

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) AFFERNI

Seduta del 24/02/2026

FATTO

Il ricorrente espone di essere stato vittima, in data 08/08/2025, di una truffa perpetrata con la tecnica dello “spoofing” e del “vishing”. In particolare, riferisce di aver ricevuto alle ore 14:40 un SMS, apparentemente proveniente dall’intermediario convenuto, che lo allertava circa un’operazione sospetta, invitandolo a contattare un numero di telefono fisso per le necessarie verifiche. Il ricorrente, fidandosi della genuinità della comunicazione, contattava il numero indicato e parlava con un sedicente operatore della banca, il quale, con fare rassicurante e professionale, lo informava di un tentativo di frode in corso e della necessità di procedere al blocco delle sue carte. Durante la conversazione telefonica, durata circa un’ora, il ricorrente, su istruzione del truffatore, compiva una serie di azioni che portavano all’installazione di un nuovo Mobile Token e alla successiva autorizzazione di quattro operazioni di pagamento da lui non volute, per un importo totale di € 6.571,50. Solo in un secondo momento, insospettitosi, il ricorrente scopriva che il numero contattato era associato ad attività truffaldine e constatava gli addebiti sul proprio conto. A sostegno della propria domanda, il ricorrente ha prodotto la documentazione relativa agli SMS ricevuti, la denuncia-querela sporta presso le competenti Autorità, il reclamo inviato all’intermediario e la relativa risposta, nonché l’estratto conto con l’evidenza delle operazioni contestate. Chiede quindi la condanna dell’intermediario convenuto alla restituzione della somma complessiva di € 6.571,50, oltre interessi, indebitamente sottrattagli a seguito di una frode informatica.

L’intermediario si è costituito in giudizio, chiedendo il rigetto del ricorso. Nelle proprie controdeduzioni, la banca resistente ha affermato la piena regolarità delle transazioni, eseguite nel rispetto delle

procedure di autenticazione forte del cliente (SCA) previste dalla normativa, e ha prodotto i log informatici a comprova dell'avvenuta autenticazione da parte del cliente. L'intermediario ha quindi eccepito la colpa grave del cliente, sostenendo che le operazioni sono state rese possibili da una condotta gravemente negligente di quest'ultimo. In particolare, l'intermediario ha evidenziato come il ricorrente abbia contattato di sua iniziativa un numero di telefono non ufficiale ricevuto via SMS e, soprattutto, abbia seguito le istruzioni del truffatore, fornendo di fatto le autorizzazioni necessarie per l'installazione di un nuovo dispositivo di sicurezza (Mobile Token) e per l'esecuzione delle successive operazioni.

Nelle proprie repliche, il ricorrente ha insistito per l'accoglimento della domanda, ribadendo la natura particolarmente sofisticata della frode, tale da ingenerare un legittimo affidamento sulla genuinità delle comunicazioni ricevute.

DIRITTO

Il Collegio ritiene che il ricorso sia infondato e debba essere respinto.

La materia del contendere è disciplinata dal D.Lgs. 27 gennaio 2010, n. 11 e successive modifiche, che ha recepito nell'ordinamento nazionale la Direttiva (UE) 2015/2366 (c.d. PSD2) in materia di servizi di pagamento.

Ai sensi dell'art. 10 del citato decreto legislativo, grava sul prestatore di servizi di pagamento (PSP) l'onere di provare che l'operazione di pagamento contestata sia stata autenticata, correttamente registrata e contabilizzata. Qualora il PSP assolva a tale onere, spetta poi a quest'ultimo dimostrare che l'utente abbia agito con dolo o colpa grave per essere esonerato dall'obbligo di rimborso, ai sensi del successivo art. 12.

Nel caso di specie, l'intermediario resistente ha fornito la prova, attraverso la produzione dei log informatici, che le operazioni contestate sono state regolarmente autenticate mediante un sistema di autenticazione forte del cliente (SCA). Dalla documentazione prodotta emerge infatti che le disposizioni sono state autorizzate tramite l'utilizzo di credenziali personali e codici OTP generati dal Mobile Token, la cui installazione su un nuovo dispositivo è stata a sua volta autorizzata dal cliente stesso nel corso della conversazione telefonica con il truffatore. L'intermediario ha quindi assolto alla prima parte dell'onere probatorio su di esso incombente.

Occorre, pertanto, valutare se la condotta del ricorrente integri la fattispecie della colpa grave. Secondo il consolidato orientamento di questo Arbitro, la colpa grave si sostanzia in una condotta connotata da una straordinaria e inescusabile imprudenza e negligenza, che si discosta in modo macroscopico dalle normali regole di prudenza che ogni utente di servizi di pagamento è tenuto ad osservare.

Nel caso in esame, il comportamento tenuto dal ricorrente integra pienamente tale fattispecie. Sebbene la tecnica dello "spoofing" (l'inserimento del messaggio fraudolento nella cronologia dei messaggi autentici della banca) possa essere considerata insidiosa, essa non può giustificare la successiva condotta del cliente. Il ricorrente, infatti, ha compiuto due azioni che costituiscono una palese violazione delle più elementari norme di diligenza: in primo luogo, ha contattato di propria iniziativa un numero di telefono sconosciuto e non ufficiale, ricevuto tramite un SMS di allarme; in secondo luogo, e in modo ancor più determinante, nel corso della telefonata ha seguito pedissequamente le istruzioni del sedicente operatore, comunicando codici personali e autorizzando, di fatto, l'attivazione di un nuovo strumento di sicurezza su un dispositivo terzo. Tale condotta ha permesso al truffatore di acquisire il pieno controllo del conto del ricorrente.

Il cliente, ricevendo notifiche e richieste di autorizzazione per operazioni che non stava compiendo, avrebbe dovuto immediatamente insospettirsi e interrompere ogni comunicazione, contattando la banca attraverso i canali ufficiali e universalmente noti. La comunicazione di credenziali personali, codici di sicurezza o l'approvazione di operazioni su istruzione di terzi tramite telefono rappresentano una condotta talmente avventata da non poter essere scusata, neppure a fronte di tecniche di

ingegneria sociale particolarmente raffinate. L'affidamento riposto in un interlocutore telefonico sconosciuto, che chiede di compiere operazioni così delicate, costituisce una macroscopica e inescusabile violazione degli obblighi di custodia e uso esclusivo delle proprie credenziali di sicurezza. La catena causale che ha portato al danno, dunque, non è stata innescata da una falla nei sistemi di sicurezza dell'intermediario, bensì è stata interrotta e deviata dalla condotta gravemente colposa del ricorrente, il quale, con le sue azioni, ha reso possibile la frode. Di conseguenza, ai sensi dell'art. 12, comma 3, del D.Lgs. n. 11/2010, l'intermediario è esonerato da qualsiasi obbligo di rimborso. Per le ragioni esposte, il ricorso deve essere integralmente respinto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE