- Expediente N.º: EXP202303533

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 1 de febrero de 2023, se presentó reclamación ante la Agencia Española de Protección de Datos contra UNICAJA BANCO, S.A.U., con NIF ***A93139053*** (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que, en fecha 25 de enero de 2023, la persona que es cotitular de la cuenta bancaria que el reclamante tiene abierta con Unicaja recibe un mensaje de texto de la entidad bancaria para autorizar una transferencia bancaria de 2000 euros. Señala que el cotitular, tras recibir un SMS de Unicaja con un código para autorizar la transferencia, le aparece una notificación en la aplicación móvil, que rechaza.

Simultáneamente, la parte reclamante recibe un mensaje de texto de Vodafone, en el que le indican que "respondiendo a su solicitud, hemos realizado el cambio de SIM que nos has indicado". Posteriormente, su línea queda fuera de servicio.

Ese mismo día solicita a la parte reclamada que bloqueen el uso de la cuenta y solicita revertir el cambio de SIM a Vodafone.

Dos días después, tras acudir presencialmente a la entidad bancaria, le informan que se han realizado dos transferencias de forma fraudulenta.

Documentación relevante aportada por la parte reclamante:

- Mensaje de texto recibido, en el que se le informa que proceden al cambio de SIM.
- Recibos de dos transferencias realizadas con fecha 25 de enero de 2023, ambas realizadas al mismo IBAN beneficiario.
- Consulta los accesos a Banca Digital en los días: del lunes 16 de enero al lunes 30 de enero de 2023
- Denuncia policial, de fecha 27 de enero de 2023.

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/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 17 de marzo de 2023 como consta en el certificado que obra en el expediente.

Con fecha 17 de abril de 2023, se recibe en esta Agencia escrito de respuesta indicando lo siguiente:

Confirman que, "*con fecha 25 de enero de 2023, se realizaron dos órdenes de transferencia desde el servicio de Banca a distancia, con cargo a la cuenta terminada en 0160 del cliente".*

[…] "ambas operaciones fueron registradas y autenticadas mediante sistema de autenticación reforzado con claves OTP (One Time Password) de un solo uso, enviada a través de SMS al número de teléfono ******TELÉFONO.1****, que coincide con el teléfono informado por el titular a Unicaja Banco a estos efectos. Las mencionadas transferencias fueron debidamente contabilizadas sin error técnico alguno de acuerdo con lo establecido en la normativa de Servicios de Pago, lo que confirma que no se han quebrantado los sistemas de seguridad de la Entidad exigidos por la mencionada regulación sectorial, y que tampoco se ha producido quebranto alguno de los principios de integridad y confidencialidad de los datos personales*."

La parte reclamada proporciona el Informe Técnico emitido por la Dirección de Ciberseguridad de UNICAJA en el que se constata lo explicado previamente mediante capturas de pantalla y logs de las claves enviadas por SMS.

La parte reclamada alega la aplicación del Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera que en su artículo 44, Prueba de la autenticación y ejecución de las operaciones de pago, establece:

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.

La parte reclamada proporciona los documentos que incluyen la información interna de UNICAJA con el detalle de los SMS remitidos por esta Entidad al dispositivo móvil de la parte reclamante, en el que consta el envío de las claves para autorizar ambas operaciones, y los registros informáticos de justificación de la autenticación de cada de las transferencias efectuadas, en el que consta que ambas operaciones fueron autenticadas mediante firma OTP por SMS.

TERCERO: Con fecha 1 de mayo de 2023, 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:

.-1-. Respecto a la cronología de los hechos denunciados y evidencias aportadas.

Por claridad, se exponen a continuación las numeraciones telefónicas involucradas en este expediente:

.- La numeración de la línea telefónica presuntamente duplicada de forma fraudulenta es ******TELÉFONO.1***, (en adelante, #TFNO_RTE)

.- La numeración de la línea telefónica del cotitular de la cuenta bancaria (***A.A.A.***) a nombre de la parte reclamante es ******TELÉFONO.2***, (en adelante, #TFNO_COT).

La parte reclamante refiere los siguientes hechos denunciados:

.- 25/01/2023: entre las 12:46 y las 12:48 horas, ***A.A.A.*** recibe cuatro llamadas en su móvil (#TFNO_COT) desde números de teléfono de Marruecos.

.- 25/01/2023: a las 12:57 horas, ***A.A.A.*** recibe un SMS de Unicaja Banco con un código para autorizar una transferencia por valor de 2.000€, y en la aplicación de su móvil salta también una notificación para autorizarla.

.- 25/01/2023, a las 12:47 horas B.B.B. recibe un SMS de la compañía Vodafone España en el #TFNO_RTE en el que se le informa que proceden al cambio de SIM.

.- 25/01/2023, alrededor de las 14:00 horas ***B.B.B.*** está fuera de servicio y lo pone en conocimiento de la compañía Vodafone España.

Vodafone asegura que procede a revertir el cambio de SIM y que confirmarán que esté realizado a las 17:00 horas del mismo día.

.- 25/01/2023, a las 14:15 horas: A.A.A. solicita a Unicaja que bloqueen de forma inmediata cualquier uso que se pueda realizar de los servicios de banca online con los usuarios y claves de ambos titulares, así como la cancelación de las tarjetas de crédito y débito, en prevención de un uso irregular de las mismas.

Unicaja Banco informa de que no se ha hecho ningún movimiento ni operación a lo largo del día, y confirma que procede a bloquear los usuarios y las tarjetas.

.- 25/01/2023, a las 15:15 horas: B.B.B. reitera a Unicaja que bloqueen de forma inmediata cualquier uso.

Unicaja Banco reitera que no se ha hecho ningún movimiento ni operación a lo largo del día.

.- 25/01/2023, a las 17:15 horas: B.B.B. llama a Vodafone España para reiterar la petición de reversión de cambio no autorizado de SIM.

.- 25/01/2023, a las 19:52 horas se ordenan dos transferencias a una cuenta en el Banco de Santander a nombre de "***C.C.C.***", por un valor total de 3.000€, a través de los servicios de banca online.

Según refiere la parte reclamante, el día 25/02/2023 se dejan programadas dos transferencias más para que se realicen al mismo beneficiario y por el mismo importe.

Se continúa accediendo durante los días 26 y 27 de enero de 2023 a los servicios de banca online con el usuario de la parte reclamante.

Se ha evidenciado en el listado de conexiones aportado que existen intentos de conexión fallidos y correctos desde diferentes direcciones IP en el intervalo de tiempo entre los días 25 y 28 de enero de 2023.

.- 27/01/2023, a las 11:00 horas ambos reclamantes acuden presencialmente a Unicaja y se les informa de las transferencias realizadas.

.- 27/01/2023, a las 23:24 horas: La parte reclamante presenta denuncia en la Policía Nacional, Dependencia Madrid-Retiro.

.-2-. Respecto al traslado

Con las evidencias aportadas por la parte reclamada tras el traslado de la reclamación, se observa la siguiente cronología de los hechos:

.- Con fecha 25/01/2023 a las 13:21, se envía una clave por SMS al teléfono ******TELÉFONO.1*** (#TFNO_RTE) para registrar un nuevo dispositivo en banca digital

.- El mismo día a las 13:25 horas, se envía una clave por SMS al (#TFNO_RTE) para validar una transferencia por importe de 2.000€.

.- También con fecha 25/01/2023 a las 13:32, se envía una clave por SMS al (#TFNO_RTE) para validar una transferencia por importe de 1.000€.

.- El cliente fue bloqueado ese mismo día a las 14:24.

Revisada la información aportada por el operador telefónico se constata que el presunto suplantador de identidad tiene activo el duplicado de tarjeta SIM fraudulento desde las 12:35 del día 25 de enero de 2023 hasta las 16:01 de ese mismo día.

Respecto a estos hechos, la parte reclamada especifica que:

"Tras las investigaciones oportunas se ha verificado que ambas operaciones de transferencia fueron validadas con anterioridad al bloqueo, de acuerdo con la operativa bancaria habitual y cumpliendo con las exigencias de seguridad adoptadas por Unicaja Banco de conformidad con la normativa aplicable.

NO obstante, las citadas transferencias se ejecutaron con posterioridad al bloqueo, debido a un fallo puntual humano que motivó que no se anularan estas operaciones concretas que estaban en vuelo. De acuerdo a lo expuesto, se ha analizado de nuevo el expediente por parte del Departamento de Atención al Cliente de Unicaja Banco, y tomando en consideración el hecho de que las órdenes cursadas se ejecutaron con posterioridad al bloqueo, confirmamos que está actualmente en curso la restitución de los importes reclamados."

(Nota: el subrayado ha sido incorporado por la Agencia)

La parte reclamada incluye en su escrito las conclusiones del Informe:

".- *Que Unicaja ha implementado y ejecutado las medidas técnicas de seguridad necesarias establecidas en la PSD2 y desarrolladas por el Reglamento 2018/389.*

.- Que Unicaja envió las claves dinámicas aleatorias de un solo uso al dispositivo informado del diente, para validar la ejecución de las operaciones.

.- Que presumiblemente, el cliente ha incurrido en un fallo de custodia adecuada de sus claves bancarias, siendo éste el único motivo que ha podido originar la comisión del fraude denunciado.

.- Que Unicaja Banco ha registrado y procesado correctamente en sus sistemas todas las operaciones ordenadas mediante las claves, personales e intransferibles, de la cliente."

Acerca de las causas que han motivado la incidencia, la parte reclamada hace alusión al duplicado de tarjeta SIM de la parte reclamante:

"En consecuencia, ha existido un espacio de tiempo, durante el cual un duplicado de la tarjeta SIM del número de teléfono del reclamante ha podido estar en poder de un tercero, supuesto causante del fraude, y ha sido precisamente durante este lapso cuando se han realizado las transferencias fraudulentas.

Y, en este sentido, conviene señalar los precedentes marcados por la Agencia de Protección de Datos, que en ocasiones los supuestos delincuentes como consecuencia de supuestos similares al acontecido, donde un tercero desconocido consigue obtener un duplicado de la tarjeta SIM del usuario de una entidad financiera para poder acceder a su Banca Digital. Así, citamos a modo de ejemplo las Resoluciones PS-00046-2021, PS-00296-2022, PS-00290-2022 o PS-00665-2022, en las cuales se han puesto de manifiesto este tipo de fraudes, sin que en ninguna de ellas se haya constatado infracción alguna por parte de las entidades de crédito en lo que respecta a la protección de datos de sus clientes."

[…]

"en relación con estas técnicas de fraude, Unicaja Banco, al igual que el resto de las entidades del sector financiero, o las propias Fuerzas y Cuerpos de Seguridad del Estado y otros organismos como el INCIBE, viene realizando en redes sociales, en medios de comunicación, en la propia web de la Entidad o en el servicio de banca a distancia, múltiples campañas informativas y de concienciación en aras de prevenir este tipo de fraudes"

UNICAJA proporciona el documento publicado en su página web, como muestra de dichas medidas de concienciación, en el que se especifican varias recomendaciones para evitar sufrir los mencionados perjuicios derivados de actuaciones fraudulentas ajenas al Banco. También remite el documento con ejemplos de comunicaciones informativas que tiene en circulación a través de todo tipo de canales (cajeros, oficinas, Banca Digital ...) con las precauciones ante posibles intentos de phishing, smishing o spoofing, y evitarlos.

Respecto a la adopción de medidas técnicas y organizativas para mitigar aquellos riesgos que pudieran derivarse de las actividades de tratamiento, la parte reclamada informa que ha sido certificada por AENOR sobre sistema de gestión de seguridad.

Se comprueba en la página web de AENOR que UNICAJA es una empresa certificada (Certificado SGPI-0002/2022) respecto de la norma: Privacidad de la Información ISO/IEC 27701:2021 con alcance:

Sistema de gestión de privacidad que da soporte a:

-Los servicios de Banca Electrónica, portal web corporativo y portales web promocionales
-Servicios de consultas, pagos, ingresos y disposiciones de efectivo en cajeros automáticos (Autoservicios Financieros),
-Servicios de gestión interna y de soporte de operaciones TIC basados en el Host
-Servicios TIC internos basados en sistemas distribuidos (entorno microinformático, intranet y data ware house) conforme a la declaración de aplicabilidad vigente, a la fecha de emisión del certificado.

.-3-. Respecto a la información aportada en las respuestas a los requerimientos de información

Con fecha 18 de julio de 2023 se realiza un requerimiento de información a la parte reclamada solicitándole, entre otros puntos, el detalle de todos los cambios realizados en su base de datos a los datos de la parte reclamante, el protocolo de acceso a la banca online, información sobre las medidas de seguridad implementadas para solicitar una OTP a la hora de autorizar una operación y el protocolo de registro de nuevos dispositivos, así como las medidas de seguridad que se implementan para registrarlos.

La parte reclamada responde a este requerimiento de información proporcionando la siguiente documentación junto a su escrito de respuesta:

.- Documento Nº 1.A: comunicación a la parte reclamante, con fecha 10 de abril de 2023, en el que se indica que no procede atender la devolución de los importes reclamados por el interesado.
.- Documento Nº 1.B: comunicación a la parte reclamante, con fecha 17 de abril de 2023, en el que se le informa que su petición va a ser atendida en el sentido interesado por el reclamante.

.- Documento Nº 2.A: llamada del cotitular, con fecha 25/01/2023 a las 14:18h, procedente del número #TFNO_COT.

.- Documento Nº 2.B: llamada de la parte reclamante con fecha 25/01/2023 a las 15:22h, procedente del número ******TELÉFONO.3***.

.- Documento Nº 2.C: llamada de la parte reclamante con fecha 28/01/2023 a las 00:39h, procedente del número #TFNO_RTE.

.- Documento Nº 2.D: llamada de la parte reclamante con fecha 30/01/2023 a las 19:12h, procedente del número #TFNO_RTE.

.- Documento Nº 3: Documento adjunto en Excel con las trazas de todas las operaciones efectuadas de banca digital, los mensajes enviados al usuario y peticiones de claves entre las fechas 1 de enero de 2023 hasta 26 de mayo de 2023.

.- Documento Nº 6:Documento acreditativo de las trazas de las operaciones entre las fechas 25 y 26 de enero de 2023.

.- Documento Nº 9: Justificante de abono restituyendo la totalidad del importe afectado por las transferencias reclamadas.

Con fecha 12 de febrero de 2024 se realiza un segundo requerimiento de información a la parte reclamada para aclarar dos solicitudes de clave de acceso a la banca digital que originaron los envíos de dichas claves a través de SMS.

Con fecha 19 de febrero de 2024, la parte reclamada responde a estos requerimientos de información proporcionando como evidencia dos grabaciones de llamadas telefónicas junto a su escrito de respuesta.

De la información recabada durante la investigación se ha puesto de manifiesto que:

.-3.1-. Respecto al Protocolo de acceso a la banca online.

(…)

.-3.2-. Respecto al Procedimiento de identificación del usuario en banca telefónica

*"**(…)**."*

.-3.3-. Respecto al Procedimiento para atender solicitudes del usuario en banca telefónica

(…)

.-3.4-. Respecto al procedimiento para recuperación de claves

(…)

.-3.5-. Respecto a las medidas de seguridad implementadas para solicitar una OTP a la hora de autorizar una operación.

(...)

.-3.6-. Respecto al Protocolo de registro de nuevos dispositivos.

(...)

.-3.7-. Respecto el caso particular de la parte reclamante

La parte reclamada proporciona un documento que incluye las trazas de todas las operaciones efectuadas de banca digital, los mensajes enviados al usuario y peticiones de claves entre las fechas 1 de enero de 2023 hasta 26 de mayo de 2023.

.-3.7.1-. Histórico de los pasos ejecutados en el presunto fraude

De la información recabada durante la investigación se ha constatado que los pasos llevados a cabo para la ejecución del presunto fraude son los siguientes:

Día 25 de enero de 2023:

.- 13:17: Dos intentos de conexión fallidos (clave incorrecta) a través de una APP en IOS (APP iPhone v2.10.0) desde una dirección IP extranjera (País IP=MA)

.- 13:19: Solicitud de cambio de claves a través del Contact Center.

.- 13:19: Se imprime la clave de acceso a Banca D.
.- 13:19: Envío de dicha clave de acceso a UNIVIA (Banca Digital) por SMS al número #TFNO_RTE.

.- 13:21: **Conexión con clave OK a Banca Digital** a través de una APP en IOS (APP iPhone v2.10.0) desde una dirección IP extranjera (País IP=MA).

.- 13:21: **Vinculación de dispositivo** seguro tras recepción de SMS con clave OTP y firma con dicha clave.
.- 13:22 a 13:24: Movimientos de consulta en la cuenta.

.- 13:25: Programación **OK** de **transferencia** SEPA de cantidad 2.000€ tras recepción de SMS con clave OTP y firma con dicha clave.

.- 13:29: Programación **fallida** de **transferencia** SEPA de cantidad 3.000€ (superado importe máximo de traspaso diario).

.- 13:32: Programación **OK** de **transferencia** SEPA de cantidad 1.000€ tras recepción de SMS con clave OTP y firma con dicha clave.

.- 13:32 a 13:54: Intentos infructuosos de envío de dinero a través de BIZUM.

.- 13:59: Intento de conexión web fallida (clave incorrecta) a través del navegador Chrome en Windows 10 desde una dirección IP española (País IP=ES)

.- 14:00: Dos intentos de conexión fallidos (clave incorrecta) a través de una APP en IOS (APP iPhone v2.10.0) desde una dirección IP extranjera (País IP=MA)

.- 14:01: Bloqueo de Contraseña (…)

.- 14:01 a 14:09: Intentos de conexión fallidos desde direcciones IP extranjera (País IP=MA) y española (País IP=ES) (Usuario revocado en sistema de seguridad).

. - 14:06: Intento de recuperación de claves que no se llega a ejecutar, pues el cliente no finaliza el proceso insertando el código OTP de validación.

.- 14:16: Solicitud de cambio de claves desde el Contact Center.

- 14:16: Se imprime la clave de acceso a Banca E.

.- 14:16: Envío de dicha clave de acceso a UNIVIA por SMS al número #TFNO_RTE.

.- 14:18: **Conexión con clave OK a Banca Digital** a través de una APP en IOS (APP iPhone v2.10.0) desde una dirección IP extranjera (País IP=MA).

.- 14:18 a 14:24: Movimientos de consulta en la cuenta e intentos infructuosos de envío de dinero a través de pago por cajero (Operación no disponible).

.- 14:24: **Bloqueo** de la cuenta de usuario (tras **llamada del cotitular** de la cuenta de la parte reclamante).

.- 14:24 a 17:05: Movimientos de consulta en la cuenta infructuosos (Usuario bloqueado temporalmente).

Día 26 de enero de 2023:

.- A lo largo del día: Intentos de conexión fallidos (Usuario bloqueado temporalmente).

Día 27 de enero de 2023:

.- 10:18 a 10:35: Intentos de conexión fallidos (Usuario bloqueado temporalmente).

. - 11:42: Visita de la parte reclamante a la oficina de UNICAJA y generación de claves de acceso a Banca Digital y a Banca Telefónica. Envío de dichas claves por SMS al número #TFNO_RTE.

.- 11:45: Conexión con clave OK a Banca Digital a través de una APP en IOS (APP iPhone v2.10.0) desde una dirección IP española (País IP=ES)

.- 14:37 a 17:34: Intentos de conexión fallidos (clave incorrecta) a través de una APP en IOS (APP iPhone v2.10.0) desde una dirección IP extranjera (País IP=MA) y Bloqueo de contraseña tras 3 intentos.

.-3.7.2-. Respecto a los cambios realizados a los datos de la parte reclamante

Tras analizar las evidencias presentadas en los documentos se comprueba que no ha habido modificación de los datos personales de la parte reclamante, salvo las contraseñas de acceso a Univia especificadas en el siguiente punto.

.-3.7.3-. Respecto al cambio de contraseñas

La parte reclamada explica que existen dos cambios de contraseña de acceso a Univia, ambos solicitados desde el Contact Center, centro XXXX.

- El canal de cambio de clave de las 13:19h fue desde el Contact Center (centro ***XXXX***, terminal ******TERMINAL.1***) y usuario ******USUARIO.1***.
- El canal de cambio de clave de las 14:16h fue desde el Contact Center (centro ***XXXX***, terminal ******TERMINAL.2***) y usuario ******USUARIO.1***).

Respecto a las medidas de seguridad superadas antes de los envíos de las claves de acceso a Univia, la parte reclamada proporciona las grabaciones de las llamadas telefónicas, en las que se aprecia cómo se contestan las preguntas que constan en el procedimiento para solicitar nueva clave (Recuperar clave) desde el Contact Center, especificadas en apartado anterior.

En particular, en ambas grabaciones se escucha cómo el suplantador de identidad proporciona la siguiente información:

(…)

Se confirma, entonces, que en estas llamadas se han efectuado las preguntas de seguridad especificadas anteriormente en el procedimiento de identificación del usuario en banca telefónica y que la persona que solicitó el cambio de contraseña conocía previamente todos los datos personales de la parte reclamante, incluso las respuestas a las preguntas de seguridad.

.-3.7.4-. Respecto de la vinculación del dispositivo de la parte reclamante

UNICAJA destaca que, actualmente, la parte reclamante no tiene registrados dispositivos.

Con relación a la primera operación para el registro de nuevos dispositivos, (la Simulación para determinar qué tipo de firma es requerida), la parte reclamada indica que la parte reclamante tiene tarjeta de coordenadas, pero tiene ***(…).*** Se confirma este extremo en las trazas aportadas.

Solicitada aclaración sobre el motivo por el cual las restricciones operativas en el período de enfriamiento tras la vinculación de un nuevo dispositivo no evitaron la realización de las transferencias efectuadas con fecha 25 de enero de 2023, la parte reclamada indica:

"Las transferencias SEPA fueron programadas, al no ejecutarse de forma instantánea y por ende tener un período en el que la operación se puede anular, no están restringidas en el período de enfriamiento. Por este motivo se procedió a la restitución de los importes reclamados, una vez detectado que, aunque las transferencias fueron efectuadas con anterioridad al bloqueo de la banca digital, las mismas se ejecutaron con posterioridad al bloqueo debido a un fallo puntual y humano que motivó que no se anularan estas operaciones que estaban en vuelo, y ello en base a un criterio estrictamente bancario."

.-3.7.4-. Respecto de la respuesta facilitada a la parte reclamante

UNICAJA aporta la comunicación, de fecha 10 de abril de 2023, en la que se indica que "*no procede atender la devolución de los importes reclamados por el interesado, al considerar que los sistemas de seguridad de la Entidad no habían sido quebrantados, habiéndose aplicado los medios de autenticación reforzados de las operaciones conforme a lo dispuesto en el artículo 44 de Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera y considerando que los adeudos no suponen una actuación contraria a la normativa y buenas prácticas bancarias."*

Con fecha 17 de abril de 2023, la parte reclamada remite una nueva comunicación a la parte reclamante informándole de que su petición va a ser atendida debido a que, "*aunque las transferencias de origen fraudulento y externo a los sistemas de Unicaja Banco fueron efectuadas con anterioridad al bloqueo por parte del interesado de la banca digital, las citadas transferencias se ejecutaron con posterioridad al bloqueo, debido a un fallo puntual humano que motivó que no se anularan estas operaciones concretas que estaban en vuelo*."

UNICAJA proporciona el documento Justificante de abono como evidencia de la restitución de los importes reclamados.

.-3.7.5-. Respecto de las comunicaciones con la parte reclamante

La parte reclamada remite detalle y grabaciones de las siguientes llamadas:

.- Llamada del cotitular con fecha 25/01/2023 a las 14:18h, procedente del número #TFNO_COT en la que el cotitular de la cuenta informa sobre la suplantación de identidad y bloquea tanto sus tarjetas como los usuarios de banca digital del titular y el cotitular.

.- Llamada de la parte reclamante con fecha 25/01/2023 a las 15:22h, procedente del número ******TELÉFONO.3***. En la que el titular anula sus tarjetas bancarias.

.- Llamada de la parte reclamante con fecha 28/01/2023 a las 00:39h,

procedente del número #TFNO_RTE, en la que se indica que la contraseña de acceso a la banca digital está bloqueada.

.- Llamada de la parte reclamante con fecha 30/01/2023 a las 19:12h, procedente del número #TFNO_RTE para obtener una nueva clave de acceso a la banca digital.

Para ello, la operadora solicita a la parte reclamante:

(…)

Se confirma que en esta llamada se han efectuado las preguntas de seguridad especificadas anteriormente en el procedimiento de identificación del usuario en banca telefónica.

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
Conclusión

Reclamación presentada debido al envío fraudulento de dos transferencias bancarias con cargo a una cuenta bancaria de la parte reclamante, la cual ha sido víctima de SIM swapping (duplicado de tarjeta SIM) que posibilitó dichas transferencias.

La parte reclamada reconoce los hechos denunciados: la realización de dos órdenes de transferencia desde el servicio de Banca a distancia, con cargo a la cuenta de la parte reclamante.

Se ha evidenciado que las transferencias se ordenaron con fecha 25 de enero de 2023 a las 13:21 y 13:32. Revisada la información aportada por el operador telefónico se ha acreditado que el presunto suplantador de identidad tiene activo el duplicado de tarjeta SIM fraudulento desde las 12:35 del día 25 de enero de 2023 hasta las 16:01 de ese mismo día.

En las grabaciones de las llamadas telefónicas se ha constatado que los presuntos suplantadores de identidad conocían todos los datos personales de la parte reclamante, incluso las respuestas a las preguntas de seguridad.

De la información recabada durante la investigación se ha puesto de manifiesto que los presuntos defraudadores consiguieron acceso a la banca digital contestando correctamente a todas las preguntas de seguridad y recibiendo así la clave de acceso a UNIVIA a través de SMS. Una vez obtenida la clave de acceso, vincularon su dispositivo seguro tras la recepción de SMS con clave OTP y firma con dicha clave y realizaron dos transferencias programadas, que fueron validadas también con firma OTP por SMS.

La parte reclamada ha proporcionado los protocolos de acceso a la banca online y sus principales controles de acceso, los procedimientos de identificación del usuario en banca telefónica, así como los procedimientos para la recuperación de claves desde los diferentes canales habilitados. La parte reclamada ha facilitado evidencias de la ejecución de tales procedimientos en el caso investigado.

La parte reclamada ha aportado información sobre las medidas de seguridad, implementadas en las fechas de los hechos, que había que superar previamente para poder solicitar una OTP a la hora de autorizar una operación.

La parte reclamada ha proporcionado el documento Justificante de abono como evidencia de la restitución de los importes reclamados.

La parte reclamada ha facilitado evidencias de sus campañas informativas y medidas de concienciación efectuadas para prevenir este tipo de fraudes.

Se ha confirmado que UNICAJA está certificada por AENOR respecto de la norma Privacidad de la Información ISO/IEC 27701:2021 con alcance Sistema de gestión de privacidad.

En síntesis, no existen evidencias de que la parte reclamada no tuviese implementadas medidas de seguridad adecuadas para evitar el fraude objeto de reclamación, si bien fueron superadas al tener los defraudadores conocimiento extensivo de los datos de los reclamantes.

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.

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 UNICAJA BANCO, S.A.U., 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.

940-301023

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