

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) MIRABELLI	Membro di designazione rappresentativa degli intermediari
(BO) TRAVERSI	Membro di designazione rappresentativa dei clienti

Relatore ELEONORA MIRABELLI

Seduta del 13/01/2026

FATTO

Il ricorrente, anche per mezzo della documentazione allegata al ricorso, riferisce di essere titolare della carta di credito n. ***511 emessa dall'intermediario ed appoggiata sul conto corrente acceso presso lo stesso. Nel pomeriggio del 09/08/2025, sua moglie inseriva un annuncio sull'app S. per la vendita di vestiario e il giorno successivo la stessa veniva contattata dall'utente E.P, la quale chiedeva un video da inviare al n. 378***946. Successivamente, in data 11/08/2025, sua moglie postava un annuncio di un vestito e veniva contattata dalla medesima utente, la quale chiedeva un video da inviare al n. 378***272, ma sua moglie inviava il video alla precedente utenza telefonica n. 378***946. L'utente chiedeva tramite WhatsApp l'invio del link dell'annuncio e l'e-mail per la conferma successiva del pagamento e la moglie del ricorrente visualizzava l'e-mail proveniente dal sito di e-commerce S. e confermava la vendita. Tuttavia – dopo la conferma – si aprivano un modulo e una chat dove venivano richiesti rispettivamente i dati di fatturazione e i documenti personali e la moglie del ricorrente comunicava quanto richiesto e inseriva, altresì, la carta del marito n. ***511 in quanto la sua risultava non funzionante. Tramite chat veniva comunicato da un lato il blocco temporaneo di € 888,00 al fine di verificare la carta inserita e, dall'altro, di dare conferma ai messaggi per la transazione. Una volta confermata l'operazione, veniva richiesta la disposizione di un'altra transazione del medesimo importo in quanto la precedente operazione non era andata a buon fine e pertanto, si accorgeva di aver subito una truffa online. Alle ore 15:58 contattava l'istituto collocatore della carta di credito per due volte al fine di richiedere l'annullamento dell'operazione, tuttavia senza riuscirvi e, dopo aver contattato

l'intermediario al n. 068***800 alle ore 16:03, l'operatore riferiva che la disposizione era ancora in transito e altresì dichiarava che avrebbe provveduto sia ad annullarla sia a ricontattare la banca ma, alle ore 16:10, ricontattava l'istituto bancario, tuttavia senza riuscire a reperire informazioni utili e dunque alle ore 16:28, chiamava il n. 800***531 dell'intermediario al fine di bloccare definitivamente la carta di credito, pertanto, quest'ultimo è esclusivamente responsabile del mancato blocco dell'operazione. Conclude il ricorrente, chiedendo a codesto Arbitro adito, la condanna della Banca al pagamento della somma di euro 888,00 illegittimamente sottrattagli.

L'intermediario, in sede di controdeduzioni, riferisce che la richiesta di rimborso è infondata in quanto il ricorrente ha ammesso di aver autorizzato la transazione di € 888,00 alle ore 15:38 dell'11/08/2025 e che la carta n. ***511 è stata bloccata alle ore 16:33 dell'11/08/2025, dopo quasi un'ora dalla transazione mentre l'SMS Alert concernente la transazione in corso – come altresì confermato dal ricorrente – è stato inviato alle ore 15:39 al n. +39 348***110 indicato dal ricorrente in sede di attivazione del servizio. Eccepisce inoltre che il ricorrente non ha prodotto alcuna allegazione in merito alla presunta truffa e che, in particolare, non vi è prova: del prodotto messo in vendita sul sito di e-commerce S., delle presunte telefonate ricevute, dell'e-mail e della chat con le indicazioni del truffatore. Inoltre, la transazione è stata contabilizzata, registrata e autenticata dal ricorrente tramite il suo *device*, su cui è stata correttamente installata l'app in data 10/12/2023, mediante digitazione del PIN. Rileva infine che le transazioni con carte di pagamento perfezionate con l'autenticazione sono irrevocabili e che pertanto, le chiamate del ricorrente al numero di assistenza e al numero verde corretto non avrebbero potuto consentire alcun annullamento del pagamento ormai accettato e concluso nel circuito. Inoltre, sussiste la colpa grave del ricorrente, il quale ha dato credito con colpevole credulità ad una chat non riconducibile all'istituto di credito mentre sarebbe stato sufficiente leggere il messaggio per comprendere l'esecuzione del pagamento; il caso di specie è qualificabile come *phishing*, con riferimento al quale la banca ha da tempo avviato una campagna di informazione e la Polizia Postale ha dato notizia sul suo sito dal 2015. Tra l'altro, non ricorrono elementi di anomalia o indici di rischio frode, trattandosi di una sola transazione che non ha esaurito il *plafond* della carta. Conclude dunque l'intermediario, chiedendo il rigetto del ricorso in quanto infondato in fatto ed in diritto.

DIRITTO

La presente controversia ha ad oggetto la richiesta di rimborso di una operazione di e-commerce di € 888,00 eseguita in data 11/08/2025 alle ore 15:38.

L'intermediario eccepisce l'inapplicabilità della normativa di cui al d.lgs. 11/2010 in materia di operazioni non autorizzate dal momento che l'operazione in contestazione è stata autenticata dal ricorrente stesso.

Al riguardo si osserva che in sede di ricorso, con riferimento alla descrizione dei fatti, il ricorrente afferma di aver effettuato per errore un pagamento di € 888,00 mediante carta di credito a seguito della truffa subita.

Nella denuncia sporta dalla moglie del ricorrente, emergono le dinamiche della truffa online concernenti una utente E.P che, dopo aver visualizzato un post all'interno dell'app di e-commerce S., contattava quest'ultima. Successivamente, l'utente invitava la moglie del ricorrente a visualizzare l'e-mail e a confermare la vendita. Tuttavia, dopo la conferma della vendita, si aprivano un modulo e una chat dove

venivano richiesti dei dati. La moglie del ricorrente inseriva i dati della sua carta prepagata, che risultava non funzionante, e pertanto la stessa procedeva a inserire i dati della carta n. ***511 intestata al marito.

Inoltre, la moglie del ricorrente dichiara che il marito ha confermato il messaggio di autorizzazione di € 888,00 ricevuto sul suo cellulare convinto della temporaneità dell'addebito in attesa della conclusione di alcune verifiche sullo strumento di pagamento.

Appare dunque di preliminare importanza soffermarsi sulla questione dell'applicabilità, al caso di specie, della disciplina prevista dal D.lgs. n. 11/2010 in caso di operazioni non autorizzate.

Secondo l'orientamento consolidato dei Collegi ABF, affinché un'operazione possa dirsi non autorizzata, rendendo così automaticamente applicabile la disciplina di cui al D.lgs. 11/2010, deve difettare il requisito del "consenso del pagatore" di cui all'art. 5 del medesimo decreto (cfr. ex multis Collegio Bologna decisione n. 8245/2022 e n. 11201/2022, Collegio di Milano decisione n. 3945/2022). Si legge nelle motivazioni delle citate decisioni che, in caso di operazioni effettuate personalmente dal titolare dello strumento di pagamento (sebbene sulla base di un consenso viziato dagli artifici e raggiri attuati dal truffatore), si deve escludere l'applicabilità del regime di protezione predisposto dal D.lgs. 11/2010.

Nella fattispecie, sulla base della documentazione agli atti, e in particolare delle dichiarazioni confessorie rilasciate dal ricorrente, risulta che l'operazione, sia pur provocata da un raggiro perpetrato da un terzo, sia stata autorizzata dallo stesso, il quale ha volontariamente inserito i dati della propria carta di credito sulla piattaforma e-commerce e cliccato sulle notifiche push inviate dall'intermediario sul device in proprio possesso al fine di approvare e validare la transazione.

Pertanto, la fattispecie non è riconducibile a quella delle operazioni non autorizzate, ex art. 10 d.lgs. 11/2010, dovendo, piuttosto, essere inquadrata nel contesto delle operazioni autorizzate dall'utilizzatore (ex art. 5). Secondo l'orientamento arbitrale che questo Collegio ritiene di condividere, infatti, tali ipotesi esulano dal regime di protezione previsto dal menzionato d.lgs. in caso di operazioni non autorizzate, posto che, affinché un'operazione possa dirsi tale, deve difettare del requisito del "consenso del pagatore" di cui all'art. 5 del medesimo decreto (*"il consenso del pagatore è un elemento necessario per la corretta esecuzione di un'operazione di pagamento. In assenza del consenso, un'operazione di pagamento non può considerarsi autorizzata"*).

Tale consenso, in simili fattispecie, appare invece sussistente, in quanto è lo stesso utente ad autorizzare l'operazione, sia pur indotto a ciò da terzi mediante raggiro (cfr. Collegio di Bologna, decisione n. 11201 del 2022). In senso conforme si vedano, ex multis: Collegio di Bologna, decisione n. 1294 del 20.01.2022 e n. 21455 del 13.10.2021; nonché Collegio di Milano, decisioni nn. Pag. 5/6 Decisione N. 216 del 12 gennaio 2023 20485/2019 e 21251/2019; Collegio di Roma, decisioni nn. 9783/2021 e 14427/2021.

Si osserva inoltre che nessuna responsabilità per condotta illegittima sia imputabile alla banca in quanto, da una parte, non vi è alcuna prova del coinvolgimento dell'intermediario nella truffa perpetrata ai danni del ricorrente e, dall'altra, si ritiene che il grado di diligenza che deve tenere la banca nei confronti della propria clientela non possa essere esteso fino al punto di inserirsi nelle scelte effettuate autonomamente dal correntista in contesti del tutto estranei alla relazione tra banca e cliente.

Alla luce di quanto sopra, il Collegio ritiene che la domanda non meriti accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE