Responsabilidad de las entidades financieras en los fraudes informáticos

El Tribunal Supremo en su ultimísima sentencia de 9 de abril de 2.025 ha vuelto a declarar que los proveedores de los servicios de pago, es decir las entidades financieras, responden de los daños y perjuicios ocasionados al cliente cuando no acredita que el servicio se prestó correctamente y la concurrencia de fraude o incumplimiento es deliberado o gravemente negligente por parte del usuario.

Todo ello, porque que un tercero acceda a las claves de acceso a la banca digital del usuario no supone per se que haya incurrido en negligencia alguna, además, notificó al proveedor de servicios de pago la utilización no autorizada del instrumento de pago, tan pronto tuvo conocimiento de ello.

El que la entidad bancaria acredite que la operación fue autenticada, registrada con exactitud y contabilizada, no es suficiente para eximirle de responsabilidad. Tenía que probar que la operación no resultó afectada por un fallo técnico u otra deficiencia del servicio prestado, y, dado que el cliente niega que la operación fuera consentida, que no hubo por parte de este último fraude, incumplimiento deliberado o negligencia grave del usuario bancario.

Esta sentencia vuelve a insistir en la responsabilidad de las entidades financieras frente a las estafas digitales o phishing.

Incidiendo en que las entidades financieras deben reembolsar las cantidades sustraídas mediante fraudes informáticos, salvo que consigan probar que el cliente actuó con negligencia grave o cometió fraude doloso; y el hecho que un tercero acceda a las credenciales del usuario no implica automáticamente una actuación negligente por parte del titular de la cuenta. Y que la filtración o el conocimiento de las claves por el tercero no sea imputable a la entidad bancaria tampoco la libera de obligación de responder ni traslada al usuario la obligación de soportar las pérdidas.

Así, la Sala de lo Civil del Tribunal Supremo expone que la controversia radica en determinar quién debe responder por las operaciones de pago no autorizadas, en tanto que realizadas por un tercero que, utilizando las credenciales del usuario que ha obtenido por cualquier medio, suplanta su identidad y accede electrónicamente a su cuenta sin su consentimiento. O, dicho de otra manera, qué debe entenderse por «operaciones de pago no autorizadas», si, en general, las que han sido realizadas por un tercero sin el consentimiento del usuario titular de la cuenta, o, exclusivamente, las efectuadas sin seguir el procedimiento legal y contractualmente fijado. Resultando probado que las operaciones de pago se ejecutaron por terceras personas, ajenas y sin el consentimiento del demandante, lo que comporta rechazar de plano las dudas sugeridas por la recurrente.

Para responder a la cuestión discutida exige recodar concretar la normativa aplicable; en este caso, la Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior, que derogó la Directiva 2007/64/CE, explica en su Considerando 7 el objetivo de la reforma, y que dice:

«En los últimos años, han aumentado los riesgos de seguridad de los pagos electrónicos, debido a la mayor complejidad técnica de estos, el incesante incremento del volumen de pagos electrónicos en todo el mundo y los nuevos tipos de servicios de pago. Disponer de servicios de pago fiables y seguros es condición esencial para el buen funcionamiento del mercado de servicios de pago, por lo que los usuarios de esos

servicios deben gozar de la debida protección frente a tales riesgos. Los servicios de pago son esenciales para el mantenimiento de actividades económicas y sociales de vital importancia.»
«Considerando 70: Para reducir los riesgos y las consecuencias de operaciones de pago no autorizadas o que hayan sido ejecutadas incorrectamente, el usuario de servicios de pago debe informar al proveedor de servicios de pago, lo antes posible, sobre toda reclamación en relación con operaciones de pago supuestamente no autorizadas o ejecutadas incorrectamente, siempre y cuando el proveedor de servicios de pago haya respetado sus obligaciones de información con arreglo a la presente Directiva. Si el usuario de servicios de pago respeta el plazo de notificación, debe poder hacer valer esas reclamaciones dentro de los plazos de prescripción nacionales. (...).
Considerando 71: En caso de una operación de pago no autorizada, el proveedor de servicios de pago deberá devolver inmediatamente el importe de dicha operación al ordenante. No obstante, cuando haya una sospecha fundada de que una operación no autorizada es el resultado de una conducta fraudulenta del usuario de servicios de pago y la sospecha se funde en motivos objetivos comunicados a la autoridad nacional pertinente, el proveedor de servicios de pago tendrá la posibilidad de efectuar, en un plazo razonable, una investigación antes de devolver el importe al ordenante. (…). Asimismo, una vez que el usuario de servicios de pago haya comunicado al proveedor de servicios de pago que su instrumento de pago puede haber sido objeto de uso fraudulento, no deben exigírsele responsabilidades por las ulteriores pérdidas que pueda ocasionar el uso no autorizado del instrumento. (...).
Considerando 72: A la hora de evaluar la posible negligencia o la negligencia grave del usuario de servicios de pago, deben tomarse en consideración todas las circunstancias. Las pruebas de una presunta negligencia, y el grado de esta, deben evaluarse con arreglo a la normativa nacional. No obstante, si el concepto de negligencia supone un incumplimiento del deber de diligencia, la negligencia grave tiene que significar algo más que la mera negligencia, lo que entraña una conducta caracterizada por un grado significativo de falta de diligencia. Un ejemplo sería el guardar las credenciales usadas para la autorización de una operación de pago junto al instrumento de pago, en un formato abierto y fácilmente detectable para terceros. Se deben considerar nulas las cláusulas contractuales y las condiciones de prestación y utilización de instrumentos de pago mediante las cuales aumente la carga de la prueba sobre el consumidor o se reduzca la carga de la prueba sobre el emisor. Además, en situaciones específicas y, más concretamente, cuando el instrumento de pago no esté presente en el punto de venta, como en el caso de los pagos en línea, resulta oportuno que el proveedor de servicios aporte pruebas de la presunta negligencia, puesto que los medios a disposición del ordenante son limitados en esos casos.»

Además, sigue la directiva exponiendo:

«Considerando 91: Los proveedores de servicios de pago son responsables de las medidas de seguridad. Dichas medidas deben ser proporcionales a los riesgos de seguridad existentes. Los proveedores de servicios de pago deben establecer un marco que permita paliar los riesgos y mantener procedimientos eficaces de gestión de incidentes.
Considerando 96: Es necesario que las credenciales de seguridad personalizadas se utilicen adecuadamente, para limitar los riesgos de captación de datos mediante suplantación de identidad (phising) y otras actividades fraudulentas. A tal fin, el usuario debe poder confiar en la adopción de medidas que protejan la confidencialidad y la integridad de sus credenciales personalizadas de seguridad. Entre estas medidas figuran, en particular, los sistemas de cifrado basados en dispositivos personales del ordenante (lectores de tarjetas o teléfonos móviles, por ejemplo) o facilitados al ordenante por su proveedor de servicios de pago gestor de cuentas por otros cauces (por SMS o mensaje de correo electrónico, por ejemplo). Las medidas, incluidos los

sistemas habituales de cifrado, que pueden dar lugar a códigos de autenticación como las contraseñas de un solo uso, pueden aumentar la seguridad de las operaciones de pago; la utilización de este tipo de códigos de autenticación por los usuarios de servicios de pago debe considerarse compatible con sus obligaciones respecto de los instrumentos de pago y las credenciales de seguridad personalizadas...»

Y la Directiva 2015/2366 ha sido traspuesta por el Real Decreto Ley 19/2018, de 23 de noviembre, de servicios de pago y otras medidas urgentes en materia financiera, cuyos arts. 36 y 41 a 46 reproducen casi miméticamente los preceptos que se acaban de transcribir.

Por todo ello, El usuario de servicios de pago debe adoptar todas las medidas razonables a fin de proteger sus credenciales de seguridad personalizadas y, en caso de extravío, sustracción o apropiación indebida del instrumento de pago o de su utilización no autorizada, ha de notificarlo al proveedor de servicios de pago de manera inmediata, tan pronto tenga conocimiento de ello.

Y en caso de que se produzca una operación de pago no autorizada o ejecutada incorrectamente, si el usuario de servicios de pago se lo comunica sin demora injustificada, el proveedor debe proceder a su rectificación y reintegrar el importe de inmediato, salvo que tenga motivos razonables para sospechar la existencia de fraude y comunique dichos motivos por escrito al Banco de España.

Por lo que cuando un usuario niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, **incumbe al proveedor la carga de demostrar** que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado por el proveedor de servicios de pago. El mero hecho del registro por el proveedor de la utilización del instrumento de pago no bastará, necesariamente, para demostrar que la operación de pago fue autorizada por el ordenante, ni que éste ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave una o varias de sus obligaciones, correspondiendo al proveedor la prueba de que el usuario del servicio de pago cometió fraude o negligencia grave.

En conclusión, la responsabilidad del proveedor de los servicios de pago, en los casos de operaciones no autorizadas o ejecutadas incorrectamente, tiene carácter cuasi objetivo, en el doble sentido de que, primero, notificada la existencia de una operación no autorizada o ejecutada incorrectamente, el proveedor debe responder salvo que acredite la existencia de fraude; y, segundo, cuando el usuario niegue haber autorizado la operación o alegue que ésta se ejecutó incorrectamente, corresponde al proveedor acreditar que la operación de pago fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio, sin que el simple registro de la operación baste para demostrar que fue autorizada ni que el usuario ha actuado de manera fraudulenta o incumplido deliberadamente o por negligencia grave.

Salvo mejor opinión en Derecho.

STS, Sala de lo Civil, sec. 1ª, de 9 de abril de 2025: https://www.poderjudicial.es/search/AN/openDocument/c26766f2870f44cfa0a8778d75e36f0d/20250425