

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) FORMAGGIA

Seduta del 07/05/2026

FATTO

Il ricorrente, nel ricorso depositato, afferma che in data 21 ottobre 2025 alle ore 12:48, riceveva una mail commerciale dell'intermediario che gli comunicava il nuovo funzionamento della sua carta di credito; che poco dopo, alle ore 13:14, riceveva un SMS dell'intermediario, con il quale gli veniva comunicato che la sua carta era stata sospesa a causa di n. 3 transazioni considerate "anomale" alla luce del suo uso abituale della carta; che le transazioni in questione erano state effettuate in data 21 ottobre 2025 (senza conoscerne l'ora) in favore di un intermediario (W) che opera trasferimento internazionale di denaro, rispettivamente per € 704,99, € 1,00 e di € 704,99, operazione, quest'ultima, bloccata dall'intermediario; che il cliente immediatamente provvedeva a contattare il servizio clienti dell'intermediario, scoprendo che un'ulteriore transazione di € 712,00 era stata effettuata il giorno prima, sempre a favore del medesimo intermediario (W); che a questo punto provvedeva a bloccare la carta e a chiedere il rimborso, cosa che il servizio clienti dell'intermediario gli riconosceva; che, contestualmente, l'intermediario provvedeva alla sostituzione della carta, con nuova registrazione e nuove credenziali; che in data 4 novembre 2025, riceveva la nuova carta e constatava che il rimborso era stato effettuato; che in data 14 novembre scopriva che il rimborso era stato revocato ed il servizio clienti gli riferiva che ciò era avvenuto poiché il cliente non aveva prodotto in tempo la documentazione richiesta per mail (che era finita nella cartella spam); che nello stesso giorno, sporgeva denuncia alle Autorità e rispondeva all'intermediario allegando quanto richiesto; che in data 17 novembre 2025, riceveva una mail dell'intermediario in cui veniva confermato il riaddebito e lo si invitava a provvedere per un reclamo ufficiale; che in data 18 novembre 2025, provvedeva a formulare il reclamo ufficiale; che in data 4 dicembre 2025 il reclamo veniva riscontrato negativamente poiché le transazioni erano

state portate a termine mediante autenticazione di tipo biometrico; che il cliente non aveva autorizzato le operazioni contestate, né aveva mai utilizzato né richiesto l'abilitazione del sistema biometrico, custodendo e utilizzando la carta con parsimonia, e non aveva cooperato, neppure involontariamente, alla truffa a suo danno.

Chiede il "rimborso delle cifre frodate".

L'intermediario, nelle controdeduzioni depositate, chiede il rigetto del ricorso rilevando che il cliente non avrebbe fornito alcun elemento utile al fine di ricostruire la vicenda, limitandosi ad affermare di non aver mai autorizzato le operazioni disconosciute; rileva che, in mancanza di elementi per ricostruire la vicenda, si poteva ritenere che il cliente, probabilmente raggirato, non avesse adempiuto con la dovuta diligenza i propri obblighi di custodia e protezione delle credenziali di sicurezza personalizzate del suo strumento di pagamento, comunicando username e password per accedere all'Area Riservata e il Codice OTP trasmesso sul cellulare per convalidare l'accesso, tramite APP, da un nuovo dispositivo mobile e impostarlo come principale e comunicando poi il Codice OTP SMS per convalidare l'attivazione della funzionalità di riconoscimento biometrico sul nuovo dispositivo certificato; che le operazioni erano state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto utilizzo del doppio fattore; che era evidente la colpa grave del cliente per aver omesso di adottare tutte le cautele necessarie a custodire i codici di accesso, partecipando, seppur inconsapevolmente, alla truffa a suo danno; che comunque l'intermediario aveva bloccato l'ultimo tentativo di pagamento, seppur in mancanza di un rischio di frode normativamente tipizzato, sospendendo la carta e inviando un apposito SMS al cliente, al fine di evitargli un danno più elevato.

Conclude chiedendo di rigettare integralmente il ricorso.

Il ricorrente replica che la natura truffaldina delle operazioni era dimostrata anche dal blocco effettuato dall'intermediario stesso circa le altre operazioni fraudolente; che il rimborso iniziale era stato revocato solo a seguito di un disguido burocratico, consistente nel ritardo di soli 5 giorni della documentazione necessaria causato dal fatto che la mail che lo informava dei documenti da inoltrare era nella casella spam; che le operazioni che non erano state bloccate presentavano le stesse anomalie (importi elevati e beneficiario estero) di quelle che, poco dopo, erano state bloccate; che le notifiche per autorizzare le operazioni erano state inviate ad un device diverso dal suo; che appariva contraddittorio il fatto che l'ultima delle notifiche di pagamento fosse stata inviata alle ore 13:19, sul device del truffatore, mentre l'SMS informativo del blocco fosse stato inviato alle ore 13:14, ossia 5 minuti prima, sul device del cliente; che non aveva in alcun modo autorizzato le operazioni.

Insiste nell'accoglimento del ricorso.

L'intermediario non ha depositato controrepliche.

DIRITTO

In fatto si osserva che il cliente, in sede di ricorso, non specifica la cifra che intende ottenere, ma si limita a chiedere il "rimborso delle cifre frodate". Alla luce del fatto che le operazioni contestate sono due e che esse ammontano rispettivamente a € 712,00 e a € 704,99, si può affermare che l'importo totale richiesto dal cliente con il presente ricorso sia di € 1.416,99. Si precisa che, per quanto emerge

dalla documentazione prodotta dall'intermediario, trattasi di due operazioni e-commerce, eseguite, rispettivamente, la prima in data 20.10.2025 alle ore 11:39 e la seconda in data 21.10.2026 alle ore 12:53.

È in atti la denuncia del cliente presentata in data 14 novembre 2025.

Anche nella denuncia il cliente descrive la truffa in termini molto scarni, limitandosi a menzionare i due pagamenti fraudolenti, il blocco della carta di credito e l'avvio della procedura di richiesta di rimborso.

Restano quindi lacunose le indicazioni sulle modalità con cui sarebbe avvenuta la truffa. Infatti, il cliente afferma semplicemente di essersi avveduto dei pagamenti contestati solo a seguito dei messaggi dell'intermediario e di non aver partecipato in alcun modo alla truffa.

Per contro, l'intermediario afferma che il cliente, seppur tacendo sulla vicenda, aveva subito una qualche forma di raggirio ed era evidentemente stato indotto a comunicare le proprie credenziali e i propri codici segreti al truffatore, partecipando, seppur inconsapevolmente, alla truffa a suo danno. Sostiene, infatti, che le operazioni contestate risultano correttamente autorizzate.

In diritto si osserva che, alla data dell'operazione contestata, trovava applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018; tale disciplina deve ritenersi integrata con le novità sui bonifici istantanei introdotte dal Regolamento 2024/886, in vigore dal 9-10-2025, con particolare riguardo all'obbligo di prevedere il servizio gratuito di verifica del beneficiario (cd. *Verification of Payee - VoP*). Le fonti normative regolanti la materia 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).

La prova di autenticazione delle operazioni, a carico dell'intermediario, rappresenta, in aderenza al dato normativo, un *prius* logico rispetto ad ogni ulteriore accertamento, compreso quello sulla colpa grave del cliente.

Secondo il consolidato orientamento dei collegi, solo nel caso in cui risulti pacifico o dimostrato che le operazioni contestate siano state compiute direttamente e interamente dal cliente (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), l'intermediario è esonerato dalla prova di autenticazione. Diversamente, ove vi siano operazioni non compiute interamente dal cliente, occorre l'accertamento della sussistenza della SCA (*Strong Customer Authentication*), con riferimento alle singole operazioni e ad ogni fase attraverso cui si sono realizzate, sempre con onere della prova a carico dell'intermediario. Infatti, secondo l'orientamento consolidato dei collegi, in aderenza al dato normativo (art. 10 del D.lgs. 11/2010), è necessario e sufficiente, ai fini dell'applicazione della PSD2, che il cliente neghi di aver autorizzato la transazione; l'autenticazione forte è dunque in particolare 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. In caso di difetto di piena prova sull'autenticazione, per ogni fase, delle transazioni disconosciute, la domanda deve essere accolta, posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente.

Resta il fatto che, comunque, non è configurabile una responsabilità oggettiva a carico dell'intermediario, sicché spetta al Collegio verificare se, in concreto, vi sia stata una responsabilità concorrente del PSP secondo le norme di diritto comune, qualora emerga dalla documentazione in atti un apporto causale dell'intermediario alla frode (quali, ad esempio, la mancanza o temporanea indisponibilità del numero verde del PSP, o il mancato rilievo di indizi di frode).

L'intermediario fornisce LOG ed altre evidenze e, negli atti, si riporta al loro contenuto, dandone in sostanza una spiegazione.

A questo proposito si rammentano i principi generali espressi dai collegi in merito alla valenza da attribuire alle informazioni presenti nei *log* prodotti dagli intermediari per provare l'autenticazione forte del cliente nelle operazioni di pagamento disconosciute (artt. 10, comma 1 e 10-bis del D.lgs. 11/2010), nei casi in cui dalla tracciatura informatica non risulti in modo esplicito uno dei fattori di autenticazione inseriti (conoscenza, possesso o inerenza). Tenuto conto che la PSD2 è tecnologicamente neutrale e non prevede 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 (Prestatore dei Servizi di Pagamento) nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione (*ex multis*, Collegio di Milano, decisione n. 6153/25 del 24/06/2025).

I collegi ritengono inoltre che eventuali dichiarazioni confessorie del cliente possano assumere valore di prova legale ai sensi dell'art. 2730 c.c..

Sulla base di tali principi consolidati nell'orientamento dei collegi, vanno esaminate le evidenze emergenti dai LOG e dagli argomenti esplicativi forniti dall'intermediario con riguardo alle varie fasi attraverso le quali si sono estrinsecate le operazioni qui contestate.

Emerge, innanzitutto, che - come già osservato - si è trattato di due operazioni e-commerce, eseguite, rispettivamente, la prima in data 20.10.2025 alle ore 11:39, per € 712,00 e la seconda in data 21.10.2026 alle ore 12:53 per € 704,99; entrambe risultano autorizzate con Browser, N.Push+ biometria.

Ora, con riferimento alle azioni antecedenti all'esecuzione delle operazioni contestate, si osserva che, quanto alla fase di *enrollment* e di *Log-in*, l'intermediario produce evidenza dell'*enrollment* di un dispositivo (X****C5G) effettuato poche ore prima della prima operazione contestata; il Log-in è avvenuto mediante l'inserimento dell'*username* e della *password* (PUSH, corrispondente a password statica, quale fattore di conoscenza), per accedere all'area personale, mediante l'inserimento del Codice OTP (SMS con OTP, quale fattore di possesso). Inoltre, nell'arco della medesima sessione, è stato inserito un secondo Codice OTP, per abilitare il riconoscimento biometrico sul device. La carta associata in fase di *enrollment* (n. ***953) corrisponde a quella presente negli estratti conto del cliente.

Sulla base delle suddette evidenze si può dunque affermare che la fase di Log-in è avvenuta mediante il corretto inserimento della *password*, quale fattore di conoscenza, e del Codice OTP, quale fattore di possesso.

Con riferimento agli SMS contenenti i Codici OTP utilizzati per l'accesso all'area riservata e per l'abilitazione del dato biometrico, dalle evidenze prodotte dall'intermediario risulta che l'SMS contenente il Codice OTP necessario per convalidare l'accesso all'area personale è stato inviato alle ore 8:35:11, che l'SMS contenente il Codice OTP necessario per abilitare il riconoscimento biometrico sul device è stato inviato alle ore 8:38:53, che entrambi gli SMS OTP sono stati inviati al numero ****938, che corrisponde a quello dichiarato dal cliente in sede di denuncia.

Con riferimento alle azioni antecedenti all'esecuzione delle operazioni contestate, si osserva che, quanto alla fase dispositiva, ciascuna operazione risulta essere stata autenticata tramite le notifiche push, corrispondenti al fattore di possesso, giunte sul device su cui è stato effettuato l'*enrollment* e l'utilizzo del dato biometrico, corrispondente al fattore di inerenza; le notifiche push risultano correttamente ricevute e lette dall'utente.

Deve pertanto ritenersi che l'intermediario abbia dimostrato, con le proprie produzioni, che le due operazioni siano state regolarmente autorizzate in presenza di SCA.

Resta da valutare la condotta delle parti per verificare la sussistenza di profili rilevanti indicativi della colpa.

Sul punto, è necessario fare le seguenti precisazioni: il cliente non riferisce alcun tipo di raggiro, assume di non aver comunicato a nessuno né le proprie credenziali né i codici riservati e di non aver mai chiesto l'abilitazione all'accesso tramite i dati biometrici; sostiene che il dispositivo sul cui è stato effettuato l'*enrollment* (X*****C5G) non è di sua proprietà e di non conoscerne il titolare; assume di essersi accorto dell'utilizzo fraudolento in quanto, alle ore 13:14 del 21 ottobre 2025, riceveva dall'intermediario un messaggio in cui gli veniva comunicato che, per motivi di sicurezza, la sua carta era stata sospesa a causa di alcune operazioni considerate "anomale" di cui gli si chiedeva conferma; nell'affermare di non aver in alcun modo collaborato alla truffa, ritiene che essa si sia verificata a causa delle lacune nel sistema di sicurezza dell'intermediario.

Le allegazioni del cliente sono smentite da quelle di controparte, fondate sulla documentazione prodotta, e ciò rende plausibile la sua versione secondo cui una spiegazione possibile alla vicenda sia quella per cui il cliente, il giorno prima, a seguito di un raggiro taciuto nel ricorso, abbia comunicato a qualcuno (rivelatosi truffatore) i dati necessari perché questi effettuasse l'*enrollment* su un nuovo dispositivo ed autorizzasse le operazioni contestate. In ogni caso, è proprio grazie al solerte intervento dell'intermediario che sono state segnalate le operazioni anomale ed è stata sospesa la carta, con impedimento a ulteriori operazioni non volute.

Secondo l'orientamento consolidato dell'ABF, il Collegio può valutare la mancata allegazione dei fatti, o la loro contraddittorietà, tra i vari elementi utili a formare il proprio convincimento circa la colpa grave del ricorrente (una volta verificata la sussistenza della SCA). In particolare, secondo l'orientamento dei Collegi, nelle contestazioni di utilizzi fraudolenti *on line* di strumenti di pagamento in cui a) l'intermediario ha offerto la prova dell'autenticazione delle transazioni disconosciute, b) il sistema di pagamento risulta conforme alla Strong Customer Authentication (SCA), c) non risultano indici di

anomalia delle operazioni e/o ulteriori elementi, in tali evenienze le mancate allegazioni del cliente sulle circostanze di fatto della frode, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme al contesto delle altre circostanze, circa la colpa grave del cliente.

Sulla questione del rimborso, il cliente lamenta il fatto che l'intermediario gli ha inizialmente riconosciuto il diritto al rimborso e, a seguito di un semplice disagio burocratico, dovuto ad un ritardo di 5 giorni nell'integrazione della documentazione necessaria, il rimborso sia stato dapprima riconosciuto e poi nuovamente addebitato.

Il cliente afferma che, a seguito del disconoscimento effettuato nella data stessa dell'ultima operazione (21 ottobre 2025), l'intermediario gli assicurava che la sua richiesta di rimborso sarebbe stata accolta; ma, per quanto emerge dagli allegati prodotti, il riscontro dell'intermediario era da disporre nelle more delle verifiche "salvo buon fine", cioè salvo riaddebito nel caso in cui le verifiche sulle operazioni disconosciute avessero fatto emergere la corretta autenticazione, come di fatto avvenuto.

Inoltre, l'intermediario, in data 22 ottobre 2025, informava il cliente che per riconoscere il diritto al rimborso – o meglio "per completare la valutazione della pratica" – il cliente avrebbe dovuto produrre ulteriore documentazione entro 15 giorni e presentare reclamo; al riguardo, il cliente afferma di non essersi accorto della mail, in quanto finita nella casella spam e che solo per tale ragione erano stati superati i giorni concessi.

Quanto al blocco, il cliente afferma di avere contattato l'intermediario in data 21 ottobre 2025, subito dopo aver avuto contezza delle operazioni fraudolente, e di averlo richiesto; l'intermediario dimostra di avervi proceduto tempestivamente, una volta contattato dal cliente, producendo evidenza da cui risulta che il blocco è stato disposto alle ore 14:21:22 dello stesso 21 ottobre 2025 (meno di un'ora e mezza dopo l'esecuzione della seconda operazione).

Dal complesso degli elementi emersi dai dati in atti, dai quali non si desumono indici di anomalia, risulta evidente che, a fronte di un puntuale e corretto comportamento dell'intermediario, il cliente è stato negligente e gravemente colpevole.

Ciò porta al rigetto del ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE