

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) BARTOLOMUCCI

Seduta del 13/01/2026

FATTO

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di essere stata vittima di una truffa in seguito all'inserzione ad un annuncio su un sito Internet per la vendita di alcuni prodotti.

Faceva presente, in particolare, di aver seguito i passaggi richiesti dalla procedura atti a trarla in inganno e ad autorizzare i pagamenti con l'erronea convinzione che i predetti pagamenti sarebbero tornati indietro.

Affermava di aver provveduto a bloccare la carta e di non riuscire ad accedere alla carta.

Chiedeva, pertanto, la ripetizione dell'importo complessivo di euro 389,00 oltre interessi.

Costituitosi ritualmente, l'intermediario riteneva che la cliente fosse rimasta vittima di phishing.

Evidenziava che le operazioni in esame fossero state autorizzate dalla cliente e correttamente eseguite, sebbene nel contesto di un'asserita truffa online operata da ignoti, tramite l'adozione del sistema 3DS.

Considerava sussistente la colpa grave della cliente la quale aveva cliccato su un allegato contenuto in un messaggio ricevuto da un sedicente acquirente, inserito le proprie credenziali e autorizzato le

operazioni di pagamento; sottolineava, peraltro, la condotta colposa tenuta dalla ricorrente nel caso in specie non fosse stato il risultato di una pressione psicologica o coercizione subita.

Sottolineava che le richieste fatte alla ricorrente fossero palesemente anomale, poiché le stesse consistevano a) nell'inserimento delle credenziali del suo strumento di pagamento; b) nell'effettuare delle transazioni, anche di importo non modesto, che presumibilmente dovevano poi essere stornate al fine di verificare l'identità della ricorrente stessa.

Sosteneva che il funzionamento ordinario non prevede che il venditore debba eseguire operazioni di pagamento bensì comporta esclusivamente la ricezione dell'importo venduto e, comunque, evidenziava la propria estraneità alla vicenda in oggetto, atteso il fatto che l'intera attività fraudolenta si fosse svolta al di fuori dell'ambiente digitale dell'intermediario, su canali e piattaforme esterne, del tutto estranei al perimetro di controllo tecnico e organizzativo dell'intermediario stesso.

Chiedeva, pertanto, il rigetto del ricorso.

Seguivano memorie di replica e controreplica con le quali le parti si riportavano ai rispettivi scritti difensivi.

DIRITTO

La domanda proposta dalla ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di alcune operazioni successivamente disconosciute.

La materia, come noto, è regolata dal d. lgs. n. 11/2010 come modificato dal d. lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/Ue (c.d. PSD2- *Payment Services Directive 2*).

Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d. *strong customer authentication* SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.

Con riferimento alla c.d. SCA gli artt. 97 e 98 della direttiva PSD2, nonché l'articolo 10-*bis* del d. lgs. n. 11/2010, oltre che le norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea e i criteri interpretativi adottati dalla stessa Autorità (cfr. in particolare il parere dell'EBA del 21 giugno 2019), hanno stabilito che essa 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. In relazione a tutte le predette fasi, la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori, che devono essere reciprocamente indipendenti e appartenere a categorie diverse: conoscenza; inerenza; possesso.

Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa *de qua* prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la

responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.

Risulta documentalmente che le operazioni contestate consistono in due pagamenti on line eseguiti il 05/08/2025 tra le ore 08:51 e le ore 08:02, per un importo complessivo di € 389,00.

Ancorché in sede denuncia alle autorità, la cliente abbia dichiarato di non aver autorizzato alcuna operazione, dalle allegazioni del ricorso (aventi natura confessoria) emerge invece che ella abbia ammesso di aver eseguito personalmente i pagamenti, specificando peraltro che "i pagamenti sono stati fatti con la promessa del ritorno dei soldi al solo fine di accertare la mia identità in quanto avevo autorizzato una vendita".

In relazione ad analoghe fattispecie, questo Collegio ha avuto modo di affermare che debba considerarsi esclusa l'applicabilità della disciplina prevista nelle ipotesi di utilizzi fraudolenti di strumenti di pagamento atteso che, "per quanto la volontà del cliente di effettuare tali operazioni sia stata viziata per effetto del raggio 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" (cfr. Collegio di Milano, decisione n. 16551/2021).

Tanto basta perché l'esecuzione dei pagamenti contestati dalla ricorrente non possano considerarsi come "operazione non autorizzata", non ricadendo quindi nell'ambito di applicazione delle norme protettive (artt. 10 e 12 del d. lgs n. 11/2010) richiamate e previste per i casi di utilizzazione fraudolenta degli strumenti di pagamento.

Dalla documentazione versata in atti non emergono ulteriori elementi che possano comunque configurare una responsabilità concorrente in capo all'intermediario.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE