

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 23/04/2026

FATTO

La ricorrente, titolare di carta di pagamento rilasciata dall'intermediario odierno convenuto, espone di aver subito una truffa tramite una piattaforma di *marketplace* su cui era interessata a vendere un articolo.

Precisa di essere stata contattata da un potenziale acquirente che le inviava un QR-code e le illustrava i *"vari passaggi"* che avrebbe dovuto eseguire per *"finalizzare la vendita"*.

Deduce di essersi fidata, *"non avendo alcuna esperienza sul sito"* e che *"l'assistente virtuale ha comunicato per ben tre volte che la transazione non è andata a buon fine e la faceva ripetere continuamente"*.

Chiede il rimborso del controvalore di tre operazioni di pagamento disconosciute, pari ad € 299,00 ciascuna per un totale di € 897,00.

Costitutosi, l'intermediario afferma che dalle verifiche tecniche eseguite sulla carta utilizzata si evince per ciascuno dei tre pagamenti *online*: l'utilizzo di codici OTP, inviati tramite SMS al numero di cellulare certificato della ricorrente (fattore di possesso); l'inserimento del 3DS-codice sicurezza *e-commerce*, ossia un codice statico impostato direttamente dall'utente (fattore di conoscenza).

Ritiene integrato il requisito della colpa grave tenuto conto delle dichiarazioni della stessa ricorrente, che non muove espresse contestazioni all'operato della banca in quanto consapevole dell'estraneità di quest'ultima rispetto alla truffa occorsa.

Fa presente di aver inviato notifiche *push* di *alert* dell'avvenuta esecuzione delle operazioni, ignorate dalla ricorrente, ad ulteriore conferma del suo comportamento negligente ed imprudente.

Chiede, dunque, il rigetto del ricorso.

DIRITTO

Premesso che 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, nella denuncia in atti la ricorrente dichiarava che:

- il finto potenziale acquirente che la contattava tramite il sito di *marketplace* le inviava un QR-code che la reindirizzava ad una “interfaccia di messaggistica”;
- le venivano illustrati i passaggi da seguire per ricevere l’accredito;
- inseriva i dati della carta di debito e le veniva richiesto per tre volte il “codice di conferma”;
- le veniva quindi richiesto di aprire un conto presso un altro intermediario, e la ricorrente dava seguito a questa richiesta;
- successivamente, visionava il sito di *marketplace* ove riscontrava che il bene risultava ancora invenduto;
- consultava il conto appena aperto, ove riscontrava un ammanco di € 299,00, nonché il conto acceso presso l’intermediario odierno resistente riscontrando l’esecuzione di tre operazioni dell’importo di € 299,00 ciascuna che costituiscono oggetto del presente ricorso.

In ordine alla prova dell’autenticazione e della corretta esecuzione di tali operazioni, l’intermediario afferma che sono state eseguite mediante:

- l’utilizzo di codici OTP, inviati tramite SMS al numero di cellulare certificato della ricorrente (fattore di possesso);
- l’inserimento del 3DS-codice sicurezza *e-commerce*, ossia un codice statico impostato direttamente dall’utente (fattore di conoscenza).

Rinvia, al riguardo, alla relazione tecnica relativa all’operatività contestata in atti.

Da *log* risulta conformemente alla ricostruzione dell’intermediario:

- l’inserimento del codice 3DS (valorizzazione della colonna “*3DSTRID*”: fattore di conoscenza);
- l’utilizzo della OTP SMS (valorizzazione “02” della colonna “*Tipo autenticazione*”: fattore di possesso).

L’intermediario produce altresì il *log* relativo alle OTP SMS dei tre pagamenti contestati, contenute in messaggi in cui si chiedeva espressamente la conferma dell’acquisto online di € 299,00 presso M***Pay .

Il numero di cellulare destinatario dei messaggi coincide con quello indicato dalla ricorrente nel modulo di ricorso e in denuncia.

Sulla scorta di tale documentazione, risulta raggiunta la prova della conformità ai requisiti normativamente previsti in tema di SCA delle operazioni contestate.

A ciò si aggiunga che, essendo la PSD2 tecnologicamente neutrale e non prevedendo un sistema informatico standard per l’inserimento e la tracciatura dei fattori di autenticazione forte, i Collegi ritengono che, per valutare l’assolvimento dell’onere della prova della SCA, possono essere valutati (oltre ai *log*) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione.

I Collegi ritengono inoltre che eventuali dichiarazioni confessorie del cliente possano assumere valore di prova legale ai sensi dell’art. 2730 c.c. (così Collegio di Bari, decisione n. 9675/2024; Collegio di Torino, decisione n. 10892/2024).

Con riferimento al caso di specie, la ricorrente ha dichiarato di aver inserito i dati della propria carta e di aver comunicato per tre volte il “*codice di conferma*”.

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).

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

Nel caso di specie, dalla disamina degli *screenshot* delle interlocuzioni tramite messaggi intercorse con il frodatore, oltre che dalla ricostruzione della truffa fatta dalla ricorrente, non si evincono interlocuzioni truffaldine tramite canali di contatto riconducibili alla banca.

A ciò si aggiunga che la ricorrente esplicitamente ammette – come già detto – di aver inserito i dati della carta e, per ben tre volte, aver approvato la richiesta di conferma.

Ne consegue che la sua condotta risulta connotata da inescusabile e grave negligenza.

In tema di sistemi di allerta, si rammenta che, secondo l’autorevole insegnamento del Collegio di Coordinamento, *“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).

Il medesimo Collegio di Coordinamento ha precisato che *“la mancata attivazione del servizio sms – alert costituisce in ogni caso una carenza organizzativa imputabile all’intermediario che, oltre a produrre l’effetto giustificativo solo a fronte della specifica dichiarazione liberatoria di rifiuto del cliente ad avvalersene (già affermata dal precedente “coordinamento”), non può non essere rilevata anche d’ufficio”* (Collegio di Coordinamento, decisione n. 8672/2024).

Nel caso di specie l’intermediario afferma di aver inviato una *“alert notify”* alla ricorrente per ognuna delle operazioni oggetto di ricorso, allegando le relative evidenze documentali.

A ciò si aggiunga che deve ritenersi comunque irrilevante un sistema di *alert ex post* in caso di invio – come nell’odierna vicenda – di SMS cc.dd. parlanti (*ex multis*, Collegio di Bari, decisioni nn. 2664/2023, 12866/2022 e 14020/2022).

Da ultimo, si rammenta che l’art. 8 d.m. n. 112/2007 identifica i casi di frode che, ai fini della normativa stessa, vanno segnalati all’Ufficio Centrale Antifrode dei Mezzi di Pagamento del Ministero dell’Economia e delle Finanze (UCAMP) per consentire un monitoraggio del mercato delle carte di pagamento.

Secondo l’orientamento condiviso dei Collegi, le relative previsioni non hanno un valore precettivo diretto sulla materia in esame, ma rappresentano utili indicatori per identificare anomalie e scenari di frode anche ai sensi dell’art. 2 del Regolamento EBA n. 2018/389, in base al quale gli intermediari sono tenuti a predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente.

Conseguentemente, una volta accertata la colpa grave del cliente, qualora sussista uno dei seguenti indici di frode:

- i. sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento, prevista al punto 1 della lett. b) del menzionato art. 8;
- ii. tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita, di cui al punto 2 della lett. a) del citato art. 8;
- iii. due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell’arco di sessanta minuti, di cui al punto 3 della lett. b) del medesimo art. 8,

la ripartizione della responsabilità con il prestatore dei servizi di pagamento (PSP) deve essere determinata caso per caso, in relazione alle circostanze di fatto, in quanto le previsioni del d.m. rappresentano un parametro per la formulazione di un giudizio in concreto della negligenza tecnica dell'intermediario (*ex multis*, Collegio di Bari, decisione n. 7126/2024; Collegio di Bologna, decisione n. 5884/2024).

Secondo la giurisprudenza arbitrale, inoltre, sebbene il d.m. n. 112/2007 faccia riferimento alla prevenzione delle frodi sulle carte di pagamento, gli indici di frode ivi disciplinati all'art. 8 possono costituire un parametro di valutazione del comportamento del PSP, ove possibile, anche con riguardo ad operazioni eseguite con altri strumenti di pagamento (ad es. bonifici o pagamenti online) in ragione dell'unicità della *ratio* sottesa a tale normativa (così Collegio di Bari, decisione n. 10175/2023; Collegio di Bologna, decisioni nn. 8394/2024 e 12960/2022; Collegio di Roma, decisione n. 8843/2023; Collegio di Milano, decisione n. 13092/2022; Collegio di Torino, decisione n. 3964/2022).

È inoltre possibile valorizzare indici di frode ulteriori a quelli del decreto ministeriale in presenza di un'operatività anomala rispetto alle movimentazioni storiche del ricorrente (ad esempio con riguardo al numero, alla tipologia, all'importo, al tempo di esecuzione e alla riconducibilità delle operazioni al medesimo beneficiario), ove vi sia un'evidenza delle stesse.

Con riguardo all'odierna vicenda, il *merchant* corrisponde in tutti e tre i casi ad una piattaforma di trasferimento di crypto-attività, anche se risulta diverso il codice numerico che segue la denominazione; inoltre l'operatività fraudolenta si è consumata nell'arco di circa 6 minuti.

La complessiva ricostruzione dell'operatività fraudolenta, pur ferma la conformità a SCA delle operazioni contestate e la condotta gravemente colposa del ricorrente, nondimeno indizia per la ricorrenza di indici di frode trascurati, per proprie carenze organizzative, dall'intermediario resistente.

Tali indici si ravvisano nell'insieme delle circostanze che hanno caratterizzato l'accaduto, e quindi non già semplicemente la constatazione del numero delle operazioni contestate e la loro esecuzione nell'arco di 24 ore, nonché la ricorrenza del medesimo beneficiario (che comunque integrano un rischio di frode), quanto piuttosto la loro concomitanza unitamente al lasso temporale dell'esecuzione di tali operazioni (come, detto 6 minuti).

Tanto precisato, secondo l'orientamento più recente condiviso dai Collegi, i principi del d.m. n. 112/2007 non hanno un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate ma sono espressione di un generale obbligo di monitoraggio delle operazioni, da valorizzare per valutare la condotta dell'intermediario; pertanto, la valutazione della responsabilità del PSP dovrebbe essere formulata con un giudizio sintetico che tenga conto della sua condotta complessiva e di tutti gli altri elementi desumibili dal caso concreto e la base di calcolo per la liquidazione della somma oggetto di condanna dovrebbe essere costituita dall'intero ammontare degli importi disconosciuti, senza esclusioni, procedendo a una distribuzione in concreto del concorso di colpa tra le parti (*ex multis*, Collegio di Bari decisione n. 7228/2025).

Di conseguenza, alla stregua delle normative e dei principi citati, ritiene questo Collegio che le operazioni controverse siano un effetto di una verosimile disfunzione organizzativa sul quale si è innestato il comportamento gravemente negligente della ricorrente, che però non ha assorbito completamente il nesso di causalità con l'evento lesivo ma ha concorso con esso (così Collegio di Bari, decisione n. 6306/2023; Collegio di Roma, decisione n. 8843/2023; Collegio Milano, decisione n. 7410/2022).

Alla luce delle suesposte considerazioni, questo Collegio ritiene che il ricorso sia meritevole di parziale accoglimento, mercè la corresponsione in favore della ricorrente della somma di €300,00 equitativamente determinata.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 300,00.

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