

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) MODICA

Seduta del 26/05/2026

FATTO

Il cliente afferma di avere ricevuto una chiamata da numero riconducibile all'intermediario alle ore 18.10 dell'8/08/2025 con cui un sedicente operatore gli segnalava transazioni sospette effettuate in *home banking*; insospettito, interrompeva la comunicazione e richiamava il numero, constatando che l'utenza era quella ufficiale. Poco dopo, riceveva una nuova chiamata da altro numero, durante la quale il sedicente operatore lo invitava ad accedere al conto per verificarne la movimentazione. Veniva quindi contattato dal numero riconducibile al Comando dei Carabinieri, da un soggetto che si qualificava come Carabiniere e gli confermava quanto riferito dal sedicente operatore e lo invitava a seguire le istruzioni del sedicente operatore. Successivamente riscontrava l'esecuzione di n. 1 transazione di € 4.900,00 in favore di esercente M* e di n. 1 operazione di pagamento a favore di un conto acceso presso intermediario B*, anch'essa non autorizzata, per € 4.900,00. Presentava denuncia presso le Autorità e reclamo all'intermediario in data 05/11/2025, che veniva riscontrato negativamente. Segnala *che* le operazioni sconosciute si presentano come sospette per elevato importo, rispetto alle operazioni normalmente disposte, e in virtù del destinatario che risulta sconosciuto.

Chiede la restituzione di € 9.800,00.

L'intermediario, afferma che le operazioni contestate risultano correttamente autenticate in-APP tramite il dispositivo mobile in possesso del cliente e associato al suo conto, nel rispetto dei requisiti SCA; che al cliente, vittima di *vishing*, deve imputarsi la colpa grave del cliente in quanto ha aderito integralmente alle istruzioni impartite dal frodatore, provvedendo ad alimentare il proprio conto corrente presso l'intermediario con somme di rilevante entità e a disporre nonché autorizzare personalmente,

mediante l'APP associata al proprio dispositivo, le operazioni di pagamento oggetto di contestazione. Sulla base delle indicazioni fornite dal truffatore, il cliente disponeva n. 15 bonifici da € 990,00 ciascuno dal proprio conto presso l'intermediario T* verso il proprio conto presso l'intermediario convenuto, alimentandolo per un importo complessivo di € 14.850,00. L'alimentazione preventiva del conto presso la convenuta ha rappresentato la condizione necessaria affinché le successive operazioni contestate potessero essere eseguite, ponendosi quale antecedente causale diretto del pregiudizio economico subito. Inoltre, il cliente non ha prodotto alcun elemento probatorio idoneo a suffragare le proprie allegazioni. Precisa di avere prontamente attivato la procedura di *recall* prevista dalle prassi interbancarie, inoltrando formale richiesta di richiamo del bonifico istantaneo all'istituto beneficiario. L'istituto beneficiario non forniva tuttavia alcun riscontro alla suddetta richiesta. Successivamente, a seguito della proposizione del ricorso all'ABF, attivava una seconda richiesta di *recall* in data 27/01/2026. In data 02/02/2026, la banca beneficiaria comunicava che i fondi erano stati immediatamente prelevati dal conto del soggetto beneficiario a seguito della frode e che non risultava possibile procedere alla restituzione delle somme. Aggiunge che, anche nella denegata ipotesi in cui le operazioni oggetto di ricorso dovessero essere considerate non autorizzate, debba essere applicato quanto previsto dall'art. 12, co. 4 del D. Lgs. 11/2010, e che pertanto il cliente debba sopportare la perdita derivante dalle operazioni di pagamento per l'importo pari a € 9.800,00, che lo stesso ha colpevolmente autorizzato.

Chiede il rigetto del ricorso.

Il cliente, replica che entrambi i numeri telefonici dai quali sono pervenute le telefonate truffaldine corrispondevano ad utenze ufficiali; che il sistema di *Internet Banking* dell'intermediario si è dimostrato gravemente permeabile; che l'intermediario non prova di avere informato con SMS *Alert* il cliente della truffa in corso né delle operazioni sospette dell'08/08/2025.

Insiste nella domanda.

L'intermediario controreplica che il mascheramento dell'utenza costituisce una tecnica di agevole realizzazione, operante su infrastrutture di rete esterne e non incidente sui sistemi dell'intermediario, sicché non è circostanza idonea, di per sé, a giustificare l'esecuzione di operazioni dispositive consapevolmente autorizzate dall'utilizzatore mediante i propri strumenti di autenticazione. Precisa di avere dimostrato l'invio di notifiche *push* in tempo reale come equivalenti ai servizi di SMS *alert*, nonché il corretto inoltro delle medesime al dispositivo del cliente. Insiste per il rigetto del ricorso.

DIRITTO

Il cliente disconosce due operazioni eseguite a valle di una truffa e chiede la restituzione dei relativi importi. Si tratta, in particolare, di un addebito su carta di debito e di un bonifico istantaneo disposti l'8/08/2025 rispettivamente alle ore 18.57 e 19.06 per il complessivo importo di € 9.800,00.

In sede di denuncia versata in atti, il cliente ha dichiarato chiaramente di aver effettuato personalmente l'operazione di bonifico di € 4.900,00 delle ore 19.06.

In casi del genere, quando è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), l'operazione non può configurarsi come fraudolenta e perciò rientra nell'ambito di applicazione della disciplina di cui al d.lgs. 27 gennaio 2010, n. 11, dovendosi la stessa considerare invece come autorizzata. Secondo l'interpretazione consolidata dei

Collegi territoriali, la disposizione contenuta nell'art. 5 del D. lgs. 11/2010 in tema di consenso necessario del pagatore, letta congiuntamente ai successivi artt. 9 e 10, induce a ritenere "autorizzata" l'operazione eseguita personalmente dal cliente ancorché il consenso sia corrotto dal dolo del frodatore: per quanto la volontà del cliente di effettuare tali operazioni sia stata viziata per effetto del raggiro subito dal terzo ignoto, l'intermediario non poteva che considerare autorizzati i pagamenti effettuati personalmente dal titolare dello strumento di pagamento, non avendo alcuna possibilità di accorgersi della truffa perpetrata ai danni del cliente (Coll. Milano, dec. nn. 8007/2020; 19945/2021, 11546/2019; Coll. Roma, dec. n. 4658/2021). Ciò non esclude naturalmente che il Collegio, tenuto conto delle peculiarità della fattispecie e delle modalità con le quali si è realizzata la truffa, possa individuare altri e diversi eventuali profili di responsabilità, per esempio sul versante del rispetto degli obblighi di protezione che gravano, per diritto comune, sul *bonus argentarius*; profili che, nel caso di specie, non ricorrono. Il Collegio, pertanto, respinge la domanda restitutoria relativa alla operazione di bonifico.

L'altra operazione di € 4.900,00, disposta tramite carta di debito, per la quale non emerge alcuna dichiarazione confessoria, ricade sotto il raggio d'azione del D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2). Ai sensi dell'art. 10, comma 1, del d.lgs. n. 11/2010, "Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti". L'assolvimento di tale onere è necessario ma non sufficiente, dovendo il prestatore ulteriormente provare, ai fini dell'esonero da responsabilità (art. 10, comma 2, d. lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 d. lgs. 11/2010: come chiarito dal Collegio di Coordinamento, "la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente" (decisione n. 22745/2019). Il Collegio, richiamati gli artt. 97 e 98 della PSD2, l'articolo 10 bis del D. Lgs. 11/2010, le 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 (in particolare il parere dell'EBA del 21 giugno 2019), richiama altresì l'art. 12 del d.lgs. 27.1.2010, n. 11, "Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento": "Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Il Collegio, ancora, ricorda che, in base all'art. 1, lett. qbis, l'"autenticazione forte del cliente" è definita come "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di

autenticazione". L'autenticazione forte è richiesta nella fase di accesso al conto/enrollment dell'app/registrazione della carta sul wallet; nella fase di esecuzione delle singole operazioni; rispetto a qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

La verifica della SCA non riguarderà il segmento della truffa consistente nello spostamento di fondi (€ 14.900,00 con vari bonifici), al fine di creare sufficiente provvista, dal conto del cliente presso altro intermediario T*: l'intermediario convenuto non ha infatti avuto nessun ruolo in tale fase della truffa.

Con riferimento alla operazione disposta tramite carta di debito, per l'accesso all'APP risulta dai log allegati l'impiego di un fattore di conoscenza (nome utente e password) e di un fattore di possesso (APP installata sul dispositivo mobile del cliente avente codice univoco *3ba7, associato al conto del ricorrente sin dal 04/02/2022).

Con riguardo alla esecuzione dell'operazione, risulta l'impiego di due fattori aventi medesima natura di possesso, vale a dire push notification e device del cliente; non c'è traccia invece di fattori di altro tipo, la cui presenza è indispensabile ai fini della autenticazione delle operazioni. A fronte del corredo documentale in atti, la SCA non può pertanto reputarsi provata.

In caso di difetto di piena prova sull'autenticazione delle transazioni disconosciute, secondo l'orientamento unanime dei Collegi, il ricorso deve essere accolto integralmente, posto che la prova di autenticazione rappresenta, in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 4.900,00.

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