

## 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) SANTARELLI         | Membro di designazione rappresentativa degli intermediari |
| (MI) GILIBERTI          | Membro di designazione rappresentativa dei clienti        |

Relatore (MI) MODICA

Seduta del 29/01/2026

### FATTO

Il cliente afferma di avere pubblicato un annuncio su una piattaforma *online* per la vendita di un oggetto; di essere stato contattato da un sedicente acquirente che lo invitava a cliccare su un *link* apparentemente riconducibile alla piattaforma stessa, per ricevere le somme pattuite per l'acquisto; che il *link* conduceva a un sito nel quale veniva simulato un sistema di verifica con *chat* di supporto, in cui gli veniva richiesto di fornire i suoi dati bancari per effettuare una transazione allo scopo di verificare l'identità del venditore; che il sedicente acquirente prelevava circa € 3.500,00 dal suo conto attraverso sistema di pagamento M\*. Ha presentato reclamo all'intermediario in data 11/08/2025, che veniva riscontrato negativamente.

Chiede la restituzione dell'importo fraudolentemente sottrattogli.

L'intermediario controdeduce che il cliente ha autorizzato l'operazione contestata tramite il dispositivo mobile in suo esclusivo possesso ed unicamente associato al suo conto, in conformità con i requisiti previsti dalla c.d. *Strong Customer Authentication*; che sussiste la colpa grave del cliente che ha

comunicato a un soggetto terzo i dati della propria carta ed il relativo codice CVV nonché il saldo disponibile sul suo conto e ha infine autorizzato personalmente, tramite l'APP di *home banking* installata sul proprio dispositivo certificato, l'operazione di pagamento controversa sulla base delle istruzioni ricevute nella *chat* fraudolenta. Segnala che il cliente ha visionato la notifica *push* di autorizzazione e ha autorizzato l'importo pari a € 3.500,00 a favore di un beneficiario che nulla aveva a che fare con il portale di vendita *online*; tale notifica *push* costituisce un presidio di sicurezza fondamentale: se il cliente l'avesse rifiutata, avrebbe potuto bloccare tempestivamente la frode e scongiurare qualsiasi danno patrimoniale. Precisa che, frode conclusa, nella medesima giornata, il cliente - accortosi di essere rimasto vittima di frode - contattava il Servizio Clienti dell'intermediario per richiedere lo storno dell'operazione oggetto di ricorso. In tale frangente, il Servizio Clienti procedeva manualmente a stornare la pre-autorizzazione a favore del cliente. Il giorno 05/08/2025, la transazione veniva annullata e il relativo importo veniva così riaccreditato sul conto del cliente. Subito dopo, il cliente trasferiva tutti i fondi presenti sul suo conto verso altro conto corrente ad egli intestato. Tuttavia, nella medesima data, l'esercente M\*, procedeva ad addebitare nuovamente l'importo in questione, in quanto - sebbene il rimborso fosse stato predisposto dalla banca su richiesta del cliente - non vi era stato di fatto nessun consenso a procedere con lo storno dell'operazione da parte dell'esercente. In assenza di tale passaggio essenziale, e considerato che la transazione era stata regolarmente autorizzata dal cliente mediante procedura *3D Secure*, M\* provvedeva legittimamente ad addebitare l'importo in oggetto; ne consegue che non si è in presenza di un doppio addebito bensì di un'unica operazione di pagamento, regolarmente autorizzata dal cliente nel contesto della frode.

Chiede il rigetto del ricorso.

Il cliente replica che, una volta ricevuto lo storno dalla banca, ha trasferito i fondi con la convinzione di proteggere i suoi risparmi da successive frodi; in data 11/08/2025 ha ricevuto rassicurazioni circa il rimborso definitivo ma lo stesso non è mai avvenuto. Aggiunge che delle generiche informative antifrode inviate tramite *email* da parte dell'intermediario non possono essere ritenute motivo sufficiente di esonero da responsabilità rispetto ad un'operazione più che sospetta; non ritiene sussistano gli estremi per definire colpa grave a suo carico.

L'intermediario controreplica che dalla ricostruzione dei fatti emerge una pluralità di condotte che integrano una violazione grave degli obblighi di diligenza imposti all'utente dei servizi di pagamento dal D. Lgs. 11/2010; il cliente ha infatti accettato modalità di pagamento del tutto atipiche e non riconducibili ai sistemi ufficiali della piattaforma di vendita *online* S\*. A ciò si aggiunge l'autorizzazione di un'operazione di € 3.500,00, importo incongruente rispetto al corrispettivo atteso per il prodotto messo in vendita (€ 110,00). Né può trascurarsi l'assurdità della richiesta formulata dal malfattore: autorizzare

un pagamento in uscita, quasi pari all'intero saldo disponibile sul conto corrente, per una presunta verifica della carta, anziché attendersi – come fisiologico in una vendita – un pagamento in entrata. Insiste per il rigetto del ricorso.

## **DIRITTO**

Il cliente disconosce un'operazione eseguita a valle di una truffa e chiede la restituzione del relativo importo. Si tratta, in particolare, di una operazione di ecommerce effettuata alle ore 17.03 del 4 agosto 2025, per la somma di € 3.500,00.

L'operazione contestata 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.

Nel caso di specie, l'intermediario ha fornito prova che l'operazione è stata autenticata a seguito di login eseguito tramite inserimento della password (fattore di conoscenza) nell'APP di home banking installata sul dispositivo mobile personale associato in via esclusiva al conto (fattore di possesso) avente device token \*c139; mediante protocollo di sicurezza 3D Secure, con convalida della relativa notifica push in-APP (elemento di possesso) nell'ambito della sessione avviata con il login (e dunque con riutilizzo del fattore di conoscenza del login, come dichiarato dallo stesso intermediario). Il cliente peraltro ha dichiarato di aver autorizzato la notifica push ricevuta, pensando si trattasse di una notifica di verifica.

Del pari provata appare la colpa grave del cliente, vittima di una truffa banale cui avrebbe potuto sottrarsi con l'impiego di una media diligenza. Dalla documentazione versata in atti emergono i contorni di un *phishing*, truffa ricorrente attuata nel caso di specie mediante richiesta via messaggio sulla piattaforma di inserire i propri dati personali attraverso un *link* a un sito clone del sito di compravendita di prodotti *online*. Rileva altresì che i messaggi truffaldini risultano inviati su una *chat* in alcun modo riferibile all'intermediario e che il cliente non si sia avveduto che il nome del beneficiario chiaramente richiamasse una piattaforma di scambio di criptovalute.

Alla luce delle specificità del caso, il Collegio reputa provata non solo l'autenticazione, la corretta registrazione e contabilizzazione dell'operazione nonché la sua regolarità formale, ma anche dimostrata la colpa grave di parte ricorrente (cfr. in proposito Collegio di Coordinamento, decisione n. 22745/2019), in quanto le modalità attuative delle operazioni disconosciute riflettono uno schema tipico e ormai noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, e-mail, sms o altri strumenti di comunicazione, a divulgare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza. Tenuto conto delle circostanze, il ricorrente deve essere considerato vittima di colpevole credulità, in quanto le modalità con le quali la truffa è stata realizzata rientrano tra quelle più diffuse e conosciute, che qualunque fruitore di servizi on line, dotato di normale avvedutezza

e prudenza, deve essere in grado di riconoscere ed evitare (cfr. Collegio di Coordinamento n. 3498 del 26/10/2012).

La riconosciuta colpa grave del cliente, pur a fronte di operazioni accompagnate da piena prova della Sca, non esclude naturalmente che il Collegio 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* anche *sub specie* di mancata gestione di eventi che segnalino la possibilità di frodi o anomalie; profili che, nella vicenda in esame, non ricorrono. Non ha fondamento, infatti, il rilievo del cliente in ordine alla scarsa chiarezza dell'intermediario nella fase successiva al disconoscimento. Dalla documentazione in atti risulta che, a seguito del disconoscimento, l'intermediario abbia provveduto al riaccredito momentaneo sul conto del cliente, il quale, immediatamente, trasferiva le somme su altro conto nell'intento di evitare un ulteriore prelievo fraudolento; successivamente, le somme venivano riaddebitate, conformemente all'art. 11, commi 1 e 3, d.lgs. 11/2010. La circostanza che tale riaddebito abbia determinato uno scoperto non è imputabile all'intermediario.

#### **PER QUESTI MOTIVI**

**Il Collegio non accoglie il ricorso.**

IL PRESIDENTE