- **Expediente Nº: EXP202304633**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: Con fecha 8 de abril de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***4FINANCE SPAIN FINANCIAL SERVICES, S.A.U.*** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202304633

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: Con fecha 17 de febrero de 2023 se notificó a la División de Innovación Tecnológica de esta Agencia una brecha de seguridad de los datos personales remitido por ***4FINANCE SPAIN FINANCIAL SERVICES, S.A.U.*** con NIF ***A86521309*** (en adelante, VIVUS) como responsable del tratamiento. Como consecuencia de los hechos conocidos, con fecha 11 de abril de 2023, la Directora de la Agencia Española de Protección de Datos ordenó a la Subdirección General de Inspección de Datos (SGID) realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

SEGUNDO: 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:

Con fecha 17 de febrero de 2023 el responsable 4FINANCE SPAIN FINANCIAL SERVICES (en adelante VIVUS) realiza una notificación inicial de la brecha de datos personales con registro de entrada REGAGE23e00010208403, en la que manifiesta haber sufrido una brecha de confidencialidad por acceso no autorizado a datos de

clientes, incluyendo datos básicos, identificativos y de contacto de un total de 427 empleados. El responsable indica que siguen investigando el incidente.

Con fecha 31 de marzo de 2023 se recibe notificación adicional de la brecha de datos personales con registro de entrada REGAGE23e00021779018, en la cual se manifiesta:

- Descripción del incidente: consistente en un acceso no autorizado a los perfiles de clientes de la base de datos de VIVUS. El incidente fue investigado internamente.
- En cuanto a la fecha de inicio afirman que es desconocida, mientras que se determina como fecha de detección el 14 de febrero de 2023.
- Indican que los datos afectados no estaban cifrados.
- Respecto a las consecuencias para las personas afectadas, afirman que no resultan afectadas, salvo algunos inconvenientes muy limitados, pero en cualquier caso reversibles.
- En cuanto a las categorías de datos afectados se encuentran: datos básicos (Ej: nombre, apellidos, fecha de nacimiento), DNI, NIE, Pasaporte y / o cualquier otro documento identificativo, datos de medios de pago (Tarjeta bancaria, etc.…), y datos de contacto.
- Número de afectados: 9636 (No hay menores), afirman que no serán comunicados.
- Afirman que lo han puesto en conocimiento de autoridades policiales.
- Método detección: Comunicación de algún afectado.
- Se incluye resumen en el que se manifiesta que mediante ataque de fuerza bruta probando combinaciones de DNI/contraseña y Email/contraseña, los ciberdelincuentes tuvieron acceso a los datos personales del perfil de cliente de 9636 personas físicas. Estos datos incluían nombre y apellidos, DNI/NIE, fecha de nacimiento, dirección postal, email, IBAN, teléfono móvil y tarjeta bancaria seudonimizada. Afirman que 139 clientes han sido víctimas de fraude al haberse solicitado un crédito a su nombre a través de la aplicación, y una vez concedido han contactado vía WhatsApp con el cliente para solicitar devolución inmediata a un número de cuenta bancaria de los ciberdelincuentes.
- Afirman que como medida reactiva han implantado 2FA.
- El responsable manifiesta que no comunicará a los afectados al no considerar alto riesgo.

Desde la presente autoridad se ordenó al responsable para que llevase a cabo la comunicación de la brecha de datos personales a los interesados conforme al artículo 34 del RGPD sin dilación indebida y con objeto de que puedan adoptar las medidas que consideren oportunas para evitar aquellos riesgos que pudieran afectar a su persona.

En fecha 11 de abril de 2023 y registro de entrada REGAGE23e00023503645, se recibe escrito por parte de VIVUS confirmando el envío de la comunicación individualizada a todos los clientes afectados por la brecha, aportando captura de pantalla de un correo electrónico donde únicamente se aprecia la dirección remitente (vivus@sm.vivus.es) (pero no las direcciones destino). El cuerpo de este correo contiene información sobre el incidente ocurrido, sobre los datos que se han podido ver afectados, las medidas adoptadas por la compañía tras el incidente, las

recomendaciones sobre posibles medidas a adoptar por parte del cliente afectado y las posibles vías de contacto para obtener más información.

Asimismo, en relación con la brecha indicada se han recibido las siguientes reclamaciones en esta Agencia por parte de personas afectadas:

Reclamación 1: en fecha 03 de febrero de 2023 y registro de entrada REGAGE23e00007166247, se recibe reclamación de ***A.A.A.*** relacionada con la presunta suplantación de identidad al haberse solicitado un préstamo en su nombre y habiendo sido este concedido por VIVUS e ingresado en una cuenta bancaria de su titularidad. El traslado de esta reclamación a VIVUS se realiza en fecha 16 de marzo de 2023 y se recibe posteriormente respuesta en fecha 13 de abril de 2023 y registro de entrada REGAGE23e00024080156.

Reclamación 2: en fecha 05 de febrero de 2023 y registro de entrada REGAGE23e00007349177, se recibe reclamación de ***B.B.B.*** relacionada con la presunta suplantación de identidad al haberse solicitado un préstamo en su nombre y habiendo sido este concedido por VIVUS e ingresado en una cuenta bancaria de su titularidad. El traslado de esta reclamación se realiza en fecha 16 de marzo de 2023 y se recibe respuesta en fecha 13 de abril de 2023 y con registro de entrada REGAGE23e00024080388.

Reclamación 3: en fecha 05 de febrero de 2023 y registro de entrada REGAGE23e00007333527, se recibe reclamación de ***C.C.C.*** relacionada con la presunta suplantación de identidad al haberse solicitado un préstamo en su nombre y habiendo sido este concedido por VIVUS e ingresado en una cuenta bancaria de su titularidad. El traslado de esta reclamación a VIVUS se realiza en fecha 16 de marzo de 2023 y se recibió respuesta en fecha 13 de abril de 2023 y registro de entrada REGAGE23e00024082969.

Reclamación 4: en fecha 06 de febrero de 2023 y registro de entrada REGAGE23e00007574937, se recibe reclamación de ***D.D.D.*** relacionada con la presunta suplantación de la identidad al haberse solicitado un préstamo en su nombre y habiendo sido este concedido por VIVUS e ingresado en una cuenta bancaria de su titularidad. Aporta copia de la denuncia ante la Policía y copia de DNI. El traslado de esta reclamación a VIVUS se realiza en fecha 16 de marzo de 2023 y se recibió respuesta en fecha 13 de abril de 2023 y registro de entrada REGAGE23e00024084764.

Reclamación 5: en fecha 11 de febrero de 2023 y registro de entrada REGAGE23e00008763533, se recibe reclamación por parte de ***E.E.E.*** relacionada con la presunta suplantación de identidad al haberse solicitado un préstamo en su nombre y habiendo sido este concedido por VIVUS e ingresado en una cuenta bancaria de su titularidad de la cual era conocedora esta compañía. Se adjunta copia de la denuncia interpuesta ante la Policía Nacional. El traslado de esta reclamación a VIVUS se realiza en fecha 16 de marzo de 2023 y se recibió respuesta en fecha 13 de abril de 2023 y con registro de entrada REGAGE23e00024084642.

Reclamación 6: en fecha 23 de febrero de 2023 y registro de entrada REGAGE23e00011468445, se recibe reclamación de ***F.F.F.*** relacionada con la

presunta suplantación de la identidad en la solicitud de un préstamo concedido por VIVUS e ingresado en una cuenta bancaria de su titularidad. El traslado de esta reclamación a VIVUS se realiza en fecha 16 de marzo de 2023 y se recibió respuesta en fecha 13 de abril de 2023 y registro de entrada REGAGE23e00024084525.

En fecha 16 de marzo de 2023 se dio traslado al responsable VIVUS de las distintas reclamaciones recibidas, solicitándose la siguiente información:

- Descripción detallada y cronológica de los hechos y especificación de las causas del incidente.
- Número de personas afectadas, categoría de los datos involucrados y posibles consecuencias para los afectados.
- Acciones tomadas para solucionar el incidente y medidas para que no vuelva a suceder.
- Análisis de riesgos del tratamiento, medidas de seguridad preventivas implantadas y evaluación de impacto en su caso.
- Copia del Registro de Actividades de Tratamientos.
- Si se ha comunicado a los afectados, el canal utilizado, fecha de comunicación y detalle del mensaje enviado. En caso de no haberse realizado la comunicación, indicar los motivos.

VIVUS respondió en fecha 13 de abril de 2023 y de forma individualizada a cada uno de los traslados realizados por esta entidad. De contenido de los mencionados escritos se extrae la siguiente información relevante:

- Para cada una de las reclamaciones se aporta un análisis detallado del escenario de afectación del cliente concreto, señalando las fechas en que tuvieron constancia de la correspondiente incidencia, así como los detalles relativos a las comunicaciones que tuvieron con cada cliente.
- En relación con las causas provocaron el incidente afirma:
    - Que en fecha 10 de agosto de 2022 fue cuando recibió la primera notificación de un cliente, el cual denunciaba haber recibido dinero en su cuenta bancaria en virtud de un préstamo que no había solicitado.
    - Que los atacantes realizaron numerosos intentos de inicio de sesión utilizando distintas direcciones IP y haciendo uso del DNI o e-mail del cliente (como nombre de usuario) y una contraseña, obtenidos a partir de fuentes externas y ajenas a VIVUS. Una vez accedían solicitaban préstamos en nombre del cliente los cuales eran aceptados y desembolsados en la cuenta del mismo. Posteriormente, los atacantes procedían a contactar con dicho cliente a través de WhatsApp solicitando la devolución del importe a un número de cuenta que era controlada por ellos.
- Afirma que existe un total de 9636 afectados y que la tipología de datos afectados era la existente en el área personal de usuario web. De forma concreta, se encontraba: Nombre y Apellidos, Fecha Nacimiento, Dirección Postal, Email, Teléfono Móvil, DNI/NIE, IBAN, Tarjeta bancaria seudonimizada, así como datos sobre préstamos en activo que tuviera concedido el usuario aún no finalizado como el importe, los intereses devengados, plazo y vencimiento.
- Respecto a las posibles consecuencias para los afectados sostiene que la naturaleza del conjunto de datos personales al que se accedió no

proporcionaba información sustancial sobre la situación financiera y que se consideraban que no entrañaba un alto riesgo para los derechos y libertades de los afectados.

- En relación con las acciones adoptadas por el responsable para solucionar el incidente, comunican la adopción de las siguientes medidas:
    - Registrar la brecha en registro de incidentes.
    - Denuncia ante Policía.
    - Comunicación oficial a los distintos clientes y a través de la página web sobre información de que la entidad no hace uso de WhatsApp.
    - Restablecer todas las contraseñas de los usuarios con fecha 11 de febrero de 2022.
    - Implantación de un sistema de doble factor de autenticación implementado en fecha 21 de febrero de 2023.
    - Modificación de la política de contraseñas de inicio de sesión, aumentando su complejidad y obligando a modificarla a todo usuario.
    - Mejora del funcionamiento del sistema SIEM, revisando el procedimiento interno de respuesta ante incidentes.
    - Inclusión de clientes afectados por fraude en una determinada categoría con el fin de evitar consecuencias derivadas.
    - Envío de comunicación a todos los clientes afectados. Se solicitará su acreditación en nuevo requerimiento.
- En respuesta a nuestra solicitud para que aporten el análisis de riesgos y las medidas de seguridad que se concluyeron, afirman lo siguiente: "*El tratamiento de los datos de acceso de los clientes a los perfiles web y la adquisición de aplicaciones online no suponen riesgos elevados para la protección de datos, por lo que no se ha realizado una Evaluación de Impacto de dichos tratamientos. No obstante, para garantizar las medidas técnicas y organizativas se implementaron las siguientes medidas de seguridad específicamente relevantes para el incidente de seguridad informado:*
    - *Monitoreo de seguridad.*
    - *Política de contraseñas: se definen reglas de complejidad mínima para las contraseñas utilizadas para iniciar sesión en los perfiles de los clientes.*
    - *Protección de aplicaciones web.*
    - *Cortafuegos y sistemas de prevención de intrusiones. Protección contra Malware.*
    - *Informes, gestión e investigación de incidentes de seguridad: la gestión de incidentes de seguridad está bien establecida y cumple con las expectativas del Grupo 4finance."*
- Afirma que, desde septiembre hasta finales de noviembre de 2020, el departamento de seguridad de la información realizó una evaluación integral de riesgos de seguridad de la información con el objetivo de evaluar y mejorar las medidas de seguridad en las áreas de software, red y distribución de datos, personas y procesos. Como resultado de ello se mejoraron las medidas de seguridad para proteger a la organización contra ataques automatizados de fuerza bruta relacionados con la averiguación de contraseñas.
- Indica haber realizado una prueba de penetración externa de la aplicación vivus.es por una firma de servicios profesionales en fechas comprendidas entre el 9 y el 17 de febrero de 2022.

- Aportan el Registro de Actividades de Tratamiento, en lengua inglesa, con la actividad de tratamiento afectada por la brecha: "*Customer Registration and Contract Signing*".
- Señalan que la violación ha sido comunicada a todos los clientes afectados en fecha 11 de abril de 2023 y que fue notificada inicialmente a la AEPD el 17 de febrero de 2023.
- Afirman que entre las medidas adoptadas para evitar nuevos incidentes ha sido clave la implantación del sistema de doble autenticación (2FA) en el servicio web.

En el marco de esta investigación, en fecha 30 de junio de 2023 se realiza un primer requerimiento de información al responsable VIVUS:

- Que se acredite la comunicación de la brecha realizada, pues únicamente se había aportado el texto de la comunicación.
- Se solicita la adopción de las medidas organizativas existentes en la organización para gestionar incidentes de seguridad que afecten a datos personales (la gestión de brechas de datos personales).
- Que se acrediten las comunicaciones que mantuvo la entidad con el primer cliente afectado que contactó con la empresa en fecha 10 de agosto de 2022.
- Que se acredite de los análisis de riesgos para garantizar tanto la seguridad de los tratamientos como los derechos y libertades de las personas afectadas, así como, en su caso, las evaluaciones de impacto.
- Que acrediten las medidas reactivas implantadas tras la brecha de seguridad, incidiendo en aquellas medidas destinadas a parar los ataques de fuerza bruta y a monitorizar la trazabilidad de los usuarios.
- Que se acredite la denuncia interpuesta ante los cuerpos de seguridad.
- Investigar los detalles del procedimiento existente para identificar a los clientes que solicitan préstamos a través del área web.

En fecha 19 de julio de 2023 y registros de entrada REGAGE23e00048973515 y REGAGE23e00049304085, se recibe respuesta al requerimiento anterior, extrayéndose de su análisis la siguiente información relevante para la investigación:

- Afirma que las credenciales de acceso utilizadas ya estaban disponibles por parte de los atacantes con carácter previo a la brecha, posiblemente procedente de filtraciones de terceras partes y fuentes externas, por lo que el presente ataque no corresponde a un ataque de fuerza bruta sino a un ataque "credential stuffing".
- Aportan documento con el volumen total de intentos de inicio de sesión fallidos desglosado por fechas. De su análisis destacan los días comprendidos entre el 4 y el 14 de febrero de 2023, con picos de hasta 18 millones de intentos fallidos en un único día.
- Indica que en los momentos previos a la brecha los sistemas de VIVUS estaban protegidos contra un elevado número de conexiones fallidas de la siguiente forma:
    - La protección contra ataques de "fuerza bruta" se implementó en la aplicación web vivus.es, aumentando el tiempo de espera de autenticación después de un intento fallido para un usuario específico.

Tras los siguientes intentos de autenticación fallidos, el tiempo de espera se duplicaba *para estos usuarios*.

- La protección contra un gran número de peticiones web falsas se implementó en el software WAF *Imperva,* principalmente con el propósito de prevenir ataques de denegación de servicio (DoS). El ajuste de configuración consistió bloquear cualquier fuente que genere más de 450 peticiones por segundo.
- Afirman que los sistemas de seguridad para el producto *vivus.es* estaban preparados para detectar y alertar sobre patrones de ataque habituales en aplicaciones web (Inyecciones SQL, Cross Site Scripting (XSS), File Inclusion Attacks, Directory Traversal Attacks, DoS/DDoS attacks etc), pero no detectaban ni alertaban sobre un elevado número de intentos de conexión fallidos.

- Se aporta grabación de la llamada telefónica recibida por parte del cliente afectado el 11 de agosto de 2022 a las 20:46 horas, en la cual el usuario afectado comunica haber recibido dinero de un préstamo que no había solicitado. Posteriormente, en fecha 12 de agosto de 2022, este cliente remitió vía email la copia de la denuncia presentada, correo que fue respondido por VIVUS el 17 de agosto de 2022 informando al cliente de lo siguiente: "*nuestra compañía ha procedido a activar el procedimiento aplicable a estos casos, que incluye la gestión del expediente como caso de fraude lo que implica la paralización de todas las acciones de recobro de la deuda ya que una vez denunciados los hechos no le será reclamada por nuestra parte*".
- Del informe preliminar del director de INFOSEC (Departamento de Seguridad de VIVUS) redactado en fecha 15 de marzo de 2023 se extraen las siguientes afirmaciones:
  - El 21 de febrero de 2023 se implementó el 2FA que paralizó el ataque.
  - Hubo 3905 casos de éxito de los 218401 intentos realizados utilizando combinación de DNI/CONTRASEÑA.
  - Hubo 6977 casos de éxito de los 2728941 intentos de acceso realizados por los atacantes usando combinaciones de EMAIL/CONTRASEÑA.
  - Del total de los accesos exitosos afirman evidencias de acceso a datos de un total de 9497 clientes de VIVUS.
- Acreditan dos análisis de penetración realizados en febrero de 2022 (a la aplicación móvil de VIVUS) y junio de 2023 (a la aplicación web que daba acceso al área personal de clientes). Del análisis de dichos informes se concluye que las vulnerabilidades que se detectaron no están vinculadas con el vector de ataque de la presente brecha de seguridad.
- Afirma que cada incidente detectado era analizado y gestionado por el procedimiento de gestión de incidentes y que se actualizó el análisis de riesgos. Se acredita documentalmente el procedimiento de gestión de incidentes anterior.
- Se aporta cuatro documentos con distintos análisis y evaluaciones de la severidad del incidente, realizados en distintos momentos temporales (a medida que se iban descubriendo casos), utilizándose para ello una metodología interna basada en la metodología propia de ENISA. En estos análisis se asignaba con un valor cuantitativo el nivel de riesgo del incidente, valorándose para ello tres parámetros principales:
  - El contexto de la brecha (siendo 1 mínimo y 4 máximo).

- La facilidad de identificación de la persona afectada (con valor entre 0 y 1 como máximo)
- Las circunstancias en las que se produjo la brecha (con valor de gravedad de 0 a 2 como máximo).

Tras el análisis se asignaba un valor final al nivel de riesgo del incidente, haciendo uso para ello de la siguiente fórmula: [*Severidad Incidente= (Contexto*Facilidad De Identificación Del Afectado) + Circunstancias*].
Del análisis de cada documento aportado con las evaluaciones anteriores se extrae para el presente informe:

- Se aporta un primer documento con la evaluación inicial del incidente cuando únicamente se conocía un caso afectado, el cual está firmado el con fecha 11 de agosto de 2022 por la DPD de la entidad. Para cuantificar el riesgo se asignó el valor mínimo al contexto (1), un valor de 0.75 a la Facilidad de Identificación (que tenía el siguiente significado según metodología "*La identificación es posible a partir de los datos violados, con necesidad de investigación para descubrir la identidad del individuo*"), concluyendo la evaluación que el incidente *NO tenía la suficiente entidad para comunicarla a la AEPD*. Esto contrasta con la tipología de datos filtrados a través del área web de cliente, ya que el conjunto de estos datos permitía una fácil identificación del individuo sin necesidad de investigación especial adicional.
- Se aporta un nuevo documento con una segunda evaluación del incidente cuando se conocían 11 clientes afectados, firmado por la DPD en fecha 1 de septiembre de 2022 y concluyéndose con un valor del riesgo BAJO, afirmándose que "*la severidad del incidente NO es de suficiente entidad para que deba notificarse a la autoridad competente ni a los interesados".* En la valoración del riesgo también se asignó un valor de 0.75 a la facilidad de identificación, siendo el valor máximo de la escala utilizada 1, con el significado "*La identificación es posible a partir de los datos filtrados sin necesidad de realizar una investigación especial para descubrir la identidad del individuo*". El conjunto de datos que se estaban filtrando a través del área web del cliente eran, entre otros, el Nombre y Apellidos, Fecha Nacimiento, Dirección Postal, Email, Teléfono Móvil, DNI/NIE, lo cuales resultan suficientes para obtener una identificación de la persona afectada sin necesidad de realizar investigación especial.
- Se aporta un tercer documento con la evaluación del incidente cuando se conocieron 83 clientes afectados, firmado por la DPD en fecha 14 de noviembre de 2022, cuyo resultado fue un valor de riesgo BAJO, afirmándose que "*el incidente NO* tiene *la suficiente entidad como para que deba comunicarse la brecha de seguridad a la Agencia Española de Protección de Datos ni a los interesados, en tanto que la información personal presuntamente vulnerada era mínima, y teniendo en cuenta que el acceso ha sido completamente restringido".* Se asignó el mismo valor para el Contexto y Facilidad de Identificación que en puntos anteriores.
- Un documento con la evaluación del incidente cuando se disponía de la siguiente información: "*menos de 35000 inicios de sesión exitosos, pero*

se desconoce el alcance de los datos de acceso, actualmente 427 clientes han sido defraudados (a fecha 17 de febrero de 2022)". Este documento está firmado por la DPD en fecha 17 febrero de 2023 y en la evaluación se concluye un nivel de riesgo MEDIO, asignándose en este caso un valor máximo de 1 a la Facilidad de Identificación del cliente afectado (superior al valor de 0.75 dado en los documentos anteriores). No obstante, el conjunto de datos personales filtrados era el mismo que para los clientes afectados anteriores. El resultado de este análisis llevó a la siguiente conclusión: "*[…] debe comunicarse a la Agencia Española de Protección de Datos. No obstante, a la vista de la categoría de datos vulnerada no se considera que haya riesgos para los derechos y libertades de los interesados, en tanto que la información personal vulnerada es mínima, por lo que se concluye que no es necesario realizar una comunicación a los clientes*".

  - Dentro de los cuatro documentos anteriores se encuentra un apartado que hace referencia a la valoración del incidente por parte del departamento de seguridad de VIVUS: "*Clasificación de gravedad determinada por la Unidad de Seguridad de la Información de acuerdo con el Procedimiento de Respuesta a Incidentes de Seguridad de la Información: ALTA GRAVEDAD (Nivel 1) debido al impacto financiero*", Pese a dicha afirmación se valoró como no necesario notificar el incidente.

- En relación con los cuatro documentos anteriormente analizados en los que VIVUS concluyó un nivel de riesgo y severidad de la brecha, por parte de esta inspección se procede a realizar una simulación con la herramienta *Asesora-Brecha*, utilizando los mismos datos que ya se disponían por parte de VIVUS en septiembre de 2022, y obteniéndose como resultado la *obligación de notificar la brecha ante esta Agencia sin dilación indebida.* De la misma forma, se hace uso de la herramienta *Comunica-Brecha* con la información que disponía el responsable en septiembre de 2022, obteniéndose como resultado "*Debería comunicar la brecha a la AEPD*". Los datos de entrada utilizados en ambas herramientas fueron los siguientes:
  - *Sector de actividad: Entidad Financiera*
  - *La brecha es consecuencia de ciberincidente con acceso no autorizado a datos personales.*
  - *Datos afectados: básicos, número DNI, dirección postal, teléfono, email, financieros sin medios de pago.*
  - *Personas afectadas: 56 (información que ya se disponía por el responsable a fecha 27 de septiembre de 2022, fecha en la que VIVUS interpone denuncia aportando el listado de afectados conocidos en ese momento).*
  - *Para las posibles consecuencias se ha considerado en la simulación el menor daño posible (pese a que las consecuencias reales y conocidas en esta fecha eran posiblemente de mayor gravedad), asignándose el valor: "las personas pueden encontrar algunos inconvenientes muy limitados y reversibles que superarán sin problema".*
- Tomando en consideración el procedimiento de valoración de severidad de ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches*, que VIVUS ha establecido como referencia:

- El *Contexto (DPC)* se valoró con valor 1, no obstante, debió asignarse valor superior, ya que según esta metodología (se hace por el presente inspector la traducción no oficial al idioma español):
  - *Datos simples, Puntuación básica preliminar = 1. La puntuación DPC podría aumentarse en 1, por ejemplo, cuando el volumen de los «datos simples» o las características del responsable del tratamiento sean tales que se pueda habilitar la elaboración de perfiles de la persona o se puedan hacer supuestos sobre la situación social/financiera de la persona), con DPC = 2, o bien:*
  - *Datos financieros, Puntuación básica preliminar = 3. La puntuación del DPC podría reducirse en 1, por ejemplo, cuando el conjunto de datos específicos incluye cierta información financiera, pero aún no proporciona ninguna visión significativa de la situación financiera de la persona (por ejemplo, números simples de cuentas bancarias sin más detalles), con DPC = 2, o bien:*
  - *Datos financieros, Puntuación básica preliminar = 3. La puntuación del DPC podría aumentarse en 1, por ejemplo, cuando, debido a la naturaleza o al volumen del conjunto de datos específicos, se divulgue información financiera completa (por ejemplo, tarjeta de crédito) que pueda permitir el fraude o se cree un perfil social/financiero detallado. DPC=4.*
- La *Facilidad de Identificación* del afectado debería valorarse como *EI = 1*, y no un valor inferior (VIVUS otorga un valor EI=0,75), tal y como se ha analizado en el punto anterior.

De ello se concluye que el valor asignado desde VIVUS a las distintas variables de la fórmula de cálculo de severidad fue inferior a lo que se debió asignar, dado el escenario que se estaba conociendo sobre el incidente de seguridad, debiéndose haber obtenido un resultado final de severidad que podría estar entre MEDIA y MUY ALTA. Dicho resultado hubiera dado lugar a que VIVUS comunicara la incidencia a la AEPD y a los afectados desde el primer suceso.

- En relación con la denuncia interpuesta por parte del responsable, en la respuesta al requerimiento se afirma: "*los casos afectados se recopilaban de forma manual y dada la dificultad a la hora identificarlos a través de la información parcial disponible, fueron necesarias hasta 4 ampliaciones de la denuncia inicial*", aportando en la respuesta la siguiente documentación.
  - Copia de la denuncia inicial interpuesta el 12 de agosto de 2022 con la información del cliente afectado el 11 de agosto de 2022.
  - Copia de la ampliación a la denuncia anterior interpuesta el 28 de septiembre de 2022 en la que afirman que en días posteriores han sido afectados nuevos clientes, solicitándose prestamos de forma fraudulenta con un importe global de 42610 euros y habiendo sido estafado 19830 euros. En esta ampliación aportan un listado con los datos de los clientes afectados a los que VIVUS realizó el ingreso del importe del préstamo solicitado de forma fraudulenta, encontrándose en este listado aproximadamente 56 números de cuenta bancaria de clientes distintos. Del análisis de este listado por el presente inspector llama la atención que la misma IP utilizada en la solicitud del préstamo

de 10 de agosto de 2022 (del que se tuvo constancia el 11 de agosto de 2022 tras recibir comunicación del cliente afectado), fue utilizada posteriormente para solicitar con éxito dos nuevos préstamos fraudulentos en fecha posterior, el 8 de octubre de 2022 a las 10:53 y a las 11:11.
    - En las denuncias acreditadas, VIVUS afirma que los atacantes habían entrado en el área personal de cada uno de estos clientes y habían solicitado un nuevo préstamo en la modalidad de contratación a distancia en nombre del cliente afectado.
- Aportan copia de un documento con las condiciones generales del préstamo que se aceptan (mediante la marcación de un checkbox) en el momento de la solicitud del préstamo online.
- En respuesta a nuestra solicitud para que detallen los procedimientos existentes para identificar a un cliente cuando se solicitaba un préstamo a través del portal web, afirman que existen dos vías de posible identificación:
    - Para solicitar un PRIMER PRÉSTAMO se utiliza el denominado “procedimiento onboarding”. Afirman que este procedimiento no fue el utilizado por los atacantes, pues todos los clientes afectados solicitaron previamente un primer préstamo. Este procedimiento de identificación inicial consiste en:
        - En una primera pantalla donde se solicita datos de contacto y se recaba consentimiento de política de privacidad y de comunicaciones comerciales.
        - En una segunda pantalla se requiere número de DNI y una contraseña para crear la cuenta o perfil.
        - En una tercera pantalla se solicita nombre, apellidos y fecha nacimiento.
        - En una cuarta pantalla se solicita una dirección en España.
        - En una quinta pantalla se solicita número de teléfono y se verifica posteriormente mediante el envío de un SMS con un código único de un solo uso que el usuario debe introducir.
        - En una sexta y última pantalla se ofrecen distintas opciones de acreditación de la identidad, bien aportando las credenciales de Banca Online (a través del servicio TINK), bien aportando la documentación acreditativa a través de un formulario y esperar llamada telefónica que verificaría los datos.
    - Para solicitar SEGUNDOS Y POSTERIORES préstamos (única vía afectada por el incidente de seguridad), únicamente se requiere la identificación en el área personal web del cliente, utilizando para ello las credenciales de usuario (DNI o EMAIL + Contraseña). Una vez ingresado en el área web bastaba con seleccionar la cantidad de dinero que se desea solicitar, el plazo de devolución deseado y aceptar las condiciones de contratación activando una casilla de verificación (checkbox).
- En relación con este proceso de identificación afirman haber adoptado e implantado tras la brecha de seguridad las siguientes medidas reactivas:
    - El restablecimiento de todas las contraseñas de los clientes de forma que, cuando los clientes acceden a su área personal, se obliga a establecer una nueva contraseña.

- Implementación de un segundo factor de autentificación (2FA), generando un código de verificación de 4 dígitos que se envía a través del canal SMS al número de teléfono registrado del cliente. Este sistema de doble Factor de Autenticación 2FA fue reforzado posteriormente en abril de 2023 mediante la adición de dos nuevas reglas (bloqueo de 5 minutos tras 3 intentos fallidos, siendo necesario nuevo código de verificación, y la necesidad de un nuevo código si el cliente se conecta y desconecta de su perfil).

- Acreditan un documento actualizado del protocolo interno para la gestión de incidentes, cuya actualización tiene fecha 29 de abril de 2023. Las modificaciones introducidas en el mismo han consistido han sido:
  - *Ajustar los plazos de las fases de respuesta a incidentes internos, en caso de retraso en la detección, para cumplir el plazo de notificación del GDPR.*
  - *Se incluye la posibilidad de involucrar a expertos legales externos en la respuesta a las violaciones de datos personales.*
  - *Se revisa la plantilla de evaluación del riesgo de la violación de datos personales incluyendo nueva calculadora de gravedad mejorada.*
- Acreditan las siguientes medidas técnicas reactivas implantadas para mejorar la detección de incidentes de seguridad:
  - Cuando los intentos de autenticación fallidos desde una única dirección IP de origen superan los umbrales diarios definidos, el sistema *Splunk SIEM* genera una alerta en tiempo real que se envía a un correo electrónico de alerta al departamento de seguridad y a *un canal de Slack*.
  - Cuando los eventos de autenticación exitosa se originan desde una única dirección IP de origen y están accediendo a más de 4 cuentas de clientes distintas en un mismo día, una alerta en tiempo real es generada por el sistema *Splunk SIEM* y es enviada a un correo electrónico del departamento de seguridad.
  - Cuando los atacantes utilizan direcciones IP estáticas durante un período prolongado éstas se introducen en una *lista negra especial* y en caso de intento de autenticación posterior se genera una alerta en tiempo real por el sistema *Splunk SIEM* y se envía al correo electrónico de alerta al departamento de seguridad.
- En respuesta a nuestra solicitud para que se acrediten los análisis de riesgos para las actividades de tratamiento afectadas por la brecha, realizan la siguiente afirmación: "*En mayo de 2022, con base en la planificación de un nuevo proceso de onboarding (completado en Octubre de 2022) se realizó el correspondiente Análisis de Riesgos en materia de Protección de Datos relativo a la Actividad de tratamiento denominada CUSTOMER REGISTRATION AND CONTRACT SIGNING.*" Se aporta documento acreditando este análisis de riesgos para los derechos y libertades de las personas físicas afectadas por los tratamientos de la actividad mencionada. De su análisis se extrae:
  - Tiene fecha de creación 06 de mayo de 2022.
  - Se identifican amenazas y factores de riesgo para los derechos y libertades de los interesados, diferenciando entre riesgo inherente y el riesgo residual, haciendo referencia de si el riesgo ha sido mitigado total

o parcialmente. No obstante, no se listan las medidas de seguridad concluidas a raíz de este análisis para mitigar los riesgos.

- Se incluye un apartado de conclusiones donde se afirma que el nivel de riesgo inherente es ALTO y residual MEDIO, realizándose también la siguiente afirmación: "*la actividad analizada implica, entre otros, la elaboración de perfiles sobre cuya base se toman decisiones que pueden producir efectos jurídicos para las personas físicas. Lo anterior, con base en el documento denominado LISTAS DE TIPOS DE TRATAMIENTOS DE DATOS QUE REQUIEREN EVALUACIÓN DE IMPACTO RELATIVA A PROTECCIÓN DE DATOS de la Agencia Española de Protección de Datos, implica una obligación para 4FINANCE como responsable del tratamiento de llevar a cabo una EIPD de forma obligatoria del tratamiento analizado.*"

- Se acredita documento para la actividad de tratamiento "*Customer Registration And Contract Signing",* con fecha de realización 13 de mayo de 2022. En ella se realiza un análisis y descripción sistemática del tratamiento, un análisis de las partes intervinientes, una evaluación de la necesidad y proporcionalidad del tratamiento y una evaluación y gestión de los riesgos, listándose medidas adoptadas en su mitigación.
- En respuesta a nuestra solicitud para que acrediten el envío de la comunicación realizada sobre el incidente a las personas afectadas, aportan listado Excel con que contiene el Email y Nombre/Apellidos de personas comunicadas, pero no se detalla la fecha en la que se realizó el envío.

En fecha 2 de agosto de 2023 se realiza nuevo requerimiento de información al responsable VIVUS respecto a las siguientes actuaciones:

- La correcta acreditación de las comunicaciones realizadas.
- La fecha de inicio de la actividad de tratamiento "*Customer Registration And Contract Signing".*
- La confirmación de si existían análisis de riesgos en fecha anterior a mayo de 2022, y su acreditación en su caso.

En fecha 18 de agosto de 2023 y registro de entrada REGAGE23e00056162842 se recibe respuesta al requerimiento anterior de cuyo análisis se extrae la siguiente información relevante para la investigación:

- Se acredita la comunicación masiva enviada a los clientes afectados en fecha 11 de abril de 2023 a las 20:09.
- Afirman que la actividad de tratamiento denominada "*Customer Registration And Contract Signing*" se inició el día 20 de diciembre de 2012 con motivo del registro del primer cliente en la plataforma.
- En relación a la confirmación de si existían análisis de riesgos realizados en fecha anterior al que ya habían aportado (mayo de 2022), se expone lo siguiente:
    - Que tras la entrada en vigor del RGPD se han realizado auditorías internas y externas en protección de datos, una de ellas a finales de 2019 y en la cual se detectó la necesidad de realizar y documentar análisis de riesgos que diera cumplimiento al art 32 del RGPD. Como consecuencia de ello "*la compañía elaboró en mayo de 2020 un análisis de riesgos en formato excel (Risk Assessment Spain) que recogía la probabilidad de ocurrencia de determinados riesgos. No*

obstante, de acuerdo con lo recogido en el informe posterior de auditoría externa del año 2021, dicho análisis de riesgos no recogía adecuadamente los riesgos para los derechos y libertades de los afectados". Se acredita captura de pantalla de este documento Excel. Del análisis por el presente inspector se concluye que se analizan factores de riesgo de forma generalizada y no para una actividad de tratamiento concreta. Además es realizado desde la perspectiva de las consecuencias e impacto para la propia compañía (pérdidas económicas e impacto financiero), no tratándose, por tanto, de un análisis de riesgos para la actividad de tratamiento afectada por la brecha que tuviera en cuenta amenazas tanto para la seguridad de los tratamientos como para los derechos y libertades de los interesados.

- Se acredita un nuevo documento "*INFORME DE ANALISIS DE RIESGOS RELATIVA A PROTECCIÓN DE DATOS*" con fecha de redacción 29 de mayo de 2021 y firmado por la Delegada de Protección de Datos. Del análisis de este documento por el presente inspector se concluye:
  - En la introducción se afirma el siguiente texto: "*El presente documento es el resultante de la realización de las actividades constitutivas de la Evaluación de Impacto en materia de Protección de Datos (en adelante DPIA), conforme a lo establecido en el artículo 35 y 36 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y las Guías prácticas elaboradas por la AEPD*".
  - Contiene los siguientes apartados *Aspectos Preparatorios y Organizativos, Identificación de Datos Afectados y Evaluación del Nivel de Riesgo*.
  - En el apartado referente a la evaluación del nivel de riesgo se analizan los siguientes factores de riesgo identificados:
    - *Intrusión Ilegítima en sistemas.*
    - *Fraude interno.*
    - *Errores humanos y tecnológicos (tanto en la gestión de préstamos, gestión de reclamaciones, comunicaciones comerciales y gestión de datos de empleados).*
  - Este análisis no es específico para la actividad de tratamiento afectada por la brecha y no tiene en cuenta factores de riesgos para los derechos y libertades de las personas afectadas por la actividad de tratamiento.
- Se afirma que en fecha posterior sí se elaboró un análisis de riesgos específico por actividad de tratamiento siguiendo la Guía de Gestión de Riesgos de esta Agencia. Este análisis se corresponde con el aportado en respuesta al requerimiento anterior y que tiene fecha de redacción mayo de 2022.
- Afirman que la compañía está trabajando en la implementación de una herramienta informática (CompaaS) que permitirá una gestión más efectiva y ágil el cumplimiento de sus obligaciones, así como registrar y revisar periódicamente su análisis de riesgos en materia de protección de datos.

CONCLUSIONES

1. El vector de ataque de la brecha estuvo causado por el acceso ilegítimo por parte de los atacantes al área web de múltiples clientes, utilizando credenciales válidas que estos conocían previamente (pares de DNI o Email + Contraseña), posiblemente a raíz de alguna filtración. El modus operandi era el siguiente:

- Una vez que los atacantes accedían al área personal del cliente afectado, procedían a solicitar préstamos que fueron aceptados de forma automática, ingresándose el importe en la cuenta bancaria asociada al cliente.
- Posteriormente, los atacantes contactaban por vía WhatsApp haciéndose pasar por VIVUS, informándoles de que por error se había concedido un nuevo préstamo en su nombre y en la que solicitaban su devolución en un número de cuenta que era controlada por los propios atacantes.

2. Ha quedado constatado que la brecha afectó a 9497 clientes de VIVUS cuya identidad fue suplantada, habiendo solicitado en nombre de muchos de ellos préstamos personales que fueron concedidos de forma automática por la plataforma.

3. En cuanto a los datos filtrados a través del área web del cliente consistieron en: nombre y apellidos, fecha nacimiento, dirección postal, email, teléfono móvil, DNI/NIE, IBAN, tarjeta bancaria seudonimizada, así como datos relativos a préstamos que se encontraban en vigor frente a la compañía.

4. Ha quedado constatado que VIVUS detectó inicialmente la brecha el 11 de agosto de 2022 a raíz de la comunicación recibida por parte de un cliente afectado. Posteriormente, en fecha 1 de septiembre de 2022 la compañía tenía constancia de al menos 11 casos afectados, y en fecha 14 de noviembre de 2022 al menos 83 clientes afectados. No obstante, la brecha no fue notificada ante la presente autoridad hasta el día 17 de febrero de 2023, cuando ya se tuvo constancia de afectación de, al menos, 427 defraudados.

5. Ha quedado acreditado que VIVUS analizó el nivel de riesgo y severidad de la brecha en distintas fechas (11 de agosto de 2022, 1 de septiembre de 2022 y 14 de noviembre de 2022), haciendo uso de una metodología interna basada en ENISA consistente en la utilización de una fórmula para calcular el valor final del riesgo a partir de variables como el *Contexto del Incidente*, la *Facilidad de Identificación* y las *Circunstancias del incidente*, asignando un valor a cada una de estas variables según una escala detallada en la propia metodología. Del valor final del riesgo obtenido de la fórmula anterior la parte reclamada consideró que NO era necesario notificar la violación a la AEPD ni a los afectados.

6. Se ha constatado que el valor asignado a algunas de estas variables fue inferior al que se debió asignar, teniendo en cuenta el conocimiento que se tenía sobre el incidente en estos momentos. Tras el uso, por parte del presente inspector, de las herramientas *Asesora Brecha* y *Comunica Brecha* utilizando la información que VIVUS conocía en septiembre de 2022, se ha obtenido como resultado en ambas herramientas la necesidad de notificar tanto a la AEPD como a los afectados.

7. En relación con la comunicación de la brecha a los afectados, ha quedado acreditado que el responsable finalmente comunicó el incidente a todos los afectados en fecha 11 de abril de 2023, tras recibir la orden de comunicar por parte de esta autoridad.

8. Ha quedado constado que no existían análisis de riesgos específicos para los derechos y libertades de las personas interesadas en la actividad de tratamiento afectada por la brecha hasta el de 6 mayo de 2022. Con anterioridad a esta fecha existieron análisis de riesgos que no eran específicos de una actividad de tratamiento y dirigidos al posible impacto financiero repercutido para el propio responsable, no analizándose riesgos para los derechos y libertades de las personas afectadas por los tratamientos. Ha quedado también acreditado que la actividad de tratamiento afectada por la brecha constaba en el Registro de Actividades de Tratamiento de VIVUS y que se inició en diciembre de 2012.

9. Ha quedado acreditada la existencia de una Evaluación de Impacto para la Protección de Datos (EIPD) de la actividad de tratamiento afectada por la brecha, realizada el 13 de mayo 2022 y que recoge la siguiente información:

- Un análisis y descripción sistemática del tratamiento
- Un análisis de la necesidad y proporcionalidad del tratamiento
- Un análisis y gestión de los riesgos.

10. En relación con las medidas preventivas implantadas en momentos previos a la brecha, se constata el siguiente listado:

- Monitorización de la seguridad: revisión de eventos, pruebas de seguridad y evaluación de vulnerabilidades.
- Política de contraseñas con reglas de complejidad mínima para iniciar sesión en el área web de clientes.
- Medidas contra ataques de fuerza bruta basadas en tiempos de espera tras intentos fallidos de inicio de sesión.
- Cortafuegos y protección contra antimalware.
- Prevención de ataques de DDOS, inyección SQL y otras amenazas a través del software *Imperva Web Aplication Firewall*.
- Análisis de penetración del portal web vivus.es en junio de 2023, previamente (febrero 2022) se había realizado otro análisis de penetración, pero con el foco en la aplicación móvil de VIVUS.
- Procedimiento interno para gestionar los incidentes de seguridad.

11. En relación con las medidas reactivas implantadas por el responsable tras conocerse la brecha de seguridad, se han constatado las siguientes:

- Implantación de un sistema de Doble Factor de Autenticación (2FA) implantado en fecha 21 de febrero de 2023. Afirman que la implantación de esta medida fue clave para solucionar la brecha ya que no se detectaron casos posteriores.
- Restablecimiento de todas las contraseñas de clientes en fecha 11 de febrero de 2022.
- Inclusión de los clientes afectados por fraude en una categoría especial para evitar posibles consecuencias derivadas.

- Mejora del sistema de monitorización SIEM con la implantación de nuevas funcionalidades de análisis en tiempo real de eventos, en concreto:
    - Generándose alertas cuando los intentos de autenticación fallidos desde una misma IP superan un umbral diario definido.
    - Generándose alertas cuando se originan eventos de autenticación exitosa desde una misma IP en más de cuatro cuentas cliente.
    - Listas negras de IP sospechosas para realizar seguimiento ante nuevas autenticaciones recibidas.
- Se realizó una comunicación a todos los clientes informando que la entidad no hace uso de WhatsApp como vía de contacto.
- Se actualizó el procedimiento interno de gestión de incidentes (a fecha 29 de abril de 2023) revisándose la plantilla para evaluar el riesgo y la gravedad de un incidente que afecte a datos personales, introduciendo ajustes en los plazos de respuesta para poder cumplir con la notificación del RGPD.

12. En relación con el proceso de identificación de clientes para la concesión de préstamos, ha quedado constatado que todos los clientes afectados ya habían solicitado un primer préstamo con anterioridad y, por tanto, ya habían realizado el proceso de identificación y registro inicial en el sistema (que requiere al usuario aportar documentación identificativa o hacer uso del servicio externo de identificación de banca online TINK). No obstante, queda acreditado que, para la solicitud de segundos y posteriores préstamos, VIVUS únicamente requería la correcta autenticación en el área web del cliente haciendo uso del nombre de usuario (DNI o Email) y su contraseña. Con posterioridad y como medida reactiva tras la brecha, VIVUS implantó el doble factor de autenticación (2FA) en el proceso de autenticación (login) de clientes en el área web, haciendo uso del envío de SMS con un código seguro de un solo uso y válido para una única conexión al área web personal del cliente, no conociéndose nuevos casos de fraude a raíz de la implantación de esta medida.

13. Del análisis de medidas preventivas y reactivas acreditadas se constata insuficiencias en la implantación de medidas técnicas para garantizar la identidad de los usuarios que solicitaban segundos (y posteriores) préstamos a través del área web. La introducción del segundo factor de autenticación (2FA) como mecanismo reactivo, pese a no ser un método que asegure la protección total ante ataques, ofrece un nivel superior de seguridad, evitando casos de suplantación de identidad aun cuando las contraseñas de los clientes ya se han visto comprometidas. Reforzar al máximo la seguridad del proceso de autenticación resultaba adecuado, teniendo en cuenta el potencial impacto que tiene la posibilidad de solicitar préstamos con el único requisito de autenticarse correctamente en el portal web.

14. Por otro lado, también se han detectado carencias en las medidas técnicas preventivas implantadas para monitorizar y, fundamentalmente, alertar ante la existencia de múltiples intentos de inicio de sesión fallidos.

TERCERO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad 4FINANCE SPAIN FINANCIAL SERVICES, S.A.U. es una gran empresa con un volumen de negocios de 66.551.000 euros en el año 2022.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento 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
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que VIVUS realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD: «Responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina.

Por su parte, el artículo 4.2 del Reglamento define el "tratamiento" de datos personales como *"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción""*

III
Obligación incumplida del artículo 5.1 f) del RGPD

El artículo 5.1 del RGPD establece los principios relativos al tratamiento, indicando, entre otras cuestiones, que 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»)."

El principio de confidencialidad, dentro del marco del RGPD, implica la obligación de garantizar que los datos personales se mantengan protegidos y únicamente puedan ser accesibles por aquellos que tienen autorización para su tratamiento, con el fin previsto y/ consentido por los titulares de los datos.

En este sentido, el RGPD define a los datos personales como ***"****toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"*

En el caso que nos ocupa, de las actuaciones de investigación realizadas por la presente autoridad, se desprende una presunta vulneración del citado principio de confidencialidad. Dicha vulneración se manifiesta a través de las siguientes circunstancias:

- El hecho, confirmado por la parte reclamada, de que los atacantes accedieran a datos personales de los clientes mediante su acceso ilegítimo utilizando combinaciones credenciales válidas (pares de DNI o Email + Contraseña). Con independencia de la forma en que accedieron a dichas credenciales, su uso para acceder a la información personal de los afectados constituye una manifestación de la vulneración del citado principio.

- El contacto posterior de los atacantes con los clientes afectados haciéndose pasar por la parte reclamada para solicitar la devolución del dinero a cuentas controladas por los atacantes. Debe de tenerse en cuenta, además, que el resultado favorable del fraude no solo se basó en la información personal obtenida ilegítimamente, sino que también se valió de la confianza que los clientes depositaron en VIVUS.

- Las distintas reclamaciones presentadas por los afectados a la presente autoridad que emergen como respuesta a las acciones ilícitas y que ponen de manifiesto tanto la exposición de sus datos personales sin su consentimiento como la gestión posterior y reactiva de la situación por parte de VIVUS.

- La denuncia presentada por la parte reclamada y posteriormente ampliada ante las cuerpos y fuerzas de seguridad en la cual ponían de manifiesto el número de afectados conocidos en dicho momento, con el fin de que realizasen las actuaciones oportunas.

- La comunicación de la brecha por la propia parte reclamada realizada tanto a la presente autoridad como a los propios afectados. Si bien dicha comunicación fue realizada de forma tardía y progresiva, supone un reconocimiento de la vulneración de la confidencialidad de los datos personales de los afectados.

Conviene señalar que la vulneración del principio de confidencialidad en el presente caso involucra un conjunto de datos personales cuya naturaleza amplifica las implicaciones de la brecha de seguridad. Ello se desprende en la circunstancia de que entre los mismos, además de datos identificativos o de contacto como nombres, direcciones, DNI/NIE, y números de teléfono, también se encontraban diversos datos financieros de los usuarios, como el IBAN e información sobre prestamos existentes en vigor.

La combinación de este tipo de datos personales, incluyendo el conocimiento sobre el estado financiero de los clientes, eleva significativamente el nivel de riesgo y las implicaciones de la vulneración de la confidencialidad. Esto se debe a la circunstancia de que dicha combinación no solo aumenta la cantidad de información disponible para un actor malicioso, sino que también amplía el espectro de posibles abusos. Dado que no se trata de datos aislados o piezas individuales de información, sino de la exposición de un conjunto integrado de datos personales y financieros, cuando se combinan, pueden ser utilizados para construir un perfil completo y detallado de la situación financiera y personal de un individuo, lo cual puede permitir a un atacante realizar operaciones de fraude y suplantación de identidad con una mayor tasa de éxito.

De forma concreta, la elaboración de un perfil sobre los individuos afectados permite a los atacantes diseñar estrategias de engaño altamente personalizadas, como el phishing o scamming, aumentando significativamente la probabilidad de éxito. Debe de tenerse en cuenta que la información detallada facilita la creación de mensajes creíbles que pueden engañar a las víctimas para que revelen aún más información o realicen acciones que comprometan su seguridad financiera y personal.

De la misma forma, el acceso no autorizado y la exposición de datos financieros, como la información sobre préstamos, colocan a los afectados en una posición de vulnerabilidad financiera significativa. Este nivel de acceso, además de poner en riesgo los activos financieros de los afectados, también puede tener un impacto negativo duradero en su historial crediticio y su reputación financiera. De la misma forma, la información sobre préstamos solicitados, aparte de ser sensible desde un punto de vista financiero, puede contener detalles sobre la situación económica y necesidades personales de los clientes que podría ser utilizada en contra de su voluntad. Esta información puede motivar, no solo conductas fraudulentas, sino también la manipulación y el chantaje, puesto que los actores maliciosos pueden explotar el conocimiento de las vulnerabilidades financieras de una persona para presionarla o inducirla a realizar acciones contra su voluntad o intereses.

Por último, no puede obviarse el número considerable de afectados de la brecha cuya magnitud llego a afectar a 9497 clientes. Esta circunstancia, de igual forma, amplia significativamente la gravedad de la vulneración del principio de confidencialidad. Debe de tenerse en cuenta que un elevado número de afectados no solo manifiesta la

escala del incidente, sino que también multiplica las oportunidades para un mal uso de la información personal, lo que aumenta de forma exponencial el riesgo de fraudes o suplantaciones de identidad, en los términos anteriormente indicados.

IV
Tipificación y calificación de la infracción del artículo 5.1.f) del RGPD

De confirmarse, la citada infracción del artículo 5.1.f) del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica “Condiciones generales para la imposición de multas administrativas” dispone:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)”

A este respecto, la LOPDGDD, en su artículo 71 “Infracciones” establece que *“Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica”.*

A efectos del plazo de prescripción, el artículo 72 “Infracciones consideradas muy graves” de la LOPDGDD indica:

“1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)”

V
Sanción por la infracción del artículo 5.1.f) del RGPD

Según el artículo 83.2 del RGPD “*Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:*

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) *las categorías de los datos de carácter personal afectados por la infracción;*
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción".

De la misma forma, el artículo 76 de la LOPDGDD establece una serie de criterios para graduar la posible sanción, siguiendo lo dispuesto en el apartado k) del anterior artículo:

"De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado."

Teniendo en cuanta dichos preceptos, en el presente supuesto se considera que procede graduar la sanción a imponer en los siguientes términos:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de daños y perjuicios que hayan sufrido;

La concurrencia de la agravante en la vulneración del principio de se manifiesta en la naturaleza, gravedad y duración de la infracción. La naturaleza de la infracción, que implicaba la exposición de datos personales y financieros, destaca el riesgo significativo para los derechos y libertades de las personas afectadas, especialmente considerando el potencial para el fraude financiero y la suplantación de identidad. La gravedad se manifiesta por el impacto directo sobre la integridad financiera y personal de los clientes, así como por el potencial daño a largo plazo en su confianza y percepción de seguridad. Además, la duración de infracción, que cesó tras la implementación efectiva de medidas correctivas, extendió innecesariamente el período de vulnerabilidad de los datos personales de los clientes, ampliando el marco temporal en el cual los datos estuvieron expuestos a riesgos de seguridad.
Asimismo, la concurrencia de la agravante también se manifiesta en el número de interesados afectados, dado que impactó a más de 9.000 clientes, lo que resalta tanto la escala del incidente como el volumen considerable de individuos cuyos derechos y libertades fueron comprometidos. Esta amplia afectación amplifica la gravedad de la infracción, dado que cada cliente afectado representa un potencial caso de fraude, suplantación de identidad, o pérdida financiera, multiplicando exponencialmente las repercusiones negativas del incidente.
Agravante prevista en el apartado b) del artículo 83.2 del RGPD:

b) la intencionalidad o negligencia en la infracción;

El Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. En este sentido, establece que en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, profesionalidad que concurre en el presente supuesto, dado que la actividad de la recurrente es de constante y abundante gestión de datos de carácter personal, lo cual implica un mayor rigor y cuidado con el fin de ajustarse a las previsiones legales.

En este caso, aunque no se sugiere una intencionalidad directa, la negligencia emerge tanto en la demora en la notificación de la brecha a los afectados (la cual tuvo lugar tras requerimiento de esta entidad) como en la reacción tardía tras el conocimiento de la vulneración de la confidencialidad de los datos personales de sus clientes. Dichos elementos reflejan una omisión en el deber de cuidado que VIVUS tenía hacia la protección de los datos de sus clientes, lo que refuerza y amplifica la gravedad de la infracción y justifica, en consecuencia, la concurrencia de esta agravante.

Agravante prevista en el apartado b) del artículo 76 del RGPD:

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

Teniendo en cuenta que el núcleo de la actividad empresarial de VIVUS se basa en la concesión de préstamos y, por ende, en el tratamiento intensivo de datos personales y financieros, dicha vinculación profundiza la gravedad de la infracción. La empresa opera en un sector donde la confianza y la seguridad de la información resulta fundamental, y por tal motivo tiene la responsabilidad garantizar con mayor rigurosidad los principios de protección de datos respecto a la información que gestiona en virtud de dicha actividad, entre la cual se encuentran datos sensibles, como datos bancarios

y/o financieros. La naturaleza de la actividad de VIVUS, en consecuencia, amplifica las consecuencias de la presunta infracción, circunstancia que justifica la concurrencia de la presente agravante.

En función de las mencionadas circunstancias, de acuerdo con lo dispuesto en el artículo 83.5 del RGPD, y sin perjuicio de lo que resulte de la instrucción del presente procedimiento, se considera adecuado fijar como posible sanción una multa de cuantía de **200.000 € (DOS CIENTOS MIL EUROS)**

VI
Obligación incumplida del artículo 32 RGPD

El artículo 32 “Seguridad del tratamiento” del RGPD establece*:*

“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”.

Resulta necesario señalar que el citado precepto no establece un listado de medidas de seguridad concretas de acuerdo con los datos objeto de tratamiento, sino que establece la obligación de que el responsable y el encargado del tratamiento apliquen medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la

naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, determinando aquellas medidas técnicas y organizativas adecuadas teniendo en cuenta la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se debe tener particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este sentido, el considerando 83 del RGPD señala *que "(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".*

En el presente caso, de conformidad con las evidencias de las que se dispone en este acuerdo de iniciación del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 32 del RGPD.

La imputación bajo el artículo 32 del RGPD en el contexto de VIVUS se basa en las presuntas deficiencias identificadas en la aplicación de medidas de seguridad técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado al riesgo que supone el tratamiento de datos personales. De las actuaciones de investigación realizadas por la presenta autoridad se han desprendido diversas circunstancias que manifiestan un incumplimiento en relación con los requerimientos específicos del artículo.

Así, aunque VIVUS realizó análisis de riesgo en distintas fechas utilizando una metodología interna basada en ENISA, se desprende de las actuaciones previas una asignación incorrecta de valores a variables clave lo cual implica una subestimación significativa del riesgo y severidad de la brecha. Ello manifiesta una posible inadecuación en la evaluación del riesgo al no tener en cuenta el estado de la técnica, los costos de implementación, y los riesgos para los derechos de las personas.

De la misma forma, la demora en la comunicación del incidente a los afectados hasta el 11 de abril de 2023, después de recibir la orden de la autoridad competente, destaca una limitación en la capacidad de VIVUS para garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento de datos. Esta demora en la notificación podría suponer mayores riesgos para los individuos afectados, incumpliendo de esta forma la obligación del artículo 32 de restaurar la disponibilidad y el acceso a los datos personales de manera rápida en caso de incidente.

Asimismo, la falta de análisis de riesgos específicos para los derechos y libertades de las personas interesadas en la actividad de tratamiento, y la concentración en impactos financieros para VIVUS en lugar de en los riesgos para los individuos afectados, subraya un enfoque inadecuado en la protección de datos desde una perspectiva centrada en el individuo.

La implementación de medidas reactivas por VIVUS, aunque necesaria y útil para abordar las consecuencias de la brecha de seguridad, al mismo tiempo revela insuficiencias en la anticipación y mitigación de riesgos para la seguridad de los datos personales. Ello resalta la importancia de una evaluación continua del riesgo, la planificación proactiva de la seguridad y una respuesta ágil a incidentes, conforme a los requisitos del artículo 32 del RGPD, circunstancias todas ellas que no han sido tenido en cuenta por VIVUS, tal y como se deduce de las actuaciones practicadas.

En este sentido, la decisión inicial de VIVUS de permitir nuevas solicitudes de préstamos sucesivos basándose únicamente en una forma de autenticación con usuario y contraseña revela una subestimación de los riesgos asociados con el robo de identidad y el fraude financiero. Basándose en que los clientes afectados ya habían completado un proceso de identificación para su primer préstamo, el sistema de VIVUS no exigía una verificación de identidad rigurosa para transacciones subsecuentes. Esta práctica abre la puerta a que actores maliciosos, si llegan a obtener credenciales de acceso de los clientes, puedan solicitar préstamos fraudulentamente.

La implementación del Doble Factor de Autenticación (2FA) por VIVUS constituye, sin duda, un avance significativo en la protección de la seguridad de los datos y la integridad de sus transacciones financieras. Sin embargo, este avance llega en un momento reactivo, después de que se hayan manifestado vulnerabilidades críticas y se haya producido una brecha de seguridad con efectos amplios. La adopción de 2FA, aunque crucial, manifiesta una oportunidad perdida de haberse anticipado y mitigado proactivamente los riesgos antes de que se materializasen en daños reales para los clientes, lo cual es, en esencia, la finalidad que persigue el citado artículo 32.

Las mencionadas carencias detectadas en las medidas preventivas previas a la brecha, especialmente en lo que respecta a la autenticación de usuarios para la solicitud de préstamos sucesivos, subrayan una adecuada evaluación de riesgo adecuada conforme a lo estipulado por el artículo 32 del RGPD. Como se indica en las conclusiones de las actuaciones de investigación, a pesar de la mejora significativa que representa el 2FA, la situación pone de relieve carencias en las medidas técnicas preventivas previas a la brecha, particularmente en lo que respecta a la monitorización

de intentos de inicio de sesión fallidos y la generación de alertas. La falta de un sistema efectivo para detectar patrones anómalos de autenticación facilita a posibles atacantes la explotación de credenciales comprometidas sin ser detectados de manera oportuna.

No puede obviarse en el presente caso la naturaleza de la actividad de VIVUS, la cual opera en el sector financiero, lo que conlleva a que el tratamiento de datos personales involucre información sensible, incluyendo detalles financieros y de identificación personal. Las circunstancias relativas a dicha actividad, supone una mayor exigencia respecto a las medidas técnicas y de seguridad con el fin de proteger los derechos en materia de protección de datos de los usuarios.

Por último, conviene destacar que la falta de medidas de seguridad adecuadas por parte de VIVUS es una cuestión que va más allá de la brecha de seguridad específica producida. Si bien la implementación de medidas reactivas como el Doble Factor de Autenticación (2FA) y la mejora del sistema de monitorización SIEM fueron pasos importantes en respuesta a la brecha, el incumplimiento de VIVUS radica en una omisión más amplia y preexistente: la falta adopción de un marco de seguridad de datos integral y proactivo.

Esta falta de medidas de seguridad adecuadas, independientemente de la brecha, señala una desconexión entre la evaluación de los riesgos potenciales y la implementación de medidas técnicas y organizativas necesarias para prevenir tales incidentes. La situación evidencia una desconexión en la cultura de seguridad de la información de VIVUS, donde las medidas tienden a ser reactivas en lugar de estar encaminadas en una estrategia de seguridad proactiva y basada en el riesgo. Esta postura reactiva limita la efectividad de las medidas de seguridad y aumenta la vulnerabilidad a futuras brechas, ya que no todas las medidas de seguridad necesarias están directamente relacionadas con la prevención de incidentes específicos, sino con la creación de un entorno seguro de forma integral.

En definitiva, las medidas adoptadas por VIVUS, la naturaleza de su actividad y su gestión reactiva con independencia de la brecha de seguridad acaecida subrayan un presunto incumplimiento del artículo 32 del RGPD) que exige la implementación de medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado al riesgo del tratamiento de datos personales. Si bien VIVUS tomó medidas reactivas, dichas acciones llegaron como respuesta a una vulnerabilidad ya explotada, en lugar de como parte de una estrategia proactiva de gestión de riesgos.

VII
Tipificación y calificación de la infracción del artículo 32 del RGPD

De confirmarse, la citada infracción del artículo 32 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica “Condiciones generales para la imposición de multas administrativas” dispone: “*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "Infracciones" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".*

A efectos del plazo de prescripción, el artículo 73 "Infracciones consideradas graves" de la LOPDGDD indica: "*En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

(…) f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

VIII
Sanción por la infracción del artículo 32 del RGPD

En los términos indicados por el mencionado artículo 83.4 del RGPD la infracción del artículo 32 se sancionará, *"con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía"*

Asimismo, de acuerdo con los criterios anteriormente establecidos supuesto se considera que en el presente supuesto procede graduar la sanción a imponer en los siguientes términos:

Agravante prevista en el apartado a) del artículo 83.2 del RGPD:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de daños y perjuicios que hayan sufrido;

En el presente supuesto se desprende la concurrencia de la citada agravante considerando la naturaleza, gravedad y duración de la presunta infracción cometida. En el caso de la naturaleza de la infracción se manifiesta en el tratamiento inadecuado de datos personales y financieros, un aspecto crítico teniendo en cuenta la sensibilidad de la información involucrada. Por su parte, la gravedad se desprende del potencial daño significativo de los derechos y libertades de los individuos afectados que posee la no adopción de las medidas de seguridad adecuadas, incluyendo riesgos de fraude y pérdida financiera. Además, la duración de la infracción, extendiéndose desde el momento de la brecha hasta la implementación tardía de medidas correctivas, justifica la concurrencia de la citada agravante.

Agravante prevista en el apartado b) del artículo 83.2 del RGPD:

b) la intencionalidad o negligencia en la infracción;

En los términos anteriormente indicados respecto a la doctrina del Tribunal Supremo respecto a la imprudencia, en el presente caso la negligencia se manifiesta en la falta de previsión y en la adopción tardía de medidas como el 2FA, que son fundamentales para la protección de datos personales. Esta negligencia indica una omisión en la aplicación de un enfoque de seguridad de datos proactivo y basado en el riesgo, indispensable para prevenir accesos no autorizados y otras formas de compromiso de datos. La negligencia, por tanto, se manifiesta en este caso en no anticipar y mitigar los riesgos, especialmente en un sector tan sensible como el financiero, lo cual justifica la concurrencia de la mencionada agravante.

Agravante prevista en el apartado b) del artículo 76 del RGPD:

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

La infracción del artículo 32 por VIVUS se ve particularmente agravada por la estrecha vinculación de su actividad empresarial con el tratamiento intenso y continuado de datos personales, dado que la concesión de préstamos implica la gestión de información personal y financiera de forma ordinaria y masiva. En este sentido, la falta de medidas de seguridad adecuadas pone en riesgo la esencia de la operatividad en que se basa este tipo de entidades y merma la confianza en el sector financiero digital. De la misma forma, la naturaleza de dicha actividad exigía una mayor rigurosidad en la adopción de las medidas de seguridad, exigencia que no fue materializada en el caso que nos ocupa.

Teniendo en cuenta las condiciones generales para la imposición de multas administrativas establecidas por el ya mencionado artículo 83.2 del RGPD, atendiendo a las circunstancias del presente supuesto y sin perjuicio de lo que resulte de la instrucción del presente procedimiento, se propone como posible sanción una multa de cuantía de **400.000 € (CUATROCIENTOS MIL EUROS).**

IX
Adopción de medidas

De confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "*ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".* La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a ***4FINANCE SPAIN FINANCIAL SERVICES, S.A.U.***, con NIF ***A86521309***, por la presunta infracción del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD y Artículo 83.4 del RGPD.

SEGUNDO: NOMBRAR como instructor/a a ***R.R.R.*** y, como secretario/a, a ***S.S.S.***, indicando que podrán ser recusados, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

TERCERO: INCORPORAR al expediente sancionador, a efectos probatorios, las distintas reclamaciones interpuestas y su documentación, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería:, sin perjuicio de lo que resulte de la instrucción:

- Por la supuesta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 de dicha norma, multa administrativa de cuantía **200.000,00 euros.**

- Por la supuesta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía **400.000,00 euros.**

QUINTO: NOTIFICAR el presente acuerdo a **4FINANCE SPAIN FINANCIAL SERVICES, S.A.U.**, con NIF **A86521309**, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de expediente que figura en el encabezamiento de este documento.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al

presente acuerdo de inicio; lo que llevará aparejada una reducción de un **20%** de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en **480.000,00 euros**, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un **20%** de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en **480.000,00 euros** y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución**. En este caso, si procediera aplicar ambas reduccione**s, el importe de la sanción quedaría establecido en **360.000,00 euros**.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (**480.000,00 euros** o **360.000,00 euros**), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para continuar con el procedimiento en concordancia con la cantidad ingresada.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo sin que se haya dictado y notificado resolución se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

935-18032024

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

>>

SEGUNDO**:** En fecha 25 de abril de 2024, la parte reclamada ha procedido al pago de la sanción en la cuantía de **360000 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

TERCERO**:** El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento 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
Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"*1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.*

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos,

el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

De acuerdo con lo señalado,
la Directora de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la terminación del procedimiento **EXP202304633**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a ***4FINANCE SPAIN FINANCIAL SERVICES, S.A.U.***.

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, los interesados podrán interponer 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.

936-040822

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