

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) SCANNELLA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore ANTONIO FORGIONE

Seduta del 31/03/2026

FATTO

Parte ricorrente espone di aver subito una frode informatica attuata mediante tecniche di *spoofing*, *vishing* e *social engineering*. In dettaglio, la parte riferisce di aver ricevuto un SMS, apparentemente inserito nella messaggistica ufficiale dell'intermediario presso cui intrattiene un conto corrente di corrispondenza, recante l'avviso di un pagamento in uscita verso un noto portale per la prenotazione *on line* di viaggi, con l'indicazione di due utenze da contattare per il relativo disconoscimento. Pur avendo verificato l'assenza di tale addebito sul proprio conto, l'istante contattava uno dei recapiti indicati. Nella conseguente conversazione, un sedicente operatore prospettava l'esistenza di finte disposizioni anomale in corso e, simulando la necessità di bloccarle, la ricontattava mascherando la propria utenza con il numero verde ufficiale della banca. Rassicurato da tale circostanza e dal fatto che l'interlocutore disponeva di informazioni bancarie riservate sul proprio conto, il ricorrente acconsentiva a confermare otto bonifici istantanei. La parte deduce che tali operazioni sarebbero state materialmente compilate dal truffatore all'interno dell'*home banking*, senza che quest'ultimo le avesse mai richiesto la comunicazione delle credenziali, essendosi il ricorrente limitato alla sola autorizzazione. Avvedutosi del raggirio e contattata la vera assistenza clienti, il ricorrente chiede il rimborso delle somme sottratte, deducendo l'inadeguatezza dei sistemi antifrode e l'omessa attivazione di *alert* informativi da parte della banca.

Costituendosi nel procedimento, l'intermediario chiede il rigetto della domanda imputando l'accaduto alla colpa grave del cliente. Deduce in fatto che i messaggi fraudolenti non si sono affatto inseriti nella

Nelle proprie controrepliche, l'intermediario si riporta integralmente alle difese già articolate, ribadendo che l'evento dannoso è riconducibile in via esclusiva alla condotta gravemente imprudente del ricorrente. Quest'ultimo, difatti, pur a fronte di reiterate campagne informative aziendali in cui si ribadisce che la banca non richiede mai i codici di sicurezza, ha attivamente e volontariamente autorizzato i pagamenti seguendo le indicazioni telefoniche di terzi, rendendo tecnicamente ineccepibili le operazioni contestate.

Passando all'esame della condotta del ricorrente, va osservato che il messaggio fraudolento che ha dato inizio alla truffa non si è incanalato all'interno della conversazione genuina precedentemente intrattenuta con l'intermediario. Dalle evidenze in atti emerge, infatti, che il nome della banca figura unicamente nel corpo del messaggio e non quale identificativo del mittente. Tale circostanza esclude che ci si trovi dinanzi a una sofisticata alterazione del mittente (c.d. *spoofing*), ed al contempo evidenzia

che la frode è stata realizzata mediante la tecnica dello *smishing*, ossia una pratica inidonea a superare la normale diligenza esigibile dall'utente dei servizi di pagamento elettronici.

Va inoltre rilevato che la parte ricorrente, in sede di repliche, deduce di non aver materialmente inserito i dati delle operazioni dispositive, ammettendo di aver autorizzato transazioni già precompilate dai frodatori.

Sotto il profilo degli obblighi informativi, va rilevato che l'intermediario ha documentato l'invio, all'utenza del ricorrente, dei messaggi necessari per autorizzare le singole transazioni. Poiché tali comunicazioni recavano i codici OTP integrati con i dati essenziali dei pagamenti, trova applicazione il consolidato orientamento arbitrale secondo cui, a fronte di messaggi che illustrano tipo, importo e destinatario dell'operazione, risulta del tutto ininfluyente l'attivazione o meno di notifiche meramente successive o *alert ex post* (Collegio ABF Palermo n. 13859/22 e n. 5893/23; Collegio ABF Torino n. 1344/23).

In ordine alla conformità ai presidi di sicurezza, giova in primo luogo richiamare la cornice normativa e regolamentare della materia. In particolare, la disciplina nazionale sulla prevenzione delle frodi inerenti alle carte di pagamento, introdotta dalla legge 166/05 e dettagliata dal D.M. attuativo 112/07, tipizza le anomalie che determinano l'insorgenza di tale rischio, individuandole, tra l'altro, nell'esecuzione di sette o più richieste di autorizzazione nelle 24 ore. Ove si realizzi tali ipotesi, al pari di una qualunque delle altre individuate nella disciplina, l'articolo 9 impone ai PSP un rigoroso obbligo di monitoraggio dell'operatività. A tal riguardo, le evidenze in atti fanno emergere il configurarsi di tale anomalia, che non è stata rilevata dall'intermediario. Le otto operazioni dispositive contestate sono state disposte, infatti, con una sequenza temporale eccezionalmente ravvicinata. Nello specifico, i pagamenti si sono concentrati in un arco temporale di appena dodici minuti, integrando un inequivocabile indicatore di frode che non è stato intercettato e cautelativamente bloccato dai sistemi di sicurezza dell'intermediario. Tutto ciò determina, in conformità all'orientamento arbitrale, l'obbligo di restituire al ricorrente una somma, equitativamente determinata nel venti per cento di tutte le operazioni contestate (in senso conforme, si veda collegio ABF Palermo, decisione 4148/24).

PER QUESTI MOTIVI

In parziale accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 1.920,00.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE