

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) FORMAGGIA

Seduta del 24/02/2026

FATTO

Il ricorrente, nella denuncia allegata al ricorso, descrive la vicenda (rimasta nel ricorso estremamente criptica) affermando che alle ore 16:46 del 13/09/2025 riceveva una telefonata dal numero ***789 da un soggetto che si presentava come operatore dell'intermediario convenuto; che con la chiamata gli veniva riferito di tentativi di bonifici tramite un dispositivo all'estero; di aver chiuso la telefonata ma di venir ricontattato dall'operatore dal numero ***7921 che confermava i tentati bonifici e chiedeva al cliente se voleva bloccarli; di aver dunque fornito il codice cliente e solo due cifre del PIN; che, dopo aver chiuso la chiamata, si rendeva conto di una serie di operazioni che avevano azzerato il conto e dell'attivazione di un prestito di € 30.000,00 da lui non autorizzato; che aveva ricevuto il rimborso dei movimenti fraudolenti della carta di credito e annullato il finanziamento; che essendo rimasto un mancato rimborso relativamente al bonifico immediato di € 1.640,00, in relazione al quale l'intermediario aveva motivato la colpa del cliente, ne chiedeva la restituzione.

Chiede quindi, imputando alla banca "falle per quanto riguarda la sicurezza informatica", l'intervento dell'Arbitro "per avere la restituzione del bonifico di € 1.640,00".

L'intermediario, nelle controdeduzioni depositate, afferma che l'operazione contestata è stata autorizzata con doppio fattore di autenticazione, nel rispetto della normativa di cui al d.lgs. 11/2010, come emerge dalla documentazione prodotta, ove è evidenziato che il 13/09/2025 è stata attivata l'app della banca sul dispositivo del truffatore, così rendendo "non attivo" il token precedentemente installato sul dispositivo del cliente; che l'installazione dell'app avviene mediante doppio fattore di autenticazione

e può essere andata a buon fine solo con la conoscenza e l'inserimento dei codici da parte del cliente; che le disposizioni contestate sono state autorizzate dal nuovo dispositivo, in seguito alla inopinabile cooperazione colpevole con il truffatore; che la banca ha dato tempestivamente seguito alla richiesta di *recall* del bonifico contestato, tuttavia senza esito; che trattandosi di bonifico istantaneo, la banca non poteva in ogni caso annullare il ricorso, come riportato all'interno delle condizioni contrattuali; che il cliente ha ricevuto la notifica *alert* dell'installazione dell'app, a seguito della quale avrebbe potuto e dovuto prendere immediati contatti con la banca, impedendo così il procrastinarsi della truffa in proprio danno. Ha quindi sottolineato la responsabilità in capo al ricorrente per aver tenuto un comportamento gravemente colposo e contrario agli obblighi di correttezza e diligente custodia delle proprie credenziali di accesso, non giustificabile dalla chiamata ricevuta da un numero apparentemente riconducibile alla banca in quanto è ampiamente risaputa l'esistenza di app che permettono di far visualizzare un diverso nome del chiamante, ed in presenza oltretutto di un servizio della banca che permette di verificare tramite apposito pulsante l'effettiva provenienza delle chiamate e di informazioni e istruzioni date alla clientela su tali fenomeni truffaldini.

Ha quindi concluso chiedendo il rigetto dell'infondato ricorso.

Il cliente non ha depositato repliche.

DIRITTO

La controversia riguarda una operazione di bonifico eseguita il 13/09/2025 alle ore 17:28 dell'importo di € 1.640,00.

Secondo le dichiarazioni del cliente, espresse in particolare dalla denuncia allegata al ricorso, e per quanto evincibile dalle evidenze prodotte dall'intermediario, il cliente è stato vittima di una truffa che ha comportato vari movimenti fraudolenti attraverso al sua carta di credito, tutti annullati e rimborsati dall'intermediario, ad eccezione del bonifico immediato di € 1.640,00; l'intermediario ha negato il rimborso di tale bonifico che, regolarmente autorizzato e autenticato, era riferibile al comportamento gravemente colposo del cliente e contrario agli obblighi di correttezza e diligente custodia delle proprie credenziali di accesso, non giustificabile dalla chiamata asseritamente ricevuta da un numero apparentemente riconducibile alla banca, a fronte degli *alert* ricevuti e delle informazioni e istruzioni date alla clientela sui fenomeni truffaldini.

Alla data delle operazioni descritte dal cliente e del bonifico oggetto della presente controversia 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. In particolare, 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, l'autenticazione forte 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. I due fattori richiesti 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 afferma che l'operazione in questione è stata autorizzata con doppio fattore di autenticazione, nel rispetto della normativa di cui al d.lgs. 11/2010, come emerge dalla documentazione prodotta, ove è evidenziato che il 13/09/2025 è stata attivata l'app della banca sul dispositivo del truffatore, così rendendo "non attivo" il token precedentemente installato sul dispositivo del cliente; che l'installazione dell'app avviene mediante doppio fattore di autenticazione ed era andata a buon fine grazie alla conoscenza e all'inserimento dei codici da parte del cliente; che le disposizioni contestate sono state autorizzate dal nuovo dispositivo, in seguito alla inopinabile cooperazione colpevole con il truffatore; che l'operazione era stata correttamente contabilizzata, registrata e autenticata.

In particolare, afferma che le fasi attraverso cui si è svolta l'operazione risultano autorizzate e autenticate. Fornisce LOG ed altre evidenze e, negli atti, si riporta al loro contenuto, dandone in sostanza una spiegazione coerente.

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.

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

Dalle evidenze e relativi Log esplicativi risulta, con riferimento alla fase di *enrollment* della nuova App Ing in data 13.9.2025 su nuovo dispositivo Smartphone, che vi è stato inserimento alle 17:08:55 del PIN (fattore di conoscenza) senza nessun errore, e invio dell'OTP (fattore di possesso) al numero di telefono che coincide con quello indicato dal ricorrente come proprio nella denuncia.

Con riferimento all'accesso in app antecedente all'esecuzione dell'operazione contestata, l'intermediario riferisce di un accesso eseguito alle ore 17:21 del 13/09/2025; produce evidenze, in merito all'inserimento dello *smartcode* (fattore di conoscenza) ("*meansType:MPIN*") alle ore 17:11 del 13 settembre 2025 e dell'identificativo dell'APP installata fraudolentemente su altro dispositivo (fattore di possesso).

Viene pertanto completata l'attivazione dell'app sul nuovo dispositivo così identificato.

L'intermediario produce inoltre evidenza dell'email di *alert* inviata al ricorrente in merito all'avvenuta attivazione dell'app: alle ore 17:09:54.

Con riferimento alle operazioni in oggetto, con particolare riguardo a quella in contestazione, l'intermediario afferma che l'operazione, dopo l'inserimento dei dati relativi al bonifico, è stata autenticata tramite *tap* in app e digitazione del codice segreto; al riguardo l'intermediario produce evidenze, dalle quali è possibile riscontrare l'inserimento del codice segreto (fattore di conoscenza) e del codice identificativo dell'app installata sul dispositivo del truffatore (appid 584d***; fattore di possesso).

L'intermediario ha inoltre prodotto evidenza dell'email di *alert* inviata per l'esecuzione del bonifico alle 17:28:22.

Sulla base delle evidenze prodotte, risulta dunque appurato che l'operazione in questione è stata autenticata con la compresenza dei due fattori di possesso e di conoscenza, e che era intervenuta in proposito una notifica da parte dell'intermediario.

Mancano evidenze di responsabilità a carico dell'intermediario, in assenza di indici di anomalie o di frode, in presenza di evidenze sull'invio di *alert* e sul suo tentativo di *recall* del bonifico, in assenza di contestazioni ed evidenze sul superamento del plafond, ed a fronte, peraltro, della mancata produzione da parte del ricorrente di evidenze in merito alla chiamata asseritamente ricevuta con conseguente impossibilità di verifica della sua eventuale riconducibilità all'intermediario resistente.

Per tutto quanto osservato il ricorso va respinto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE