

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) GIGLIOTTI	Membro designato dalla Banca d'Italia
(NA) COCCIOLI	Membro designato dalla Banca d'Italia
(NA) MIOLA	Membro di designazione rappresentativa degli intermediari
(NA) VERDICCHIO	Membro di designazione rappresentativa dei clienti

Relatore FULVIO GIGLIOTTI

Seduta del 10/02/2026

FATTO

1. Con ricorso del 6.10.2025 – previo reclamo del 15.7.2025 (e altro successivo del 6.2025), riscontrato negativamente dall'intermediario – la ricorrente, titolare di una carta di credito rilasciata dall'intermediario convenuto, ha rappresentato che in occasione della verifica dei movimenti della carta, riscontrava un addebito di € 446,77 relativo a un'operazione di pagamento online da lei mai autorizzata

Ha quindi domandato il rimborso della somma a suo avviso indebitamente addebitata.

2. Si è costituito l'intermediario, chiedendo il rigetto del ricorso.

In particolare, ha evidenziato parte resistente che:

- l'operazione contestata è stata eseguita tramite dispositivo personale della ricorrente, autorizzandola a mezzo *token* attivato l'ultima volta il 20/6/2025 sul medesimo dispositivo utilizzato per l'esecuzione della transazione contestata;

- i log informatici danno evidenza di accesso e autorizzazione con autenticazione forte, e nessuna anomalia tecnica è stata rilevata.

Assumendo, quindi, che la cliente si sia resa gravemente inadempiente all'obbligo di custodia degli

strumenti e dei codici di accesso che consentono l'utilizzo del servizio online, ha concluso per il rigetto del ricorso.

3. In sede di repliche, parte ricorrente ha ribadito che, nella data dell'operazione disconosciuta, aveva utilizzato la carta esclusivamente per due pagamenti presso esercizi commerciali fisici, entrambi effettuati con inserimento della carta e digitazione del PIN, come risultante dall'estratto movimenti, sostenendo di non aver eseguito alcun pagamento online e di non aver mai utilizzato il servizio Token per quell'operazione.

Ha quindi dedotto la verosimile clonazione della carta, evidenziando che il fatto di aver disconosciuto una sola operazione, pur avendo effettuato nella stessa giornata ulteriori pagamenti pienamente leciti, confermerebbe la sua buona fede e l'assenza di comportamenti negligenti.

Controreplicando, parte resistente ha evidenziato che la ricorrente ha comunque omesso di indicare qualsiasi dettaglio ricostruttivo della truffa asseritamente subita, evidenziando che in mancanza di elementi dimostrati dalla cliente (in questo caso effettivamente né indicati, né provati da parte ricorrente), che possano far ritenere provata la sussistenza di una clonazione degli strumenti utilizzati, si concretizzerebbe piuttosto, secondo un orientamento pacifico) una presunzione di diritto della colpa grave della cliente medesima.

Ha quindi insistito per il rigetto del ricorso.

DIRITTO

4. Ritiene il Collegio che la domanda della ricorrente non sia da accogliere, per le ragioni di seguito illustrate.

5. 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 PSD2, 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).

6. 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

adempito 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.

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, peraltro, un orientamento consolidato ritiene che la mancata allegazione delle circostanze di fatto della vicenda (nella specie, asseritamente) fraudolenta, da parte del ricorrente, debba essere intesa quale indizio idoneo a fondare una valutazione in termini di colpa grave della condotta del cliente, qualora il carattere non circostanziato degli utilizzi non autorizzati si sia accompagnato alla prova dell'autenticazione forte da parte dell'intermediario resistente (in tal senso, da ult., Coll. ABF Torino, n. 8755/2025; ma v., anche, *ex multis*: Coll. ABF Milano, n. 8588/2025; Coll. ABF Bari, n. 8052/2025; Coll. ABF Bologna, n. 7965/2025).

7. Quanto sopra premesso, osserva il Collegio che, alla luce del quadro normativo sopra richiamato, e della connotazione fattuale della vicenda per la quale si procede, per come risultante dalle evidenze in atti, è emerso che la ricorrente ha eseguito l'accesso a un portale *on line* e ha predisposto l'acquisto; all'atto del pagamento ha digitato il numero di carta, il mese e l'anno di scadenza, il suo nome e cognome, il codice di sicurezza (CVV) e ha confermato l'operazione.

Più in dettaglio, dalle evidenze in atti, come prodotte dall'intermediario, è emerso che:

- per poter accedere all'area riservata tramite il sito dell'intermediario, il cliente deve inserire, in due sessioni separate, il codice cliente (composto da 7 cifre e assegnato al momento della conclusione del contratto) e la propria data di nascita; e poi il PIN (assegnato inizialmente e successivamente modificabile dal cliente);
- in seguito al corretto inserimento di detti codici, il cliente deve autorizzare l'accesso mediante il servizio Token, ovvero il servizio di Autenticazione forte a mezzo di un software dell'applicazione fornita dall'intermediario, che genera il codice *Token*;
- viene quindi trasmessa sul dispositivo in possesso del cliente (ovvero il dispositivo mobile, ad es. smartphone, sul quale è attivo il *token*) la richiesta di autorizzazione, mediante la generazione del "codice *token*", che consiste in un codice monouso generato con l'app.

Sul proprio dispositivo, quindi, il cliente visualizza la seguente notifica:

- autorizzazione operazione
- tipologia "*login*"
- data e ora richiesta operazione
- autorizza o annulla.

Cliccando sulla scelta "autorizza" è richiesta l'ulteriore conferma che prevede l'inserimento di Smart Code/codice Biometrico. In seguito a questa ulteriore autorizzazione, sul dispositivo in possesso del cliente compare la notifica di operazione autorizzata "Hai autorizzato l'operazione con successo! Controlla l'esito nel tuo *browser*".

Nel caso di specie, dopo aver effettuato l'accesso sopra descritto, la ricorrente ha effettuato l'operazione dispositiva procedendo ad autenticazione con doppio fattore. In particolare, per come emerge dai log acquisiti in atti (allegati E e F alle controdeduzioni di parte resistente):

- all'atto del pagamento è stato digitato il numero della Carta, mese e anno di scadenza, nome e

cognome del titolare della Carta, codice di sicurezza (CVV), che sono stati evidentemente in possesso del solo Cliente.

Successivamente, la Cliente ha ricevuto la notifica PUSH (nella quale erano indicati i dettagli dell'operazione) sul proprio *smartphone*, nel quale era già attivato il *token* (primo fattore SCA: possesso); Ha autorizzato l'operazione cliccando "autorizza" su tale notifica, digitando, a seguire, lo *smartcode* oppure tramite impronta digitale/*faceid* (secondo fattore SCA: conoscenza o inerenza).

Risulta quindi provato il rispetto della procedura di SCA richiesta per procedere all'operazione dispositiva.

8. Resta quindi da valutare la sussistenza di una colpa grave della ricorrente. In proposito, come già anticipato, rileva il Collegio che parte ricorrente non ha fornito alcuna ricostruzione fattuale della asserita truffa o clonazione della carta.

La stessa, invero, si è unicamente limitata, anche in sede di denuncia, al disconoscimento dell'operazione sopra descritta. Deve allora tenersi conto di quanto già precisato con riguardo alla rilevanza della mancata allegazione delle circostanze di fatto relative all'operazione asseritamente fraudolenta: rilevanza che un orientamento assolutamente compatto dei Collegi territoriali apprezza in termini di presunzione della colpa grave del ricorrente, la quale, pertanto, deve essere ritenuta presente.

Nessun rilievo, poi, sotto altro profilo, potrebbe assumere l'eventuale assenza di messaggi di *alert*, atteso che – pur nel contrasto delle parti sul punto (la resistente ha dedotto, producendo apposita evidenza di avere inviato una mail alla cliente informandola dell'avvenuta esecuzione dell'operazione contestata; mentre parte ricorrente ha negato di avere ricevuto alcun *alert*) – deve necessariamente considerarsi che, trattandosi di operazione unica, l'eventuale mancata attivazione ovvero il mancato funzionamento del servizio non risulterebbe rilevante, in quanto l'*alert* non avrebbe comunque potuto limitare, in concreto, il pregiudizio dell'utente.

9. Ne consegue che, risultando provata la procedura di SCA, ed essendo da predicare anche la sussistenza della colpa grave della ricorrente, il ricorso non può essere accolto.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE