

RECIENTE SENTENCIA DEL TRIBUNAL SUPREMO EN RELACIÓN CON LA NORMATIVA COMUNITARIA Y NACIONAL EN MATERIA DE SERVICIOS DE PAGO EN SUPUESTOS DE ESTAFA “SIM PHISHING”

El “SIM PHISHING”, también conocido como “SIM SWAPPING” o fraude por duplicado de SIM, es una modalidad de fraude cibernético consistente en la duplicación o clonación de la tarjeta SIM de un usuario legítimo, suplantando así su identidad ante la operadora de telefonía correspondiente y logrando acceder a servicios y cuentas bancarias de aquél, aprovechando los códigos de verificación que se remiten vía SMS.

La reciente Sentencia 571/2025, de 9 de abril de 2025, dictada por el Tribunal Supremo, Sala de lo Civil (Rec. 1151/2023), aborda la normativa comunitaria y nacional en materia de servicios de pago, adentrándose en el análisis de la delimitación de las obligaciones tanto del usuario -en particular, la notificación sin demora tan pronto tenga conocimiento de la utilización no autorizada del instrumento de pago- como del proveedor de servicios de pago.

En tal sentido, la citada Sentencia viene a establecer un régimen de responsabilidad cuasi objetiva del proveedor de servicios de pago en supuestos de estafas “SIM PHISHING”.

Así, se determina que cuando un usuario (cliente) niegue haber autorizado una operación de pago ya ejecutada o alegue que ésta se ejecutó de manera incorrecta, recae sobre el proveedor de servicios de pago la carga de probar que la operación fue autenticada, registrada con exactitud y contabilizada, y que no se vio afectada por un fallo técnico u otra deficiencia del servicio prestado.

El Alto Tribunal sostiene asimismo que el mero hecho del registro no basta para acreditar 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 sus obligaciones, extremo cuya prueba corresponde al proveedor.

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 bien entendido 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.

Además, la meritada resolución dispone que las buenas prácticas 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, etc.), y las dirigidas a incrementar el control y vigilancia cuando se han recibido noticias o alertas de un posible aumento del riesgo.

Bores y Cía
Abogados

Tlf.: 954 933 782 | Fax: 954 412 279

Avda. de la Palmera, nº 28 B - Ático, Edif. Patricio, 41012 - Sevilla

<http://bores-abogados.com>

