

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BARTOLINI	Membro designato dalla Banca d'Italia
(BA) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore FILIPPO BOTTALICO

Seduta del 28/01/2026

FATTO

La ricorrente afferma che, in data 14/09/2025, aveva deciso di acquistare “2 divani” dal sito web del produttore e che durante l’operazione di acquisto le veniva chiesto di inserire un codice.

Precisa che, in seguito all’inserimento del predetto codice, le era comparso il messaggio “AUTORIZZAZIONE NEGATA”, e che attualmente la sua carta prepagata risulta “bloccata”.

Lamenta la presenza di due operazioni non autorizzate rispettivamente di € 124,98 ed € 123,64.

Chiede quindi il rimborso della somma complessiva di € 248,62.

Costituitosi, l’intermediario resistente afferma che la ricorrente è titolare di carta di debito n. ***85 e richiede nel presente procedimento il rimborso della somma pari ad € 248,62 relativa a due operazioni di pagamento autorizzate *online* in data 14/09/2025 tramite *app*.

Precisa che tali operazioni erano state eseguite solo in seguito alla “autenticazione forte del cliente”, considerato che risulta regolarmente avvenuta la fase di *enrollment* della carta prepagata sul *device* utilizzato per l’esecuzione delle operazioni, avvenuta il 13/07/2025; *login* il 14/09/2025 mediante inserimento del codice *****ID; disposizione di pagamento, per la quale fornisce evidenza informatica attestante la modalità autorizzativa conforme alla SCA per ciascuna operazione.

Precisa, altresì, che la predetta fase di *login* non è in alcun modo collegabile a quella dispositiva, in quanto le operazioni in esame erano state autorizzate su un sito di *e-commerce*; “poco prima” dell’esecuzione delle operazioni in esame la ricorrente aveva eseguito due operazioni di ricarica della carta prepagata, autorizzate dallo stesso *device* utilizzato per autorizzare le successive operazioni disconosciute.

Rappresenta che le procedure di autenticazione forte adottate possono essere la procedura “*primaria*” mediante notifica *push* in *app* ed inserimento del codice *****ID (formato da sei caratteri e scelto dall’utente in fase di abilitazione dei prodotti finanziari in *app*); la procedura “*secondaria*” mediante OTP ricevuto a mezzo SMS e *password*.

Precisa che nel caso in esame era stata attivata la procedura “*primaria*” e che per l’utilizzo di tale procedura è necessario in via preventiva installare l’*app* sul *device*, associando lo strumento di pagamento e configurando il codice *****ID mediante inserimento delle credenziali di accesso (*username* e *password*), dei dati dalla carta prepagata (PAN, CVV2 e data di scadenza) e della *password* dinamica “*usa e getta*” inviata via SMS sull’utenza mobile fornita dalla cliente e associata allo strumento di pagamento.

Dopo aver ricostruito il funzionamento del codice *****ID, precisa che qualora il cliente sbagli l’inserimento del codice alfanumerico per più di cinque volte, è previsto il blocco del codice stesso.

Rappresenta, altresì, che le operazioni erano state eseguite e autorizzate dallo stesso device “*enrollato dalla ricorrente e mai modificato*”.

Ritiene, pertanto, di aver implementato un sistema conforme al dettato normativo, garantendo la sicurezza dei propri servizi, senza che fosse emersa alcuna anomalia o malfunzionamento delle relative procedure.

Fa presente che, a fronte di un rischio di frode “*potenziale o accertato*”, è prevista l’attivazione di contromisure che hanno la finalità di tutelare il cliente, le quali consistono nell’inibizione dell’operatività della carta di pagamento, precisando che nel caso in esame il blocco della carta era avvenuto il 14/09/2025, alle ore 11:54.

Evidenzia altresì che mette a disposizione della propria clientela il servizio di SMS-*alert*, che può essere attivato gratuitamente ed offre la possibilità di controllare i movimenti relativi alla carta.

Precisa che l’invio dell’informativa al cliente sulle operazioni in uscita/entrata viene trasmessa tramite SMS-*alert*, ovvero tramite notifica *push* in *app*.

Ritiene che la ricorrente fosse stata vittima di *phishing* tradizionale, avendo la stessa visitato un sito web “*poco sicuro*” ed eseguito volontariamente le operazioni in esame nell’errata convinzione di acquistare “*degli articoli di mobilio*”.

Con riguardo alla nozione di colpa grave, sostiene che la stessa è da intendersi come una “*inescusabile imprudenza, negligenza o imperizia*” che si verifica in seguito alla violazione di quel “*grado minimo ed elementare di diligenza generalmente osservato da tutti*”.

Richiama, altresì, l’orientamento assunto dai Collegi ABF secondo cui nei casi di utilizzi fraudolenti online dello strumento di pagamento, qualora il cliente non abbia allegato le circostanze di fatto della frode ed a fronte della prova di autenticazione ed in assenza di indici di anomalia, la colpa grave del cliente si presume.

Aggiunge che, ai sensi dell’art. 8 d.lgs. n. 11/2010, ha predisposto i presidi consistenti nella trasmissione con cadenza periodica appositi avvisi, con cui sono resi edotti i clienti di eventuali comportamenti anomali che dovrebbero essere considerati come *alert*; creazione di apposite pagine *web* in cui risulta presente un manuale di ausilio all’utente su come difendersi dalle truffe.

Conclude affermando che la condotta della ricorrente era connotata da una “*colpevole credulità*”, considerato che le operazioni in esame erano state autorizzate dalla stessa nel rispetto della SCA.

Chiede, pertanto, il rigetto del ricorso.

DIRITTO

Con l’odierno ricorso, la ricorrente disconosce due operazioni di pagamento, per un valore complessivo di € 248,62, effettuate *online* su un sito di *e-commerce* il 14/09/2025, rispettivamente alle ore 09:17:41 (€ 124,98) e 09:43:52 (€ 123,64), tramite la carta prepagata n. ***85 a lei intestata ed emessa dall’intermediario resistente.

Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27/01/2010, n. 11, come modificato dal d.lgs. 15/12/2017, 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 13/01/2018. La ricorrente non menziona il deposito di una denuncia-querela in relazione ai fatti oggetto del presente ricorso, né tantomeno vi è evidenza in tal senso.

Le operazioni risultano dalle specifiche evidenze contabili interne prodotte in atti dall'intermediario. L'intermediario inoltre produce specifica evidenza contabile interna attestante l'avvenuto blocco della carta di debito n. ***85 in data 18/09/2025, alle ore 07:56:39, quindi successivamente rispetto all'esecuzione delle due operazioni disconosciute.

In ordine all'autenticazione e all'esecuzione delle operazioni contestate, l'intermediario afferma che, innanzitutto, la ricorrente ha proceduto all'*enrollment* della carta di pagamento n. ***85 sul dispositivo utilizzato per la esecuzione delle operazioni, producendo la relativa documentazione a supporto.

Il numero di cellulare ivi riportato corrisponde a quello indicato nel modulo di ricorso.

Prosegue sostenendo che, nonostante la ricorrente abbia fatto accesso alla propria area personale del sistema di *internet banking* nella data delle operazioni contestate (di cui, peraltro, fornisce prova), detto accesso non è in alcun modo collegabile alla disposizione delle operazioni, essendo state eseguite attraverso siti di *e-commerce*.

L'intermediario precisa che per tali operazioni il cliente accede sul *merchant* attraverso il quale vuole effettuare l'acquisto e, dopo aver inserito i dati dello strumento di pagamento e la propria *password*, per autorizzare l'operazione può ricevere una notifica in *app* e inserire come mezzo autorizzativo il codice ***ID.

Per questo tipo di operazioni, dunque, non è necessario effettuare *login* né in *app* né sul sito dell'intermediario.

In ordine all'autenticazione delle operazioni, produce i relativi *log*, corredati di legenda esplicativa; le operazioni risultano eseguite tramite la modalità di pagamento "*primaria*", la quale prevede l'invio di una notifica *push* in *app* e l'inserimento del codice *****ID (formato da sei caratteri e scelto dall'utente in fase di abilitazione dei prodotti finanziari in *app*).

Nella legenda sono riportati i codici utilizzati nei *log*.

In particolare, è specificato che il "*deviceID*" rappresenta l'identificativo del telefono utilizzato dalla cliente per apporre la firma con il codice *****ID; la voce "*appID*" corrisponde all'identificativo dell'*app* utilizzata dalla cliente per apporre la firma con il codice *****ID e la descrizione "*transaction-challenge*" rappresenta la richiesta di autorizzazione disposta dalla cliente sul canale e firmata in formato *jwt* dal canale stesso e autorizzata dal cliente con il proprio codice *****ID.

L'intermediario allega, altresì, evidenza attestante l'utilizzo del protocollo 3DSecure per le due operazioni in esame.

È utile precisare altresì che poco prima dell'esecuzione delle operazioni in contestazione la ricorrente provvedeva ad eseguire due operazioni di ricarica dello strumento di pagamento autorizzate dallo stesso dispositivo utilizzato per le operazioni disconosciute, come risulta dalla documentazione prodotta dall'intermediario.

Tanto ricostruito, questo Collegio non intende discostarsi dal proprio orientamento che ritiene siffatta documentazione tecnica allegata alle controdeduzioni idonea a dimostrare la corretta autenticazione e la regolarità formale delle singole operazioni disconosciute ex art. 10, co. 1 d.lgs. n. 11/2010 con un sistema *SCA-compliant*, nell'ipotesi di esecuzione delle stesse con l'utilizzo dell'*app* installata sul device dell'utente (ex multis Collegio di Bari, decisione n. 224/2025).

Senonché "*la previsione di cui all'art. 10, comma 2, del d. lgs. n. 11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che 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" (Collegio di Coordinamento, decisione n. 22745/2019).

La mancanza della prova di autenticazione, in altri termini, è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente, poiché la prova di autenticazione rappresenta, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente.

Ebbene, secondo la consolidata giurisprudenza arbitrale nelle contestazioni di utilizzi fraudolenti online di strumenti di pagamento in cui:

- i. l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute;
- ii. il sistema di pagamento risulta conforme alla *Strong Customer Authentication* (SCA);
- iii. non risultano indici di anomalia delle operazioni e/o ulteriori elementi,

le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo (cfr. Collegio di Bari, decisioni nn. 9006/2024 e 8247/2024).

Nel caso di specie, la ricorrente non offre alcun elemento a sostegno dell'asserita frode patita, limitandosi a chiedere il ristoro delle somme relative ad operazioni – a suo dire – non autorizzate, e si limita ad allegare la schermata relativa al blocco della carta e la contabile riportante le operazioni disconosciute.

In tema di sistemi di allerta, si rammenta che fra *"i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto"* (Collegio di Coordinamento, decisione n. 24366/2019).

Sul punto, l'intermediario sostiene di mettere a disposizione della propria clientela il servizio di SMS-alert, che può essere attivato gratuitamente ed offre la possibilità di controllare i movimenti relativi alla carta, ma non fornisce prova né della sua attivazione e del funzionamento del caso di specie, né del rifiuto della ricorrente ad avvalersene.

Precisa che l'invio dell'informativa al cliente sulle operazioni in uscita/entrata viene trasmessa tramite SMS-alert, ovvero tramite notifica *push* in *app*, producendo in atti il *log* attestante l'invio di un SMS *"antifrode"* il 14/09/2025, alle ore 09:44:31, dal quale però non è possibile evincere il contenuto del messaggio.

Precisa, altresì, che tale messaggio richiede all'utente di confermare la genuinità dell'operazione; in caso di *"risposta negativa"* viene apposto un blocco *"cautelativo"* sullo strumento di pagamento, come di fatto avvenuto e confermato dal messaggio allegato dalla ricorrente.

Tuttavia si tratta di un messaggio successivo non solo alla prima, ma anche alla seconda operazione contestata, avente una finalità ben diversa dall'allerta, tanto è vero che non ha impedito la perpetrazione della truffa in danno della ricorrente.

Secondo la giurisprudenza consolidata di questo Arbitro – la mancata attivazione ovvero il mancato funzionamento di tale servizio (o di servizio assimilabile) sono ritenuti irrilevanti nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta ovvero di più transazioni ma a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato, in quanto la ricezione dell'alert non potrebbe in concreto limitare il pregiudizio dell'utente (cfr. Collegio di Bari, decisione n. 7328/2022; Collegio di Milano, decisione n. 6356/2022).

Nel caso di specie, le operazioni contestate sono due e sono state eseguite a distanza di quasi mezz'ora l'una dall'altra; pertanto, se il servizio di allerta fosse stato attivo, la ricorrente avrebbe potuto inibire l'operatività dello strumento di pagamento dopo l'esecuzione della prima operazione, non subendo il pregiudizio della seconda, che, pertanto, deve essere accollato all'intermediario resistente.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 123,64.

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