

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

Relatore (MI) GILIBERTI

Seduta del 18/12/2025

## FATTO

Parte ricorrente nel proprio ricorso sostiene che:

- ha subito una truffa informatica ad opera di una società di cripto valute, a esito della quale le sono stati sottratti € 883,96 attraverso due pagamenti di importo pari a € 441,98 ciascuno;
- non possiede cripto valute e non ha usufruito di alcun bene o servizio a seguito di tali pagamenti;
- ha ricevuto un' e-mail apparentemente da E\*, sito web dedicato all'e-commerce, del tutto conforme a quelle originali, in cui le veniva chiesto di verificare la sua carta di debito per ricevere un accredito;
- ha cliccato sul link presente nella mail;

- si è aperta una pagina di verifica dei dati e, una volta inseriti i dati, una chat di supporto, in cui un sedicente operatore l'ha invitata a proseguire con un piccolo addebito (asseritamente necessario per effettuare la verifica della carta), assicurandole che la somma addebitata le sarebbe stata immediatamente rimborsata;
- ha condiviso in chat i codici richiesti e ho subito visto un addebito di € 441,98;
- ha avvisato sulla chat del pagamento ed è stata invitata a trasmettere il nuovo codice ricevuto via sms, asseritamente al fine di ricevere il rimborso della somma, che le veniva riferito essere stata precedentemente bloccata dal sistema;
- ha trasmesso il secondo codice e ha visto un secondo addebito di € 441,98;
- ha compreso che stesse accadendo qualcosa di anomalo;
- ha manifestato le sue perplessità nella chat e ha ricevuto in risposta i dati identificativi del presunto operatore (nome, identificativo e codice a barre);
- ha contattato il servizio clienti dell'intermediario per bloccare i pagamenti;
- l'intermediario ha risposto che non si poteva fare altro che attendere che i pagamenti passassero dalla sezione non contabilizzati a quella contabilizzati, per poter poi procedere al disconoscimento e alla richiesta di rimborso;
- ha bloccato temporaneamente la carta di debito;
- lo stesso giorno della truffa ha inviato una PEC all'intermediario, con allegata la denuncia sporta;
- l'intermediario ha scelto di estinguere la sua carta;
- ha atteso che i due pagamenti venissero contabilizzati e ha proceduto con la richiesta di rimborso;
- l'intermediario ha negato il rimborso.

Pertanto, chiede il rimborso dell'importo di € 883,96.

L'intermediario chiede il rigetto della domanda sostenendo che:

- la cliente è titolare di conto corrente con collegata carta di debito n. \*42;
- in data 25 giugno 2025, sono state disposte, tramite la carta di debito, due operazioni di pagamento, di importo complessivo pari a € 883,96;
- in pari data, ore 16:33, la cliente ha provveduto cautelativamente a bloccare la carta;
- la cliente ha presentato vari reclami, riscontrati con un diniego;
- la cliente è rimasta vittima di phishing: come descritto nel ricorso, ha ricevuto una mail apparentemente dalla società E\* (in alcun modo riconducibile allo stesso) e ha dato seguito alle richieste ivi contenute, cliccando sul link presente nella comunicazione e fornendo via chat, a un operatore non identificato, dati personali segreti, di sua esclusiva conoscenza;
- ha effettuato diverse iniziative volte a informare e educare i propri clienti sul tema della cyber security; inoltre, all'interno del proprio sito, fornisce tutte le indicazioni utili alla clientela per conoscere e prevenire le truffe informatiche;
- le operazioni contestate sono state correttamente autorizzate e contabilizzate, conformemente a SCA, mediante inserimento del codice OTP 3DSecure (inoltrato sul recapito di cellulare della cliente) e della password statica (PIN statico on line);
- allega i LOG forniti dalla società N\*, emittente dello strumento di pagamento e gestore del servizio;
- come ammesso dalla ricorrente, la stessa ha condiviso/non custodito diligentemente i dati della carta e i codici autorizzativi inviati alla stessa;
- si configura una colpa grave della cliente con riferimento alla violazione degli obblighi di conservazione e custodia delle credenziali e dei codici OTP;
- ha senza ritardo inviato notifiche via e-mail delle operazioni effettuate sulla casella di posta della cliente;
- alla luce delle evidenze documentali fornite, la cliente avrebbe potuto accorgersi facilmente dell'anomalia e inattendibilità delle mail e dei messaggi ricevuti via chat con il presunto operatore della società E\*.

In sede di replica la parte ricorrente afferma che:

- ha fornito i codici OTP, ma a causa della falsa rappresentazione della loro funzione operata dai truffatori;
- non era consapevole di autorizzare operazioni di acquisto verso una società di criptovalute;
- in data 01/07/2025 si è avveduta di un ammanco di € 883,96, suddiviso in due addebiti non contabilizzati di € 441,98 ciascuno; ha immediatamente contattato l'intermediario, che gli ha riferito che si trattava di somme prenotate, con riaccredito in 24 ore.
- In sede di controreplica l'intermediario ha precisato che le transazioni, una volta correttamente finalizzate, risultano già tecnicamente concluse e non più revocabili.

### DIRITTO

Nel caso di specie trova applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU, entrato in vigore il 13/01/2018.

Il ricorso ha ad oggetto n. 2 operazioni contestate per un importo complessivo di € 883,96 e, sebbene la ricorrente dichiari di aver sporto denuncia lo stesso giorno della truffa, tale documento non è presente in atti.

Facendo richiamo a quanto riferito in sede di ricorso, risulta che la stessa parte abbia cliccato sul link presente nella mail di phishing, inserito i propri dati personali e comunicato al truffatore, via chat, i codici OTP.

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.

Sul punto, l'intermediario afferma che le operazioni sono state autenticate tramite:

- inserimento del codice OTP 3DSecure (inoltrato sul cellulare della cliente);
- password statica (PIN statico on line).

Di ciò viene fornita relativa evidenza documentale.

Inoltre, la stessa ricorrente riconosce di aver inserito sulla pagina clone i dati della carta di debito (in particolare nome del titolare, numero della carta, scadenza e CVV); di aver fornito al truffatore, tramite chat, i codici OTP.

Le superiori dichiarazioni sono valutate, a dire del Collegio, in termini di prova legale ai sensi dell'art. 2730 c.c.

In termini generali, la ricorrente risulta essere stata vittima di "*phishing*", una forma di truffa attuata mediante richiesta via e-mail di inserire i propri dati personali attraverso un link a un sito clone a quello ufficiale dell'intermediario.

L'orientamento dei Collegi evidenzia ormai da tempo che simili tipologie di truffa si svolgono secondo uno schema tipico e noto, consistente nell'indurre il titolare dello strumento, tramite e-mail a comunicare 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.

La diffusione del fenomeno è tale che in detti casi la condotta del cliente, secondo l'orientamento dei Collegi, è generalmente connotata da colpa grave, in quanto l'impiego di una media diligenza sarebbe sufficiente a impedire la truffa.

Come detto, la cliente riferisce di aver cliccato sul link presente nella mail, di aver inserito i propri dati e di aver successivamente comunicato al truffatore, tramite chat, i codici OTP ricevuti tramite SMS. Riferisce inoltre che, dopo aver comunicato al truffatore il primo codice OTP e aver riscontrato un addebito pari a € 441,98, ha comunicato allo stesso anche il secondo codice OTP ricevuto via SMS.

Da ultimo, la ricorrente contesta all'intermediario di non aver bloccato i pagamenti, nonostante lo abbia contattato immediatamente dopo aver subito la truffa, quando (come riferito dallo stesso intermediario) i pagamenti risultavano ancora non contabilizzati. L'intermediario replica che le transazioni, una volta finalizzate, risultavano già tecnicamente concluse e non più revocabili, fornendo, in ogni caso, evidenza di aver eseguito il blocco della carta pochi minuti dopo l'esecuzione della truffa.

In tale contesto, a dire del Collegio, assume rilievo il contenuto e la tipologia dei messaggi scambiati con il truffatore. Dalla documentazione resa disponibile dalla medesima parte si osserva come il tenore delle comunicazioni intervenute al momento della truffa sia approssimativo e i messaggi rivolti alla ricorrente spesso connotati da errori grammaticali e, più in generale, da imprecisioni che avrebbero dovuto quantomeno insospettire il destinatario inducendolo a comprendere di essere caduto in un raggio.

Le considerazioni di cui sopra inducono pertanto il Collegio a ritenere che sussista colpa grave della ricorrente.

### **PER QUESTI MOTIVI**

**Il Collegio non accoglie il ricorso.**

**IL PRESIDENTE**