- Expediente N.º: EXP202201718

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: Don ***A.A.A.*** (en adelante, la parte reclamante) con fecha 27 de diciembre de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra BANCO BILBAO VIZCAYA ARGENTARIA, S.A., con NIF ***A48265169*** (en adelante, la parte reclamada o BBVA).

Los motivos en que basa la reclamación son los siguientes:

El reclamante es titular de una cuenta abierta en la entidad reclamada, la cual tiene asociada una tarjeta de débito. Manifiesta que, en fecha 11 de octubre de 2021, se realizó un cargo fraudulento en su tarjeta, correspondiente a una compra que el reclamante no había realizado, de un importe de 1500 euros. Al tratarse de un importe alto, la entidad reclamada procedió, con posterioridad, al bloqueo de la actividad en la App del reclamante, por seguridad. Aporta denuncia presentada ante la Policía, en fecha 14 de octubre de 2021, comunicación de la incidencia a la entidad reclamada, el 14 de octubre de 2021, pantallazo relativo a la operación fraudulenta y reclamación ante la OMIC, de fecha 15 de noviembre de 2021.

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 LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, 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 14 de febrero de 2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 23 de febrero de 2022 se recibe en esta Agencia escrito de respuesta que no aportaba información alguna sobre la reclamación que le fue trasladada.

TERCERO: Con fecha 22 de marzo de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

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:

1. El reclamante es cliente de la parte reclamada en virtud de un contrato de tarjeta de crédito, suscrito desde la banca a distancia el 28/04/2017. Aportan copia del contrato de tarjeta en el que figura un límite pactado de 1800 euros.

La parte reclamada indica que ha analizado la operativa llevada a cabo a través de la tarjeta de crédito vinculada al referido contrato, y en este caso las operaciones se han llevado a cabo mediante firma biométrica, para lo que ha sido necesario activar el acceso biométrico en el móvil y activar la firma con biometría. Aportan registro del envío de dos SMS al número móvil que indican fue validado por el reclamante, SMS en los que le informan de las claves OTP para autentificar la solicitud (fecha 11 de octubre de 2021, misma fecha que el cargo reclamado).

Indican que para registrar la firma biométrica es necesario introducir una clave OTP que fue enviada por SMS al teléfono móvil validado del reclamante. La firma con biometría permite a los clientes usar su huella, iris o el reconocimiento facial para firmar algunas de las operaciones que se realizan a través de la app de la entidad. Una vez activada, los clientes pueden firmar sus operaciones sin necesidad de recibir un SMS con una clave de firma. Indican que en el caso que nos ocupa, la operación con tarjeta de crédito controvertida, el segundo factor de autentificación fue la firma biométrica que previamente había sido activada mediante validación de la clave OTP.

La parte reclamada informa que, a raíz de la incidencia interpuesta por el reclamante, en fecha de 14 de octubre de 2021, en cumplimiento de la normativa vigente restituyeron la cuenta de pago al estado en que se encontraba antes de la operación cuestionada. Aportan apunte de anulación del importe de 1500 euros, de fecha 15 de octubre de 2021.

A continuación, la parte reclamada inicia a través del área especializada en fraudes las labores de investigación, recabando los registros y documentación tanto interna como externa para dilucidar si se trata de una operación realizada correctamente desde el punto de vista operativo. Concluyen tras el análisis de las evidencias e informe del proveedor de servicios de pago, que la operación de comercio electrónico denunciada por el reclamante desde el punto de vista estrictamente operativo debe considerarse correcta, pues se realizó sin fallos, y sin que pueda considerarse una operación no autorizada en los términos establecidos en la normativa de Servicios de Pago.

Destacan que en el momento de la compra el reclamante tuvo que: (i) disponer de la información contenida en la tarjeta, esto es numeración, fecha de caducidad y código CVV; (ii) tener en su poder el dispositivo validado donde la parte reclamante le había remitido la clave OTP para activar la firma con biometría; (iii) validar la operación mediante reconocimiento facial, de iris o huella digital.

Indican que comunicaron al reclamante la resolución de la incidencia y procedieron a retroceder el abono realizado en la cuenta del reclamante. Ante ello, el reclamante presentó ante el Servicio de Atención al Cliente una reclamación manifestando su disconformidad con la resolución anterior. El 23 de noviembre de 2021 se desestimó la

petición de reclamante. Se verifica que, en la comunicación remitida al reclamante, cuya copia aportan, se cita:

"Analizando la operativa llevada a cabo por la tarjeta a la que se hace referencia en su escrito las operaciones están realizadas sin que exista ningún tipo de falsificación al estar validadas mediante clave OTP enviada por SMS a su teléfono móvil.
Por ello le comunicamos que lamentablemente en esta ocasión no nos es posible atender favorablemente su petición."

En relación con las medidas de seguridad o controles adoptados con carácter previo a la operación de compra, los representantes de la parte reclamada manifiestan que:

- Se emitió una alerta al reclamante vía Email y Push (SMS) (datos de contacto validados) de aviso de acceso desde otro dispositivo móvil.

- Se comunicó al reclamante vía Email y Push (datos de contacto validados) la activación de la firma biométrica.

- Se le informó vía Email y Push de que se le había bloqueado la banca electrónica por sospecha de actividad fraudulenta, lo que pudo impedir posteriores disposiciones no reconocidas por el cliente.

Han aportado captura de pantalla con el registro de la remisión al teléfono móvil del reclamante la clave OTP para activar la firma biométrica. Se verifica que el número de teléfono al que se remitió la clave OTP, que figura en el citado registro, se corresponde con el número de teléfono aportado por el reclamante como suyo en la denuncia ante la policía nacional adjunta a su reclamación.

2. Realizado un requerimiento de información, con fecha 4 de abril de 2022, la entidad reclamada responde en fecha 21 del mismo mes y año, con la siguiente información y documentación adicional:

- El origen del cargo es un comercio electrónico, no estando la tarjeta presente, con el principal medio de autentificar al cliente mediante 3DS (3-D Secure, o tres dominios seguros). Aportan copia del informe correspondiente al cargo facilitado por el proveedor de servicios de pago.

- El mismo día de la operación la parte reclamada remitió a la parte reclamante una alerta por doble conducto - email y push - de que la aplicación de banca online se había dado de alta en otro dispositivo distinto (inicio de sesión desde un nuevo dispositivo). Aportan captura de pantalla del registro de ambas comunicaciones y de los datos del cliente con la indicación de estado "validado" (dirección de correo y número de teléfono móvil). Se verifica que el número de línea móvil se corresponde con el número aportado por el reclamante como suyo en la denuncia ante la policía nacional adjunta a su reclamación.

- Aportan también captura de pantalla con la comunicación, también por doble conducto - email y push - que la entidad reclamada realizó al reclamante comunicando el bloqueo de forma temporal de su acceso a la banca digital con el siguiente motivo *"Hemos detectado una actividad sospechosa reciente y por tu seguridad, se ha*

bloqueado de forma temporal tu usuario de acceso a tu banca digital." (Texto del correo electrónico).

- Los representantes de la parte reclamada manifiestan que la operación controvertida se ejecutó correctamente y fue autentificada, y no obstante de forma preventiva la entidad procedió a restringir la operativa de la tarjeta de crédito con la finalidad de verificar con el cliente que las operaciones que solicitaba a través de la banca digital no eran consecuencia de un engaño. Indican que tienen establecidos en sus sistemas patrones que ayudan a detectar operaciones que requieran de medidas de seguridad adicionales por prevención y que en este caso se ha alertado al usuario de que se ha producido un acceso a su banca digital a través de un dispositivo diferente al habitual. La entidad permite dicho acceso, dado que operativamente es correcto (se realiza introduciendo el código de usuario y clave correcta) y porque es muy habitual que los usuarios de banca digital entren desde diferentes dispositivos, pero se envía una alerta al cliente de manera preventiva, de tal manera que si no se reconociera dicho acceso el usuario podría bloquear temporalmente y de forma inmediata su banca digital.

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
Síntesis de los hechos

A este respecto, de lo contenido en las actuaciones previas de investigación, acerca de las medidas de seguridad que BBVA tiene implementadas para evitar actuaciones fraudulentas en compras on line y verificar que el comprador es el titular de la tarjeta utilizada, se observa lo siguiente:

La parte reclamante reclamó porque, en fecha 11 de octubre de 2021, se realizó un cargo fraudulento en su tarjeta, correspondiente a una compra que no había realizado, de un importe de 1500 euros. Al tratarse de un importe alto, la entidad reclamada procedió, con posterioridad, al bloqueo de la actividad en la App del reclamante, por seguridad.

La parte reclamada ha aportado información y acreditación documental de los controles desplegados con relación al cargo con tarjeta reclamado, habiéndose evidenciado en concreto lo siguiente:

La operación controvertida de tarjeta de crédito se corresponde con una operación realizada por comercio electrónico (por Internet, sin estar la tarjeta presente). Para su realización se tuvo que disponer de la información contenida en la tarjeta: su numeración, fecha de caducidad y código CVV. La operación fue validada mediante firma biométrica.

La operativa con firma biométrica fue activada el mismo día de la operación mediante clave OTP (clave de un solo uso remitida por SMS) enviada a la línea móvil del reclamante. La parte reclamada ha aportado evidencias de este extremo consistentes en captura de pantalla con el registro de la remisión de la clave OTP para dicha activación, y se ha verificado que el número de teléfono al que se remitió se corresponde con el número de teléfono aportado por el reclamante como suyo en la denuncia ante la policía nacional adjunta a su reclamación.

También se remitió previamente una alerta de inicio de sesión en dispositivo nuevo, habiendo aportado la parte reclamada evidencias de este envío, por correo electrónico y SMS, comprobándose que el número de destino del SMS se corresponde igualmente con el número de teléfono aportado por el reclamante como suyo en su denuncia ante la policía nacional.

Por último, la parte reclamada bloqueó la operativa online para el usuario de forma preventiva avisando al reclamante y aportando evidencias del envío de dicha alerta, por correo electrónico y SMS al mismo número de teléfono.

IV
Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos, al haber actuado BBVA de forma diligente una vez conocida la utilización fraudulenta de la tarjeta de débito de un cliente de la entidad reclamada.

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 Don ***A.A.A.*** y a BANCO BILBAO VIZCAYA ARGENTARIA, S.A.

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.

940-110422

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