CIBERATAQUES: PHISHING Y FRAUDE DEL CEO. UNA APROXIMACIÓN JURÍDICA.

1.- Introducción. Ciberataques más comunes en la actualidad.

En este artículo queremos comentar dos tipos de ciberataques que se dan en la práctica de forma cada vez más frecuente, que son los siguientes:

- **Suplantación de la identidad del banco (phishing):** Este ataque suele consistir en correos electrónicos en los que el atacante se hace pasar por una entidad financiera y trata de que el usuario le revele su información confidencial, como datos de cuenta bancaria, usuario y clave de acceso. Tras obtener esa información, el atacante accede a la cuenta de la víctima y realiza una serie de transferencias a su favor o directamente realiza pagos a cargo de la cuenta de la víctima.

- **Suplantación de la identidad de una empresa o de un directivo (fraude del CEO):** Este tipo de ataque suele consistir en la interceptación de una conversación entre empresas, a través de correos electrónicos, en la que se está hablando de un pago pendiente. Una vez interceptada la conversación, el atacante sustituye un número de cuenta bancaria a la que se va a realizar un pago por la suya. Normalmente se hace mediante la manipulación de una factura, o haciéndose pasar por una persona de la organización y ordenando un pago a una persona con poderes para ello. Incluso se están dando casos de mensajes telefónicos con voz simulada por inteligencia artificial.

Estos dos tipos de ataque tienen en común que en ellos interviene una entidad financiera que, en principio, siempre es ajena al fraude, pero que participa o se ve involucrada en su comisión. En el primer caso, porque el atacante se hace pasar por la entidad para obtener de forma fraudulenta los datos de acceso a la cuenta bancaria de la víctima y apropiarse de su dinero. En el segundo, porque la entidad recibe una orden de transferencia de un cliente que ha sido engañado, y ejecuta esa orden sin saber que el beneficiario de la misma es el atacante.

2.- Marco jurídico aplicable. Principales normas a tener en cuenta.

La norma principal a tener en cuenta en estos casos es el Real Decreto-ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, que derogó la Ley 16/2009, de 13 de noviembre, de servicios de pago.

Además, es importante la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo en lo relativo a las normas técnicas de regulación para la autenticación reforzada de clientes y unos estándares de comunicación abiertos comunes y seguros. Y también el Reglamento Delegado (UE) 2018/389 de la Comisión, de 27 de noviembre de 2017, por el que se complementa la Directiva anterior.

Estas normas regulan los servicios de pago, que básicamente son los ingresos, retirada de efectivo, transferencias, domiciliaciones y pagos con tarjeta. Y, en lo que nos interesa para este artículo, regulan los procedimientos para ejecutar órdenes de pago, las obligaciones de las entidades de servicios de pago, las medidas de seguridad que deben establecer y su régimen de responsabilidad.

Vamos a resumir los principales preceptos de estas normas, enfocándonos en los dos tipos de fraude comentados al inicio:

- **Partes intervinientes**: Las partes serán el ordenante de una transferencia, la entidad de servicios de pago del ordenante y quien recibe la orden de pago, el beneficiario de la transferencia, que será el atacante en los dos tipos de fraude que comentamos, y la entidad de servicios de pago del beneficiario que es quien recibe el pago.

- **Procedimiento de ejecución de operaciones de pago**: Para poder realizar operaciones de pago, los usuarios deberán autenticarse conforme a la norma técnica, y utilizar el identificador único del otro usuario del servicio de pago (arts. 68 y 3.22 y 59 LSP).

  Surgen aquí algunos conceptos muy importantes a efectos de analizar la posible responsabilidad de las entidades de servicios de pago participantes. El primero de ellos es la autenticación. El art. 68 de la LSP establece que para acceder a la cuenta, realizar una operación de pago o realizar cualquier operación remota que pueda dar lugar a un fraude o abuso, el operador de servicios de pago aplicará la autenticación reforzada del cliente. Esta autenticación reforzada consiste en el proceso por el que la entidad debe comprobar la identidad del

usuario de los servicios de pago, mediante dos o más elementos. En la práctica, consiste en una clave que sólo el usuario conoce, más una clave que se envía al teléfono o más una huella digital.

El segundo concepto importante es el identificador único, que se define como una combinación de números y letras o signos que sirve para identificar de forma inequívoca al otro usuario del servicio de pago (art. 3.22 LSP). En los países de la zona SEPA se corresponde con el IBAN o número de cuenta.

- **Responsabilidad de cada entidad de servicios de pago**: El art. 45 de la LSP regula la responsabilidad de la entidad de servicios de pago en caso de operaciones no autorizadas, estableciendo que la entidad devolverá el importe de la operación no autorizada de inmediato, salvo que el ordenante haya cometido fraude. El art. 46 establece que el ordenante será quien deba soportar las pérdidas si ha actuado de manera fraudulenta o si ha incumplido deliberadamente o por negligencia grave las obligaciones de proteger sus credenciales y avisar a la entidad en caso de pérdida o extravío, robo de la información, etc. Por otra parte, los arts. 59 y 60 LSP regulan la responsabilidad por el uso de identificadores únicos incorrectos, estableciendo que si una orden de pago se realiza conforme a un identificador único facilitado por el ordenante, la entidad de servicios de pago no tiene responsabilidad en caso de que resulte ser incorrecto.

3.- Diferencia jurídica entre ambos tipos de fraude.

Al analizar las normas mencionadas en el apartado anterior, vemos que el tratamiento que recibe la entidad de servicios de pago en uno y otro tipo de ciberataque es muy distinto.

En el primero, es decir, el caso de phishing, la entidad de servicios de pago tiene una responsabilidad prácticamente objetiva. El art. 45 LSP es rotundo cuando manifiesta que "devolverá el importe de la operación no autorizada de inmediato". Estamos ante un caso de una operación que no cuenta con el consentimiento del titular de la cuenta, porque mediante fraude o estafa un tercero se ha apropiado de sus datos y ha sido este tercero el que ha accedido a su cuenta bancaria y ha dado la orden de transferencia o pago a la entidad. La operación se ejecuta sin que el perjudicado lo sepa, ni mucho menos lo autorice.

Podría parecer que dicho régimen de responsabilidad objetiva deja escaso margen de defensa a las entidades de servicios de pago. Sin embargo, el art. 46 prevé que será el ordenante de una transferencia quien deba soportar las pérdidas cuando haya actuado de forma fraudulenta o con negligencia grave, al haber incumplido su obligación de tomar las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas, y de denunciar sin demora el extravío o sustracción de las mismas, o del instrumento de pago.

En el segundo caso, en cambio, el conocido como fraude del CEO, es el propio perjudicado el que accede a su cuenta bancaria con sus propios datos y credenciales (mediante la autenticación reforzada) y quien facilita los datos del identificador único, es decir, el IBAN o número de cuenta bancaria del destinatario de la transferencia. El fraude está en que el IBAN no se corresponde con el beneficiario que el perjudicado cree, sino con un tercero. No se trata por tanto de una operación de pago no autorizada del art. 45 LSP. Sí que ha sido autorizada, pero el ordenante ha sido engañado.

Y aquí es donde surge la siguiente pregunta: ¿cómo es posible que se autorice una transferencia a un número de cuenta que no se corresponde con el beneficiario, cuyo nombre se facilita al realizar la transferencia? En otras palabras, ¿tiene responsabilidad la entidad de pagos del ordenante o la del beneficiario por no comprobar que el IBAN coincida con el titular que el ordenante indica en la transferencia?

Los arts. 59 y 60 LSP establecen un régimen de responsabilidad para la entidad de servicios de pago completamente distinto que en el caso anterior de phishing. En este caso, de fraude del CEO, la LSP establece que el proveedor de servicios de pago no será responsable en caso de que el usuario le facilite un identificador único incorrecto, aunque le haya facilitado información adicional como el nombre del beneficiario a quien cree estar haciendo la transferencia.

Sobre esta cuestión es interesante la nota que publica el Banco de España en su página web[1], en la que dice: *"La normativa de servicios de pago tampoco establece el deber de las entidades de comprobar que el nombre del beneficiario se corresponde con el del titular del número de cuenta de destino de la transferencia ni otros datos adicionales, más allá de la coincidencia del IBAN beneficiario con el indicado en la orden de pago".*

[1] https://clientebancario.bde.es/f/webcb/RCL/ProductosServiciosBancarios/ServiciosPago/Memoria2020Identificadorunico.pdf

Y cita una sentencia del TJUE, de 21 de marzo de 2019[2] que se pronunció sobre esta cuestión, de la siguiente manera: *"El artículo 74, apartado 2, de la Directiva 2007/64/CE del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE, debe interpretarse en el sentido de que, cuando una orden de pago se ejecute de acuerdo con el identificador único facilitado por el usuario de servicios de pago y tal identificador no corresponda al nombre del beneficiario indicado por ese mismo usuario, la limitación de la responsabilidad del proveedor de servicios de pago establecida en esta disposición se aplicará tanto al proveedor de servicios de pago del ordenante como al proveedor de servicios de pago del beneficiario"*. Es decir, que la exoneración de responsabilidad que establece el art. 59 LSP beneficiaría tanto a la entidad de servicios de pago del ordenante como a la del beneficiario.

De lo anterior se desprende que no cabe interpretar la norma de otra manera que la no responsabilidad de las entidades de servicios de pago intervinientes en un fraude del CEO, porque la propia norma lo excluye.

También es de interés la recomendación que hace el defensor del pueblo en este sentido, quien recomienda[3] *"Establecer un sistema para que el usuario de servicios de pago al realizar una transferencia pueda comprobar la identidad del beneficiario de la cuenta de forma inequívoca"*. Por tanto, si lo recomienda es porque no existe la obligación para las entidades de comprobar que el beneficiario de la transferencia es quien el ordenante piensa, y no un tercero.

Podemos afirmar según lo anterior, que la diferencia entre ambos tipos de fraude (phishing vs fraude del CEO) es que el primero es un caso de operaciones no autorizadas al que aplica el art. 45 LSP (la entidad de servicios de pago devolverá el importe de la operación no autorizada de forma inmediata), mientras que el segundo es un caso de operación ejecutada con un identificador único incorrecto, al que aplica el art. 59 LSP (la operación se considerará correctamente ejecutada y no dará lugar a responsabilidad de la entidad de servicios de pago).

---

[2] https://curia.europa.eu/juris/document/document.jsf;jsessionid=0FBDAD3C28644AA0C48796925851B89D?text=&docid=212014&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=2249319

[3] https://www.defensordelpueblo.es/resoluciones/establecer-un-sistema-para-que-el-usuario-de-servicios-de-pago-al-realizar-una-transferencia-pueda-comprobar-la-identidad-del-beneficiario-de-la-cuenta-de-forma-inequivoca/

Cuestión distinta será como los tribunales de los diferentes estados miembros irán interpretando y decidiendo, según las circunstancias concurrentes de cada caso.

4.- El problema del fraude del CEO.

Como podemos observar, en los casos del llamado fraude del CEO, en el que una persona se hace pasar por un directivo de la empresa con facultad para aprobar pagos y da una orden de transferencia, o intercepta unas comunicaciones en las que se habla de un pago y modifica el número de cuenta destinataria del pago, parece que no cabe reclamar a las entidades de servicios de pago ni del ordenante ni del beneficiario.

El problema viene dado por el concepto de "identificador único", que la LSP, siguiendo obviamente la Directiva mencionada al inicio de este artículo, define de la siguiente manera en el art. 3.22: *"una combinación de letras, números o signos especificados por el proveedor de servicios de pago al usuario de dichos servicios, que este último debe proporcionar a fin de identificar de forma inequívoca al otro usuario del servicio de pago o la cuenta de pago de ese otro usuario en una operación de pago".* Y sobre el que el art. 59 LSP, que ya hemos comentado, dice que *"Cuando una orden de pago se ejecute de acuerdo con el identificador único, se considerará correctamente ejecutada en relación con el beneficiario especificado en dicho identificador"*.

Podría interpretarse que el identificador único no es sólo el número de cuenta o IBAN (en caso de zona SEPA), sino que es el número más el nombre del beneficiario. El art. 68.2 LSP establece que *"En lo que se refiere a la iniciación de las operaciones de pago electrónico mencionada en el apartado 1, letra b) (operaciones de pago) respecto de las operaciones remotas de pago electrónico, los proveedores de servicios de pago aplicarán una autenticación reforzada de clientes que incluya elementos que asocien dinámicamente la operación a un importe y un beneficiario determinados"*. El problema es la palabra *"clientes"*. ¿Podría entenderse que cliente es tanto el ordenante de una transferencia como un beneficiario? En ese caso, podría argumentarse que la entidad del ordenante o la del beneficiario deberían asegurarse de que el beneficiario indicado en la orden de pago coincide con el beneficiario titular de la cuenta de destino. No obstante, dicha interpretación amplia del término no se ajustaría a la práctica bancaria generalmente admitida ni a normativa o jurisprudencia.

Sin embargo, como ya hemos visto, el propio art. 59 establece que toda la información adicional al identificador único facilitada al realizar la transferencia no afecta a la limitación de responsabilidad de la que gozan las entidades de servicios de pago en estos casos. Y ello viene además corroborado por la Sentencia del TJUE citada con anterioridad y la memoria del Banco de España.

Pero, ¿por qué ocurre esto? ¿No debería ser obligado para las entidades comprobar que el beneficiario indicado por el ordenante de una transferencia coincide con el titular de la cuenta de destino? ¿No impediría esto el fraude del CEO? Suponemos que la respuesta es más de carácter técnico que jurídico, y que si en cada transferencia bancaria la entidad ordenante y la receptora tuvieran que confirmar que el IBAN o número de cuenta coincide con un titular en concreto, haría que la operativa fuera mucho más lenta. Pero también es cierto que las entidades ya se comunican entre sí en cada transferencia, por lo que no parece que debiera ser tan complicado añadir esa comprobación. Así como para identificar al propio cliente existe la autenticación reforzada, parece lógico que una simple comprobación de que la transferencia se realiza a la cuenta de quien dice ser su titular, y no de un tercero, pudiera hacerse sin grandes complicaciones.

En cualquier caso, la realidad es que la literalidad de la norma y la interpretación que se ha hecho precisamente a raíz casos de fraude del CEO, conducen a dificultar o impedir la reclamación contra la entidad de servicios de pago.

5.- Breve referencia a la jurisprudencia sobre el fraude del CEO.

Así como las sentencias sobre phishing son casi en su totalidad condenatorias de la entidad de servicios de pago, debido a la responsabilidad cuasi objetiva que establece la LSP, ocurre todo lo contrario con los casos de fraude del CEO.

No obstante, si analizamos distintas sentencias de audiencias provinciales, podemos observar cómo en función del caso concreto, el que ha sufrido el perjuicio puede tener una puerta abierta a la reclamación, bien sea contra la entidad de servicios de pago, o bien contra la otra empresa a través de la cual el atacante ha podido perpetrar el fraude.

En unos casos, las sentencias consideran que, si una empresa tenía unos procedimientos habituales, incluso en algunos casos pactados con la entidad financiera, ésta debería detectar las órdenes inusuales, bien sea por su importe, bien por el país de destino, o por ambas. En algunos casos se condena a la entidad financiera al pago de todo o parte del fraude sufrido por su cliente a través del fraude del CEO.

En otros casos, alguna sentencia apunta la posible responsabilidad de la empresa a través de la que el atacante o hacker ha interceptado las conversaciones y se ha podido hacer pasar por un empleado, sustituyendo el número de cuenta a la que el perjudicado debía realizar un pago. Cabría en un caso concreto entrar a analizar quién ha sufrido la brecha de seguridad y si eso puede considerarse un comportamiento negligente

causante del daño, o si por el contrario podría ser considerado como una causa de fuerza mayor.

Por tanto, la conclusión que podemos alcanzar es que en los casos de phishing es muy posible recuperar el importe defraudado, porque tanto la normativa como la jurisprudencia son favorables al perjudicado, salvo que la entidad de servicios de pago consiga acreditar que ha existido fraude por parte del ordenante, o negligencia grave en el cumplimiento de sus obligaciones. Sin embargo, en los casos de fraude del CEO, las posibilidades son bastante reducidas, a menos que por las circunstancias del caso concreto sea posible atribuir alguna negligencia en su actuación a un tercero, pero habrá que analizar muy bien cada caso.

Esta publicación no constituye asesoramiento alguno ni y es meramente divulgativo. Para más información o asesoramiento contacten a: info@gimenez-salinas.es