

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) GIGLIOTTI	Membro designato dalla Banca d'Italia
(NA) NERVI	Membro di designazione rappresentativa degli intermediari
(NA) SORRENTINO	Membro di designazione rappresentativa dei clienti

Relatore FULVIO GIGLIOTTI

Seduta del 31/03/2026

FATTO

1. Con ricorso del 29.11.2025 – previo reclamo (del 3.11.2025), riscontrato negativamente dall'intermediario resistente – la ricorrente, dopo aver premesso di essere titolare di un rapporto di c/c intrattenuto presso l'intermediario resistente, ha esposto di aver ricevuto, in data 30.10.2025, un messaggio sms che la avvisava di una autorizzazione per un pagamento di euro 1.275,00 a favore di un sito di prenotazioni viaggi, ed indicava un numero di telefono da contattare nel caso di disconoscimento di predetta operazione.

Non avendo disposto una tale operazione e volendo disconoscerla, contattava il numero indicato, al quale rispondeva un operatore che la rassicurava, dicendole di aver bloccato tale pagamento; successivamente, volendo ulteriori rassicurazioni sull'effettivo blocco dell'operazione, contattava la filiale presso la quale intratteneva il conto corrente, e in tale occasione la avvisavano che, invece, risultava essere stato da lei compiuto un bonifico, a favore di una persona a lei ignota, dell'importo di euro 1.690,00.

Ritenendo che l'intermediario non abbia adottato le misure di sicurezza idonee ad evitare possibili frodi, ha quindi proposto il reclamo e, poi, il ricorso introduttivo della procedura davanti all'Arbitro, chiedendo il rimborso della somma ad essa addebitata, e il risarcimento del danno.

2. Si è costituito l'intermediario, rilevando la ricostruzione parziale ed approssimativa dell'accaduto da parte della ricorrente, che non ha prodotto evidenze del messaggio sms che afferma di aver ricevuto (richiamando anche, al riguardo, precedenti decisioni ABF che affermano la presunzione di colpa grave del cliente, qualora l'utente non circostanzi adeguatamente l'utilizzo fraudolento).

Parte resistente ha anche evidenziato che i numeri telefonici indicati da parte ricorrente in sede di denuncia non hanno alcun collegamento con l'intermediario, elemento che evidenzia la negligenza della cliente (che avrebbe dovuto insospettirsi sulla genuinità del messaggio ricevuto).

In ogni caso, poi, ha osservato che l'originario *enrollment* della *app* al *device* della ricorrente è stato effettuato in data 22.05.2023, oltre due anni prima dell'operazione contestata, e che da allora non si è verificato alcun cambiamento di *device*; l'operazione oggetto di ricorso infine, è stata compiuta con regolare procedura di SCA, dopo un accesso *web* al conto *on line*, effettuato con l'inserimento di *user-id* e *password* ed autorizzato tramite *app* con inserimento del PIN dispositivo; lo stesso PIN dispositivo, inserito tramite *app*, è servito per autorizzare il bonifico poi sconosciuto.

Ritenendo, quindi, di aver agito del tutto correttamente, e stigmatizzando la condotta gravemente colposa della ricorrente, ha concluso per il rigetto del ricorso.

DIRITTO

3. Ritiene il Collegio, per le ragioni di seguito illustrate, che il ricorso non possa essere accolto.

4. L'operazione contestata è stata posta in essere sotto il vigore del D.lgs. 27 gennaio 2010, n. 11, come modificato dal D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366, relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13 gennaio 2018; le fonti normative che, nel contesto considerato, regolano la c.d. "autenticazione forte" (in gergo, individuata dall'acronimo SCA: *strong customer authentication*) sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10-bis del D. lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA (*European Banking Authority*) 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, parere del 21 giugno 2019).

Secondo le previsioni normative sopra richiamate, riferibili alla fattispecie, la responsabilità di un Prestatore dei servizi di pagamento (PSP) è esclusa quando, *avendo esso dato prova di utilizzare meccanismi di "autenticazione forte" dell'utente*, sia anche riuscito a dimostrare una condotta dolosa o gravemente colposa dell'utente del servizio (con la precisazione che si intende per "autenticazione forte" 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).

Più in particolare, quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7 D. lgs. n. 11/2010.

Piuttosto, sarà onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente: in mancanza di ciò, egli sarà tenuto responsabile dei pregiudizi subiti dall'utente, in ragione del rischio d'impresa sopportato.

5. Ne consegue che l'intermediario non si libera dalla responsabilità provando la mera regolarità formale delle transazioni, dovendo lo stesso, ai sensi dell'art. 10 del D. lgs. n. 11/2010, documentare elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, anche in via presuntiva, della colpa grave (o del dolo) dell'utente (cfr. Collegio di Coordinamento ABF, n. 22745 del 10 ottobre 2019).

In proposito, è orientamento condiviso dai Collegi quello secondo il quale occorre distinguere, anzitutto, la truffa più insidiosa dello *spoofing* (con contraffazione dell'Id di provenienza degli SMS e delle

chiamate), dal caso del semplice *phishing/vishing/smishing*, in cui i numeri telefonici o i messaggi non sono riconducibili all'intermediario e "*il cliente è vittima di una colpevole credulità*" (cfr. Collegio di Coordinamento, n. 3498/2012) ed è quindi solitamente tenuto a sopportare – per colpa grave – tutte le perdite derivanti da operazioni di pagamento non autorizzate.

Con specifico riguardo a tale tipologia di truffe, inoltre, i Collegi hanno unanimemente concluso che la mancata allegazione, da parte del cliente, del messaggio civetta determina il rigetto del ricorso, in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario (con conseguente impossibilità di fondare un legittimo affidamento dell'utente circa la genuinità del messaggio).

6. Quanto sopra premesso, rileva il Collegio che, nel caso di specie (per quanto documentato in atti):

- l'associazione della carta della ricorrente al sistema autorizzativo di tipo dinamico, sul dispositivo della cliente (*enrollment*) è avvenuta nel maggio 2023, in modo regolare, e non è mai stato effettuato alcun cambio;

- l'operazione dispositiva è stata effettuata dopo accesso al sito *web*, avvenuto con l'inserimento della *user-id* e convalidata mediante *push notification* sul *device* con inserimento del PIN dispositivo (come attestato dalle evidenze prodotte dall'intermediario);

- la ricorrente ha riferito, in sede di denuncia, di aver ricevuto un messaggio sms, da un numero non riferibile all'intermediario, contenente un numero di telefono non evidentemente riferibile all'intermediario, che provvedeva a contattare;

- parte ricorrente, tuttavia, non ha prodotto alcuna evidenza del citato sms (messaggio civetta) e del suo contenuto; inoltre, il contatto telefonico indicato in denuncia dalla stessa ricorrente non corrisponde a numeri riconducibili all'intermediario resistente;

- non risulta alcuna evidenza di sms *alert*, ma, trattandosi di operazione unica, si tratta di circostanza priva di rilievo;

- è stato anche chiesto un risarcimento del danno, ma senza alcuna evidenza né dell'*an* che del *quantum* del medesimo.

7. In ragione di quanto precede, osserva il Collegio che mentre risulta attestato il rispetto della procedura di SCA richiesta (tanto per l'originaria fase di *enrollment* che per l'operazione dispositiva disconosciuta), parte ricorrente non ha allegato alcuna evidenza del preteso messaggio fraudolento che ha innescato la frode; e, inoltre, il numero di telefono dalla stessa contattato, quale emergente dalla denuncia da essa presentata, non è riconducibile all'intermediario resistente.

8. Per quanto emerso in atti, dunque, deve concludersi che ricorre una condotta gravemente colposa della ricorrente, ancorché essa sia rimasta ingenuamente vittima di una truffa evidente, rispetto alla quale, peraltro, neppure risulta possibile valutare specificamente né il livello reale di insidiosità (essendo rimasto privo di ogni dimostrazione il contenuto del messaggio civetta; e risultando, comunque, dalla stessa denuncia della ricorrente, il colpevole "abboccamento" della stessa); né potenziali profili di colpa concorrente dell'intermediario resistente.

Ne segue, a giudizio del Collegio, che il ricorso non merita accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE