

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	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) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) FORMAGGIA

Seduta del 17/03/2026

FATTO

La ricorrente, nel ricorso depositato, afferma che in data 23/09/2025 riceveva un SMS riguardante un pagamento sospetto che sembrava provenire dall'intermediario in quanto appariva in coda a un *thread* genuino; che chiamava il numero indicato nell'SMS; che dopo aver ascoltato una voce registrata identica a quella del numero verde dell'intermediario, interloquiva con un soggetto che si presentava come operatore dell'intermediario, il quale ribadiva sussistesse un tentativo di pagamento sospetto e attivava una asserita procedura antifrode, inducendolo pertanto a confermare dati sensibili (nome, data di nascita, telefono, numero e CCV della carta di debito) e ad autorizzare pagamenti per un totale di € 13.797,50, nonostante non avesse comunicato alcun OTP; che dopo ogni conferma riceveva un messaggio di asserito blocco delle operazioni; che non aveva ricevuto alcun *alert* automatico nonostante l'elevato numero di operazioni in breve tempo; che aveva presentato denuncia presso le Autorità e reclamo all'intermediario in data 16/10/2025, riscontrato negativamente.

Chiede "il rimborso della somma di 13.797,50 oggetto del reclamo ... che mi è stata sottratta per mezzo di un sofisticato raggio, in quanto i pagamenti non sono stati autorizzati con il mio consenso".

L'intermediario, nelle controdeduzioni, sostiene che il ricorso era irricevibile in quanto le operazioni contestate (n. 3 addebiti su carta di debito, n. 2 bonifici istantanei e n. 1 *MoneyB****) risultano correttamente autenticate in-APP tramite il dispositivo mobile in esclusivo possesso del cliente ed unicamente associato al suo conto, in conformità con i requisiti previsti dalla c.d. *Strong Customer*

Authentication ; che non risultava alcuna intrusione all'interno del conto corrente del cliente né il cliente aveva denunciato lo smarrimento o il furto del proprio *smartphone*; che lo stesso cliente -in sede di denuncia, nel ricorso introduttivo e nelle comunicazioni con il Servizio Clienti- aveva ammesso di aver comunicato al frodatore i propri dati personali e gli estremi dello strumento di pagamento, oltre ad aver autorizzato autonomamente tutte le operazioni oggetto di contestazione; che il caso in esame esulava pertanto dal regime di protezione previsto dal D. Lgs. n. 11/2010; che le operazioni erano state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali; che sussisteva la colpa grave del cliente in quanto lo stesso aveva eseguito le azioni che di volta in volta gli venivano indicate dal frodatore; che, a fronte delle richieste palesemente irragionevoli avanzate dal frodatore, il cliente avrebbe dovuto fin da subito provvedere a contattare la banca attraverso i canali di comunicazione ufficiali; che, riguardo ai messaggi "civetta" asseritamente ricevuti dal cliente, negli *screenshot* prodotti non compare il numero telefonico riconducibile alla banca, bensì la sola denominazione, con conseguente irrilevanza probatoria degli stessi; che in nessuno degli SMS riportati è presente l'indicazione della data in cui la supposta frode si sarebbe verificata ed il loro contenuto, oltre a presentare evidenti errori ortografici e sintattici, era incoerente e illogico rispetto alla prassi operativa della banca; che l'intermediario si era tempestivamente attivato per il recupero delle somme, inoltrando per ciascuna operazione una richiesta di richiamo interbancario (*recall*) all'intermediario beneficiario, ma era risultata impossibile la restituzione degli importi contestati.

Ha concluso chiedendo "il rigetto *in toto* del ricorso in quanto infondato in fatto e in diritto per le ragioni di cui in narrativa".

Il cliente, nelle repliche, conferma quanto affermato in ricorso e ribadisce di essere stato vittima di una complessa condotta fraudolenta; che l'inserimento del PIN e la conferma delle notifiche *push* rappresentano atti materiali compiuti ma non comportano automaticamente la comprensione della reale natura delle operazioni e la consapevolezza delle conseguenze economiche; di non aver mai comunicato alcun dato del suo conto o della propria carta di debito a terzi; che il frodatore, per indurlo a fidarsi, comunicava egli stesso tutti i dati della sua carta di debito, come da integrazione di denuncia; che il servizio assistenza clienti dell'intermediario non era immediatamente accessibile tramite contatto telefonico; che l'intermediario avrebbe dovuto valutare la coerenza delle operazioni con il profilo del cliente, considerando che le n.6 operazioni fraudolente in APP di pagamento per un totale di quasi 1.400,00 € erano avvenute nell'intervallo di tempo di soli 30-35 minuti e avrebbe dovuto attivare presidi di allerta in presenza di operazioni anomale per importo o frequenza; che, nel contesto della frode, le notifiche *push* e le richieste di conferma non erano state percepite come segnali di allarme bensì come passaggi coerenti con le istruzioni ricevute dall'interlocutore; che gli *alert* ricevuti durante la telefonata con il truffatore sono *alert* automatici che si attivano anche in presenza di telefonate effettuate a numeri conosciuti dal cliente.

Insiste per l'accoglimento del ricorso.

L'intermediario, nelle controrepliche, si riporta alle precedenti deduzioni precisando che le modalità fraudolente prospettate dal cliente difettano di quei requisiti di elevatissima sofisticazione tecnologica in presenza dei quali, secondo l'orientamento consolidato dell'Arbitro Bancario Finanziario, possono eccezionalmente giustificarsi l'elisione dell'efficacia dei presidi di sicurezza della banca e l'insorgenza di un affidamento scusabile in capo all'utente; che il comportamento del cliente, il quale ha personalmente autorizzato tutte le operazioni mediante *Strong Customer Authentication* sul proprio dispositivo, integra gli estremi della colpa grave, ai sensi degli artt. 7 e 12 del D.lgs. 11/2010 e conformemente alla costante giurisprudenza dell'Arbitro Bancario Finanziario; che l'iniziativa assunta dal cliente di contattare un'utenza del tutto estranea all'intermediario integra un comportamento gravemente imprudente, rilevante ai fini della qualificazione della colpa grave; che dalle dichiarazioni del cliente emerge in modo inequivocabile che tutte le disposizioni di pagamento sono state consapevolmente disposte e autorizzate dallo stesso, seppur verosimilmente indotto da un soggetto

terzo, che sono state effettuate tramite APP e dispositivo ad essa associato, senza alcuna anomalia tecnica o compromissione esterna; che nessuna norma imponeva, nella presente fattispecie, l'interruzione o il blocco delle operazioni contestate, in assenza di evidenti anomalie; che peraltro, il cliente, a fronte di un saldo inizialmente insufficiente, si era attivato per rifinanziare il conto corrente mediante l'esecuzione di bonifici, su sollecitazione del soggetto ingannatore, così consentendo la prosecuzione delle operazioni illecite; che il sistema di notifiche *push*, funzionalmente equivalente agli SMS *alert*, aveva operato regolarmente, inviando al dispositivo personale del cliente tutte le richieste di autorizzazione relative alle singole operazioni, fornendo dettagli completi e permettendo la piena identificazione delle stesse; che i *log* informatici prodotti attestano in modo incontrovertibile l'avvenuto invio e la ricezione delle notifiche *push*, che l'APP aveva inoltre attivato un *overlay anti-vishing* volto ad allertare l'utente del rischio di frode telefonica e a invitarlo a contattare immediatamente la banca tramite canali ufficiali, che il cliente aveva deliberatamente ignorato tali avvisi, eludendo consapevolmente un presidio di sicurezza.

L'intermediario insiste per il rigetto del ricorso.

DIRITTO

In fatto si sottolinea che le operazioni disconosciute sono complessivamente n. 6, sono state effettuate il 23/09/2025 tra le 23.04 e le 23.39, assommano ad un importo complessivo di Euro 13.797,50. Nello specifico trattasi, in ordine, di un trasferimento peer-to-peer (denominato MoneyB***), di tre pagamenti con carta e di due bonifici.

Nella denuncia del cliente presentata in data 24.9.2025 e nella integrazione di denuncia in data 9.10.2025, il ricorrente descrive i fatti secondo una narrativa per lo più in linea con quella degli atti rassegnati nella presente procedura. In particolare, per quel che rileva, dalle dichiarazioni rese dal cliente nella denuncia risulta che lo stesso confermava tutti i n. 6 pagamenti disconosciuti –inizializzati dal frodatore– in APP, credendo che servissero a fermare una frode a suo danno. Tuttavia il ricorrente, nelle repliche, insiste nell'affermazione di non aver mai comunicato alcun dato del suo conto o della propria carta di debito a terzi e che il frodatore, per indurlo a fidarsi, gli aveva comunicato egli stesso tutti i dati della sua carta di debito; si tratta di dichiarazioni che non risultano presenti nell'integrazione di denuncia.

Alla data delle operazioni non era ancora in vigore l'obbligo di *Verification of Payee* introdotto dal Regolamento UE 2024/886 in materia di pagamenti istantanei.

Trovava invece 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.

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. 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 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.

E 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).

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.

L'intermediario fornisce evidenze e LOG esplicativi, riportandosi, negli atti, al loro contenuto.

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..

Sulla base di tali principi consolidati nell'orientamento dei collegi, vanno dunque 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.

Pertanto, si procede ad esaminare la prova di autenticazione delle operazioni ai sensi del D. Lgs. 11/2010, con riguardo alle varie fasi attraverso le quali si sono estrinsecate le operazioni qui contestate, tendo conto delle evidenze prodotte, degli elementi emergenti dai LOG, degli argomenti esplicativi forniti dall'intermediario.

Se ne ricava che le operazioni disconosciute venivano eseguite all'interno di n. 6 sessioni *in-APP* avviate dal cliente il giorno 23/09/2025 rispettivamente alle ore 23:01, 23:07, 23:15, 23:19, 23:29 e 23:32 tramite SCA, ovvero mediante l'inserimento dell'ID biometrico (fattore di inerenza) e l'utilizzo dell'APP installata sul dispositivo mobile personale del cliente associato in via esclusiva al suo conto (fattore di possesso).

Nel dettaglio, con riferimento alle azioni precedenti all'esecuzione delle operazioni contestate, si osserva, quanto alla fase di accesso all'APP, che la prova della sussistenza della SCA è data dal fatto che i *login* sono avvenuti tramite inserimento delle credenziali biometriche del cliente (fattore di inerenza – *login _whith_refresh_token*) nella APP installata sul dispositivo mobile associato in via esclusiva al conto del cliente (avente device token *0017-fattore di possesso - *MFA_OSC*) dal 21/09/2025.

Con riferimento alle operazioni contestate, si osserva, quanto alla prima operazione (peer-to-peer) di *MoneyB**** (sistema di trasferimento istantaneo di denaro tra utenti dell'intermediario), che essa risulta essere stata autorizzata dal *device* personale associato al conto del cliente alle ore 23:04 del 23/09/2025 in seguito a immissione del codice PIN di conferma dispositivo, quale fattore di conoscenza (- *PIN Validation*) e conferma di *push*, (*RESULT - Transaction Successfully Certified*), quale fattore di possesso.

Quanto alle n.3 operazioni tramite carta di debito, esse risultano essere state autorizzate da dispositivo mobile in uso al cliente alle ore 23:11, 23:29 e 23:31 del 23/09/2025 in seguito a convalida delle relative notifiche *push* di pagamento inviate all'interno dell'APP installata sul dispositivo mobile *device_token* *0017 associato univocamente al conto del cliente (*Transaction Successfully Certified*), quale fattore di possesso, e tramite fattore biometrico, quale fattore di inerenza (come da all.9, in corrispondenza della dicitura *AUTH_METHOD – KB*). Le operazioni sono state autenticate previo inserimento dei dati della carta di pagamento sul sito *web* di riferimento (*Trans Condition - El Comm Secure w/cert e El Comm Stored*). Il ricorrente non ha mosso contestazioni specifiche sulle suddette evidenze prodotte.

Quanto alle n.2 operazioni di bonifico istantaneo, esse risultano autorizzate dal *device* associato al conto del cliente rispettivamente alle ore 23:35 e 23:39 del 23/09/2025 in seguito a immissione del codice PIN di conferma dispositivo, quale fattore di conoscenza (- *PIN Validation*) e convalida delle relative notifiche *push* all'interno dell'APP installata sul dispositivo mobile *device_token* *0017 in uso al cliente, quale fattore di possesso (- *Transaction Successfully Certified*).

Appurata la sussistenza della SCA, resta da considerare la condotta delle parti per valutare la sussistenza della colpa.

Nella specie, si ritiene che la condotta del cliente sia connotata da colpa grave. Questi invero, ingenuamente e imprudentemente, si è lasciato convincere a compiere una serie ravvicinata di operazioni e a fornire dati personali secondo una tecnica truffaldina ormai così diffusa e nota da aver perso il carattere dell'insidiosità, e ciò nonostante i messaggi civetta riportassero errori e imprecisioni che avrebbero dovuto almeno suscitare la sua attenzione e insospettirlo. Inoltre, risulta dalle evidenze prodotte che la sua chiamata (effettuata dal cliente stesso) non era riconducibile al numero dell'intermediario. Vi sono evidenze dimostrative che il cliente ha consapevolmente ignorato più volte i *disclaimer* di sicurezza, sottraendosi così a un presidio di tutela espressamente volto a prevenire condotte fraudolente (come risulta dai *log* - recanti l'indicazione *vishing.canceled*). Ed ancora, vi sono evidenze attestanti la ricezione di *alert* durante la telefonata con il truffatore (ai quali impropriamente il ricorrente non attribuisce rilevanza in quanto asseritamente automatici); *alert* peraltro ritenuti dalla giurisprudenza non necessari in presenza di una unica operazione o di più operazioni avvenute, come quelle in esame, in uno spazio molto ravvicinato. Per contro, si tiene esente da colpe concorrenti la condotta dell'intermediario, considerato che risulta avviato il tentativo di *recall* per i n. 2 bonifici contestati, che non risulta il superamento del plafond di spesa né risultano contestazioni del cliente su tale circostanza e sul blocco dello strumento di pagamento, che non risultano gli indici di anomalia o rischio di frode normalmente considerati dai collegi come rilevabili dagli intermediari.

Per tutto quanto rilevato il ricorso non può essere accolto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE