

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) SCARANO

Seduta del 14/04/2026

FATTO

Con ricorso presentato in data 08.12.2025, il cliente espone di aver riscontrato, in data 31.10.2025, accedendo all'applicazione bancaria, la presenza di cinque addebiti anomali eseguiti tra il 15 e il 31 ottobre 2025 sulla propria carta prepagata, per un importo complessivo di € 1.467,95. A seguito di alcune verifiche, accertava che i pagamenti erano stati effettuati in Romania.

Il ricorrente dichiara di non aver in alcun modo effettuato né autorizzato le operazioni in contestazione, di essere l'unico utilizzatore della carta, di non averla mai ceduta a terzi e di non aver mai comunicato il codice segreto a nessuno. Afferma altresì di non aver ricevuto le consuete notifiche di addebito via e-mail successivamente all'esecuzione dei pagamenti e che l'applicazione dell'intermediario aveva smesso di funzionare, rendendosi necessaria una sua reinstallazione con nuovi codici di accesso.

Il ricorrente riferisce di aver provveduto al blocco della carta e di aver sporto denuncia alle Autorità competenti in data 05.11.2025. In data 10.11.2025 aveva disconosciuto le operazioni contestate, ottenendo inizialmente il rimborso da parte dell'intermediario. Tuttavia, in data 19.11.2025, l'intermediario, all'esito di propri accertamenti, lo informava del ri-addebito delle somme. In pari data il ricorrente formulava formale reclamo, che veniva riscontrato negativamente dall'intermediario. Conclude chiedendo il rimborso delle somme corrispondenti alle operazioni disconosciute.

Nelle controdeduzioni, l'intermediario chiede il rigetto del ricorso, affermando che le operazioni contestate sono state correttamente contabilizzate, registrate e autenticate, in quanto poste in essere mediante la carta prepagata del ricorrente, attraverso il dispositivo da lui usualmente utilizzato. Secondo l'intermediario, il ricorrente avrebbe ricevuto sull'applicazione mobile notifiche *push* contenenti la descrizione dettagliata di ciascun pagamento — comprensive dell'importo, del beneficiario e degli estremi della carta — e le avrebbe autorizzate mediante l'inserimento del proprio Codice PIN. Le notifiche *push* risultano regolarmente consegnate sul dispositivo certificato del cliente. L'intermediario precisa altresì che, per ciascuna delle operazioni eseguite, al ricorrente sono stati inviati messaggi SMS, ad eccezione del primo non recapitato per fatto imputabile al cliente stesso, cosicché questi avrebbe avuto immediata contezza dell'avvenuta esecuzione dei singoli pagamenti. Aggiunge che le operazioni contestate sono state eseguite in totale assenza di anomalie e che la circostanza per cui numerose notifiche *push* non abbiano dato luogo a pagamenti dimostra che, in assenza della validazione tramite digitazione del Codice PIN da parte del titolare, i pagamenti non avrebbero potuto andare a buon fine. Eccepisce, inoltre, che il ricorrente non abbia mai denunciato lo smarrimento né il furto della carta di pagamento o del dispositivo tramite cui sono state autorizzate le operazioni contestate. Sostiene la sussistenza della colpa grave del cliente, il quale non avrebbe fornito elementi minimi utili alla ricostruzione della vicenda, limitandosi a disconoscere genericamente le operazioni senza indicare fatti che rendano plausibile una responsabilità dell'intermediario. Evidenzia infine che, ove il ricorrente avesse prestato attenzione alle notifiche *push* e agli SMS ricevuti nel corso delle due settimane in cui si è svolta l'operatività contestata, avrebbe potuto evitare l'autorizzazione dei pagamenti o, quanto meno, avrebbe potuto limitare il danno.

In sede di replica, il ricorrente ribadisce di aver contattato l'intermediario e bloccato ogni operatività non appena venuto a conoscenza dell'accaduto. Conferma di non aver mai comunicato volontariamente a terzi le proprie credenziali, i codici di accesso o i sistemi di autenticazione e di non aver mai autorizzato né riconosciuto le operazioni in contestazione. Sostiene che il proprio dispositivo sia stato oggetto di un attacco informatico e insiste per l'accoglimento del ricorso, chiedendo altresì la corresponsione degli interessi e il rimborso delle spese sostenute.

L'intermediario, nelle proprie controrepliche, sottolinea che, mentre la prima operazione disconosciuta risale al 15.10.2025, il blocco della carta è stato disposto solo il 31.10.2025, a dimostrazione di una notevole negligenza del ricorrente, il quale avrebbe potuto evitare le operazioni successive con un blocco tempestivo. Ribadisce che sia le notifiche *push* sia gli SMS di avviso sono stati regolarmente inviati sul dispositivo del cliente, dandogli la possibilità di attivarsi tempestivamente e che, nelle due settimane in cui è stata posta in essere l'operatività contestata, il cliente non ha verificato la movimentazione del proprio conto. Aggiunge che dai log prodotti risulta per cinque volte l'inserimento del numero completo della carta prepagata, comprensivo di data di scadenza e Codice CVV, seguito dall'autorizzazione mediante inserimento del Codice PIN, conosciuto solo dal cliente. Insiste nel rigetto del ricorso, in quanto infondato in fatto e in diritto.

DIRITTO

In via preliminare, occorre rilevare che con le repliche il ricorrente ha chiesto, per la prima volta, la corresponsione degli interessi e il rimborso delle spese sostenute. Tale domanda, tuttavia, deve

ritenersi inammissibile. Come noto, le Disposizioni ABF, alla Sezione VI, Par. 1, prevedono espressamente: *“Entro il termine perentorio di 25 giorni dalla ricezione delle controdeduzioni, il cliente può trasmettere una memoria di replica. Resta comunque preclusa la possibilità di ampliare la domanda iniziale”*. Ne consegue che la domanda accessoria formulata dal ricorrente con detta memoria, non contenuta nel ricorso originario, non può essere esaminata.

Nel merito, le operazioni oggetto di contestazione rientrano nell'ambito di applicazione del D.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13.01.2018) del D.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno e alla disciplina in materia di *strong customer authentication* (SCA).

Ai sensi dell'art. 10 del D.lgs. 11/2010, è onere dell'intermediario provare che le operazioni contestate siano state correttamente autenticate, registrate e contabilizzate e che non vi siano stati malfunzionamenti dei sistemi; solo successivamente spetta all'intermediario provare dolo o colpa grave in capo all'utilizzatore (Collegio di Coordinamento, decisione n. 22745/2019).

Con riferimento alla SCA, le fonti normative sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10 bis del D.lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA 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 (v. in particolare il parere dell'EBA del 21 giugno 2019). Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1) accede al suo conto di pagamento online; 2) dispone un'operazione di pagamento elettronico; 3) effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Nel caso in esame, le operazioni disconosciute consistono in cinque pagamenti per un importo complessivo di € 1.474,95, eseguiti mediante carta di credito nelle seguenti date e orari: 15.10.2025 alle ore 01:56 per € 166,99; 30.10.2025 alle ore 11:23 per € 326,99; 30.10.2025 alle ore 18:52 per € 326,99; 30.10.2025 alle ore 19:31 per € 326,99; 31.10.2025 alle ore 12:18 per € 326,99.

L'intermediario documenta che il cliente in data 15.10.2025 alle ore 01:50 si è connesso con il proprio dispositivo, identificato con codice univoco e il cui numero corrisponde a quello dichiarato dal cliente in sede di denuncia.

Precisa che il cliente non ha effettuato nessun accesso (*log-in*) per dare esecuzione alle operazioni, in quanto le stesse sono state autorizzate mediante ricezione delle notifiche *push* sull'APP e successivo inserimento del Codice PIN.

In particolare, rispetto a tale fase dispositiva, la documentazione prodotta in atti evidenzia: la notifica *push* inviata, risulta parlante, in quanto specifica l'importo, il beneficiario e la carta utilizzata per l'operazione da autorizzare; la notifica risulta regolarmente consegnata sul dispositivo certificato del cliente, con stato positivo e assenza di errori; il dispositivo utilizzato è sempre il medesimo anche nei giorni precedenti e successivi alle operazioni contestate; l'autorizzazione è avvenuta, dieci secondi dopo l'invio della notifica *push*, mediante l'inserimento del Codice PIN. Tutte e cinque le operazioni contestate risultano essere state autorizzate con le stesse modalità.

Sulla base delle evidenze prodotte, come affermato dall'intermediario, il sistema di autenticazione risulta conforme ai requisiti della SCA, con il concorso del fattore di possesso (ricezione e validazione della notifica *push* sul dispositivo certificato) e del fattore di conoscenza (inserimento del Codice PIN).

Quanto alla condotta delle parti e ai profili rilevanti ai fini della valutazione della sussistenza o meno della colpa grave, il ricorrente non ha fornito alcuna allegazione concreta circa le modalità con le quali sarebbero state autorizzate le operazioni fraudolente, limitandosi ad affermare che i pagamenti sono stati eseguiti in Romania e a ipotizzare un attacco *hacker* al proprio cellulare, senza produrre elementi documentali a sostegno di tale ricostruzione.

Nella denuncia presentata dal ricorrente in data 05.11.2025 la vicenda è descritta nei medesimi termini esposti nel ricorso, vale a dire disconoscendo gli addebiti, dichiarando di non aver effettuato le operazioni, di essere l'unico utilizzatore della carta, di non averla mai ceduta a terzi, di non aver mai comunicato il codice segreto a nessuno e di non aver ricevuto le consuete notifiche di addebito via e-mail.

L'assenza di qualsivoglia elemento circostanziale da parte del cliente, che si è limitato a disconoscere le operazioni senza indicare fatti idonei a supportare la sussistenza di una truffa particolarmente sofisticata, è stata contestata dall'intermediario, il quale ha altresì evidenziato che il ricorrente non ha mai denunciato né lo smarrimento né il furto della carta di pagamento o del dispositivo.

Secondo l'orientamento consolidato dei Collegi, in materia di utilizzi fraudolenti *online* non circostanziati - in cui l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute, il sistema di pagamento risulta conforme alla SCA e 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 cliente medesimo (cfr. Collegio di Milano, decisioni nn. 10876/2022 e 2036/2023).

In particolare, i Collegi sono unanimi nel ritenere che la mancata allegazione, da parte del cliente, del messaggio civetta (ovvero, per il *vishing*, del registro delle chiamate) debba determinare il rigetto del ricorso, in quanto non consente di verificare se il mittente/chiamante risulti riconducibile all'intermediario e, pertanto, se sia configurabile un legittimo affidamento dell'utente circa la genuinità del messaggio o della telefonata ricevuti.

Ritenuta pertanto nel caso di specie la colpa grave del ricorrente, il Collegio rileva che dall'esame degli atti emerge la sussistenza di un indice di anomalia riconducibile alla previsione di cui all'art. 8, lett. a), punto 2, del D.M. 112/2007, che segnala come caso di frode tre o più richieste di autorizzazione sulla stessa carta effettuate nelle 24 ore presso un medesimo punto vendita. Nel caso di specie, tre operazioni sono state effettuate in data 30.10.2025 verso lo stesso beneficiario nell'arco della medesima giornata. Si evidenzia altresì che la prima operazione è stata eseguita alle ore 01:56, ossia nel pieno della notte, circostanza che integra ulteriore anomalia rispetto all'operatività ordinaria del cliente.

Secondo l'orientamento condiviso dei Collegi, i principi del D.M. 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. I Collegi possono altresì valorizzare indici di frode ulteriori rispetto a quelli del D.M. 112/2007, in presenza di un'operatività anomala rispetto alle movimentazioni storiche del ricorrente (cfr. Collegio di Milano, decisione n. 12409/2023).

Una volta accertata la colpa grave del cliente, in presenza di tali indici di frode, la ripartizione della responsabilità con il prestatore dei servizi di pagamento 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 sulla negligenza tecnica dell'intermediario. La base di calcolo per la liquidazione della somma oggetto di eventuale condanna è costituita dall'intero ammontare degli

importi disconosciuti, senza esclusioni, procedendo a una distribuzione in concreto del concorso di colpa tra le parti.

D'altro canto, occorre evidenziare un ulteriore profilo di criticità dell'operatività dell'intermediario con riferimento alle notifiche di avvenuta esecuzione delle operazioni, atteso che per quattro delle cinque operazioni contestate — quelle eseguite tra il 30 e il 31.10.2025 — l'intermediario documenta l'invio dell'SMS di avviso, mentre per la prima operazione del 15.10.2025, stando alle evidenze prodotte dallo stesso intermediario, il messaggio non risulta recapitato al destinatario, con stato di esito negativo ("op_rejected").

Come noto, in relazione al servizio di SMS *alert*, il Collegio di Coordinamento ha chiarito che tra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di SMS *alert* o servizi assimilabili, da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene (cfr. Collegio di Coordinamento, decisione n. 8672/2024). La mancata attivazione del servizio, ovvero il suo mancato funzionamento, costituisce in via generale un profilo di responsabilità dell'intermediario, con la precisazione che in materia occorre adottare una interpretazione sostanzialistica del servizio di SMS *alert*, considerata la sua natura di presidio di sicurezza *ex post*, nel senso che 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. ex multis Collegio di Milano, decisione n. 7807/2022). Nel caso di specie, il mancato recapito del singolo SMS relativo alla prima operazione, eseguita in isolamento rispetto alle successive - queste ultime avvenute ben 15 giorni dopo - risulta suscettibile di valutazione ai fini della responsabilità dell'intermediario con riguardo alla possibilità che un tempestivo avviso avrebbe potuto indurre il cliente ad attivarsi per bloccare la carta prima dell'esecuzione delle ulteriori operazioni, con conseguente limitazione del danno.

Alla luce di tutte le considerazioni svolte, il Collegio ritiene che sussista la colpa grave del ricorrente in ragione della mancata allegazione di qualsiasi elemento circostanziale utile a ricostruire le modalità della frode, a fronte di un sistema di autenticazione risultato conforme ai requisiti della SCA. Tuttavia, in considerazione della presenza di indici di anomalia rilevanti — segnatamente tre operazioni verso lo stesso beneficiario nella medesima giornata del 30.10.2025 e un'operazione eseguita nel pieno della notte del 15.10.2025 — nonché del mancato recapito dell'SMS di avviso relativo alla prima operazione del 15.10.2025, circostanza che integra un profilo di responsabilità dell'intermediario suscettibile di incidere sul danno subito per le operazioni successive, il Collegio ritiene che la responsabilità debba essere ripartita tra le parti, applicando un concorso di colpa e condanna l'intermediario a rimborsare al ricorrente il danno corrispondente a due operazioni eseguite nelle 24 ore tra il 30 e il 31.10. 2025, per un importo complessivo di € 653,98, arrotondato ad € 654,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 654,00.

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 alla parte

ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE