA, S.A. con NIF A48265169 (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

En fecha 27 de agosto de 2021, la entidad reclamada activa una tarjeta de débito asociada a los datos de la reclamante y envía dicha tarjeta a un domicilio desconocido de un tercero, el cual valiéndose de dicha tarjeta, realiza varias extracciones de dinero de la cuenta de la reclamante, a través de un cajero. Tras lo ocurrido, en fecha 3 de septiembre de 2021, presenta reclamación ante el departamento de fraude y ante el defensor del cliente, le indican que han bloqueado la tarjeta controvertida y manifiesta que recibe respuesta indicando que su reclamación se ha resuelto desfavorablemente, reiterando su reclamación al no estar conforme con dicha respuesta, puesto que considera que se ha realizado un tratamiento de datos sin su consentimiento, no habiendo cumplido dicha entidad con las adopción de medidas adecuadas de seguridad. Asimismo, presenta reclamación ante el delegado de protección de datos (el 3 de diciembre de 2021) y recibe respuesta, en fecha 13 de enero de 2022, indicando que dichas cuestiones deben resolverse por parte del servicio de atención al cliente y no en ese buzón. En fecha 25 de octubre de 2021, recibe respuesta del servicio de atención al cliente (en relación con la devolución de los importes cobrados indebidamente), siendo de nuevo desfavorable la reclamación formulada, indicando la entidad que "no existe falsificación al estar efectuadas las transacciones con lectura del chip/plástico original y verificación de PIN". Por otro lado, en las reclamaciones telefónicas efectuadas, la entidad reclamada indica a la reclamante que han comprobado que "hay movimientos extraños en los registros de la conexión IP registrados por la entidad, por lo que consideran realizar un bloqueo del usuario" de la parte reclamante, no pudiendo esta, por tanto, acceder a su área de cliente a través de la web ni de la App. Aporta número de tarjeta controvertida, fecha de su activación y domicilio a la que se remitió (información que fue facilitada telefónicamente por la entidad reclamada), intercambio de e-mails con el delegado de protección de datos, número de referencia facilitado a su reclamación, e-mail de reclamación (de fecha 3 de diciembre de 2021), respuesta de la entidad (de fecha 13 de diciembre de 2021) indicando que se ratifican en lo ya manifestado en una respuesta anterior y escrito de fecha (14 de enero de 2022) reiterando su disconformidad.

Junto a la notificación se aporta:

- Escrito enviado por el SAC de la parte reclamada a la parte reclamante el día 13 de diciembre de 2021 en el que se le indica que ha recibido su escrito del

día 3 de diciembre de 2021 y que se ratifican en la respuesta que se le facilitó previamente. Asimismo, se le señalan los pasos a seguir si no está conforme con la resolución de su reclamación.

- Reclamación presentada por la parte reclamante el día 3 de diciembre de 2021, dirigida al Servicio de Atención al Cliente (SAC) y al Defensor del Cliente de la parte reclamada.
- Email enviado por el delegado de protección de datos de la parte reclamada (*****EMAIL.1**) a la parte reclamante el día 13 de enero de 2022, como contestación al email que previamente remitió la parte reclamante el día 12 de enero de 2022, en el que se le indica que debe facilitarle respuesta el Servicio de Atención al Cliente de la parte reclamada.
- Escrito enviado por la parte reclamante a la parte reclamada el día 14 de enero de 2022 en contestación al email recibido por ésta el día 13 de enero de 2022, señalando que no está conforme con la resolución del caso.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGD), se dio traslado de dicha reclamación a la parte reclamada/ALIAS, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 20 de abril de 2022, como consta en el acuse de recibo que obra en el expediente.

Con fecha 23 de mayo de 2022 se recibe en esta Agencia escrito de respuesta indicando lo siguiente:

- Descripción detallada y cronológica de los hechos:

La parte reclamada adjunta la denuncia presentada por la parte reclamante ante la Dirección General de la Policía (en adelante, DGP). En esta denuncia, se señala lo siguiente:

*“COMPARECE: En calidad de DENUNCIANTE, quien mediante DNI nº *****NIF.1**, acredita ser **A.A.A.**, país de nacionalidad ESPAÑA, mujer, nacida en Burgos, el día 07/07/1972, hija de Barlaan y Laurentina, con domicilio en Calle *****DIRECCIÓN.1**, de *****LOCALIDAD.1**, teléfono *****TELÉFONO.1**, y;*

[...]

*Que denuncia el fraude informático que se detallan a continuación entra las 23:47 horas, del día 03/09/2021 y las 00:04 horas, del día 04/09/2021, en Calle *****DIRECCIÓN.1** de *****LOCALIDAD.1**.*

[...]

Que manifiesta haber sufrido un fraude vía telemáticamente ya que el dicente manifiesta haber recibido dos cobros que no reconoce.

*Que la denunciante manifiesta que todo comenzó el día 27 de agosto cuando recibe a su correo un precontrato de servicio de pago de una tarjeta bancaria con nº *****TARJETA.1** que desconoce.*

Que la dicente no ha solicitado esa tarjeta, sin darle más importancia a este hecho ya que no ha recibido ninguna tarjeta física y por lo tanto no da cuenta de lo sucedido.

Que el día 3 de septiembre a las 23:47 horas recibe notificación en su teléfono móvil de un cargo de 2000 euros, produciéndose el mismo cargo por el mismo importe pocos minutos después, siendo esto el día 4 de septiembre a las 00:04 horas.

*Que la dicente procede a entrar en la App del banco *****BANCO.1** donde le aparece una nueva tarjeta asociada a su cuenta, con nº *****TARJETA.2**, de la cual desconocía.*

Que los cobros de un total de 4000 euros se producen desde la tarjeta mencionada, procediendo inmediatamente a su bloqueo.

*Que seguidamente la denunciante se pone en contacto con el banco *****BANCO.1** para que le den datos sobre esta situación, informándole de que los cargos se han retirado de un cajero *****BANCO.1** de *****LOCALIDAD.2** Avda. *****DIRECCIÓN.2**.*

*Que el banco le indica que esta tarjeta se activó el 27 de agosto y fue enviada a la dirección C/ *****DIRECCIÓN.3** de *****LOCALIDAD.3**.*

[...]

Que PREGUNTADA si ha facilitado la numeración de la tarjeta a terceras personas mediante email, Whatsapp, Facebook, etc., RESPONDE que: No.

Que PREGUNTADA por el uso que se le da habitualmente a la tarjeta RESPONDE que: un uso normal, en establecimientos, bares y lugares similares.

[...]

Que PREGUNTADA si en este acto la tarjeta todavía obra en su poder RESPONDE que: No, ya que la tarjeta nunca la recibió, ni solicitó.”.

Que PREGUNTADA si ha accedido a la página web de su entidad bancaria a través de enlace recibido por correo electrónico o redes sociales RESPONDE que: No, solamente a través de la aplicación instalada en su dispositivo móvil.

[...]”.

La parte reclamada adjunta un pantallazo con un email enviado por la parte reclamante (*****EMAIL.2**) a la parte reclamada (*****EMAIL.3**) el día 18 de octubre de 2021 informando sobre los hechos denunciados.

Asimismo, la parte reclamada adjunta un documento (Documento nº 2) con la comprobación realizada por su Servicio de Atención al Cliente (en adelante, SAC) del diario del cajero desde el que se realizaron las dos operaciones denunciadas, comprobando que *“ambas disposiciones de efectivo se habían realizado con la tarjeta original e informando del número Pin”*.

Se adjunta otro documento (Documento nº 3) con la comunicación enviada desde el SAC de la parte reclamada a la parte reclamante del día 25 de octubre de 2021 informando que:

“las operaciones están realizadas sin que exista ningún tipo de falsificación, al estar efectuadas con lectura del chip / plástico original y verificación de Pin.

Por ello le comunicamos que lamentablemente en esta ocasión no, nos es posible atender favorablemente su petición, quedando desde este Servicio de Atención al Cliente a su disposición para cualquier aclaración adicional al respecto si lo considera oportuno.

*Si usted no está conforme con la resolución de esta reclamación, puede solicitar su revisión por el Defensor del Cliente del Grupo *****BANCO.1**, en la dirección de correo electrónico: defensordelcliente@bva.com [...]”*.

Se adjunta otro documento (Documento nº 4) con un email enviado por la parte reclamante al Defensor del Cliente de la parte reclamada y con copia a tres empleados de la parte reclamada el día 24 de marzo de 2022, siguiendo los pasos indicados por el SAC, al no estar de acuerdo con la resolución. En el email, la parte reclamante indica:

*“Les adjunto de nuevo la carta de 25 de octubre de Atención al Cliente *****BANCO.1** (caso *****CASO.1**) cuya resolución no es la correcta. En ella indica que se ha hecho un uso sin falsificación de la tarjeta a la que se hace referencia y no es la veracidad de los hechos. Los “malos” han utilizado mis credenciales para entrar en la banca online, han solicitado una tarjeta que han enviado a una dirección, han utilizado y cambiado mis datos y han extraído 4000€ de mi cuenta. Todos estos hechos nos los he realizado yo que soy el cliente, ni he tenido conocimiento de ello hasta que se cometió el fraude. [...]”*

El día 7 de abril de 2022, el Defensor del Cliente de la parte reclamada comunica a la parte reclamante que se ha resuelto favorablemente su solicitud y que en el plazo de unos días le será reintegrado el importe reclamado, según se indica en el documento adjunto (Documento nº 5):

“A este respecto, le informamos que, analizados de nuevo los hechos objeto de su reclamación, las condiciones concretas de las obligaciones asumidas por las partes y sus particulares circunstancias, desde este Servicio hemos procedido de manera

favorable, por lo que en los próximos días se procederá al abono del importe de 4.000 euros, objeto de su reclamación”

Por último, el día 28 de abril de 2022 la parte reclamada traslada a la parte reclamante la contestación a la reclamación trasladada desde esta Agencia (Documento nº 6):

*“Nos dirigimos a usted en relación al escrito que envió a esta entidad con fecha 21 de abril de 2022, a través de la Agencia Española de Protección de Datos, Su número de referencia es 8890748.
[...]*

*En este sentido, le informamos que hemos comprobado que con fecha 7 de abril de 2022 han sido abonadas en su cuenta nº *****CUENTA.1** las cantidades reclamadas por usted, por un importe total de 4.000 €”.*

- Medidas de seguridad adoptadas y otra información relevante:

La parte reclamada indica lo siguiente:

*“Dentro de las condiciones de uso de la Banca Online de *****BANCO.1** se incluye el apartado Responsabilidad de *****BANCO.1**, donde se describen aquellos casos en los que el cliente/usuario debe ser especialmente cuidadoso con el estado de sus dispositivos y los sistemas antivirus que tiene instalados en los mismos, no siendo responsable el Banco de los daños y perjuicios causados al usuario, que se ocasionan por las vulnerabilidades en sus sistemas y herramientas.*

De igual manera, la entidad realiza iniciativas de concienciación a los clientes en los distintos canales disponibles.

Como muestra de ello, tenemos la campaña lanzada para clientes el 9 de junio de 2021, por la que se publicó en la web del Banco, un artículo titulado “Qué es el spoofing y que tipos hay”.”

La parte reclamada adjunta pantallazos del artículo “Qué es el spoofing y que tipos hay” con las variantes de este tipo de ciberataque, así como de consejos a sus clientes en materia de seguridad digital.

TERCERO: Con fecha 26 de mayo de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

El día 22 de junio de 2022 se envió un requerimiento de información a la parte reclamada que fue contestado el día 19 de julio de 2022.

La contestación dada por la parte reclamada contiene los siguientes puntos:

1. Acreditación del motivo por el que se emitió dicha tarjeta a nombre de la parte reclamante. En caso de que la emisión fuera a solicitud de la parte reclamante, aportar acreditación de dicha solicitud.

Sobre este punto, la parte reclamada señala lo siguiente:

*“Se acompaña a efectos de acreditar la contratación de la tarjeta *****TARJETA.3** (TARJETA AHORA *****BANCO.1**) el 27/08/2021 a las 11:18:00 (GMT +2), por el usuario de Banca Online **XXXX-***NIF.1** que corresponde con la reclamante, el informe GF.12410 de Trazabilidad realizado por Global Forensics – eDiscovery el 15 de julio de 2022 (Documento nº 1).”*

En dicho Documento nº 1 se adjunta un pantallazo de la ficha de cliente registrada en los sistemas de la parte reclamada donde, entre otros datos, se puede observar su nombre, apellidos, NIF y domicilio (mismos datos que los aportados por la parte reclamante en su denuncia ante la DGP).

También se aporta pantallazo de los sistemas de la parte reclamada con el detalle del contrato de la tarjeta contratada el día 27/08/2021, tarjeta terminada en 5191 (número de contrato *****CONTRATO.1**) con la que se realizaron los reintegros reclamados en cajero automático.

Asimismo, se aportan trazas informáticas de la contratación de la tarjeta (número de contrato *****CONTRATO.1**) por la parte reclamante el día 27/08/2021 a las 11:18 horas (GMT +2) a través de la Banca a Distancia Web. El mecanismo de autenticación fue mediante usuario y contraseña.

Otra traza informática aportada se corresponde con la modificación de los límites de la tarjeta (número de contrato *****CONTRATO.1**), también a través de la Banca a Distancia Web y mediante autenticación con usuario y contraseña.

En cuanto a los canales de comunicación con la parte reclamada registrados en los sistemas de la parte reclamada, ésta adjunta pantallazo de sus sistemas con fecha de actualización de 15/02/2021 donde figura el teléfono móvil (*****TELÉFONO.1**) y la dirección de correo electrónico (*****EMAIL.2**), mismo número de teléfono móvil que el indicado por la parte reclamante en su denuncia ante la DGP y misma dirección de correo electrónico que se puede observar en las mensajes intercambiados por correo electrónico entre la parte reclamante y la parte reclamada con motivo de los hechos reclamados.

En cuanto a las comunicaciones mantenidas por la parte reclamada con la parte reclamante con motivo de la contratación de la tarjeta con la que se hicieron los reintegros reclamados en cajero automático, la parte reclamada adjunta pantallazos de las siguientes comunicaciones:

- “Información contractual Firma Digital Consumo” enviada por correo electrónico a la dirección de correo electrónico de la parte reclamante (*****EMAIL.2**) el día 27 de agosto de 2021 a las 11:17 horas.

En este caso, hay que señalar que la parte reclamante reconoció la recepción de este correo electrónico en la denuncia que presentó ante la DGP.

- “Envío del PIN de la tarjeta al cliente” enviada mediante SMS al número de teléfono **XXXX***TELÉFONO.1** (mismo número de teléfono que el aportado por la parte reclamante en su denuncia ante la DGP) el día 27/08/2021 a las 20:14 horas. Se adjunta el mensaje enviado a la parte reclamante: “El PIN de la tarjeta *XXXX es \$_DATA0001. ACTIVALA en la App *****BANCO.1**. Por seguridad borra este mensaje”.

Con esta información, la parte reclamada también contesta al punto cinco del requerimiento de información en el que se pedía la información que conste en sus sistemas sobre el envío del código pin de dicha tarjeta por SMS donde figure la fecha, hora, número de teléfono y datos identificativos del destinatario de dicho código pin.

Por otro lado, la parte reclamada hace referencia al comentario de la parte reclamante en su escrito de reclamación presentada ante el SAC y Defensor del Cliente de la parte reclamada el día 03/12/2021 en el que señalaba lo siguiente:

*“Con fecha 27 de septiembre¹ Dña. **A.A.A.** recibe un email con un borrador de contrato de tarjeta con asunto “Antes de firmar, revisa la documentación de Contratación de tarjetas” Documento Nº 1. En este sentido, la Sra. **A.A.A.** contacta con su sucursal para informar que ha recibido dicho contrato suponiendo que el contrato corresponde a la tarjeta número *9808, e informa que la dirección no es correcta y que ya dispone de la tarjeta física *9808 no procediendo a su firma. También informa a la sucursal que ha recibido un SMS de suspensión de cuenta. El agente que la atiende la comunicación responde indicando que no tiene importancia que la dirección no sea incorrecta y que el SMS corresponde a actualización del DNI”*

En contestación a un segundo requerimiento de información enviado el día 22 de julio de 2022 a la parte reclamada que fue contestado por ésta el día 9 de agosto de 2022, ésta hace referencia a la práctica llevada a cabo por los ciberdelincuentes mediante el envío masivo de SMS para recabar datos de los clientes de banca con el objetivo de obtener sus credenciales de acceso a la banca online. Asimismo, la parte reclamada señala que “no envió ningún SMS a la Sra. **A.A.A.** indicando que se había producido la suspensión de su cuenta”.

Asimismo, se puede derivar de ello, dado que la parte reclamante recibió un SMS, que no se llevó a cabo un duplicado de tarjeta SIM no autorizado por la parte reclamante puesto que, en este caso, su terminal móvil hubiera dejado de operar normalmente.

1. Copia de la documentación que acredite la contratación de dicha tarjeta por la parte reclamante.

1

La parte reclamada adjunta un documento (Documento nº 2) con la información precontractual y el contrato de la tarjeta con la que se realizaron los reintegros reclamados en cajero automático.

En cuanto a los datos personales de la parte reclamante que figuran en la documentación contractual, destaca la dirección (Calle *****DIRECCIÓN.3**, *****LOCALIDAD.3**, *****LOCALIDAD.1**), dirección distinta a la indicada por la parte reclamante en su denuncia ante la DGP. Por otro lado, el nombre y el NIF sí se corresponden con los que aportó la parte reclamante en su denuncia ante la DGP.

Como se indica más adelante, este contrato figura firmado por la parte reclamante mediante firma electrónica (clave OTP enviada por SMS al número de teléfono móvil facilitado por la parte reclamante en su denuncia ante la DGP) con motivo de su solicitud a través del canal Banca a Distancia Web el día 27/08/2021 a las 11:18 horas.

2. Información que conste en sus sistemas de dónde (dirección postal) y en qué fecha se envió dicha tarjeta. En caso de que la tarjeta fuera recogida personalmente, aportar copia del recibí.

Sobre este punto, la parte reclamada indica:

*“El 27/08/2021 se modificó el domicilio de correspondencia por:
Calle *****DIRECCIÓN.1**
*****LOCALIDAD.1**, España
CP: XXXX”*

Además, sobre este punto, adjunta pantallazo de sus sistemas con el histórico de modificaciones de los datos de la parte reclamante donde se indica que se produjo un cambio en el domicilio fiscal de la misma ese día 27 de agosto de 2021.

En contestación al segundo requerimiento de información, la parte reclamada, aportando más detalle del cambio sobre el domicilio postal de la parte reclamante, indica que el día 27 de agosto de 2021 se modificó a través del canal *****BANCO.1** NET el domicilio de correspondencia Calle *****DIRECCIÓN.1**, *****LOCALIDAD.1**, España, **XXXX** por el correspondiente a Calle *****DIRECCIÓN.3**, *****LOCALIDAD.3**, *****LOCALIDAD.1**, **XXXX**. Sobre este punto, la parte reclamada adjunta pantallazo de sus sistemas.

Esta última dirección es la que consta en la información precontractual de la tarjeta (“Folleto de información precontractual y previa al contrato de servicios de pago”) con la que se realizaron los reintegros reclamados en cajero automático. A este respecto, hay que indicar que la dirección (Calle *****DIRECCIÓN.3**, **XXXX**, *****LOCALIDAD.3**, *****LOCALIDAD.1**), que consta en dicha información precontractual, no coincide con la dirección indicada por la parte reclamante en su denuncia ante la DGP.

También la parte reclamada aporta pantallazos de las comunicaciones enviadas a la parte reclamante, en concreto, mediante mensaje PUSH-MOOM a su dispositivo móvil, donde se indica:

“Tu tarjeta está en camino. Tu nueva tarjeta terminada en XXXX ya ha sido enviada. La recibirás por correo próximamente”

En este segundo requerimiento también se solicitó a la parte reclamada la acreditación de la dirección postal a la que efectivamente se envió la tarjeta con la que se realizaron las operaciones reclamadas. La parte reclamada señala que *“La tarjeta se envió por correo ordinario a la dirección que consta en el documento de información precontractual y contrato de tarjeta (aportado como Documento nº 2 junto a la contestación de 19/07/2022)”*. Asimismo, adjunta pantallazo de sus sistemas donde se observa la siguiente información:

Tarjeta	Terminada en XXXX
Fecha de emisión	27-08-2021
Forma de envío	Correo ordinario
Fecha de envío a domicilio	31-08-2021
Dirección de envío	***DIRECCIÓN.3
Tarjeta devuelta a oficina (S/N)	N

Por último, hay que recordar lo indicado por la parte reclamante en la denuncia presentada ante la DGP:

*“Que la denunciante manifiesta que todo comenzó el día 27 de agosto cuando recibe a su correo un precontrato de servicio de pago de una tarjeta bancaria con nº *****TARJETA.1** que desconoce.*

Que la dicente no ha solicitado esa tarjeta, sin darle más importancia a este hecho ya que no ha recibido ninguna tarjeta física² y por lo tanto no da cuenta de lo sucedido.”

3. Información que conste en los sistemas relativos a cambios en la tarjeta.

En este punto del requerimiento, lo que se le pedía a la parte reclamada era la “Información que conste en sus sistemas de cómo se activó dicha tarjeta (a través de la app, a través de la web o en un cajero automático), fecha y hora en la que se activó, y datos identificativos del usuario que la activó”.

A esto, la parte reclamada contesta:

“Se realizó una modificación de límites de la tarjeta a las 11:19:27 desde la misma dirección IP de alta, mediante doble factor de autenticación clave OTP/SMS.”

El día 22 de junio de 2022, se accedió a la página web *****EMAIL.4** donde se indica que las tarjetas se pueden activar a través de los siguientes canales: app, web y cajero automático. Pero, a tenor de la respuesta dada a este punto por la parte reclamada, no se contesta sobre el canal empleado para activar la tarjeta ni de cuándo se produjo dicha activación.

En el segundo requerimiento también se hizo hincapié sobre este punto, pidiendo la información que constara en sus sistemas de cómo se activó dicha tarjeta (a través de la app, a través de la web, en un cajero automático u otro), fecha y hora en la que se activó, y datos identificativos del usuario que la activó. Sobre ello, la parte reclamada adjuntó pantallazo de sus sistemas donde se puede comprobar que la activación tuvo lugar el día 1 de septiembre de 2021 a las 12:13:08 a través de la oficina 7013 que se corresponde con la oficina de banca online, según indica la parte reclamada. Si la activación se hace a través de la banca online, en dicha página web de la parte reclamada (*****EMAIL.4**) se indica lo siguiente:

*“Una de las maneras más rápidas de activar tu tarjeta es a través de *****BANCO.1.XX**. Una vez que te has identificado correctamente como usuario, tan solo debes ir al apartado “Tarjetas”. En este punto podrás elegir varias opciones para operar con tu nueva tarjeta, entre las que se encuentra la función de activarla introduciendo el código PIN.”*

Asimismo, en relación a la información que figura en dicho pantallazo, la parte reclamada señala que la tarjeta se bloqueó por robo el día 4 de septiembre de 2021 a las 01:12:46, tal y como señaló la parte reclamante en su denuncia ante la DGP, y fue cancelada el día 7 de septiembre de 2021 a las 09:56:46.

4. Evidencias del envío de claves OTP/SMS al número móvil validado del cliente.

La parte reclamada indica:

*“Con la finalidad de acreditar que las operaciones se realizaron con un doble factor de autenticación se copia captura de pantalla de 3 OTP/SMS enviadas al número de contacto de la reclamante, que son necesarias para la ejecución de las acciones indicadas (cambio domicilio, contratación y modificación de límite). En ese momento se le envió la notificación pertinente (enviada al e-mail) y el 3 y 4 de septiembre, tras la recepción de la tarjeta y desde un cajero en *****LOCALIDAD.2**, se realizan las 2 retiradas de efectivo con contactles + PIN (según se acredita con la documentación que se acompaña en este expediente - diario del cajero y de la disposición en concreto objeto de este expediente -.”*

Adjunta pantallazo de los mensajes OTP enviados a la parte reclamante donde consta la fecha de los hechos, la hora a la que se enviaron y el número de teléfono móvil al que se enviaron todos estos mensajes OTP. En dichos pantallazos se puede observar que se enviaron 4 mensajes OTP a la parte reclamante (número de teléfono **XXXX***TELÉFONO.1**), pero en la contestación, la parte reclamada sólo hace referencia a tres operaciones (cambio de dirección fiscal, alta de una tarjeta y modificación de límite de una tarjeta) y tampoco se indica a cuál de esas tres operaciones se corresponde cada uno de estos mensajes OTP, aunque es cierto que, por la hora, se puede intuir a qué operación se corresponde cada mensaje OTP (el segundo se correspondería con el cambio de dirección fiscal, el tercero con el alta de la tarjeta y el cuarto con la modificación de límites de la tarjeta):

Mensaje	Fecha y hora	Contacto
BANCO.1 : Para realizar tu operación utiliza el código XXXXXX	2021-08-27 09:11:01.964Z	00XXTELÉFONO.1



BANCO.1: Para realizar tu operación utiliza el código XXXXXX	2021-08-27 09:16:31.680Z	00XXTELÉFONO.1
BANCO.1: Para realizar tu operación utiliza el código XXXXXX	2021-08-27 09:17:40.016Z	00XXTELÉFONO.1
BANCO.1: Para realizar tu operación utiliza el código XXXXXX	2021-08-27 09:18:55.363Z	XXXXTELÉFONO.1

Fecha	Tipo Trans
27/08/2021 11:17:06	Cambio Dirección Fiscal
27/08/2021 11:18:00	Finaliza el alta de una tarjeta
27/08/2021 11:19:27	Modificar límites de una tarjeta

Respecto al cambio del límite, aunque la parte reclamada no aporta más detalle sobre este cambio, hay que decir que en el contrato de la tarjeta figura un límite de disposición diaria en cajeros de 1.000 euros. Gracias a este cambio, se pudieron realizar dos disposiciones de 2.000 euros cada una en dos días consecutivos (3 y 4 de septiembre de 2021), tal y como relata la parte reclamante en su reclamación.

El día 22 de junio de 2022 se envió mediante notificación postal un requerimiento de información a la parte reclamante de cara a aclarar algunos puntos (copia del correo electrónico con el borrador del contrato de tarjeta terminada en 5191, copia del extracto bancario donde se detallan los reintegros no consentidos por su parte y copia de algunos correos electrónicos enviados por la parte reclamada a la parte reclamante en relación a su reclamación), con fecha de acuse de recibo de 30 de junio de 2022, pero este requerimiento no ha sido atendido por la parte reclamante.

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

II

Seguridad del tratamiento

El artículo 32 del RGPD estipula lo siguiente:

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la seudonimización y el cifrado de datos personales;*
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros."

III

Principios relativos al tratamiento

La letra f) del artículo 5.1 del RGPD propugna:

"1. Los datos personales serán:

(...)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

IV

Hechos objeto de reclamación

El día 27 de agosto de 2021, a través de la banca online de la parte reclamada, se llevaron a cabo una serie de operaciones, en concreto, modificación del domicilio fiscal de la parte reclamante, alta de una nueva tarjeta (terminada en XXXX) y

modificación de los límites de dicha tarjeta. La parte reclamada acredita el envío de sendos mensajes OTP al número de teléfono móvil de la parte reclamante (mismo número de teléfono que indicó la parte reclamante en su denuncia ante la DGP) para confirmar todas estas operaciones.

La parte reclamada envió el código pin mediante SMS al número de teléfono móvil de la parte reclamante (mismo número de teléfono que el aportado por la parte reclamante en su denuncia ante la DGP) el día 27 de agosto de 2021 a las 20:14 horas.

Dicha tarjeta (terminada en 5191) fue enviada por la parte reclamada a la parte reclamante el día 31 de agosto de 2021 mediante correo postal. La dirección postal a la que se envió la tarjeta fue modificada a través de la banca online (una de las tres operaciones anteriormente mencionadas), dirección postal que figura en la documentación precontractual correspondiente a esa tarjeta ("Folleto de información precontractual y previa al contrato de servicios de pago"), documentación que fue enviada por la parte reclamada a la dirección de correo electrónico de la parte reclamante (*****EMAIL.2**), tal y como aquélla ha acreditado. El resto de los datos de la parte reclamante que figuran en la documentación precontractual de la tarjeta, en concreto, nombre y NIF de la parte reclamante, coinciden con los que ésta señaló en su denuncia ante la DGP.

Sobre la activación de la tarjeta, la parte reclamada indica que se realizó a través de la banca online. En su página web se indica que, si se activa a través de la banca online, se puede proceder a su activación mediante la introducción del código pin que, según la información aportada por ésta, fue enviado mediante SMS al número de teléfono móvil de la parte reclamante (mismo número de teléfono que indicó la parte reclamante en su denuncia ante la DGP) ese mismo día 27 de agosto de 2021.

La parte reclamante señala en su denuncia ante la DGP que el día 27 de agosto de 2021 recibió un correo electrónico de la parte reclamada en su dirección de correo electrónico *****EMAIL.2** donde se adjuntaba la documentación contractual de una tarjeta bancaria terminada en 5191 que no reconocía. La parte reclamada ha acreditado, tal y como se ha comentado anteriormente, el envío de dicha documentación a dicha dirección de correo electrónico de la parte reclamante. Asimismo, en su denuncia ante la DGP, la parte reclamante indica que, al no haber recibido ninguna tarjeta física en su domicilio, no dio cuenta de lo sucedido.

En un correo electrónico enviado por la parte reclamante a la parte reclamada, aquélla indica que le enviaron un mensaje SMS el día 27 de agosto de 2021 comunicando la suspensión de su cuenta bancaria, pero la parte reclamada indica que ese mensaje no fue enviado por ella, haciendo referencia a que éste es uno de los medios empleados por los ciberdelincuentes habitualmente para tratar de robar las credenciales de acceso a la banca online de los clientes de servicios bancarios. Dado que la parte reclamante recibió un SMS, se puede concluir que no se llevó a cabo un duplicado de tarjeta SIM no autorizado por la parte reclamante puesto que, en este caso, su terminal móvil hubiera dejado de operar normalmente.

Los días 3 de septiembre a las 23:47 horas y 4 de septiembre de 2021, a las 00:04 se llevaron a cabo las operaciones reclamadas, dos reintegros en cajero

automático por un importe de 2000 euros ,cada uno de ellos, mediante el uso físico de la tarjeta terminada en 5191 e informando del correspondiente código pin. La parte reclamante, al recibir la notificación en su teléfono móvil de estos reintegros y no reconocerlos como propios, accedió a la aplicación móvil (App) de la parte reclamada donde observó que figuraba una tarjeta (terminada en XXXX) que no reconocía, por lo que procedió a su bloqueo el día 4 de septiembre de 2021 a las 01:12:46, tal y como ha acreditado la parte reclamada con información de sus sistemas.

Por último, hay que señalar que el día 22 de junio de 2022 se envió un requerimiento de información a la parte reclamante, con fecha de acuse de recibo de 30 de junio de 2022, a fin de recabar algunos datos y comunicaciones mantenidas entre ella y la parte reclamada, pero éste no ha sido contestado.

Del relato de los hechos realizado se desprende que la parte reclamada tiene medidas de seguridad adecuadas para verificar la titularidad de la tarjeta de crédito solicitada, y no existen evidencias de que no hubiera actuado de forma diligente una vez conocido el problema, del cual se advierte en la página web de la parte reclamada.

En resumen, la parte reclamante se queja de que recibió en su móvil notificación de movimientos de una tarjeta de crédito a su nombre, pero de la cual no disponía. Tras las actuaciones previas de investigación realizadas, se deduce que han entrado fraudulentamente en la cuenta de la parte reclamante a través de internet; solicitando, a través de la web, el cambio de domicilio y la variación del límite de disposición

Del relato de los hechos realizado se desprende que la parte reclamada tiene medidas de seguridad adecuadas para verificar la titularidad de la tarjeta de crédito solicitada, y no existen evidencias de que no hubiera actuado de forma diligente una vez conocido el problema, del cual se advierte en la página web de la parte reclamada. Las operaciones efectuadas para dar de alta la tarjeta, cambiar el domicilio y la cantidad diaria de disposición, precisaron de una clave OTP que se envió al móvil de la parte reclamante, y los presuntos estafadores no tenían ni el móvil ni un duplicado de la SIM.

Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, y teniendo en consideración que quienes efectuaron las operaciones objeto de reclamación se identificaron correctamente en la web, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Así pues, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a BANCO BILBAO VIZCAYA ARGENTARIA, S.A. y a la parte reclamante.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

940-091222

Mar España Martí
Directora de la Agencia Española de Protección de Datos