CNMC
COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA

RESOLUCION Expte. S/DC/0536/14, CAIXABANK

CONSEJO. SALA DE COMPETENCIA

PRESIDENTE
D. José María Marín Quemada

CONSEJEROS
Dª. María Ortiz Aguilar
D. Fernando Torremocha y García-Sáenz
D. Benigno Valdés Díaz
Dª. Idoia Zenarrutzabeitia Beldarraín

SECRETARIO
D. Tomás Suárez-Inclán González

En Barcelona, a 29 de septiembre de 2015.

La Sala de Competencia del Consejo de la Comisión Nacional de los Mercados y la Competencia (CNMC), con la composición expresada al margen, ha dictado la presente Resolución en el expediente S/DC/0536/14, CAIXABANK, tramitado ante la denuncia formulada por parte de FINTONIC Servicios Financieros, S.L. (FINTONIC) contra CAIXABANK, S.A. (CAIXABANK), en base a una supuesta infracción del artículo 3 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia (LDC) (folios 1 a 501).

ANTECEDENTES DE HECHO

1. Con fecha 18 de septiembre de 2014, tuvo entrada en la Comisión Nacional de los Mercados y la Competencia (CNMC) denuncia presentada por FINTONIC Servicios Financieros, S.L. (FINTONIC) contra CAIXABANK, S.A. (CAIXABANK) por supuestas conductas prohibidas por la Ley 15/2007, de 3 de julio, de Defensa de la Competencia (LDC), consistentes en dificultar por varios medios a sus usuarios el acceso a la banca online de CAIXABANK y obstaculizar, de este modo, el acceso a FINTONIC a la información que precisa sobre las cuentas bancarias de dichos usuarios para el desarrollo de su actividad. En el mismo escrito se solicitaba como medida cautelar el cese inmediato por parte de CAIXABANK de los actos de obstaculización denunciados (folios 1-501).

2. La Dirección de Competencia (DC), de conformidad con lo dispuesto en el artículo 49.2 de la LDC, llevó a cabo una información reservada en el marco de la cual requirió a la denunciada, con fecha 3 de diciembre de 2014, información sobre el funcionamiento de la banca online y sus medidas de seguridad, así como su política frente a agregadores financieros (folios 617-620). La respuesta a esta solicitud de información por parte de CAIXABANK tuvo entrada en la CNMC el 7 de enero de 2015 (folios 656-751), y la complementó con información adicional el 15 de enero de 2015 (folios 752-760) y el 27 de febrero de 2015 (folios 774-782).

3. FINTONIC, ha aportado con fechas 15, 21, 24 y 28 de octubre de 2014, 16 de enero y 3 de marzo de 2015, información complementaria sobre el objeto de la denuncia (folios 504-517, 518-554, 555-613, 614-616, 761-773, 785-800).

4. Con fecha 18 de mayo de 2015, la DC elevó su Informe y Propuesta de Resolución al Consejo de la CNMC.

5. La Sala de Competencia del Consejo de la CNMC deliberó y falló el asunto en su reunión de 29 de septiembre de 2015.

HECHOS ACREDITADOS

En su Propuesta de Archivo a esta Sala de Competencia la DC realiza la siguiente descripción del denunciante y denunciado:

1. LAS PARTES

1.1. Denunciante: FINTONIC SERVICIOS FINANCIEROS, S.L. (FINTONIC).

FINTONIC es una compañía española creada en 2011 dedicada a la prestación de servicios de gestión y simplificación de la contabilidad personal a través de internet. La actividad desarrollada por FINTONIC es la propia de los llamados “agregadores financieros” (folios 5 y 526).

1.2. Denunciada: CAIXABANK, S.A. (CAIXABANK):

Fundación Bancaria Caixa d’Estalvis i Pensions de Barcelona (LA CAIXA) es una entidad de crédito de naturaleza fundacional y carácter benéfico social que no está controlada por ninguna persona física o jurídica. Su actividad principal es la prestación de servicios bancarios, fundamentalmente de banca minorista, que realiza desde 2011 a través de CAIXABANK, S.A. (CAIXABANK).

2. MERCADOS AFECTADOS

La DC en su Propuesta de Archivo distingue dos mercados afectados:

2.1. Mercado de servicios de información sobre cuentas (Agregadores financieros)

La DC considera que, si bien no hay precedentes nacionales que definan el mercado de servicios de información sobre cuentas o "agregadores financieros", la Comisión Europea ha definido estos servicios en su Propuesta de Directiva sobre Servicios de Pago que publicó en julio de 2013 como *"un servicio de pago por el que se proporciona, a un usuario de servicios de pago y de forma agregada y fácil de utilizar, información sobre una o varias cuentas de pago de las que dicho usuario sea titular en uno o varios proveedores de servicios de pago gestores de cuenta".*

En dicha Propuesta, la Comisión reconoce que se trata de una serie de servicios complementarios surgidos en los últimos años gracias a los avances tecnológicos y que deben considerarse servicios de pago. Se les denomina proveedores de servicios terceros (TPP por sus siglas en inglés *Third Party Providers*).

En España, además de FINTONIC, operan actualmente otros proveedores de servicios de agregación de cuentas, como BankiaLink y BBVA, Mooverang (creada por la Organización de Consumidores y Usuarios, OCU) y MyValue, si bien el primer agregador financiero que existió en el país fue el desarrollado por Bankinter en 2001.

2.2. Mercado de Banca Minorista

En cuanto al sector de servicios bancarios la DC expone en su propuesta la distinción en tres mercados atendiendo a criterios derivados de la demanda y de la naturaleza y composición del tipo de servicios ofrecidos: banca minorista, banca corporativa y banca de inversiones.

Señala además, cada uno de estos mercados opera a través de diferentes canales de venta, de forma que las características de la competencia difieren en cada uno de ellos.

En lo que se refiere al mercado de banca minorista (expediente C/0587/14 BANCO POPULAR/CITIBANK -ACTIVOS-) la DC señala que engloba los servicios y productos prestados a particulares y pequeñas empresas: las cuentas corrientes y a la vista, los depósitos, las cuentas de ahorro, la comercialización de recursos fuera de balance (fondos de inversión, fondos de pensiones y patrimonios personales), los créditos y préstamos, incluidos los préstamos personales (de consumo, hipotecarios).

Debido a que la banca minorista mantiene una operativa para una base amplia de clientes que efectúan gran número de operaciones de pequeña cuantía, habitualmente necesita una amplia red de sucursales para satisfacer una clientela numerosa y con frecuencia dispersa.

3. MARCO REGULATORIO

En su propuesta de archivo la DC examina el marco regulatorio referido a los servicios de pago y a la protección de datos de carácter personal, exponiendo el siguiente análisis:

"Normativa comunitaria

a) Directiva sobre servicios de pago o DSP y Propuesta de Segunda Directiva de Servicios de Pago

(20) *La mencionada Propuesta de Segunda Directiva sobre Servicios de Pago incorpora en ella, y a la vez deroga, la Directiva 2007/64/CE del Parlamento Europeo y del Consejo*[1] *(Directiva sobre servicios de pago o DSP), que "fija las bases de un marco jurídico armonizado para la creación de un mercado de pagos integrado, de modo que aumenta la equidad en las condiciones de competencia y facilita en mayor medida el acceso de todos los interesados al actual marco regulador de los pagos."*

(21) *Junto a ello, la DSP contribuye al reforzamiento y protección de los derechos de los usuarios de los servicios de pago y facilita la aplicación operativa de los instrumentos de la zona única de pagos en euros, lo que se ha denominado SEPA (Single Euro Payments Area), que se ha de desarrollar por la industria privada con el impulso del Banco Central Europeo y de los Bancos Centrales nacionales.*

(22) *En la DSP se definen los servicios de pago y las entidades de pago, si bien no aparecen definidos los nuevos servicios de pago que sí contempla la propuesta de 2ª Directiva de Servicios de Pago.*

(23) *También aparecen definidas en la DSP las obligaciones y responsabilidades de usuarios y proveedores de servicios en cuanto a la autenticación y ejecución de operaciones de pago*

(24) *La DSP vigente no se aplica a los nuevos servicios y proveedores de servicios que permiten el acceso a las cuentas de pago, como los agregadores financieros. Sin embargo, la Propuesta incorpora al ámbito de aplicación de la DSP los proveedores de servicios terceros que ofrecen, en particular, servicios de iniciación de pagos e información de cuentas basados en la banca en línea. Así, la Propuesta de Directiva recoge la definición del servicio de agregadores financieros y también las fuentes de*

[1] Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de
pago en el mercado interior. http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32007L0064&rid=1

problemas identificadas por la Comisión en su Estudio de Impacto y, entre ellas, destaca el "vacío legal para determinados proveedores de servicios por internet de reciente aparición […] El vacío legal podría inhibir la innovación e impedir que se creen condiciones adecuadas de acceso al mercado."

(25) *El Estudio de Impacto de la Comisión de la Propuesta de Directiva*[2] *pone de manifiesto, haciendo referencia al vacío legal al que se enfrentan los proveedores de ciertos servicios de pago, como los servicios de iniciación de pagos y de información sobre cuentas, que "estos proveedores se enfrentan a serias dificultades para acceder a la información sobre la disponibilidad de los fondos en las cuentas de pago. Sin embargo, esta información es necesaria para la autorización de la tarjetas, la iniciación de pagos y (en su caso) para la garantía de pagos. El acceso a esta información por parte de terceros crearía una presión a la baja sobre las tasas de intercambio actuales, gracias a la creciente competencia de nuevos jugadores, dando lugar a beneficios para los comerciantes y los consumidores, y contribuyendo a la reducción de costes globales de pago en beneficio de la sociedad." En este aspecto, el Estudio concluye que "la falta de acceso a la información sobre fondos y la ausencia de un status legal en la Directiva dificulta la entrada en el mercado de terceras partes como nuevos esquemas de tarjetas, servicios de iniciación de pagos y otros. Definir condiciones de acceso seguras, garantizar un status legal así como derechos y obligaciones para los proveedores terceros dará certidumbre legal a los proveedores terceros y a los bancos y beneficiará a los consumidores […] La mayoría de los bancos y tarjetas se oponen a permitir el acceso a proveedores terceros y nuevas tarjetas con la opción recomendada, si bien algunos de ellos cambiarían de opinión a cambio de una compensación financiera por el acceso".*

(26) *En este sentido, la propuesta de Directiva, indica que las condiciones de acceso a información sobre las cuentas, requisitos de autenticación y rectificación de operaciones se regularán en futuras normas (artículo 58 de la Propuesta de Directiva).*

Normativa nacional

a) Ley de Servicios de Pago (LSP)

(27) *La Ley 16/2009, de 13 de noviembre, de Servicios de Pagos (LSP)*[3] *viene a incorporar la Directiva 2007/64/CE, del Parlamento Europeo y del Consejo, de 13 de noviembre, sobre servicios de pago en el mercado interior cuyo*

[2] http://ec.europa.eu/internal_market/payments/docs/framework/130724_impact-assessment-full-text_en.pdf
[3] http://www.boe.es/buscar/pdf/2009/BOE-A-2009-18118-consolidado.pdf

objetivo general es garantizar que los pagos realizados en el ámbito de la Unión Europea (en concreto, las transferencias, los adeudos directos y las operaciones de pago directo efectuadas mediante tarjeta) puedan realizarse con la misma facilidad, eficiencia y seguridad que los pagos nacionales internos de los Estados miembros.

(28) *Los objetivos de la LSP serán los mismos que los de la DSP: estimular la competencia entre los mercados nacionales y asegurar la igualdad de oportunidades para competir, aumentar la transparencia en el mercado, tanto para los prestadores de los servicios como de los usuarios, y establecer un sistema común de derechos y obligaciones para proveedores y para usuarios en relación con la prestación y utilización de los servicios de pago, si bien no aparecen definidos los nuevos servicios de pago que contempla la propuesta de 2ª Directiva de Servicios de Pago.*

b) Ley de Protección de Datos de Carácter Personal (LPD)

(29) *El tratamiento de datos personales en una entidad bancaria atiende a diferentes finalidades, está sujeto a la normativa en la materia, y por tanto, pueden ser objeto de la implantación de varios niveles de seguridad. La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LPD)[4] y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RPD)[5] son las normas nacionales vigentes en la materia.*

(30) *El RPD distingue en sus artículos 80 y 81 distintos niveles de seguridad en función de la naturaleza de los datos y, de acuerdo con la actividad de la entidad, puede deducirse que deben implantarse medidas de seguridad de nivel medio[6] (que deben aplicarse a aquellos ficheros de los que sean responsables las entidades financieras para fines relacionados con la prestación de servicios financieros), que incluyen también las de nivel básico (que se aplican a todos los ficheros o tratamientos de datos de carácter personal).*

(31) *En relación a la seguridad de los datos, el artículo 9 de la LPD establece que "1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. 2. No se registrarán datos de carácter personal*

[4] http://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf
[5] http://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf
[6] Sección II del Capítulo III del RPD.

en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas. 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley".

(32) *Además de la confidencialidad recogida en la LPD, en el sector financiero se debe aplicar el secreto bancario y la especial confidencialidad que se debe tener con respecto a los datos de los usuarios. Se entiende por secreto bancario, la protección que los bancos e instituciones financieras deben otorgar a la información relativa a los depósitos y captaciones de cualquier naturaleza que reciban de sus clientes al considerar que esta información es parte de la privacidad de los clientes del sistema financiero*[7]*.*

(33) *En este sentido, la Agencia Española de Protección de Datos, en sus "Conclusiones relativas al plan de inspección de oficio al sector de la banca a distancia con objeto de verificar el grado de adecuación de sus ficheros de clientes y clientes potenciales a la Ley Orgánica 15/1999, de protección de datos de carácter personal", hacía las siguientes recomendaciones "Se recomienda incluir en los contratos de trabajo cláusulas relativas al deber de secreto respecto de los datos personales a los que tienen acceso los empleados como consecuencia de su actividad, ya sean los propios empleados de la entidad como los empleados de las empresas prestatarias de servicios para la entidad con acceso a los datos personales de los clientes. Se recomienda también que las páginas web de acceso a los servicios se diseñen de tal manera que no proporcionen al usuario más datos personales que los introducidos por el propio usuario, hasta que éste no haya superado con éxito los controles de identificación y autenticación*".

4. HECHOS ACREDITADOS

A juicio de la DC, FINTONIC denuncia a CAIXABANK por obstaculizar su actividad, lo que constituye a juicio de FINTONIC una infracción del artículo 3 de la LDC "*mediante la comisión de actos de competencia desleal que, por falsear la libre competencia en el incipiente mercado de la prestación de servicios de información sobre cuentas bancarias, afectan gravemente al interés público*" (folio 6) y una violación del artículo 4 de la ley 3/1991 de 10 de enero de Competencia Desleal (en adelante LCD), por constituir *"actos de competencia desleal contrarios a las exigencias de la buena fe que sanciona el artículo 4 de la LCD*" (folio 16).

[7] Es importante señalar también la obligatoriedad de comunicar operaciones sospechosas conforme a la Ley al Servicio Ejecutivo del Banco de España de prevención de blanqueo de capitales (SEPBLAC).

Según el denunciante, CAIXABANK no permite la actualización de los movimientos de las cuentas en la aplicación de FINTONIC, y hostiga a sus usuarios cuando éstos quieren acceder, a través de FINTONIC, a los datos de los productos financieros que tienen contratados con CAIXABANK mediante la aplicación online de ésta[8]. Las prácticas denunciadas se estarían llevando a cabo desde marzo de 2013. Sin esta información de los usuarios, FINTONIC no puede prestar servicios.

CAIXABANK afirma haberse puesto en contacto con clientes con claves cedidas a FINTONIC para recomendarles que sean prudentes y que jamás introduzcan las claves de acceso de Línea Abierta en ningún otro lugar que no sea una página web oficial de CAIXABANK, aconsejándoles un cambio de contraseña (folio 673).

El día 14 de enero CAIXABANK remitió un burofax a FINTONIC en el que se le instaba a cesar en el envío de comunicaciones a los clientes en las que se señala a CAIXABANK como el banco que más cobra a sus usuarios ya que se trata de información supuestamente falsa, y se les pide que identifiquen las fuentes utilizadas además de señalar cuánto tiempo llevan enviando estas comunicaciones. Adicionalmente, se les pide que cesen de acceder a la banca electrónica de CAIXABANK suplantando la identidad de sus clientes. La entidad les informa de que tiene intención de pedir una indemnización por daños y, en caso de no llegar a un acuerdo amistoso, denunciar a FINTONIC (folios 756-760 y 766-770).

FINTONIC ha explicado a esta DC que el informe al que hace referencia se trata de un resumen basado en las comisiones reales cobradas a los usuarios de FINTONIC en el tercer trimestre de 2014 (folio 764). La denunciante considera este burofax un nuevo acto de obstaculización y hostigamiento.

En concreto las prácticas denunciadas se refieren a:

a. Introducción de un *captcha*[9] para que los usuarios de FINTONIC clientes de CAIXABANK no puedan actualizar sus respectivas cuentas de usuario automáticamente (folio 7).

b. Bloqueo del Protocolo de Internet[10] (IP) de FINTONIC, que se presta a través de una pasarela tecnológica de obtención de datos (folio 7).

[8] FINTONIC calcula que el 20% de sus usuarios son clientes de CAIXABANK, seguido de BBVA (cercano al 15% de sus usuarios), ING y Santander (con cuotas ligeramente superiores al 10%) (folio 544).

[9] Acrónimo de la expresión inglesa *Completely Automated Public Turing test to tell Computers and Humans Apart (prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos).* Se trata de una prueba desafío-respuesta utilizada en computación para determinar cuándo el usuario es o no humano.

[10] Internet Protocol o IP, es un protocolo de comunicación de datos digitales.

c. Bloqueo o cancelación de las credenciales de acceso a la banca en línea de CAIXABANK a los usuarios de FINTONIC (y clientes a su vez de CAIXABANK) (folios 7 y 542).

d. Llamadas telefónicas alertando a los usuarios sobre supuestos fallos de seguridad en sus cuentas online y/o exigencias de cancelar su relación con FINTONIC (folios 7 y 542).

Esta conducta sería especialmente grave, según la denuncia, ya que la actividad de FINTONIC depende esencialmente de la información proporcionada por las entidades bancarias por lo que un bloqueo al acceso de la plataforma de banca online de las entidades supondría la imposibilidad de operar para FINTONIC y para el resto de operadores, además de verse dañada su reputación (folios 547 y 550).

Actualmente, FINTONIC proporciona el servicio de agregación de cuentas a clientes de 57 entidades financieras, con las que no le une ningún tipo de relación contractual, ya que son los clientes de esas entidades los que acceden a su información financiera a través de FINTONIC (folio 11).

La DC al objeto de comprender el contexto de la denuncia, resume la operativa del agregador financiero FINTONIC, y de la banca electrónica de CAIXABANK:

“

a. Operativa de FINTONIC

(44) *En el caso del agregador FINTONIC, la utilización de la plataforma comienza con el registro del usuario con una dirección de correo electrónico y una contraseña. A continuación se eligen cada una de las entidades financieras en las que tiene contratadas cuentas, tarjetas, depósitos, etc. y se pide la introducción por el usuario en la web de FINTONIC de las claves de acceso a la plataforma de banca online de cada una de ellas (que pueden consistir en usuario y contraseña, DNI y contraseña, número de tarjeta y contraseña, etc., dependiendo de la política de cada una de ellas). Esto le permitirá acceder a su posición financiera integral a través de un único sitio web y un único portal. Si se modifican las claves de acceso al banco también habrá que modificarlas en la plataforma de FINTONIC. Estas claves de acceso, según FINTONIC, son diferentes de la firma electrónica, que es la que permite realizar operaciones con las cuentas , por lo que ni los usuarios pueden realizar operaciones o movimientos de fondos a través de la plataforma de FINTONIC, ni ésta tendría acceso a las claves que permiten esos movimientos (folio 526).*

(45) *A continuación se realizan una serie de preguntas personales, como la edad, para diseñar un perfil de usuario que permita a la entidad realizar recomendaciones personalizadas.*

(46) *Las credenciales del usuario se encriptan y, a través de la pasarela tecnológica de Eurobits, se accede a los portales de banca electrónica de las entidades de las que es cliente el usuario registrado (folio 528). Según la empresa, nadie puede acceder a los movimientos del usuario ni a sus datos de acceso, todo está gestionado por algoritmos y nunca será compartido con terceros, asegurando cumplir en todo momento con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LPD) (folio 526).*

(47) *Los movimientos se actualizan todas las noches automáticamente, excepto para los bancos que piden claves dinámicas, como tarjetas de coordenadas o mensajes al móvil, en los que el usuario deberá realizar la actualización de forma manual.*

(48) *FINTONIC asegura que el usuario puede cancelar la suscripción a la aplicación en cualquier momento, y el agregador se encargará de borrar toda la información personal, incluyendo las claves de acceso (folio 526).*

b. Operativa de la banca electrónica de CAIXABANK

(49) *El servicio de banca electrónica de CAIXABANK, Línea Abierta, incluye la consulta de las características principales del producto o servicio contratado con CAIXABANK, ejecución de órdenes relativas a servicios bancarios, de pago, inversión o seguros previamente contratados, contratación de nuevos productos y servicios utilizando la firma electrónica, contratación y consulta de productos financieros y servicios de inversión, comunicaciones de la entidad, etc.*[11] *(folio 679). Este servicio no es gratuito sino que devenga una serie de comisiones (folio 680).*

(50) *El acceso al servicio de banca electrónica Línea Abierta por parte de los clientes de CAIXABANK se realiza desde cualquier ordenador con conexión a internet a través de la página web habilitada al efecto por la entidad, mediante un interfaz que requiere la introducción de un identificador de usuario y una clave de acceso numérica de 4 posiciones (el denominado PIN) proporcionados por CAIXABANK y que, una vez validados, permiten al titular el acceso a las operativas de consulta (folios 657 y 677). Según CAIXABANK, el identificador y las claves de acceso tienen la consideración de firma electrónica (folio 678).*

[11] El servicio de Línea Abierta permite operar sobre los productos y servicios de La Caixa y de otras entidades de su grupo así como con los que La Caixa haya alcanzado acuerdos de colaboración. Entre otras, en la actualidad dichas entidades son : Comercia Global PaymentsEntidad de Pago, S.L. , Caixa Card 1 Establecimiento Financiero de Crédito, CAIXABANK Electronic Money EDE, S.L., Nuevo Micro Bank S.A.U., SegurCaixa Adeslas S.A. de Seguros y Reaseguros, VidaCaixa S.A. Sociedad Unipersonal, InverCaixa GestiónS.G II.C., S.A.U.

(51) *Cuando las operaciones suponen movimientos de fondos, el usuario debe introducir una segunda clave, o bien utilizar la "Tarjeta Línea Abierta". Esta tarjeta, denominada "tarjeta de coordenadas", contiene un total de 60 claves diferentes en su dorso (cada una asociada a una clave de firma de 4 dígitos numéricos) que serán solicitados de forma aleatoria por el sistema para verificar la identidad del ordenante. Las tarjetas de coordenadas son todas distintas y se le proporciona al cliente cuando se da de alta en el servicio de banca electrónica (folio 657).*

(52) *Si un cliente desea incrementar la seguridad en la identificación para el acceso a "Línea Abierta", se le ofrece la posibilidad de complementar la identificación con un certificado digital, admitiéndose a estos efectos el uso del DNI electrónico si se accede desde un ordenador.*

(53) *La denunciada aclara que existen otros mecanismos de seguridad reforzada, como la firma OTP recibida por SMS al móvil (CaixaPIN) (folios 666 y 667).*

(54) *Las claves de acceso a la banca electrónica, según CAIXABANK, representan legal y contractualmente una firma electrónica que identifica a una persona física o jurídica, concreta y singular, y genera obligaciones y responsabilidades a su titular por su uso, que se detallan en el contrato[12]. Tales firmas electrónicas se rigen por el principio comunitario de custodia y uso exclusivamente personal, que se detalla en el artículo 28.a de la LSP[13]. Puesto que se trata de una firma electrónica personal, intransferible y singular, que identifica a un usuario concreto, la normativa aplicable no prevé el acceso de múltiples personas a través de ella (folio 658).*

Usuarios autorizados y/o apoderados

[12] CONDICIONES GENERALES ESPECÍFICAS DEL SRVICIO LINEA ABIERTA: "*3.3 FIRMA ELECTRÓNICA DE LÍNEA ABIERTA. los distintos servicios prestados por Línea Abierta, requerirán el uso del identificador y de una, o de las dos claves de acceso y firma, según se establezca en cada momento. El identificador junto a las claves de acceso y firma consignados junto a otros datos electrónicos generados por Línea Abierta o asociados con ellos, serán utilizados como medio de identificación del contratante, o en su caso del usuario autorizado, teniendo la consideración de firma electrónica del contratante o del usuario autorizado. Dicha firma electrónica tendrá el mismo valor respecto de los datos consignados en los documentos electrónicos generados en el entorno de Línea Abierta que la firma manuscrita en relación con los datos consignados en papel" (FOLIO 678).*

[13] *"Artículo 28. Obligaciones del proveedor de servicios de pago en relación con los instrumentos de pago.*
El proveedor de servicios de pago emisor de un instrumento de pago cumplirá las obligaciones siguientes:
a) Cerciorarse de que los elementos de seguridad personalizados del instrumento de pago solo sean accesibles para el usuario de servicios de pago facultado para utilizar dicho instrumento. En particular, soportará los riesgos que puedan derivarse del envío al ordenante tanto de un instrumento de pago como de cualquier elemento de seguridad personalizado del mismo."

(55) *El contrato vigente del servicio Línea Directa que se firma con los clientes (folio 680) contemplan la posibilidad de que un cliente pueda nombrar a usuarios autorizados o apoderados, esto es, un tercero que puede actuar en nombre y/o por cuenta de un cliente en relación a sus cuentas y la información relacionada con ellas. Esta posibilidad se recoge en las "Condiciones Generales del Servicio de Línea Abierta" (folios 513-514 y 679-680) y en la "Norma 5 Servicio de Línea Abierta", que regula la banca electrónica de CAIXABANK (folios 686-715).*

(56) *Las "Condiciones Generales" distinguen cuando el contratante ejercita los derechos derivados del contrato a través de un apoderado o representante legal, y cuando el contratante designa una o más personas autorizadas para poder acceder en su nombre a determinados servicios*[14] *(folios 513-514 y 679-680).*

(57) *El apartado 1.2 de la Norma relativo a los usuarios establece que "Dentro de un contrato se podrán dar de alta varios usuarios. Cada usuario es una persona física autorizada a acceder a los productos del titular del contrato [...]. En casos especiales, también podrá existir un contrato de persona física que autorice a un apoderado a acceder a sus productos de forma remota, en cuyo caso el contrato de persona física podrá contener varios usuarios, uno asignado al titular, y otro asignado al apoderado designado por la persona física. En los contratos de personas jurídicas se darán de alta tanto usuarios como apoderados de la empresa que vayan a operar de forma remota con los servicios electrónicos de "la Caixa". Cada usuario debe estar asignado a alguno de los apoderados de la empresa; no existen, por tanto, los usuarios anónimos, dentro de un contrato SAU. Cada uno de los usuarios de un contrato tiene una serie de características que lo identifican, que se detallan a continuación: Número de usuario […], Nombre de usuario […], Tipo de usuario […], tipo de operaciones permitidas […], parámetros […], cuentas relacionadas […]".*

(58) *En cuanto al tipo de operaciones permitidas al usuario tercero pueden ir desde sólo consulta, consultas y preparación de operaciones*[15]*, permitir todo tipo de operaciones y personalizar el acceso de dicho usuario. Este usuario tercero autorizado/apoderado será, por tanto, responsable de toda la operativa que se realice en la banca electrónica de CAIXABANK bajo su nombre y número de usuario (folios 680 y 697).*

(59) *En octubre de 2014 CAIXABANK incluyó en el contrato de Adhesión a los Productos y Servicios de LA CAIXA en su cláusula 3 de las Condiciones*

[14] El usuario autorizado sólo podrá acceder a los niveles de servicio básico, consultas o consultas y preparación.
[15] La preparación se refiere a las tareas administrativas relacionadas con las operaciones que van a ser firmadas o autorizadas por los apoderados posteriormente. Para estos casos se da de alta un « usuario preparador ».

Generales Especificas del Servicio Línea Abierta, la prohibición explícita de "todo tipo de comunicación, incorporación, extracción de información o datos con finalidad comercial y profesional, o cualquier tipo por parte de terceros. En consecuencia, queda expresamente prohibida la cesión del uso del servicio de "Línea Abierta" por parte del Contratante a terceras personas o entidades excepto si "la Caixa" presta previamente, de forma expresa su consentimiento. En particular, se considerará prohibida la cesión del uso del servicio a terceros de los identificadores, de las claves de acceso y de firma y de cualquier otro elemento de seguridad personalizado que "la Caixa" haya facilitado al Contratante, especialmente si la misma se ha producido en el marco de una relación contractual de carácter mercantil entre el Contratante y terceros prestadores de servicios de pago, bancarios o auxiliares, como agregadores financieros" (folio 513).

(60) *CAIXABANK justifica esa cláusula en la aceptación de las condiciones del contrato en las que se especifica que el cliente se compromete a un uso propio, personal y confidencial del servicio de Línea Abierta.*

(61) *La denunciada aclara que este servicio de Línea Abierta está destinado a uso doméstico, quedando fuera del ámbito de aplicación los usos con fines profesionales y comerciales, como es la actividad de FINTONIC (folios 513 y 673, 677).*

(62) *Además, según CAIXABANK, se contempla igualmente la posibilidad del usuario autorizado (folio 513) dentro de la cual, entraría la posibilidad de que el cliente autorice en este caso a FINTONIC, como cliente autorizado (folios 661, 774, 781).*

(63) *La autorización a usuarios terceros se presta formalmente por medio de la cumplimentación de unos formularios habilitados al efecto. Existen en este sentido tres modelos de autorización, según CAIXABANK, dependiendo de la identidad del apoderado: la autorización que se utiliza entre personas físicas, la que se utiliza cuando una persona jurídica permite el acceso de una o más personas físicas y la autorización por la que se autoriza a terceros para acceder a consultas e instrucciones preparatorias (folios 660 y 747-751).*

(64) *El procedimiento de apoderamiento/autorización de acceso de terceros requiere ineludiblemente de autorización de acceso y operativa por parte del titular, la validación y el registro formal de la misma y la suscripción de un contrato específico con el tercero autorizado/apoderado, con la que se le suministra un par de nombres de usuario y claves de acceso (folio 660), distintos a los del cliente, lo que permite a la entidad conocer la identidad de quien ha realizado el acceso (folios 661 y 668).*

Política de seguridad

(65) *CAIXABANK está legalmente obligado y es, por tanto, responsable según la LSP y el RPD, de la adecuada protección del usuario de banca electrónica frente a fraudes y accesos a sus datos bancarios por parte de terceros que no consten formalmente identificados como apoderados o autorizados. Asimismo, está obligado a soportar los riesgos derivados de las eventuales violaciones de la seguridad del instrumento de pago electrónico así como a cumplir con la normativa de protección de datos personales y de secreto bancario. Además, la carga de la prueba de los posibles errores o fraudes en relación tanto a la autenticación como a la ejecución de operaciones de banca electrónica recaerá en todo caso sobre la entidad bancaria.*

(66) *CAIXABANK ha implementado diferentes mecanismos de seguridad en los que las contraseñas son custodiadas o procesadas por sistemas intermedios que garantizan que únicamente el cliente las conozca, de forma que ni siquiera CAIXABANK las conoce. Las claves que introduce el cliente salen de su navegador ya cifradas, para lo que se utilizan algoritmos no reversibles y en ningún momento transmite o se trabaja con la contraseña sin cifrar (folios 666 y 752).*

(67) *No obstante, los datos de identificación del usuario y contraseña, necesarios para acceder al servicio de banca electrónica, son personales e intransferibles por lo que el usuario es el responsable último de todas las acciones que se realicen con su identificador, por lo que está obligado a mantener la confidencialidad de estos datos (folio 658).*

(68) *Para poder cumplir con sus obligaciones, CAIXABANK tiene implementados distintos sistemas de seguridad informática que permiten detectar accesos no autorizados a los datos de sus clientes. Así, cuando el acceso se realiza desde una dirección IP que resulta "extraña" al cliente (por ejemplo, no haber sido anteriormente utilizada por éste, o bien por tener su origen en el extranjero), o cuando la introducción de las claves se hace a una velocidad excesiva (lo que suele ser una indicación de que el acceso no se está realizando por un particular sino por un sistema automatizado), como los utilizados, entre otros, por quienes intentan el acceso a sistemas protegidos mediante el método denominado de "ataque de fuerza bruta"[16], los protocolos de seguridad emiten una alarma cuya finalidad es evitar accesos incontrolados por terceros no autorizados[17].*

(69) *Para garantizar la seguridad de la plataforma de banca online y proteger las bases de datos, CAIXABANK realiza regularmente auditorías de seguridad y*

[16] El «ataque de fuerza bruta" consiste en tratar de lograr el acceso probando todas las combinaciones de' claves posibles mediante sistemas informáticos.

[17] Según la información aportada por CAIXABANK suministrada por una empresa externa de seguridad, en 2014 se produjeron 11.922 ataques desde internet dirigidos a las infraestructuras de CAIXABANK (folios 665 y 755), y CAIXABANK estima que más de mil clientes suyos son usuarios de agregadores financieros (folio 673).

mejoras de las medidas de protección de los sistemas de seguridad, que evitan o bloquean los accesos realizados por sistemas de conexión automática (robots, es decir, no son conexiones hechas por humanos), que son los utilizados en los ataques informáticos y también por los agregadores financieros (folio 665).

(70) *Cuando se detectan accesos ilícitos desde una conexión robotizada, se inhabilita temporalmente la IP originaria, por ser sospechosa de estar realizando accesos masivos con credenciales obtenidas ilícitamente para obtener irregularmente información de clientes. Esto explicaría, según CAIXABANK, que se hayan podido bloquear las conexiones automatizadas ejecutadas por FINTONIC (folio 665).*

(71) *En cuanto al uso de códigos de verificación captcha no se utilizan desde junio de 2014. Esta medida se aplicaba automáticamente cuando se detectaban conexiones robotizadas con las claves de acceso del cliente, manteniéndose de forma permanente para cualquier intento de conexión a Línea Abierta con esas claves. En la actualidad, los sistemas mediante códigos captcha han sido sustituidos por CAIXABANK por mecanismos mejorados de detección de comportamientos robóticos que identifican las conexiones no humanas en el momento de conexión (folios 665, 668 y 752).*

(72) *Según CAIXABANK, la entidad no tiene una política especial de acceso a los datos bancarios de sus clientes por parte de agregadores financieros, sino que aplica su política general de seguridad de banca electrónica (folio 657), y considera cualquier acceso no autorizado, incluidos los agregadores, como una amenaza a la seguridad del sistema (folio 668).*

(73) *La entidad, según la denunciada, no es capaz de distinguir si el que accede a la banca electrónica es un cliente, un agregador o un tercero no autorizado. Los sistemas de seguridad informática en banca electrónica contemplan sólo dos posibilidades: si se identifica a un cliente autorizado el sistema le permite operar, pero si se detecta un tercero no autorizado se bloquea el acceso. CAIXABANK además trata de analizar las pautas de esos accesos no autorizados para encontrar patrones de actuación que les permita identificarlos más adelante y mejorar sus sistemas de seguridad. Con estos métodos, según CAIXABANK, se puede "intuir" (folio 663) generalmente quién está detrás de un acceso no autorizado, si bien nunca se sabe con certeza. Por ejemplo, los casos de suplantación de identidad suelen utilizar medios robotizados, acceden a la plataforma a diario y habitualmente de madrugada. Aun así, CAIXABANK ha identificado con sus sistemas de monitorización la actividad de varios agregadores, entre ellos FINTONIC, Mooverang, MyValue y Ahorroy (folio 663).*

(74) *Por otro lado, las claves de acceso una vez en manos de los agregadores no son custodiados por CAIXABANK, esto es, no son administrados, gestionados, supervisados ni auditados por ésta, por lo que la entidad, según la*

denunciada, no puede garantizar que su protección sea la adecuada y que no sean objeto de ataques informáticos que puedan tener como finalidad la comisión de un fraude (folio 664).

(75) *La probabilidad de ataque informático, según la entidad, se duplica, ya que pueden ser objeto de fraude tanto CAIXABANK como FINTONIC, pudiéndose producir ataques a través de FINTONIC que al no ser detectados ni controlados no podrían monitorizarse y evitarse en sucesivas ocasiones (folio 664).*

(76) *CAIXABANK está sometida a la normativa Payment Card Industry (PCI)*[18] *sobre seguridad de las tarjetas financieras (folio 667), que es una guía que ayuda a las organizaciones que procesan, almacenan y/o transmiten datos de titulares de tarjeta a asegurar dichos datos, con el fin de evitar los fraudes que involucran tarjetas de pago débito y crédito. Las compañías que procesan, guardan o trasmiten datos de tarjetas deben cumplir con el estándar o se arriesgan a la pérdida de sus permisos para procesar las tarjetas de crédito y débito, enfrentar auditorías o pagos de multas. Los comerciantes y proveedores de servicios de tarjetas de crédito y débito, deben validar su cumplimiento al estándar en forma periódica*[19]*. CAIXABANK opina que si se introduce un intermediario en la cadena de acceso a los sistemas que muestran la información de las tarjetas, éste también debería someterse a la normativa PCI (folio 667).*

(77) *En 2013 el Banco Central Europeo publicó unas Recomendaciones para la seguridad de los pagos por internet, que deberían aplicarse antes del 1 de febrero de 2015, e inició una consulta pública sobre las recomendaciones para la seguridad de los servicios de acceso a cuentas de pago elaboradas por el Foro Europeo*[20]*, que finalmente se publicaron a principios de 2014*[21]*. Dentro de estas Recomendaciones se encuentra que los proveedores terceros (TPP) se aseguren de que el acceso a los datos está protegido por sistemas robustos de autenticación de usuarios, que el registro, suscripción y autenticación del cliente se lleve a cabo en un entorno seguro, que el TPP fije un número limitado de intentos de acceso y tiempo máximo de sesión, etc. No*

[18] *Payment Card Industry Data Security Standard*, Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.
[19] Sólo a las compañías que procesan menos de 80,000 transacciones por año se les permite realizar una autoevaluación utilizando un cuestionario provisto por el Consorcio del PCI (PCI SSC).
[20] http://www.bde.es/f/webbde/GAP/Secciones/SalaPrensa/ComunicadosBCE/NotasInformativasBCE/13/Arc/Fic/presbce2013-15.pdf
http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html
[21] En las recomendaciones de 2014 pone que el BCE ha decidido publicarlas mientras no se apruebe la 2DSP. Originalmente, era un documento destinado a la Autoridad Bancaria Europea, EBA, que deberá hacer una guía de medidas de seguridad, mientras tanto no se espera que las recomendaciones sean aplicadas por los países miembros del Foro Europeo de seguridad de pagos minoristas.
http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

obstante, los proveedores terceros no están sometidos aún a supervisión por lo que dependen de la futura segunda Directiva de Servicios de Pago."

FUNDAMENTOS DE DERECHO

PRIMERO.- Competencia para resolver.

De acuerdo con lo previsto en la disposición adicional primera de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia, mediante Orden ECC/1796/2013, de 4 de octubre, del Ministerio de Economía y Competitividad, se determinó el 7 de octubre de 2013 como fecha de puesta en funcionamiento de la CNMC. Según la disposición adicional segunda de la misma Ley "*las referencias que la legislación vigente contiene a la Comisión Nacional de la Competencia* […] *se entenderán realizadas a la Comisión Nacional de los Mercados y la Competencia* […]" y "*Las referencias que la Ley 15/2007, de 3 de julio, contiene a la Dirección de Investigación de la Comisión Nacional de Competencia se entenderán realizadas a la Dirección de Competencia de la Comisión Nacional de los Mercados y la Competencia*".

Por otro lado, de acuerdo con el artículo 5.1.c) de la Ley 3/2013, a la CNMC compete "*aplicar lo dispuesto en la Ley 15/2007, de 3 de julio, en materia de conductas que supongan impedir, restringir y falsear la competencia*". El artículo 20.2 de la misma ley atribuye al Consejo la función de "*resolver los procedimientos sancionadores previstos en la Ley 15/2007, de 3 de julio*" y según el artículo 14.1.a) del Estatuto orgánico de la CNMC aprobado por Real Decreto 657/2013, de 30 de agosto, "*la Sala de la Competencia conocerá de los asuntos relacionados con la aplicación de la Ley 15/2007, de 3 de julio*".

Finalmente, el artículo 49 de la LDC señala que corresponde al Consejo, a propuesta de la DC, acordar no incoar los procedimientos derivados de la presunta realización de las conductas prohibidas por los artículos 1, 2 y 3 de esta Ley y el archivo de las actuaciones cuando considere que no hay indicios de infracción de la Ley.

En consecuencia, la competencia para adoptar el presente acuerdo corresponde a la Sala de Competencia del Consejo de la CNMC.

SEGUNDO.- Objeto y valoración jurídica del órgano instructor.

El objeto de la presente resolución es determinar si, tal y como sostiene la DC, las conductas investigadas no presentan indicios de infracción de la LDC y procede el archivo de las actuaciones, de conformidad con el artículo 49.3 de la LDC.

En concreto la DC propone la no incoación del procedimiento sancionador y el archivo de las actuaciones en los siguientes términos:

(102) Por ello, de acuerdo con lo previsto en el artículo 49.3 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia, se propone la no incoación del procedimiento sancionador, así como el archivo de las actuaciones seguidas como consecuencia de la denuncia presentada por la empresa FINTONIC, por considerar que no hay indicios de infracción de la mencionada Ley.

(103) Elévese esta Propuesta de Archivo al Consejo de la Comisión Nacional de los Mercados y la Competencia, junto con la denuncia y las actuaciones practicadas, de acuerdo con lo previsto en el artículo 27 del Reglamento de Defensa de la Competencia, aprobado por Real Decreto 261/2008, de 22 de febrero.

Para alcanzar esta conclusión la DC realiza la siguiente valoración de las conductas investigadas:

En primer lugar, la DC considera que el análisis de los hechos en base al artículo 3 implica identificar, si la conducta de la empresa denunciada se enmarca en alguno de los actos de competencia desleal tipificados en la Ley 3/1991,de 10 de enero, de Competencia Desleal (LCD), limitando la capacidad de competir de otras empresas.

En su denuncia FINTONIC considera que los hechos denunciados constituyen un acto de competencia desleal de obstaculización y hostigamiento que sería sancionable según la cláusula general de la LCD, recogida en su artículo 4, en la que se reputa como desleal todo comportamiento que resulte objetivamente contrario a las exigencias de la buena fe, ya que según el denunciante: *"a) no cuentan con una justificación objetiva; b) afectan negativamente a la posición concurrencial de un tercero (Fintonic); c) interfieren el normal desarrollo de la actividad de Fintonic en el mercado; y d) le impiden entrar o afianzarse en el mercado. Y ello sin perjuicio de que los Actos de Obstaculización y Hostigamiento procuren o sean adecuados para procurar a quien los realiza un provecho propio*" (folio 16).

No obstante, la DC considera que la conducta denunciada no tiene cabida en los supuestos tipificados como desleales en la LCD y, por tanto, no se cumple el primero de los requisitos exigidos para la posible aplicación del artículo 3 de la LDC.

La DC considera que, según la información disponible en el expediente, las limitaciones impuestas por CAIXABANK al denunciante en relación con el acceso de sus clientes a plataformas como la de FINTONIC, así como los contactos que CAIXABANK ha podido mantener con sus clientes en relación con la utilización del agregador financiero, se justifican por motivos de seguridad contra el fraude y protección de datos personales, admitiendo dicho acceso siempre que no sea a través de la operativa de cesión de contraseñas, que es como opera FINTONIC. El acceso a la banca online tal y como se está haciendo en la actualidad por parte

de FINTONIC es entendido e interpretado por CAIXABANK como suplantación de identidad. El uso por parte de terceros de las claves del cliente está, según CAIXABANK, violando la condición de intransferibilidad de las mismas establecidas contractualmente, además de imposibilitar a la entidad la identificación del usuario que está efectivamente realizando el acceso y si está autorizado para ello, por lo que no serían efectivos los sistemas de seguridad que impiden el *phishing*[22] (suplantación de identidad) y otros actos ilícitos (folio 662). Si bien admite CAIXABANK que la cesión a terceros de las claves personales de usuario y contraseña no es suficiente para ejecutar operaciones transaccionales, sí debilita, según indica, la robustez de los mecanismos de autenticación del sistema de banca electrónica (folio 666).

La DC concluye que sería la operativa de FINTONIC la que, por motivos de seguridad, no estaría siendo compatible con la operativa de CAIXABANK.

En su propuesta de archivo la DC recuerda que CAIXABANK ha sugerido a FINTONIC la posibilidad de firmar un contrato de usuario autorizado o apoderado entre el cliente y el agregador financiero, lo que podría suponer una alternativa al acceso a través de la banca online con las claves del usuario, garantizando así que se cumplieran los protocolos de seguridad de la entidad al poder identificar claramente el usuario que accede a la información del cliente (folios 661, 774, 781), y haciendo posible por tanto, la utilización de FINTONIC por parte de los usuarios de CAIXABANK.

Igualmente el órgano instructor señala que los usuarios también podrían optar por el envío de los datos en formato Excel, que se pueden descargar desde la plataforma de Caixabank por el usuario y pueden ser compartidos y manipulados, de forma que el usuario pueda facilitárselos al agregador (folio 661).

Teniendo en cuenta todo lo anterior, la DC concluye que los clientes de CAIXABANK sí podrían utilizar la plataforma de FINTONIC, respetando la operativa de la denunciada que se justifica en base a razones objetivas de seguridad, establecidas tanto por protocolos internos de CAIXABANK, como por la normativa existente.

La DC señala de nuevo que CAIXABANK está sometida a la normativa *Payment Card Industry (*PCI)[23] sobre seguridad de las tarjetas financieras (folio 667), y por tanto, debe cumplir con el estándar o arriesgarse a la pérdida de sus permisos para procesar las tarjetas de crédito y débito y enfrentar auditorías o pagos de multas, por lo que CAIXABANK opina que si se introduce un intermediario en la cadena de acceso a los sistemas que muestran la información de las tarjetas, como FINTONIC, éste también debería someterse a la normativa PCI (folio 667).

[22] Se denomina phishing al intento de adquirir información sensible, claves de usuario, contraseñas o detalles de tarjetas bancarias haciéndose pasar por una entidad fiable en las comunicaciones electrónicas.
[23] https://www.pcicomplianceguide.org/pci-faqs-2/

En segundo lugar y con respecto a la normativa vigente en materia de protección de datos (LPD y RPD), la DC considera que los datos relativos a los clientes de CAIXABANK son de carácter personal, a los que hay que aplicar medidas de seguridad de nivel medio, siendo CAIXABANK el responsable del tratamiento de los datos, pues es quien decide la finalidad, contenido y uso (art. 3 de la LPD). Los responsables de tratamiento deben cumplir con el deber de secreto (art. 10 LPD) e implementar las medidas de seguridad necesarias para custodiar los datos en su poder, garantizando la eficacia de dichas medidas para evitar accesos ilícitos, lo que según la denunciada, es incompatible con las pretensiones de FINTONIC (folio 669).

Por último, la DC señala que, según la información aportada, los usuarios de FINTONIC que son clientes de CAIXABANK representan en torno al 20% del total de usuarios del servicio de agregación, por lo que CAIXABANK no es un operador esencial para la subsistencia de FINTONIC. Además, hay que resaltar que no se trata de usuarios de una única entidad sino que ese 20% es además cliente de otras entidades financieras que sí están disponibles en FINTONIC, por lo que en cualquier caso, podrían seguir utilizando el servicio para estas otras. También subraya que FINTONIC ha manifestado en varias ocasiones ser el líder del mercado de agregación financiera en España (folios 5, 10, 18 y 547), con una cuota de mercado estimada en 2012 de en torno al 75-80% (folio 554), por lo que los actos denunciados no le han impedido entrar y afianzarse en el mercado, como se mencionaba en el párrafo (82).

Desde esta perspectiva y para lo que interesa a la competencia y su protección la DC destaca que la negativa de CAIXABANK no elimina la posibilidad de existencia de una operador como FINTONIC en el mercado dado que el porcentaje de clientes que el denunciante podría perder potencialmente como consecuencia de la negativa no es relevante para el desarrollo de su negocio, siendo ya líder en el sector. Dicha negativa está además justificada, considerando la DC que debe ponderar adecuadamente los efectos de la limitación impuesta por la denunciada sobre el desarrollo de un nuevo servicio en el mercado con la necesidad de facilitar el cumplimiento de las obligaciones de seguridad que tiene CAIXABANK con sus clientes.

Por todo ello, la DC concluye que la decisión de CAIXABANK de no facilitar el acceso de sus clientes a sus datos de banca online cuando actúan a través de FINTONIC en los términos deseados por la denunciante, no es una decisión que pueda reputarse desleal en los términos previstos por la LCD, no reuniendo por tanto, los requisitos necesarios del artículo 3 de la LDC, y que atiende a razones objetivas y justificadas.

La DC aclara que CAIXABANK no niega el acceso a los usuarios de FINTONIC a sus cuentas de banca online, sino que requiere que se realice en base a un determinado protocolo de seguridad, con el fin de controlar que el acceso no está siendo fraudulento, con las consiguientes responsabilidades que de ello podrían

derivarse para la denunciada. Además, la regulación en la materia que se encuentra actualmente vigente, no es aplicable a los nuevos servicios y proveedores de servicios como los agregadores financieros y no existe obligación legal para la denunciada de facilitar el acceso a los usuarios de los agregadores financieros en los términos que FINTONIC pretende. La regulación aplicable a los proveedores de servicios de información sobre cuentas, está pendiente de desarrollar, tal y como la propia Comisión Europea indica en su Propuesta de Directiva y en el Estudio de Impacto de la Propuesta[24], por lo que todavía no están definidas unas condiciones de acceso seguras, ni los derechos y obligaciones para dichos proveedores que aseguren una certidumbre legal tanto para éstos como para los bancos.

De hecho, la normativa vigente actualmente (Directiva de Servicios de Pago) en su artículo 56 es interpretada por el Consejo Europeo de Pagos (*European Payments Council*, representante de los Proveedores de Servicios de Pago[25]) de manera estricta, como indica en un comunicado en relación con la DSP2, y por lo tanto, considera que bajo ninguna circunstancia el consumidor debe compartir sus claves de seguridad con terceros[26], respaldando de hecho que dicho principio continúe siendo aplicado en la futura DSP2[27].

En definitiva, la DC concluye que la actuación de CAIXABANK no reúne los requisitos del artículo 3 de la LDC, por lo que la DC propone la no incoación del correspondiente procedimiento sancionador y el archivo de las actuaciones. En relación con las medidas cautelares solicitadas por el denunciante, considera que no procede pronunciarse sobre las mismas ya que, de acuerdo con el artículo 54 de la LDC, solamente se podrán adoptar una vez incoado el expediente.

---

[24] http://ec.europa.eu/internal_market/payments/docs/framework/130724_impact-assessment-full-text_en.pdf

[25] http://www.europeanpaymentscouncil.eu/index.cfm/about-epc/the-european-payments-council/

[26] Artículo 56 de la DSP : « *Obligaciones del usuario de servicios de pago en relación con los instrumentos de pago 1. El usuario de servicios de pago habilitado para utilizar el instrumento de pago deberá cumplir las obligaciones siguientes: a) utilizar el instrumento de pago de conformidad con las condiciones que regulen la emisión y utilización del instrumento de pago, y b) en caso de extravío, robo o sustracción del instrumento de pago, o de utilización no autorizada de este, notificarlo al proveedor de servicios de pago o a la entidad que este designe sin demoras indebidas en cuanto tenga conocimiento de ello. 2. En particular, a efectos del apartado 1, letra a), el usuario de servicios de pago, en cuanto reciba un instrumento de pago, tomará todas las medidas razonables a fin de proteger los elementos de seguridad personalizados de que vaya provisto."*

[27] http://www.europeanpaymentscouncil.eu/pdf/EPC_Article_334.pdf « *The EPC disapproves of the possibility for TPPs to use the personal security credentials of the payment service user, (i.e. the account holder or consumer), to get access to a customer's account, thus impersonating the account holder. The EPC, therefore, strongly recommends maintaining the principle that a consumer should never have to share his or her personal security credentials with third parties. This is a pre-condition to ensuring the continued security of consumer's funds and data in the online banking environment."*

No obstante, la Propuesta de Archivo también señala que, ante la aparición de nueva información o un cambio en las circunstancias presentes en el mercado, el órgano de investigación podría iniciar nuevas actuaciones al objeto de comprobar la compatibilidad de tales conductas con la normativa de competencia.

TERCERO.- Valoración de la Sala de Competencia

La Sala debe valorar si, tal y como sostiene la DC, las conductas investigadas no presentan indicios de infracción de la LDC y procede el archivo de las actuaciones, de conformidad con el artículo 49.3 de la LDC o si, por el contrario, en la negativa de CAIXABANK al acceso a su servicio de banca online por parte de FINTONIC utilizando las claves de acceso de sus clientes podrían existir indicios de una restricción de la competencia prohibida por la LDC que motivaran la continuación de las investigaciones de cara al total discernimiento de los hechos.

La denunciante sostiene que esta conducta de CAIXABANK, constituyen actos de obstaculización y hostigamiento, que violarían el artículo 4 de la LCD y supondrían una infracción del artículo 3 de la LDC al restringir o falsear la competencia en el mercado, afectando al interés público.

Por su parte, la DC considera que la actuación de CAIXABANK no reúne los requisitos para determinar la existencia de una infracción del artículo 3 de la LDC, por lo que propone la no incoación del correspondiente procedimiento sancionador y el archivo de las actuaciones.

El artículo 3 de la LDC Falseamiento de la libre competencia por actos desleales, establece que *"La Comisión Nacional de la Competencia o los órganos competentes de las Comunidades Autónomas conocerán en los términos que la presente Ley establece para las conductas prohibidas, de los actos de competencia desleal que por falsear la libre competencia afecten al interés público".*

Por su parte el artículo 4 de la LCD ("*Cláusula general*") dispone lo siguiente:

> *1. Se reputa desleal todo comportamiento que resulte objetivamente contrario a las exigencias de la buena fe.*
>
> *En las relaciones con consumidores y usuarios se entenderá contrario a las exigencias de la buena fe el comportamiento de un empresario o profesional contrario a la diligencia profesional, entendida ésta como el nivel de competencia y cuidados especiales que cabe esperar de un empresario conforme a las prácticas honestas del mercado, que distorsione*

o pueda distorsionar de manera significativa el comportamiento económico del consumidor medio o del miembro medio del grupo destinatario de la práctica, si se trata de una práctica comercial dirigida a un grupo concreto de consumidores.

A los efectos de esta ley se entiende por comportamiento económico del consumidor o usuario toda decisión por la que éste opta por actuar o por abstenerse de hacerlo en relación con:

a) La selección de una oferta u oferente.
b) La contratación de un bien o servicio, así como, en su caso, de qué manera y en qué condiciones contratarlo.
c) El pago del precio, total o parcial, o cualquier otra forma de pago.
d) La conservación del bien o servicio.
e) El ejercicio de los derechos contractuales en relación con los bienes y servicios.

Igualmente, a los efectos de esta ley se entiende por distorsionar de manera significativa el comportamiento económico del consumidor medio, utilizar una práctica comercial para mermar de manera apreciable su capacidad de adoptar una decisión con pleno conocimiento de causa, haciendo así que tome una decisión sobre su comportamiento económico que de otro modo no hubiera tomado."

Siguiendo la doctrina expuesta en anteriores resoluciones de los antiguos Tribunal de Defensa de la Competencia (TDC) y CNC relativas a conductas tipificadas por el artículo 3 LDC (entre otras la resolución del TDC de 26 de febrero de 2004, Expte. 560/03, Grupo Freixenet; y de la CNC de 20 de diciembre de 2007, Expte 703/06, Agencias de Carga/Correos; de 2 de enero de 2008, Expte r 710/06, Castellana Subastas Holding; de 28 de enero de 2009, Expte 2659/05, Rotores; de 10 de junio de 2009, Expdte 2741/06, SIGNUS ECOVALOR; de 28 de mayo de 2010, Exp. S/0227/10, ATR ENDESA) son tres los requisitos para que exista una conducta de falseamiento de la competencia por actos desleales:

1) Existencia de un ilícito desleal tipificado en la Ley 3/1991 de 10 de enero de Competencia Desleal (en adelante LCD);
2) Falseamiento de la libre competencia; y,
3) Afectación del interés público.

Estos tres elementos son cumulativos e independientes entre sí, de modo que la conducta que el artículo 3 LDC tipifica exige que en la conducta que está siendo enjuiciada estén presentes los tres. Además, de acuerdo con los precedentes el articulo 3 LDC se dirige esencialmente a reprimir comportamientos que afecten significativamente a la competencia como señalan diversas resoluciones de la

CNC (entre otras, las resoluciones de 30 de noviembre de 2007, Expte. S/0013/07, La tienda en casa; de 11 de marzo de 2008, Expdte S/0041/08, Tu Billete; de 29 de junio de 2009, Expte S/0148/09, Correos/Viajes Crisol; de 28 de julio de 2009, Expte. S/0151/08, La Sexta; de 30 de noviembre de 2009, Expte S/0191/09, AGUARDIENTES; de 30 de junio de 2010, Expdte S/0137/09, TELEFONICA; de 2 de diciembre de 2010, Expdte S/0265/10, cofradía de Pescadores de Sant Pere de l' Atmella).

En relación con el primer requisito, la existencia de una infracción de la LCD, la DC considera que las limitaciones impuestas por CAIXABANK al denunciante en relación con el acceso de sus clientes a FINTONIC y los contactos de la entidad con clientes del agregador, se justifican por motivos de seguridad contra el fraude y protección de datos personales. A juicio de CAIXABANK (folio 669) la actividad de FINTONIC debilita la robustez de los mecanismos de autenticación del sistema de banca electrónica, por lo que CAIXABANK no podría garantizar la seguridad y privacidad integral de los datos de los clientes.

Además, la DC también señala que CAIXABANK ofrece alternativas al denunciante para evitar estas restricciones, como la firma de un contrato de usuario autorizado o apoderado entre el cliente y el agregador financiero, que garantice que se cumplan los protocolos de seguridad de la entidad y poder identificar claramente el usuario que accede a la información del cliente (folios 661, 774, 781). También propone que los usuarios envíen los datos en formato excel, que se pueden descargar desde la plataforma de Caixabank, de forma que el usuario pueda facilitárselos al agregador (folio 661).

Como ha señalado la sentencia de la Audiencia Provincial de Barcelona (rec. Nº 160/2011) de 12 de abril de 2011, define los actos de obstaculización como una *"de las manifestaciones de la cláusula general prohibitiva"* del artículo 4 de la LCD y considera que "*se definen en este contexto como aquellos actos que sin contar con una justificación objetiva afectan negativamente a la posición concurrencial de un tercero o de cualquier forma interfieren el normal desarrollo de su actividad en el mercado, impidiéndole entrar o afianzarse en él o introducir o afianzar en él alguna de sus prestaciones, sin perjuicio de que en ocasiones procuren o sean adecuados para procurar a quien los realiza un provecho propio".* Por ello, una justificación objetiva como la ofrecida por CAIXABANK referida a motivos de seguridad contra el fraude podría ser suficiente para no considerar la conducta realizada por la entidad bancaria frente a FINTONIC como de obstaculización.

No obstante, la actitud de CAIXABANK frente a la actuación de FINTONIC ofrece también datos en los que podría acreditarse que la preocupación predominante de la entidad bancaria en determinados momentos no se ha limitado a la seguridad de los datos de sus clientes sino también a la posible incidencia en su negocio de la información trasmitida a sus clientes por FINTONIC respecto a aspectos del negocio bancario relativos a comisiones, gatos y rentabilidad de los productos

ofertados por CAIXBANK respecto a los de otros competidores en el mercado de la banca minorista.

Según expone CAIXABANK en su respuesta al requerimiento de información efectuado por la DC (folio 664) respecto a los hechos denunciados por FINTONIC "*Los problemas detectados por CAIXABANK son los mismos para los distintos agregadores financieras, y se relacionan con la seguridad legal, de utilizar un modelo de suplantación de la identidad legal de banca electrónica del cliente, así como del sistema informático"*.

Sin embargo, consta en la información reservada realizada por la DC (folios756-760 y 766-770) que el 14 de enero de 2015 CAIXABANK remitió un burofax a FINTONIC firmado por el Director de la Asesoría Jurídica Corporativa en el que se instaba al agregador financiero a cesar en el envío de comunicaciones a los clientes en las que se señala a CAIXABANK como el banco que más cobra a sus usuarios ya que, según la carta enviada, FINTONIC estaba "*divulgando afirmaciones falsas relativas a los servicios de esta entidad, incurriendo por ello en múltiples y muy graves actos de competencia desleal contrarios asimismo a las normas legales de marcas y publicidad e irrogando unos graves perjuicios a esta Entidad Financiera que deberán reparar".*

En el mismo escrito remitido por burofax CAIXABANK solicita a FINTONIC que identifique "*la totalidad de (i) fuentes, (i) datos y (iii) método/s utilizado/s para realizar las manifestaciones inciertas, no veraces y contrarias a la más elemental buena fe*", así como otros datos relativos al número de comunicaciones remitidas y al plazo de tiempo que lleva enviándolas el denunciante.

Por último, CAIXABANK también requiere a FINTONIC que cesar, con carácter inmediato "*en el constante uso ilegal de firmas electrónicas de clientes, debiendo abstenerse de acceder la banca electrónica de clientes de CAIXABANK suplantando su identidad*" y en "*en inducir a los clientes de CAIXABANK a infringir gravemente tanto la legalidad vigente como los contratos de banca electrónica, solicitándoles que les comuniquen a Vds. sus firmas electrónica"*. La entidad bancaria informa también a FINTONIC de su intención de pedir una indemnización por daños y, en caso de no llegar a un acuerdo amistoso, denunciar a FINTONIC (folios 756-760 y 766-770).

A la luz de las consideraciones anteriores, y teniendo en cuenta la importancia de la seguridad y privacidad de los datos en internet, más si cabe tratándose de datos bancarios, si bien algunos de los argumentos aportados por CAIXABANK a la hora de justificar ciertas limitaciones impuestas a la operativa de FINTONIC podrían considerarse suficientes, ha quedado acreditado que la preocupación de CAIXABANK por la operativa de FINTONIC no se limitaba a los puntos de seguridad jurídica e informática apuntados, teniendo en cuenta el número de sus clientes de los que tiene constancia que han cedido sus claves a FINTONIC es limitado (folio 673, en torno a un millar).

Por tanto, si bien la DC considera que los actos denunciados no han impedido a FINTONIC entrar y afianzarse en el mercado ya que solo el 20% de sus usuarios son clientes de CAIXABANK, esta Sala estima que la reacción de las entidades bancarias frente a la actividad de los agregadores financieros puede tener repercusiones directas en la presencia en el mercado de los mismos y debe ser tenida en consideración en su totalidad en la evaluación de los hechos, sin que la legítima preocupación por la seguridad jurídica e informática del negocio bancario pueda servir para disfrazar alguna actitud anticompertitiva.

No obstante, a la vista de la denuncia presentada, de la documentación que obra en el expediente y del análisis de los hechos realizado por la DC, esta Sala no aprecia en la actividad de CAIXABANK indicios de una conducta desleal en los términos previstos por la Ley 3/1991, de 10 de enero, de Competencia Desleal, no reuniendo por tanto, los requisitos necesarios del artículo 3 de la LDC. No existiendo, pues, indicios de prácticas prohibidas por el artículo 3 de la LDC, el Consejo considera ajustada a Derecho la Propuesta de Archivo de las actuaciones realizadas en el marco del expediente S/DC/0536/14, CAIXABANK**.**

Ahora bien, aunque la Sala considera que en los hechos denunciados no se encuentran indicios suficientes de una posible infracción del art. 4 de la LCD (y por ende, del artículo 3 de la LDC) para proseguir la investigación, coincide igualmente con la DC en estimar que la aparición de nueva información o un cambio en las circunstancias presentes en el mercado, podrían motivar que la DC pudiera iniciar nuevas actuaciones al objeto de comprobar la compatibilidad de las conductas de CAIXABANK con la normativa de competencia.

Por todo lo anterior, vistos los preceptos citados y los demás de general aplicación, el Consejo en Sala de Competencia,

HA RESUELTO

ÚNICO.- No incoar procedimiento sancionador y archivar las actuaciones seguidas por la Dirección de Competencia de la CNMC en el expediente S/DC/0536/14, CAIXABANK, como consecuencia de la denuncia presentada por FINTONIC SERVICIOS FINANCIEROS S.L., por considerar que en este expediente no hay indicios de infracción de los artículos 1 y 2 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia ni 101 y 102 del Tratado de Funcionamiento de la Unión Europea.

Comuníquese esta Resolución a la Dirección de Competencia de la Comisión Nacional de los Mercados y la Competencia y notifíquese a los interesados, haciéndoles saber que contra ella no cabe recurso alguno en vía administrativa, pudiendo interponer recurso contencioso-administrativo ante la Audiencia Nacional, en el plazo de dos meses a contar desde su notificación.