Responsabilidad cuasi objetiva del proveedor de servicios de pago en casos de phishing:

La jurisprudencia española, siguiendo las directrices del TSJUE ha establecido que en los casos de estafa informática "Phishing" la responsabilidad del banco es **cuasi objetiva**, todo ello conforme al artículo 44 de la Ley de Servicios de Pago que impone la carga de la prueba a la entidad financiera para demostrar que la operación fue autorizada o que el usuario actuó con negligencia grave o fraude. Ley que sigue la aplicación de la Directiva PSD2 sobre servicios de pago.

Este criterio viene refrendado por la más reciente **sentencia del Tribunal Supremo, de 9 de abril de 2.025**; la cual establece que con arreglo a la normativa comunitaria y nacional aplicable y a la jurisprudencia comunitaria recaída en interpretación de esta materia se puede concluir que 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.

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.

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.**

Por lo cual 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.

Además, indicando que las operaciones no autorizadas incluyen aquellas que se han iniciado con las claves de usuario y contraseña del usuario -necesarias para acceder al sistema de banca digital- y confirmado mediante la inserción del SMS enviado por el propio sistema al dispositivo móvil facilitado por el usuario, siempre que éste niegue

haberlas autorizado, en cuyo caso el banco deberá 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 que presta.

A este respecto, la mención «deficiencia del servicio» no significa error o fallo del sistema informático o electrónico -posibilidad que estaría prevista en el concepto de «fallo técnico»-, sino que abarca cualquier falta de diligencia o mala praxis en la prestación del servicio, en el entendimiento de que el grado de diligencia exigible al proveedor de los servicios de pago no es el propio del buen padre de familia, sino que la naturaleza de la actividad y los riesgos que entraña el servicio que se presta, sobre todo en una relación empresario/consumidor, obliga a elevar el nivel de diligencia a un plano superior, como es el del ordenado y experto comerciante.

Y las buenas prácticas bancarias pasan por adoptar las medidas de seguridad necesarias para garantizar el correcto funcionamiento del sistema de servicios de pago, entre las cuales destacan las orientadas a detectar de forma automática la concurrencia de indicios de que puede tratarse de una operación anómala y generar una alerta o un bloqueo temporal (reiteración de transferencias sin solución de continuidad, horario en que se producen, importe de las mismas, destinatarios, antecedentes en el uso de la cuenta...), o las dirigidas a incrementar el control y vigilancia cuando se han recibido noticias o alertas de un posible aumento del riesgo.

Siguiendo esta doctrina jurisprudencial la Audiencia Provincial de Asturias, sec. 5ª, de 5 de junio de 2.025, nº 285/2025, rec. 36/2025, declara que la responsabilidad del proveedor de servicios de pago es cuasi objetiva conforme al artículo 44 de la Ley de Servicios de Pago (LSP), que impone la carga de la prueba a la entidad financiera para demostrar que la operación fue autorizada o que el usuario actuó con negligencia grave o fraude; en el caso de una víctima de un fraude informático que resultó en la transferencia no autorizada de 5.701,23 euros desde su cuenta.

La responsabilidad del proveedor de servicios de pago es cuasi objetiva conforme al artículo 44 de la Ley de Servicios de Pago (LSP), que impone la carga de la prueba a la entidad para demostrar que la operación fue autorizada o que el usuario actuó con negligencia grave o fraude; además, la complejidad del phishing y la insuficiencia de las pruebas aportadas por la entidad justifican la condena, en línea con la jurisprudencia y la normativa europea PSD2.

Asimismo, anteriormente ya se seguía dicho criterio; como puede ser las sentencias de la AP de Asturias de 10 de octubre de 2.024, Rollo 308/2024; AP de Almería, Sec. 1ª, de 31 de enero de 2.023, o la AP Coruña de 5 de octubre de 2.023. Como la AP de Navarra de 9 de marzo de 2.023. Incidiendo que no resulta suficiente, por sí solo, haber completado los mecanismos reforzados de autenticación establecidos por la entidad, debido a que si no se han implementado otros sistemas para restringir sólo al usuario el acceso al canal de banca electrónica que autentifica, no puede descansar automáticamente toda la responsabilidad en dicho usuario, dado que al proveedor del servicio de pago le compete la responsabilidad respecto del buen funcionamiento y la seguridad del mismo y es obligación esencial de las entidades prestadoras del servicio el dotarse de medidas suficientes que garanticen al usuario la seguridad de las operaciones por lo que, en el supuesto de insuficiencia o mal funcionamiento de las adoptadas, deben ser las entidades bancarias las que asuman las consecuencias derivadas de los fallos de seguridad del sistema.

Salvo mejor opinión en Derecho.