RESPONSABILIDAD CUASI OBJETIVA DEL PROVEEDOR DE SERVICIOS DE PAGO POR LAS TRANSFERENCIAS FRAUDULENTAS

SAP Madrid (Secc. 9ª) núm. 178/2015, de 4 de mayo (JUR 2015\151311)

Karolina Lyczkowska
Centro de Estudios de Consumo
Professional Support Lawyer en DLA Piper Spain

Fecha de publicación: 3 de julio de 2015

En esta sentencia se condena a una entidad bancaria a reembolsarle a su cliente el importe de 17 390,35 euros que suman las transferencias realizadas de forma fraudulenta y sin la autorización de la demandante, mediante una técnica conocida como *phishing*.

Phishing es el nombre que recibe una forma de abuso informático que se origina con la suplantación de la identidad del banco por parte del *phisher* con la finalidad de adquirir la información confidencial sobre contraseñas de cuentas bancarias o cualquier otra información que le permita entrar en las cuentas de los usuarios en Internet de banca electrónica. Normalmente, el internauta recibe un correo electrónico a través del cual se le pide que acceda a la página web de la supuesta entidad bancaria para realizar la modificación de sus claves o verificación de las mismas y es cuando la información es captada por el *phisher*.

En el caso enjuiciado, se realizaron una serie de transferencias a través de la Banca electrónica entre los días 21 y 26 de marzo 2010 a favor de destinatarios desconocidos para la demandante. Este hecho fue denunciado por la actora ante el cuartel de guardia civil. En mayo de 2010, la entidad bancaria con la que tuvo la cuenta la actora le mandó una carta en la que se le comunicaba que se había puesto en marcha un nuevo sistema de medidas de seguridad, con la finalidad de reforzar la seguridad de las operaciones. La clienta pide que se le indemnice por la totalidad de las transferencias fraudulentas, pero el banco se niega, aduciendo la supuesta negligencia de la actora.

La sentencia declara no probada la actitud negligente de la demandante, pues sólo queda demostrado que a principios del mes de marzo la actora realizó una transferencia a través de la banca electrónica, facilitando las claves que le fueron pedidas. No queda probado cuántas claves han sido proporcionadas por la actora (la entidad bancaria alega que se han introducido todas las claves de la tarjeta de coordenadas), pero en todo caso, la sentencia entiende que no ha existido conducta negligente pues si la actora realiza una transferencia es lógico que introduzca las claves que le pida el sistema. Además, el sistema de seguridad del banco debió

haber detectado movimientos inusuales, si realmente aquel día se introdujeron todas las posibles claves de la tarjeta de coordenadas. También resulta sorprendente que el sistema de seguridad del banco no haya descubierto como sospechoso que entre los días 21 y 26 de marzo 2010 se estaban realizando tres o cuatro transferencias diarias que incluso superaban los límites internos del banco, cuando en los 14 meses que llevaba siendo la actora la titular de la cuenta tan solo había realizado dos transacciones a través de la banca electrónica. Igualmente, debió haber llamado la atención del sistema que todas las transferencias se hacían a favor de personas con nombres extranjeros inusuales, al seguir el *phisher* la táctica estándar de los destinatarios "muleros". Finalmente, el hecho de que la entidad bancaria haya decidido cambiar las medidas de seguridad de su página web poco después de los sucesos, de lo que informaba a la actora en la carta mencionada, hace posible pensar que los ataques de *phishing* que se produjeron en aquel tiempo se debían a la insuficiencia del sistema propio del banco.

En base a todos estos criterios la sentencia condena a la entidad al reembolso de las cantidades, señalando que la Ley de los Servicios de Pago establece un sistema de responsabilidad cuasi objetiva para la entidad financiera, previendo que en caso de disposiciones fraudulentas el proveedor de servicios de pago deberá devolver de inmediato el importe de la operación no autorizada (art. 31), quedando exento de esta obligación solo en el caso de que la operación no autorizada sea fruto de la actuación fraudulenta del cliente o del incumplimiento, deliberado o por negligencia grave, de una o varias de sus obligaciones (art. 32). Además, la Ley prevé una inversión de la carga de la prueba, en tanto es el proveedor de los servicios quien debe probar que la operación fue debidamente autenticada, cuando el usuario de los servicios lo niegue (art. 30).