

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) PERON	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) PERON

Seduta del 31/03/2026

FATTO

Parte ricorrente riferisce al Collegio di aver ricevuto, in data 09/06/2025, una telefonata da un numero apparentemente riconducibile all'intermediario, dato che il display mostrava la denominazione dell'istituto. Durante la conversazione, un sedicente operatore l'informava di un presunto tentativo di frode in corso in Croazia per l'importo di € 160,00, convincendola della necessità di bloccare l'operazione. Indotta così in errore, parte ricorrente forniva i dati della propria carta di credito, inclusi scadenza e codice di sicurezza, e accettava una notifica tramite App convinta di interrompere l'azione fraudolenta. Successivamente, pur ricevendo due SMS con codici autorizzativi, parte ricorrente si insospettiva e interrompeva la chiamata senza comunicarli. Dopo aver proceduto autonomamente al blocco della carta e alla denuncia presso le Autorità, parte ricorrente veniva contattata dall'intermediario emittente N***, che confermava la truffa in atto e l'avvenuto blocco dell'applicazione. Contattando il numero verde, parte ricorrente apprendeva che era stata eseguita un'operazione fraudolenta di € 2.500,00, mentre una seconda da € 3.000,00 non era andata a buon fine. In un successivo contatto telefonico il 10/06/2025, emergeva inoltre che il ritardo nel blocco della carta da parte dell'intermediario avrebbe facilitato l'esecuzione delle transazioni illecite. Nonostante la

presentazione del modulo di disconoscimento in data 13/06/2025 e il successivo reclamo formale del 14/07/2025, l'intermediario riscontrava negativamente la richiesta di rimborso.

Parte ricorrente chiede quindi il rimborso di € 2.950,00, sottrattigli dal truffatore.

L'intermediario, ricostruiti i fatti, controdeduce che parte ricorrente è stata vittima di un attacco di ID *caller spoofing* e che le operazioni contestate sono state correttamente contabilizzate, registrate e autenticate, in quanto effettuate mediante l'inserimento delle credenziali corrette. Secondo l'intermediario, sussiste una colpa grave in capo alla parte ricorrente, la quale avrebbe fornito volontariamente al truffatore i dati e i codici necessari per autorizzare le transazioni. Infine, viene precisato che non sono stati riscontrati malfunzionamenti o intrusioni nei sistemi informatici dell'intermediario stesso.

L'intermediario chiede quindi in via principale il rigetto del ricorso in quanto infondato in fatto ed in diritto. In via subordinata, qualora fossero ravvisabili gli estremi di una responsabilità concorrente ex art. 1227 c.c., determinare l'entità degli importi da ripartirsi tra le parti. In via di estremo subordine, considerare che controparte dovrà comunque sopportare la perdita di € 50,00, come stabilita dall'art. 12, co. 3, D.lgs. 11/2010.

Parte ricorrente, richiamati i propri scritti, replica sostenendo che l'intermediario abbia tentato di invertire l'onere della prova a proprio favore. Specifica di non aver mai fornito i codici ricevuti via SMS né di aver mai risposto a tali messaggi, sottolineando come l'operazione sia stata processata con il protocollo "3D Secure" senza tuttavia fornire un riscontro adeguato su chi abbia effettivamente inserito i codici e tramite quale dispositivo. Secondo parte ricorrente, la semplice comunicazione dei dati della carta di credito non costituisce una violazione degli obblighi di diligenza, anche in considerazione del fatto che la carta risulta "non iscritta" al servizio "3D Secure2". Si ribadisce, infine, che la parte ricorrente è stata vittima di una sofisticata truffa nota come ID *caller spoofing*; pertanto, con le repliche depositate in data 22/03/2026, insiste nella domanda confermando quanto già rappresentato nel ricorso.

L'intermediario, controreplica affermando che parte ricorrente è stata vittima di ID *caller spoofing* e precisa che l'attuale mancata iscrizione della carta al servizio 3D Secure è dovuta esclusivamente alla sua estinzione. L'intermediario nega qualsiasi inversione dell'onere della prova e richiamando le proprie precedenti difese, insiste per il rigetto del ricorso.

DIRITTO

La fattispecie in oggetto concerne la richiesta di rimborso di parte ricorrente del complessivo importo di € 2.950,00, sottratto a seguito di un'operazione fraudolenta di pagamento online eseguita in data 09/06/2025 alle ore 19:47.

L'operazione contestata è disciplinata dal D.lgs. 27/01/2010 n. 11 di recepimento della Direttiva sui servizi di pagamento (Direttiva 2007/64/CE del 13 novembre 2007) e del relativo Provvedimento attuativo della Banca d'Italia del 05.07.2011. Come è noto, i principi fissati da tale impianto normativo, in materia di *strong customer authentication* (SCA), fissano due passaggi ineludibili che attengono al piano degli oneri probatori:

a) è l'intermediario a dover provare (oltre all'insussistenza di malfunzionamenti) l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute, avendo presente che l'autenticazione forte (SCA) è richiesta sia nella fase di accesso al conto / enrollment dell'applicazione / registrazione della carta sul wallet, sia nella fase di esecuzione delle singole operazioni; inoltre la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza, inerenza, possesso. Tali elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse;

b) è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento. In quest'ambito dunque, costante giurisprudenza arbitrale, ritiene che

l'eventuale negligenza del cliente possa solo venire in rilievo solo allorquando l'intermediario abbia fornito la prova piena della scrupolosa osservanza del sistema di SCA e della predisposizione di congegni di alert. Peraltro secondo l'orientamento dei Collegi, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP. Resta ovviamente ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto agli obblighi di cui all'art. 7 con dolo o colpa grave, ai sensi dell'art. 12 D.lgs. 11/2010. Nel caso in esame dalle dichiarazioni rese dalla parte ricorrente risulta che la stessa abbia comunicato al frodatore i numeri finali della carta di credito, la data di scadenza e il codice di sicurezza. In seguito a tale evento, parte ricorrente riceveva una notifica push tramite l'applicazione che provvedeva ad accettare nell'erronea convinzione di bloccare l'operazione fraudolenta in corso.

Poiché, dunque il concorso causale dell'utente è avvenuto parzialmente in fase dispositiva/autorizzativa, la transazione non può intendersi per ciò solo autorizzata e il Collegio passa a esaminare il sistema di autenticazione forte dell'intermediario.

In proposito, l'intermediario afferma che l'operazione è stata correttamente contabilizzata, registrata e autenticata, sostenendo che l'operazione in parola abbia avuto seguito attraverso il servizio "3D Secure" a due fattori, pienamente conforme ai requisiti normativi della "SCA - Strong Customer Authentication". L'intermediario precisa, infatti, che l'autenticazione è avvenuta mediante l'utilizzo dei dati statici della carta, quali il numero di PAN, il nome e cognome, la scadenza e il codice CVV, unitamente al codice OTP ricevuto dalla parte ricorrente via SMS e alla password statica Key6.

Il Collegio constata che dai log prodotti risulta che l'operazione contestata è stata autenticata tramite OTP ricevuto via SMS sul numero di cellulare di parte ricorrente (fattore di possesso) e Key 6, password statica (fattore di conoscenza). Alla luce delle evidenze in atti, il Collegio conclude che il sistema predisposto dall'intermediario è conforme ai criteri previsti per l'autenticazione forte a "due fattori", il che, in conformità con l'orientamento consolidato dell'Arbitro, induce a ritenere, in assenza di ulteriori indici di anomalia dell'operazione, che parte resistente abbia assolto all'onere di provare l'adempimento degli obblighi su di essa gravanti ai sensi dell'art. 8 del D.lgs. n. 11/2010, (cfr. *ex multis* Collegio di Milano, decisione n. 8294/2022).

Il Collegio, ritenuta provata la SCA, procede a verificare se parte ricorrente abbia agito con colpa grave e se vi sia stato un concorso di colpa da parte dell'intermediario.

Parte ricorrente riferisce di aver ricevuto in data 22/03/2025 una chiamata dal numero 05***, nel corso della quale il soggetto interlocutore si qualificava come operatore dell'intermediario. Afferma inoltre che, nel corso della conversazione, apprendeva di un tentativo di frode in corso dalla Croazia per € 160,00, e le veniva richiesto il suo intervento per bloccarlo. In questo contesto, parte ricorrente comunicava al truffatore i numeri finali della carta di credito, la scadenza e il codice di sicurezza; inseguito riceveva i codici OTP via SMS senza tuttavia comunicarli al malintenzionato. Si ritiene dunque sussistente una condotta colposa posta in essere dalla parte ricorrente nella causazione della frode.

Tuttavia, il Collegio constata che il numero della chiamata corrisponde a un recapito dell'intermediario per le comunicazioni all'estero, la fattispecie è dunque qualificabile come ID *caller spoofing*, in grado di tradire l'affidamento del destinatario. In proposito si ricorda che l'orientamento costante dell'ABF, riconduce questo tipo di truffa come fattispecie insidiosa in termini di supposta genuinità dei contatti. Siffatta situazione è considerata come sintomo di una imperfezione nella sicurezza del sistema approntato dall'intermediario, in grado di giustificare un concorso di colpa fra le parti con il riconoscimento a favore del ricorrente dell'importo, equitativamente calcolato, di € 983,00 (cfr. *ex multis* Collegio di Roma, decisioni n. 10893/2025 e n. 2396/2025).

Infine, si ricorda che per i casi di utilizzi fraudolenti *on line*, la richiesta di applicazione della franchigia formulata dall'intermediario non può accogliersi in «quanto la stessa è prevista in ipotesi di 'utilizzo

indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita' (art. 12, co. 3 d.lgs. n.11/2010)» (così Collegio di Coordinamento, decisione n. 22745/2019).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 983,00.

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