JUS

Uso fraudulento de los instrumentos de pago en la normativa italiana y europea

Gianfranco Liace

Recibido: 13 de octubre de 2025 / Aceptado: 14 de octubre de 2025 / Publicado: 9 de enero de 2026
Sección: Artículos

Resumen: El presente artículo analiza el uso fraudulento de los instrumentos de pago en el contexto de la digitalización de los servicios financieros, abordando fenómenos como el *phishing, smishing, vishing, spoofing*, *man in the middle* y el fraude *sim swap*. Su objetivo es examinar la evolución de estas prácticas y las respuestas normativas y jurisprudenciales, particularmente en relación con la carga de la prueba, la responsabilidad de bancos y usuarios, y la eficacia de medidas como la autenticación fuerte y el servicio de *SMS-Alert*. Entre los principales hallazgos se destaca que la jurisprudencia tiende a exigir a los proveedores de servicios de pago una diligencia técnica elevada para prevenir fraudes, mientras que en ciertos casos se reconoce la responsabilidad exclusiva del usuario por negligencia grave. El trabajo concluye que la lucha contra el fraude requiere un equilibrio entre protección al consumidor y seguridad jurídica para las instituciones financieras. La originalidad del artículo radica en ofrecer una visión integral de los perfiles civiles, contractuales y penales, contribuyendo al debate sobre la responsabilidad compartida en el ecosistema digital de pagos.

Palabras clave: Fraude informático, instrumentos de pago, *phishing*, responsabilidad bancaria, autenticación fuerte.

Summary: This article analyzes the fraudulent use of payment instruments within the digitalization of financial services, focusing on practices such as phishing, smishing, vishing, spoofing, *man in the middle* attacks, and *SIM swap* fraud. Its objective is to examine the evolution of these schemes and the regulatory and case-law responses, particularly regarding the burden of proof, the liability of banks and users, and the effectiveness of tools such as strong customer authentication and SMS-Alert services. Findings show that

JUS DERECHO SOCIEDAD ESTADO, nueva época, núm. 22, julio-diciembre, 2025, es una publicación electrónica semestral editada por la Universidad Juárez del Estado de Durango (UJED) con domicilio en Constitución, núm. 404, colonia Centro, C.P. 34000, Durango, Durango, teléfono 618-827-1295, página web: http://jus.ujed.mx, editorialujed@ujed.mx. Editor responsable: Martín Gallardo García. Reserva de Derechos al Uso Exclusivo número: 04-2024-011809451300-102, ISSN: 2594-4033, otorgados por el Instituto Nacional del Derecho de Autor. Responsable de la actualización de este número: Oficina Editorial Universitaria, Constitución, núm. 404, colonia Centro, C.P. 34000, Durango, Durango. Responsable de la última actualización: Manuel Rojas Villarreal. Fecha de última modificación, 9 de enero de 2026.

case law increasingly requires payment service providers to exercise high technical diligence to prevent fraud, while in certain circumstances users are held exclusively liable due to gross negligence. The study concludes that combating fraud demands a balance between consumer protection and legal certainty for financial institutions. The originality of this contribution lies in providing a comprehensive view of civil, contractual, and criminal aspects, offering added value to the ongoing debate on shared liability in the digital payment ecosystem.

Keywords: Cyber fraud, payment instruments, phishing, banking liability, strong authentication.

1. Introducción

El presente trabajo aborda el fenómeno del uso fraudulento de los instrumentos de pago desde la perspectiva de la normativa vigente en Italia. Los sistemas de pago en Europa están regulados por una normativa común impulsada por la Unión Europea cuyo objetivo es armonizar los distintos regímenes y mecanismos de regulación de los países miembros.

No obstante, este estudio se enfoca en el caso italiano, analizando su estructura jurídica, los tipos de fraude más frecuentes y las medidas adoptadas para su prevención y sanción. Esta precisión resulta esencial para comprender el alcance territorial y normativo del análisis, así como su relevancia dentro del marco europeo.

El Informe Anual del Árbitro Bancario y Financiero publicado el 6 de julio de 2023 señala:

> La digitalización de los servicios e instrumentos de pago está cambiando el tamaño, la forma, la frecuencia y el impacto de los usos fraudulentos: según un estudio realizado a nivel mundial, entre 2019 y 2021, los ataques fraudulentos en línea crecieron a un ritmo mucho mayor que las transacciones en línea regulares (233 y 65%, respectivamente). Las estadísticas más recientes publicadas por el Banco de Italia confirman la creciente popularidad en Italia de los servicios e instrumentos de pago digitales entre el público, tanto en términos de unidades como de valor de las transacciones. Al igual que en otros países, el uso de efectivo disminuyó aún más durante la crisis pandémica. Esta tendencia se reflejó en la composición de los litigios presentados a la ABF: en el período 2017-2022, el número de reclamaciones relacionadas con el uso fraudulento de instrumentos de pago aumentó en más de 130 puntos porcentuales.

La actividad desarrollada por los intermediarios, en la medida en que también está relacionada con el tratamiento informático de datos personales,[1] debe considerarse peligrosa debido a los fraudes informáticos cada vez más frecuentes (el llamado *phishing*) destinados a obtener fraudulentamente dichos datos para realizar transacciones ilícitas, en su mayoría dirigidas a acceder a los datos personales del titular de la cuenta para transferir sumas de su cuenta corriente a la de un tercero.[2]

También hay que señalar que el uso creciente de instrumentos de pago como las tarjetas de crédito y débito expone a sus usuarios a un uso fraudulento por parte de terceros. A este respecto, cabe señalar que el fraude con tarjetas puede ser de dos tipos diferentes: el *skimming*, que consiste en una técnica delictiva por la que, gracias al uso de un *skimmer* (dispositivo de lectura y almacenamiento del contenido presente en las bandas magnéticas de las tarjetas electrónicas), el defraudador se apodera de los datos de la tarjeta de pago, incluido el código PIN (en el caso de los cajeros automáticos o de las tarjetas de crédito multifunción). El *skimming* identifica las estafas basadas en la clonación de tarjetas de crédito, débito, etc. El *phishing*, por su parte, es una técnica de fraude en línea por la que, mediante el envío de correos electrónicos falsos muy similares a los enviados por las entidades emisoras o sitios de comercio electrónico conocidos, el estafador obtiene el número de tarjeta de crédito, el código PIN y los datos personales del titular de la tarjeta. El *phishing* identifica principalmente las estafas basadas en transacciones en línea no autorizadas por el titular de la tarjeta.

La jurisprudencia, de forma concurrente, ha precisado que, en el cumplimiento de las obligaciones inherentes al ejercicio de una actividad profesional, la diligencia debe apreciarse atendiendo a la naturaleza de la actividad ejercida, conforme al artículo 1176, co. 2, del Código Civil. En particular, en la relación contractual de *home banking*, el banco tiene la condición de contratista cualificado, que, no ajeno a los métodos de fraude mediante *phishing* largamente conocidos en el sector, está obligado a adaptarse a la evolución de los nuevos sistemas de seguridad.[3]

La extensión del fenómeno es tal que los Colegios ABF sostienen desde hace tiempo que el uso de una diligencia media es suficiente para conjurar

1 Liace, Fiorucci, *Conto corrente. Contratti bancari*, in *Commentario Scialoja-Branca-De Nova*, Bologna, 2025, p. 396.

2 Trib. Rovigo, 10 de julio de 2023.

3 Trib. Milano, 4 de diciembre de 2014.

el peligro y prevenir el fraude. En particular, la Junta de Coordinación ha distinguido:[4]

1. Las hipótesis de *phishing* tradicional caracterizado por el envío de un simple mensaje de correo electrónico, telefónico (el llamado *vishing*) o SMS (el llamado *smishing*) invitando al cliente a teclear sus credenciales de acceso; muchos de los intentos de fraude llevados a cabo en el ámbito de los servicios de pago tienen lugar según este esquema típico y ampliamente conocido, consistente en inducir al titular del instrumento, según el caso por teléfono, correo electrónico, mensaje de texto u otras herramientas de comunicación, a comunicar o introducir sus credenciales personalizadas en dispositivos o plataformas informáticas, normalmente alegando falsamente la existencia de intentos de acceso abusivos o, más en general, la oportunidad de verificar o implementar elementos de seguridad;
2. La forma más insidiosa, consistente en un enrevesado mecanismo de agresión [que] tiene lugar a través de un sofisticado método de intrusión caracterizado por un efecto sorpresa capaz de desplazar al usuario, gracias a la perfecta inserción en el entorno informático original y a la correlativa simulación de un mensaje que a cualquiera sólo podría parecer auténtico.

2. La carga de la prueba

El artículo 10, apartado 1, del Decreto Legislativo n.º 11, de 27 de enero de 2010, establece que, en caso de impugnación de una operación de pago por el usuario de servicios de pago, incumbe al proveedor de servicios de pago demostrar que la operación fue autenticada, registrada y contabilizada correctamente, y que no se vio afectada por el mal funcionamiento de los procedimientos necesarios para su ejecución o por otras disfunciones.[5]

4 Decisiones n. 3498/2012 y 1820/2013.

5 La jurisprudencia de mérito ha destacado que en materia de responsabilidad del banco por operaciones en cuenta corriente realizadas mediante instrumentos electrónicos, en caso de que el titular de la cuenta niegue haber autorizado la operación de pago, es carga del intermediario probar tanto la inexistencia de disfunciones en el sistema, como la autenticación, el correcto registro y contabilización de las operaciones desautorizadas; también es carga del intermediario probar cualquier otro hecho susceptible de integrar la negligencia grave del usuario. En su defecto, el banco soporta todas las consecuencias de las operaciones desautorizadas, sin limitación ni exención alguna. En este sentido véase Trib. Biella, 10 julio 2024; Ciraolo, *Pagamento fraudolento con carta di credito e ripartizione della responsabilità.*

Por lo tanto, basta con que el usuario reniegue de una transacción fraudulenta para que el proveedor de servicios de pago soporte esta carga penetrante de probar la autenticación fuerte del cliente (llamada "autenticación fuerte del cliente" *Strong Customer Authentication,* SCA), mediante un procedimiento que permite validar la identificación de un usuario basándose en el uso de dos o más elementos de autenticación (llamada "autenticación de dos factores"), pertenecientes al menos a dos de las siguientes categorías: 1) elemento de conocimiento (un quid que sólo el usuario conoce, como, por ejemplo una contraseña o un PIN); 2) elemento de posesión (algo que sólo el usuario posee, como un token/llave, o un *smartphone*); 3) elemento de inherencia (algo que caracteriza al usuario, como el reconocimiento facial o una huella dactilar). El incumplimiento de este deber conduce, de forma inmediata y directa, al establecimiento del derecho del cliente a ser reembolsado por el intermediario de los daños derivados de la operación de pago fraudulenta, con independencia del grado de culpabilidad en que éste haya podido incurrir; todo ello, podría decirse, en aplicación de una suerte de responsabilidad objetiva por el siniestro.

Cabe señalar, no obstante, que el citado art. 10.1 no se aplica cuando no pueda decirse que la operación de pago ha sido desautorizada, que es el caso cuando la misma operación ha sido ejecutada directa o personalmente por el cliente del banco. Cuando es ejecutada íntegramente por el ordenante (con introducción de la instrucción de pago y todos los factores de autenticación), de hecho, la operación debe considerarse autorizada y no está sujeta al régimen de responsabilidad previsto en la DSP2, es decir, en la Directiva (UE) 2015/2366 sobre servicios de pago en el mercado interior.

Esto incluye las operaciones realizadas por el ordenante siguiendo las instrucciones del defraudador, sin conocimiento de haber concertado una operación, lo que ocurre, por ejemplo, en las denominadas operaciones "al dictado".[6]

En tales casos, de hecho, no puede decirse que la transacción haya sido desautorizada de conformidad con el artículo 5 del Decreto Legislativo n.º 11/2010 porque el demandante era consciente de que la estaba realizando, incluso si fue inducido fraudulentamente a hacerlo.

Dagli orientamenti attuali alla revisione della PSD, in *Dir. banc. merc. fin*., 2017, p. 150 ss.; Cirelli, *Utilizzo non autorizzato dello strumento di pagamento e responsabilità della banca*, in *Giur. comm*., 2022, p. 438 ss.

6 ABF Collegio di Roma, decisión n. 10302/2024.

Prosiguiendo, el párrafo segundo del artículo 10 del Decreto Legislativo n.º 11/2010 especifica que:

> cuando el usuario de servicios de pago niega haber autorizado una operación de pago ejecutada, la utilización de un instrumento de pago registrado por el proveedor de servicios de pago [...] no basta necesariamente por sí sola para demostrar que la operación fue autorizada por el usuario de servicios de pago, ni que el usuario de servicios de pago actuó de forma fraudulenta o incumplió con dolo o negligencia grave una o varias de las obligaciones establecidas en el artículo 7.[7]

La Junta de Coordinación, en su resolución n.º 22745/19, precisó que la disposición del artículo 10, apartado 2, del Decreto Legislativo n.º 11/2010 en relación con la carga que recae sobre el PSP de probar el dolo, la culpa o la negligencia grave del usuario, debe interpretarse en el sentido de que la aportación de documentos dirigidos a probar la autenticidad y la regularidad formal de la operación impugnada no satisface, por sí sola, la carga de la prueba, ya que es necesario que el intermediario aporte específicamente la indicación de una serie de elementos fácticos que caractericen la forma en que se realizó la operación de los que pueda deducirse la prueba de la negligencia grave del usuario.

La misma norma, por lo tanto, subraya que sigue correspondiendo al proveedor de servicios de pago probar el fraude, la conducta dolosa o la negligencia grave del usuario de servicios de pago en el cumplimiento de sus obligaciones. El usuario de servicios de pago está obligado a utilizar el instrumento de pago de conformidad con las condiciones, establecidas en el contrato marco que rigen su emisión y utilización. Además, el titular del instrumento de pago está obligado a custodiar cuidadosamente las credenciales y contraseñas de acceso y a no revelarlas a nadie. Asimismo, está obligado a notificar al proveedor de servicios de pago o a la persona designada por éste la pérdida, robo, apropiación indebida o uso no autorizado del instrumento en cuanto tenga conocimiento de ello.

Según la orientación de la ABF, el hecho de que el usuario no presente los registros, por ejemplo adjuntando la captura de pantalla, del mensaje falso o de la llamada telefónica recibida del autodenominado operador del proveedor de servicios de pago, da lugar al rechazo de la reclamación, ya que este incumplimiento no permite verificar si el remitente puede ser rastrea-

7 Decreto Legislativo n. 11/2010.

do hasta el proveedor de servicios de pago y si, por lo tanto, el cliente podía haber tenido expectativas legítimas en cuanto a la autenticidad del mensaje/contacto telefónico.[8] Si el proveedor de servicios de pago desea invocar la responsabilidad exclusiva del usuario de servicios de pago, deberá aportar también pruebas de fraude, dolo o negligencia grave por parte del usuario de servicios de pago.

De hecho, las decisiones de la ABF señalan que: "en materia de uso no autorizado de instrumentos de pago, frente a la desautorización de operaciones de pago por parte del usuario víctima de un fraude según las modalidades denominadas *phishing/smishing*, recae sobre el proveedor de servicios de pago la carga de probar que la operación fue autenticada, correctamente registrada y contabilizada de conformidad con el artículo 10, apartado 1, del Decreto Legislativo nº 11/2010".[9]

La ABE con su "Dictamen" de 21 de junio de 2019 ha reforzado los cumplimientos exigidos a efectos de una SCA, asumiendo por un lado que los datos impresos en la tarjeta de pago no constituyen un elemento de posesión y ni siquiera un elemento de conocimiento a efectos de la SCA, y por otro que ni siquiera el código OTP es en sí mismo un elemento de conocimiento suficiente. Por este motivo, la autenticación basada en datos facilitados por el usuario al defraudador, incluso de forma imprudente, ya no puede considerarse un procedimiento seguro para autorizar la transacción, en ausencia de otros elementos de naturaleza dinámica. A este respecto, la ABE, con Q&A ID 2020_5516, aclaró que, a efectos de autenticar una transacción, es posible que los PSP *reutilicen*, dentro de la misma sesión, un elemento utilizado para acceder a la cuenta de pago.

3. Los diferentes tipos de utilización fraudulenta de los sistemas de pago

La evolución tecnológica ha propiciado el desarrollo de nuevos y cada vez más sofisticados sistemas de utilización fraudulenta de los instrumentos de pago, por lo que resulta especialmente difícil elaborar un historial exhaustivo.

Una de las formas más agresivas de fraude es la denominada *man in the middle* (MITB), que es una forma de ciberataque en la que los delincuentes, aprovechando la debilidad de los protocolos basados en la web, se intro-

8 ABF Collegio di Milano, decisión n. 1447/2024.
9 ABF Collegio di Bologna, decisión n. 23858/2021.

ducen entre las entidades de un canal de comunicación para robar datos. Existe una definición legal de MITB, que ha sido facilitada por la ABF. La Junta de Coordinación ha señalado que:

> En su máxima expresión de eficacia agresiva, el programa malicioso, una vez que ha anidado en un cierto número de ordenadores, genera lo que en la jerga se denomina una botnet, es decir, precisamente una red de máquinas igualmente infectadas por el mismo virus. El malware –que se remonta a la categoría más amplia de los llamados troyanos ("caballos de Troya") y está dotado de sofisticadas capacidades para burlar el mejor software antivirus– merodea silenciosamente en el ordenador de la víctima sin crear disfunciones ni alteraciones del sistema que llamen la atención del usuario. El malware permanece completamente "en reposo", activándose sólo cuando el usuario se conecta a un sitio financiero de los que son objetivo del programa (bancos objetivo). En ese preciso momento, el malware se "despierta" y entra en acción, capturando la conexión del usuario y proponiéndole una página de vídeo exactamente idéntica a la que el usuario está acostumbrado a reconocer cuando accede regularmente al sitio de su intermediario.[10]

En el MITB, como se ha ilustrado anteriormente, existe un sofisticado método de intrusión en el ordenador del usuario estafado caracterizado por un efecto sorpresa capaz de desconcertarlo gracias a la perfecta inserción en el entorno informático original y a la correlativa simulación de un mensaje que a cualquiera sólo podría parecer auténtico, dado que la única diferencia radica en las siglas del protocolo de transferencia, identificado como un http normal y no como un https protegido (donde la 's' final significa *secured*, protegido). Es evidente que la citada variación normalmente escapa a la atención de cualquiera que se acerque a una página de la red, y más que nada, es inadvertida por quien accede a un sitio bancario para realizar una operación.

Distinta es la posición del Colegio ABF de Bolonia que, con independencia del caso de que se trate, *phishing* o MITB, considera que cuando la operación está correctamente autorizada y autenticada, existe responsabilidad del titular del instrumento de pago.[11] En concreto, el mismo colegiado precisa que la conducta gravemente negligente del cliente se evidencia cuando el acceso al home *banking* se produce introduciendo correctamente las credenciales de acceso, el código de usuario y el código PIN, además del código OTP generado por el *token* en posesión exclusiva del cliente. El acceso

10 ABF Collegio di Coordinamento, decisión n. 34983/2012.
11 ABF Collegio di Bologna, decisión n. 23847/2019.

a los contenidos del home *banking*, por tanto, está asegurado por un sistema de autenticación fuerte, es decir, por la introducción de un código dinámico "desechable" en posesión exclusiva del solicitante.

La ABF considera que existe responsabilidad del intermediario cuando éste no adopta todas las medidas de seguridad adecuadas para impedir las hipótesis de *spoofing*, por ejemplo, cuando el cliente ha recibido el mensaje fraudulento que ha entrado en el historial de comunicaciones del servicio del intermediario, en el mismo chat.[12]

Sin embargo, la ABF, de forma razonable, ha considerado la existencia de una prueba de la falta grave del demandante, en la hipótesis de que, a pesar de que el mensaje fraudulento haya sido incluido en el historial de conversaciones auténticas con el intermediario, el mismo mensaje presentare indicios de falta de fiabilidad o anomalías (por ejemplo, la invitación a seleccionar un enlace no referible al intermediario, la presencia de errores gramaticales, etc.) que deberían haber alertado al usuario prudente.[13]

El *spoofing* es una forma de agresión informática que consiste en alterar los datos del remitente de un mensaje de texto para que parezca proceder de una persona distinta, sustituyendo el número original por un texto alfanumérico que pueda ser rastreado hasta el utilizado por el intermediario para sus mensajes auténticos. El *smishing*, por su parte, es una forma de *phishing* que utiliza el teléfono móvil como forma de ataque y se realiza a través de mensajes de texto o SMS. El *vishing*, por su parte, se produce cuando la llamada telefónica realizada por el falso operador parece referirse a una cuenta bancaria, normalmente también al llamado número gratuito del banco. La palabra *vishing* procede de la combinación de los términos *voice* (voz) y *phishing* (suplantación de identidad). Se trata de llamadas telefónicas realizadas con el fin de obtener información personal o financiera o códigos de seguridad.

A este respecto, cabe señalar que la ABF considera que: "las operaciones impugnadas fueron el resultado de un fenómeno de *vishing* realizado en perjuicio del cliente, utilizando el método de *spoofing* (aplicado al número gratuito del intermediario). La difusión del fenómeno es tal que los Colegios ABF sostienen desde hace tiempo que el uso de una diligencia media es suficiente para conjurar el peligro y prevenir el fraude".[14]

12 ABF Collegio di Milano, decisión n. 15621/2021.
13 ABF Collegio di Bologna, decisión n. 4485/2023.
14 ABF Collegio di Torino, decisión n. 2129/2021.

4. El caso del fraude SIM swap y la posición de la jurisprudencia

El SIM swap es un tipo de fraude informático que consiste en apoderarse del número de teléfono móvil del titular desprevenido para acceder a una serie de servicios e informaciones vinculadas a la SIM.

Sobre este tema, existe un contraste entre las decisiones de la ABF y la jurisprudencia de mérito. Según la ABF, en los casos de fraude SIM swap, las solicitudes del titular del instrumento de pago son –por lo general– dignas de plena aceptación,[15] ya que la sustitución de la tarjeta SIM debe equipararse a la falta de autenticación de la operación de pago en virtud y a los efectos del artículo 10 del Decreto Legislativo 11/2010. La sustitución de la tarjeta SIM, aunque referible a un tercero (la compañía telefónica), entra dentro del riesgo típico de la actividad empresarial del intermediario, que hace uso de una modalidad de autenticación (SMS, OTP) confiando en parte el procedimiento de autenticación a un tercero.[16]

Como se ha dicho, una parte de la jurisprudencia ha adoptado, en cambio, una posición diferente de la de la ABF, centrándose, en particular, de manera compartible, en el análisis de la conducta del operador telefónico.[17] Según los jueces de mérito, en estos casos en particular, antes de proceder al duplicado de la tarjeta SIM solicitada por el infractor, la compañía telefónica debería haber verificado la identidad del solicitante, así como la autenticidad y fiabilidad de la denuncia de siniestro presentada a tal efecto. Sólo la ausencia de los mencionados cumplimientos permitió a los malhechores obtener las credenciales dinámicas necesarias para llevar a cabo la operación ilícita.

El Tribunal de Nápoles Norte señaló que: considerando las características estructurales del fraude Sim swap y la específica circunstancia de que, no obstante la posesión de las credenciales estáticas (usuario y contraseña), el fraude no podría haberse perfeccionado si los terceros no hubieran logrado intervenir la cuenta telefónica certificada, inutilizándola y desviando a su favor el envío de las credenciales dinámicas OTP y OTS mediante la sustitución de la SIM.[18]

La citada jurisprudencia ha constatado, por tanto, una responsabilidad exclusiva del operador telefónico, por haber realizado una verificación sólo superficial y negligente de la identidad de la persona que solicitaba la

15 ABF Collegio di Milano, decisión n. 6758/2021.
16 ABF Collegio di Milano, decisión n. 2190/2024.
17 Trib. Roma, 20 de julio de 2023.
18 Trib. Napoli Nord, 30 diciembre 2024.

sustitución; verificación que fue, por tanto, la causa previa a la posterior ejecución de la operación fraudulenta.[19]

5. La activación de la notificación SMS-Alert

En el caso de operaciones efectuadas mediante *home banking*, es responsabilidad del banco verificar la trazabilidad de dichas operaciones a la voluntad del cliente, utilizando para ello la diligencia del *bonus argentarius*, de modo que la posible utilización por terceros de las claves de acceso al sistema entra dentro del riesgo profesional del prestador de servicios de pago, que puede ser previsto y evitado mediante la adopción de medidas técnicas adecuadas dirigidas a verificar la trazabilidad de las citadas operaciones a la voluntad del titular de la cuenta. En este orden de cosas, el banco solo no es responsable del perjuicio sufrido por el cliente si prueba que el hecho es imputable a una conducta dolosa del titular o a una conducta tan temeraria que no podía preverse de antemano.[20]

La jurisprudencia de legitimación ha señalado reiteradamente que no puede omitirse la comprobación de que la entidad bancaria ha adoptado las medidas oportunas para garantizar la seguridad del servicio; de hecho, la diligencia impuesta al profesional es de carácter técnico y debe valorarse teniendo en cuenta los riesgos típicos del ámbito profesional de referencia y, por tanto, tomando como parámetro la figura del banquero prudente.[21]

Por ello, a propósito de la responsabilidad del banco en el caso de operaciones realizadas mediante instrumentos electrónicos –también para garantizar la confianza de los usuarios en la seguridad del sistema– se considera razonable introducir en el ámbito del riesgo profesional del prestador de servicios de pago, previsible y evitable con medidas adecuadas dirigidas a verificar la trazabilidad de las operaciones a la voluntad del cliente, la posibilidad de que terceros utilicen las claves de acceso al sistema, no imputable a la intencionalidad del titular o a una conducta tan temeraria que no pueda ser atajada de antemano.

En virtud de esta premisa, es necesario, llegados a este punto, verificar cuál es la función del SMS-Alerta. La función que cumple el mensaje es ciertamente protectora, constituyendo una salvaguarda para la transparencia, la concienciación y la seguridad de los pagos. En particular, en el contexto

19 App. Genova, 12 de junio de 2024; App. Genova, 13 de diciembre de 2024; App. Genova, 12 de febrero de 2025.

20 App. Firenze, 8 de septiembre de 2022.

21 Cass., 3 de febrero de 2017, n. 2950.

de fraudes como los denominados hacking social y perpetrados no gracias a un fallo del sistema informático del intermediario, sino mediante la manipulación psicológica del cliente, el SMS-Alert puede inducir al titular del servicio de pago a darse cuenta de la verdadera naturaleza de la transacción que está realizando materialmente, para ponerle fin.

En particular, la Junta de Coordinación de la ABF afirmó el principio de que: "Incluso en el caso de que se descarte la clonación del instrumento de pago, el hecho de que el intermediario no demuestre la activación del servicio de alerta por SMS constituye un incumplimiento de la correcta ejecución de las obligaciones que le incumben".[22]

Por lo tanto, la activación del instrumento de Alerta SMS forma parte de las obligaciones del proveedor de servicios de pago. La no activación de este servicio constituye en cualquier caso una deficiencia organizativa imputable al intermediario, que sólo es excusable cuando el cliente emite una renuncia expresa a hacer uso del mismo. Del mismo modo, debe considerarse que el intermediario no es responsable del perjuicio sufrido por el cliente bancario como consecuencia de una operación de pago no autorizada, que fue correctamente autenticada, aprobada y contabilizada[23] siempre que, habida cuenta del contexto temporal en el que se cometió el fraude (por ejemplo transferencia instantánea fraudulenta, ejecutada inmediatamente antes o después de la alerta SMS) o de otro modo (por ejemplo, robo o indisponibilidad del dispositivo en el que se entregó el SMS), el mensaje de alerta no podría haberlo evitado en ningún caso. En estos casos, de hecho, no habría relación causal entre la falta de envío del SMS y la comisión del fraude.

6. La responsabilidad del titular del instrumento de pago

En el caso del *phishing* tradicional, la falta de precaución del usuario es difícilmente excusable, ya que se trata de fenómenos ampliamente conocidos, que cualquier usuario dotado de una previsión y prudencia normales –como se cree que son las personas habituadas al uso del *home banking*– debe ser capaz de detectar, no dejándose engañar. Por lo tanto, en la hipótesis del *phishing* tradicional, el cliente es víctima de una credulidad culpable, ya que se le induce a comunicar sus credenciales de autenticación fuera del circuito operativo del intermediario.[24]

22 ABF Collegio di Coordinamento, decisión n. 8672/2024.

23 Artículo 10, apartado 1, del Decreto Legislativo n. 11/2010.

24 Semeraro, *Modelli di responsabilità e private enforcement: appunti su PSD2 e operazioni di pagamento non autorizzate*, in *Riv. dir. banc.*, 2022, p. 825.

Además, la jurisprudencia ha demostrado que:

> En el caso de fraude informático mediante *phishing*, si el titular de la cuenta facilita imprudentemente a los defraudadores sus credenciales de acceso (identificador y contraseña), la responsabilidad por los daños patrimoniales consiguientes (como transferencias no autorizadas) no puede atribuirse al banco, que ha adoptado sistemas de seguridad y campañas de información adecuados. La conducta imprudente del titular de la cuenta rompe el nexo causal entre la posible actividad peligrosa de la entidad y el daño sufrido, excluyendo así la responsabilidad del banco en virtud del artículo 2050 del Código Civil.[25]

De nuevo, la ABF reconoce la negligencia grave del usuario en el caso de robo del monedero dejado en el interior del coche aunque estuviera cerrado con llave, ya que la circunstancia denotaría también una falta de diligencia en la custodia del instrumento de pago.[26] Asimismo, la brevedad del lapso de tiempo transcurrido entre la sustracción y la retirada y el uso de la tarjeta sustraída sugieren que el código PIN se guardó junto con la tarjeta de pago y que, por tanto, el autor se apoderó de ambos.[27]

También se incurre en responsabilidad si el titular del instrumento de pago introduce sus códigos personales (que se le solicitan en un correo electrónico fraudulento), lo que permite al defraudador desconocido utilizarlos posteriormente para efectuar una orden de transferencia desde la cuenta del perjudicado.[28]

También es concebible la responsabilidad del titular del instrumento de pago cuando la transacción se realiza al dictado. Sobre este punto, las decisiones de la ABF son particularmente interesantes. El citado organismo de resolución alternativa de litigios ha precisado que: "la recarga fue realizada por la propia actora, por tanto, no puede ser objeto de restitución por haber sido realizada 'voluntariamente' por la propia actora en el cajero de la demandada, siguiendo todas las instrucciones del defraudador. Además, en el presente caso, la transacción no puede considerarse no autorizada, ya que fue realizada personalmente por la demandante, por lo que no se dan las condiciones previstas por la citada normativa para la devolución del importe a favor de la misma".[29]

25 Trib. Parma, 7 de noviembre de 2024, n. 1415.
26 ABF Collegio di Milano, decisión n. 4921/2024.
27 ABF Collegio di Roma, decisión n. 3966/2024.
28 Cass., 13 de marzo de 2023, n. 7214.
29 ABF Collegio di Napoli, decisión n. 1683/2022.

La ABF opina, por tanto, que el demandante incurrió en negligencia grave en la custodia de los códigos de acceso, circunstancia que conlleva la responsabilidad del usuario con arreglo al artículo 12, apartado 3, del Decreto Legislativo n.º 11/2010, y no permite acceder a la solicitud de reembolso de las sumas indebidamente malversadas.[30]

Los pagos efectuados íntegramente por el titular del instrumento de pago no entran, según la consolidada orientación de la ABF, en el ámbito de la responsabilidad objetiva del proveedor de servicios de pago por operaciones no autorizadas por los clientes: un supuesto que, como subrayó el Tribunal de Justicia en su sentencia de 2 de septiembre de 2021, asunto C-337/20, se rige exclusivamente por el Decreto Legislativo n.º 11/2010.

7. El envío de la tarjeta de pago. La denominada técnica del encajonamiento

Otro perfil de la responsabilidad del intermediario lo constituye el envío de la tarjeta por servicio postal ordinario. Según la orientación de los Colegios ABF, la responsabilidad del intermediario existe cuando la apropiación indebida del instrumento de pago se produce mediante la denominada técnica del *boxing* (apropiación ilícita de la tarjeta por un tercero en la fase de entrega al cliente), probablemente como resultado de la denominada ingeniería social.[31] En estos casos, la asignación del riesgo del envío del instrumento de pago depende de una disposición reglamentaria específica, a saber, el artículo 8, apartado 2, del Decreto Legislativo n.º 11/2010, según el cual los riesgos derivados del envío de un instrumento de pago o de las correspondientes credenciales de seguridad personalizadas corren a cargo del proveedor de servicios de pago.

8. Perfiles de derecho penal. Resumen

Constituye delito de blanqueo de capitales la conducta de quien, sin haber participado en el delito subyacente, pone a disposición su propia cuenta bancaria para obstaculizar el origen delictivo de las sumas obtenidas por otros de la actividad ilícita de suplantación de identidad y, por tanto, de la comisión del delito de fraude informático, al permitir el abono en su propia cuenta[32] de las sumas indebidamente obtenidas.

30 Cass. 26 de noviembre de 2020, n. 26916.
31 ABF Collegio di Bologna, decisión n. 1918/2023.
32 Cass. Penale, 2 de diciembre de 2022, n. 6395.

A falta de otras pruebas circunstanciales, la mera titularidad de la tarjeta de pago receptora del abono ilícito no es suficiente para acreditar la responsabilidad penal respecto del delito de estafa informática, siendo necesario averiguar si el citado titular fue el responsable del envío del correo electrónico o mensaje de texto que contenía el enlace que posibilitó la intrusión abusiva en el sistema informático.

La jurisprudencia en la materia ha subrayado que: "El mero abono en la propia cuenta corriente y la consiguiente retirada de dinero procedente de reintegros y transferencias online no autorizadas (*phishing*), aunque se realicen por terceros, sólo es constitutivo del delito de blanqueo de capitales; para lo cual, a efectos del elemento subjetivo, basta con que exista una posible intencionalidad, es decir, la aceptación del riesgo de que las cantidades tengan un origen delictivo".[33]

El delito se consuma no en el momento del hecho informático, sino cuando el agente obtiene la disponibilidad *electrónica* de sumas incluso sin cobrarlas materialmente, sino sólo haciendo que se abonen en su cuenta corriente. La jurisprudencia de legitimación tiende a anticipar el momento de la consumación en la fase de la intervención sin derecho: el delito de estafa informática se consuma cuando el agente interviene sobre los datos del sistema informático de forma que modifica su funcionamiento respecto del que era posible anteriormente, no siendo necesaria una alteración real de los programas insertados en el servidor.[34] También se ha sostenido jurisprudencialmente que constituye estafa la conducta de *phishing* consistente en pescar, mediante la entrada no autorizada en el sistema informático de una entidad financiera o mediante falsos correos electrónicos dirigidos a los clientes de los intermediarios, los datos significativos de las relaciones de cuentas corrientes mantenidas por los intermediarios.[35]

La S.C. sostiene que: "El delito de blanqueo de capitales no es concurrente con el de fraude informático realizado mediante el denominado *phishing*, es decir, el envío de correos electrónicos con el logotipo falsificado de una entidad de crédito o de una empresa de comercio electrónico mediante los cuales se invita al destinatario a facilitar datos bancarios confidenciales".[36]

33 App. Ancona, 23 de febrero de 2021, n. 1607.
34 Cass. penale, 19 de febrero de 2015, n. 32383.
35 Trib. Monza, 7 de mayo de 2009.
36 Cass. penale, 9 febrero 2017, n. 10067

Sumario

Bibliografía

ABF Collegio di Bologna, decisión n. 23858/2021.

ABF Collegio di Bologna, decisión n. 1918/2023.

ABF Collegio di Bologna, decisión n. 23847/2019.

ABF Collegio di Bologna, decisión n. 4485/2023.

ABF Collegio di Coordinamento, decisión n. 8672/2024.

ABF Collegio di Coordinamento, decisión n. 34983/2012.

ABF Collegio di Milano, decisión n. 1447/2024.

ABF Collegio di Milano, decisión n. 15621/2021.

ABF Collegio di Milano, decisión n. 2190/2024.

ABF Collegio di Milano, decisión n. 4921/2024.

ABF Collegio di Milano, decisión n. 6758/2021.

ABF Collegio di Napoli, decisión n. 1683/2022.

ABF Collegio di Roma, decisión n. 10302/2024.

ABF Collegio di Roma, decisión n. 3966/2024.

ABF Collegio di Torino, decisión n. 2129/2021.

App. Ancona, 23 de febrero de 2021, n. 1607.

App. Firenze, 8 de septiembre de 2022.

App. Genova, 12 de junio de 2024; App. Genova, 13 de diciembre de 2024; App. Genova, 12 de febrero de 2025.

Artículo 10, apartado 1, del Decreto Legislativo n. 11/2010.

Cass. 26 de noviembre de 2020, n. 26916.

Cass. penale, 19 de febrero de 2015, n. 32383.

Cass. Penale, 2 de diciembre de 2022, n. 6395.

Cass. penale, 9 febrero 2017, n. 10067.

Cass., 13 de marzo de 2023, n. 7214.

Cass., 3 de febrero de 2017, n. 2950.

Ciraolo, *Pagamento fraudolento con carta di credito e ripartizione della responsabilità. Dagli orientamenti attuali alla revisione della PSD*, en *Dir. banc. merc. fin.*, 2017.

Cirelli, *Utilizzo non autorizzato dello strumento di pagamento e responsabilità della banca*, en *Giur. comm.*, 2022.

Decisiones n. 3498/2012 y 1820/2013.

Decreto Legislativo n. 11/2010.

Liace, Fiorucci, *Conto corrente. Contratti bancari*, in *Commentario Scialoja-Branca-De Nova*, Bologna, 2025.

Semeraro, *Modelli di responsabilità e private enforcement: appunti su PSD2 e operazioni di pagamento non autorizzate*, in *Riv. dir. banc.*, 2022.

Trib. Biella, 10 julio 2024.

Trib. Milano, 4 de diciembre de 2014.

Trib. Monza, 7 de mayo de 2009.

Trib. Napoli Nord, 30 de diciembre 2024.

Trib. Parma, 7 de noviembre de 2024, n. 1415.

Trib. Roma, 20 de julio de 2023.

Trib. Rovigo, 10 julio de 2023.

Sobre el autor

Gianfranco Liace. Universitá degli Studi di Salerno, Italia. https://orcid.org/0000-0001-6459-9970 *gliace@unisa.it*