RDMF | REVISTA DE DERECHO DEL MERCADO FINANCIERO

PHISHING

Banco Santander condenado a devolver el importe de la operación de pago a una víctima de phishing

SAP, Madrid, Sección 10, núm. 24/2023, de 13 de enero de 2023, recurso: 918/2022. Ponente: Excma. Dña. Amalia de Santísima Trinidad Sanz Franco

Fraude phishing – Responsabilidad de la entidad bancaria (sinopsis de Fernando Zunzunegui y Mercedes Viudes)

Fraude phishing: "[…] [El día 29 de octubre de 2020 la actora accedió a la banca electrónica del Banco de Santander para realizar una transferencia y, pese a que lo intentó de forma reiterada, no se le remitió la clave de seguridad al móvil para poder hacerla. El día 30 de octubre de 2020 se personó en su sucursal bancaria, expuso a una empleada lo sucedido y se comprobó por ésta que el número de teléfono que les figuraba era el mismo y que no advertía ninguna irregularidad. Por la tarde, la demandante se dio cuenta que el saldo de la cuenta era inferior al que tenía por la mañana, por lo que de forma inmediata se puso en contacto telefónico con la entidad bancaria, informándole que había sido víctima de un fraude, cancelando sus tarjetas de crédito y la banca electrónica. El sábado 31 de octubre de 2020, llama al departamento de fraude del banco y le informan de que aún hay más movimientos irregulares pendientes de cargar en su cuenta y que debía denunciar ante la policía lo sucedido. Envió un correo electrónico a cada una de las oficinas bancarias en las que tiene abierta cuenta advirtiendo de lo sucedido para que no cargasen ninguna cantidad. También presentó denuncia en comisaría. Se le cargaron de forma fraudulenta en su cuenta corriente […] la suma total de 17.350,00 euros. […] **[E]stamos ante un fraude llamado "phishing", por el que se suplanta la identidad de la entidad bancaria para obtener información sobre las claves o credenciales de las cuentas bancarias o tarjetas de crédito/débito. Se envía un correo electrónico con la apariencia de ser remitido por la entidad bancaria, que contiene un enlace a una página que aparenta ser sitio oficial de ésta, pero que en realidad pertenece a un dominio bajo control del phiser.** […]" [Énfasis añadido]

Responsabilidad de la entidad bancaria: "[…] Sobre la jurisprudencia aplicable, la sentencia de la Audiencia Provincial de Madrid, sección 11ª, de fecha 28 de febrero de 2022, hace un compendio de la misma y se menciona la sentencia de la Audiencia Provincial de Madrid (Sección 9ª) núm. 178/2015 de 4 mayo de 2015 (JUR 2015\151311), que se pronuncia en el sentido siguiente: …" Salvo actuación fraudulenta, incumplimiento deliberado o negligencia grave del ordenante (Art.32), la responsabilidad será del proveedor del servicio de pago, lo que supone que a él le corresponde la cargade la prueba de que la orden de pago no se vio afectada por un fallo técnico o cualquier otra deficiencia" (art30). **La responsabilidad contemplada en esta Ley es cuasi-objetiva, es decir, se trata de una responsabilidad de la entidad que presta servicios de pago que sólo permite exonerarse mediante la prueba de la culpa grave del ordenante.** […] La Sentencia de la Audiencia Provincial de Zaragoza de fecha 14 de mayo de 2013 condenó a BARCLAYS BANK

Descargado de http://www.rdmf.es/.

a reintegrar 20.947 € al cliente víctima de phising. La Sentencia señala: "que la Ley de Servicios de Pago expresa con claridad que, salvo una tardanza injustificada del usuario del servicio de banca electrónica en comunicar la irregularidad de las operaciones, será el banco quien deberá devolverle de inmediato el importe de la operación no autorizada y, en su caso, restablecerá la cuenta de pago en que haya adeudado dicho importe al estado que habría existido de no haberse efectuado la operación de pago no autorizada. Por ello y salvo actuación fraudulenta o negligencia grave del titular de la cuenta, la responsabilidad de la operación es del banco al que corresponde además de probar el correcto funcionamiento del sistema informático…" […] La interpretación efectuada por la Juzgadora ad quem de la Ley 16/2009, de 13 de noviembre, de servicios de pago, es acorde no sólo con la literalidad de la norma, sino con el espíritu y finalidad de la misma (ex. art.3 CC), lo que obligó a la determinación de la responsabilidad de la entidad bancaria a pasar de sus afirmaciones sobre la implementación de un modelo seguro de banca online […] **Tampoco sirve de excusa a la entidad apelada la inclusión de avisos en la web y otro medios de la entidad sobre el comportamiento seguro que en el uso de la plataforma había de tener el cliente, sino que la entidad bancaria debe dotar a la banca electrónica de las medidas de seguridad necesarias para prevenir unos tipos de fraude ya muy extendidos y que, como lo prueba el supuesto que nos ocupa, siguen produciéndose por falta de una medida adecuada por las entidades bancarias, que ponen a disposición de sus clientes la banca online y la contratación electrónica como dotados de una seguridad que no garantizan**. […] [N]o podemos calificar la posible negligencia de la demandante en la conservación de sus claves como "grave" en ningún caso. Estamos ante un tipo de fraude muy específico del que es fácil ser víctima, sin que ello implique una actuación negligente del cliente, dado lo bien articulada en su ejecución que está esta modalidad de fraude. […] **Al entender la Sala que la entidad bancaria actuó sin tomar las medidas de diligencia y seguridad exigidas, la consecuencia del incumplimiento es la obligación de devolver de inmediato el importe de la operación, lo que al no efectuarse de inmediato supone un nuevo incumplimiento**. […]. " [Énfasis añadido]

Texto completo de la sentencia

***