

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(BA) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore SABRINA PERON

Seduta del 03/03/2026

FATTO

Parte ricorrente rappresenta al Collegio di aver ricevuto, in data 21.10.2025, un SMS apparentemente riconducibile all'intermediario nel quale veniva segnalato un tentativo di transazione sospetto di € 3.200,00, invitandola a contattare un numero di assistenza specifico per ulteriori informazioni. Chiamato il numero indicato, rispondeva un sedicente operatore il quale, riferendo di vari tentativi di prelievo in corso, convinceva la parte ricorrente a disinvestire alcune somme e ad accettare tramite App due richieste di autorizzazione per pagamenti di € 1.990,00 ciascuno, presentandoli come necessari

per il recupero dei fondi. Successivamente, su indicazione del medesimo interlocutore, parte ricorrente eseguiva due bonifici istantanei verso il proprio conto presso l'intermediario convenuto per complessivi € 3.590,00 disponendo poi con tali fondi un ulteriore bonifico di € 3.824,62 a favore di un terzo. Solo dopo la chiusura della telefonata, si avvedeva di essere stata vittima di una frode informatica attuata tramite tecniche di manipolazione psicologica, nonostante avesse sempre mantenuto l'esclusivo controllo dei propri dispositivi e delle credenziali di sicurezza. Parte ricorrente tentava di contattare il servizio clienti per bloccare le operazioni ancora in stato "in attesa", riscontrando tuttavia l'assenza di un servizio telefonico diretto con un operatore umano e la presenza di una chatbot automatizzata limitata a risposte predefinite. Nonostante l'invio di e-mail e la segnalazione urgente di blocco tramite l'App, l'intermediario rispondeva con messaggi automatici rinviandola per la gestione del problema ai canali digitali. Nei giorni successivi, mentre il bonifico veniva infine rifiutato dall'istituto ricevente con conseguente riaccredito delle somme, l'esercente coinvolto nei pagamenti con carta richiedeva i dati IBAN dell'ordinante e del beneficiario per le verifiche del caso. Parte ricorrente si rivolgeva prontamente all'intermediario, il quale avviava la procedura di recall solo il 31 ottobre, ossia dieci giorni dopo la prima segnalazione, e senza fornire le informazioni necessarie sui destinatari dei pagamenti. Infine, nel mese di novembre, l'intermediario comunicava l'impossibilità di procedere al rimborso in quanto le operazioni risultavano regolarmente autorizzate e il tentativo di recupero era fallito a causa del già avvenuto trasferimento dei fondi. Parte ricorrente lamenta pertanto la responsabilità dell'intermediario per la gestione inefficiente delle segnalazioni e per l'inadeguatezza degli strumenti di assistenza, la cui tardività ha impedito il blocco tempestivo di operazioni che erano ancora tecnicamente revocabili. Parte ricorrente chiede quindi che il Collegio, riconoscendo la responsabilità dell'intermediario, disponga il rimborso delle somme fraudolentemente sottratte.

L'intermediario non si è costituito nel presente procedimento, sebbene abbia ricevuto il ricorso che gli è stato correttamente trasmesso in data 21/11/2025.

DIRITTO

Il presente ricorso concerne la domanda di parte ricorrente di ottenere il rimborso di € 3.980,00 sottrattiti tramite due disposizioni di pagamento on-line (di € 1.990,00 ciascuna) personalmente eseguite, in data 21/10/2025, dalla stessa parte ricorrente a causa di una truffa subita.

Ciò posto il Collegio constata che le operazioni oggetto di contestazione non rientrano nell'ambito di applicazione della disciplina di cui al D.lgs. 27 gennaio 2010, n. 11 (di recepimento della Direttiva sui servizi di pagamento, come modificato dal D.lgs. n. 218/17 in attuazione della direttiva 2015/2366/EU - PSD2), essendo emerso in modo pacifico che le transazioni sono state eseguite direttamente dalla parte ricorrente. Difatti, dalle risultanze della denuncia in atti e dalla prospettazione dei fatti contenuta nel ricorso, si evince che parte ricorrente riconosce espressamente di aver effettuato personalmente le operazioni seguendo le indicazioni fornite da un operatore fraudolento. Tale azione è stata preceduta dalla ricezione di un SMS, che preannunciava un contatto telefonico finalizzato al blocco di un'operazione sospetta. Si noti che parte ricorrente specifica di aver sempre mantenuto il pieno ed esclusivo controllo del proprio telefono, con cui ha autorizzato le operazioni, così come di PIN, password, credenziali di accesso e codici di sicurezza e di non aver mai comunicato a terzi le proprie credenziali. Ne deriva che, nel caso di specie, le operazioni, sia pure a causa di un raggiro perpetrato da un terzo, sono state interamente eseguite ed autorizzate dalla parte ricorrente che ha eseguito le indicazioni ricevute dal frodatore. Ebbene secondo l'orientamento dei Collegi, dal momento che l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di

tutti i fattori di autenticazione), la stessa deve considerarsi autorizzata e, pertanto, non viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate di cui alla direttiva 2015/2366/EU ("PSD2") e al D.lgs. n. 11/2010, ragion per cui non si procede all'esame del sistema di autenticazione forte dell'intermediario.

Sulla base della rappresentazione dei fatti e dalle evidenze in atti, la tipologia di truffa subita dall'attrice è qualificabile come social hacking. Questa truffa si concretizza «nell'impartire telefonicamente istruzioni manipolative al titolare della carta, lasciando che sia lo stesso titolare a disporre e autenticare i singoli pagamenti, senza che il frodatore venga mai a conoscenza dei codici di accesso. In questo si distingue da una più comune ipotesi di c.d. vishing, in cui è il truffatore a disporre e autenticare le operazioni, sulla base dei codici di accesso carpiri con l'inganno dall'ignaro interlocutore telefonico» (così, Collegio di Milano, decisione n. 432/2023). Ne deriva che, nel caso di specie, le operazioni contestate, sia pure a causa di un raggiro perpetrato da un terzo, sono state autorizzate dalla parte ricorrente e non sono quindi soggette al regime di responsabilità previsto dalla PSD2 (cfr. *ex multis*, Collegio di Palermo, decisione n. 8841/2025; Collegio di Roma, decisione n. 8538/2021).

L'inapplicabilità alla controversia in esame del regime di responsabilità dei prestatori di servizi di pagamento delineata dal citato D.lgs. n. 11/2010, comporta il non accoglimento del ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE