COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore MODICA

Seduta del 27/05/2025

FATTO

Il cliente disconosce tre operazioni eseguite a valle di una truffa. In particolare, afferma che il proprio padre, che disponeva della carta, ha ricevuto un'e-mail in data 18.1.2025, apparentemente proveniente da una piattaforma di intrattenimento televisivo, con la quale si chiedeva un aggiornamento dei dati di pagamento; ha inserito i dati della carta tratto in inganno dalla circostanza che avrebbe dovuto effettivamente aggiornare i dati di pagamento di alcuni servizi. Ravvisato l'addebito in conto corrente di n. 3 pagamenti fraudolenti di € 434,18 ciascuno per totali € 1.402,54, il ricorrente ha contattato il numero verde della propria banca per chiedere il blocco dello strumento di pagamento. Chiede il rimborso di € 1.402,54

L'intermediario controdeduce che le operazioni contestate sono state correttamente contabilizzate, registrate e autenticate tramite SCA; che i pagamenti sono stati autorizzati con l'elemento biometrico rilevato dal device abilitato su cui la banca inviava le notifiche push relative alle singole operazioni; che l'utilizzatore versa in colpa grave in quanto le transazioni sono da ricondurre ad un banale phising; che, inoltre, lo stesso utilizzatore ha ammesso di non aver verificato con attenzione l'e-mail ricevuta. Rileva poi che dalla denuncia allegata emerge chiaramente che ad utilizzare la carta fosse il padre del ricorrente, il quale pertanto è venuto meno all'obbligo di garantire la sicurezza dello strumento di pagamento.

Chiede il rigetto del ricorso.
In sede di repliche, il cliente rileva che la circostanza che un familiare fosse autorizzato a usare la carta per determinati pagamenti non ha alcuna rilevanza rispetto alla natura fraudolenta della transazione oggetto del presente ricorso; che la truffa è stata perpetrata con una metodologia altamente ingannevole; che il sistema di autenticazione forte (Strong Customer Authentication - SCA), previsto dalla PSD2, non sembra essere stato adeguatamente applicato in questa circostanza. Insiste per l'accoglimento del ricorso.
In sede di controrepliche, l'intermediario afferma che la truffa di cui è stato vittima il ricorrente è ormai particolarmente diffusa e nota e, nel caso di specie, non è stata perpetrata tramite una tecnica sofisticata in quanto il mittente del messaggio e la presenza del link nel testo del messaggio avrebbero dovuto porre un cliente dotato di normale avvedutezza e prudenza in condizioni di non subire l'inganno. Ribadisce di aver fornito evidenza dei due fattori utilizzati per autorizzare le operazioni. Insiste per il rigetto del ricorso.

DIRITTO

Le operazioni contestate, tre pagamenti pos eseguiti alle ore 14:28, 14;29 e 14:30 del 18 gennaio 2025 per l'importo complessivo di 1.302,54 €, ricadono sotto il raggio d'azione del D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).
Ai sensi dell'art. 10, comma 1, del d.lgs. n. 11/2010, "Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti". L'assolvimento di tale onere è necessario ma non sufficiente, dovendo il prestatore ulteriormente provare, ai fini dell'esonero da responsabilità (art. 10, comma 2, d. lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 d. lgs. 11/2010: come chiarito dal Collegio di Coordinamento, "la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente" (decisione n. 22745/2019).
Il Collegio, richiamati gli artt. 97 e 98 della PDS2, l'articolo 10 bis del D. Lgs. 11/2010, le norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare il parere dell'EBA del 21 giugno 2019), richiama altresì l'art. 12 del d.lgs. 27.1.2010, n. 11, "Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento": "Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Il Collegio, ancora, ricorda che, in base all'art. 1, lett. qbis, l'"autenticazione forte del cliente" è definita come "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza

l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione". L'autenticazione forte è richiesta quando il cliente accede al suo conto di pagamento online; dispone un'operazione di pagamento elettronico; effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

Nel caso di specie, l'intermediario ha provato intanto che l'attivazione dell'elemento biometrico sul device è avvenuta molti mesi prima della truffa e quindi presumibilmente effettuata dalla stessa parte ricorrente. Soprattutto, le evidenze prodotte fanno emergere che le operazioni sono state confermata tramite device (codice utente del cliente IB**198); la presenza della notifica push inviata al dispositivo; la presenza della conferma della operazione mediante dato biometrico ("codice 02"), dell'autenticazione del titolare ("Y"); dell'esito dell'autenticazione ("ok autenticated"). Dunque, le operazioni risultano correttamente autorizzate mediante il ricorso a un elemento di possesso (il dispositivo) e a un elemento di inerenza (il dato biometrico).

Del pari provata appare la colpa grave dell'utilizzatore dello strumento di pagamento. Nella vicenda in esame non rileva, ai fini del giudizio sulla gravità della colpa, la circostanza che il ricorrente abbia affidato lo strumento di pagamento a un proprio prossimo congiunto; piuttosto, dalla documentazione prodotta risulta che il padre del ricorrente abbia ricevuto una mail (in data 18.1.2025) ritenendo che provenisse da una piattaforma di intrattenimento televisivo, nella quale veniva chiesto un aggiornamento dei dati di pagamento. Senonché, per un verso, l'indirizzo mail dal quale proviene la mail, seppur riporta la denominazione della società, non risulta ad essa riferibile; per altro verso, lo stesso utilizzatore riferisce di avere abbassato la soglia di attenzione perché in effetti di lì a poco avrebbe dovuto veramente aggiornare i dati di pagamento di alcuni servizi in quanto aveva recentemente cambiato carta. Dalle evidenze in atti emerge chiaramente come la vicenda descritta sia ascrivibile al "phishing", una truffa attuata secondo uno schema ricorrente e noto, consistente nell'indurre il titolare dello strumento, tramite e-mail, a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o, più genericamente, l'opportunità di verificare o implementare caratteristiche di sicurezza. La diffusione del fenomeno, le modalità piuttosto rudimentali con cui prende corpo e le reiterate campagne di sensibilizzazione poste in essere dagli intermediari sono tali da far ritenere che l'utilizzatore sia caduto vittima di una truffa banale, cui facilmente avrebbe potuto sottrarsi con l'impiego di una media diligenza. Come rilevato dal Collegio di Coordinamento (decisione n. 1820/13), nell'ipotesi del "phishing", "il cliente è vittima di una colpevole credulità: colpevole in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di internet".

La provata colpa grave del cliente non esclude naturalmente che il Collegio, tenuto conto delle peculiarità della fattispecie e delle modalità con le quali si è realizzata la truffa, possa individuare altri e diversi eventuali profili di responsabilità, per esempio sul versante del rispetto degli obblighi di protezione che gravano, per diritto comune, sul *bonus argentarius*, anche sub specie di mancata prevenzione o gestione di indici di anomalia o frode; profili che, nel caso di specie, non ricorrono. Risultano eseguite infatti n. 3 operazioni con la medesima carta di debito nell'arco temporale di 3 minuti circa, tutte aventi medesimo importo (€ 434,18) presso lo stesso esercente on line; risultano altresì due successive operazioni, eseguite rispettivamente alle ore 14.31 e 14.39 non andate a buon fine: segno

che l'intermediario si è tempestivamente attivato appena concretizzatosi l'indice di cui al punto 2, lett. a), art. 8, D.M. 112/2007.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TINA