

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) RIZZO

Seduta del 18/12/2025

FATTO

Il cliente, nel ricorso, afferma quanto segue:

- in data 26/07/2025, a Rio de Janeiro (Ipanema), tentava di pagare un importo di 80 BRL (circa € 12) presso un venditore ambulante;
- dopo vari tentativi negati (digitale, contactless e con PIN, inserito una sola volta), l'esercente si rendeva irreperibile;

- poco dopo riscontrava due addebiti fraudolenti, alle ore 17:21 e 17:23 italiane, rispettivamente di € 819,26 ed € 409,64, per un totale di € 1.228,90;
- immediatamente bloccava la carta e segnalava l'accaduto, sporgendo poi regolare denuncia ai Carabinieri;
- sul POS era chiaramente visibile l'importo corretto di 80 BRL e tutte le operazioni apparivano negate.

Il ricorrente domanda, quindi, il rimborso della somma di € 1.228,90.

Nelle controdeduzioni, l'intermediario convenuto, riportato il fatto, afferma quanto segue:

- il cliente era titolare della carta n. 5167***7970 appoggiata sul conto corrente n. 03972***7913;
- in data 29/07/2025, il cliente inseriva il disconoscimento, dopo aver bloccato la carta;
- in data 14/08/2025, comunicava che le operazioni non presentavano anomalie o malfunzionamenti, che la carta non risultava clonata e che le transazioni erano state correttamente contabilizzate, registrate e autenticate con l'utilizzo del dispositivo originale, tramite lettura del microchip e inserimento del PIN;
- pertanto, negava il rimborso e provvedeva al riaddebito delle somme temporaneamente accreditate a seguito di disconoscimento;
- in data 19/08/2025, il cliente sporgeva reclamo, contestando l'esito del disconoscimento;
- le dichiarazioni del cliente non collimano con le evidenze dei tabulati della carta, i quali non presentano traccia dei riferiti tentativi eseguiti con il telefono, nonché delle diverse operazioni asseritamente eseguite con lo strumento di pagamento fisico;
- dai log informatici è possibile constatare che, nell'arco temporale di due minuti, sono state inserite tre operazioni di importo differente, una delle quali è stata negata per verosimile time out della linea;
- pertanto, può ipotizzarsi che, mentre il cliente tentava di eseguire l'operazione di 80 BRL, l'esercente abbia carpito le credenziali non ben custodite e, con la scusa della mancata transazione, abbia inserito le due operazioni di cui oggi è doglianza;
- in alternativa, può ipotizzarsi che l'importo delle transazioni sia stato inserito sul POS dall'esercente e poi autenticato dal cliente stesso con la digitazione del PIN;
- il cliente era presente al momento dei pagamenti e l'attività fraudolenta è avvenuta in sua presenza, risultando pertanto ravvisabile a suo carico una colpa grave per omessa vigilanza delle credenziali a lui affidata o per utilizzo incauto dello strumento di pagamento;
- come sostenuto in precedenza dal Collegio di Milano, "l'impiego della tecnologia a microchip rende l'ipotesi della clonazione, se non di impossibile evenienza, almeno altamente improbabile, facendo dunque ritenere che l'operazione disconosciuta non possa che essere ricondotta a una conservazione molto distratta della carta e del PIN";
- le operazioni sono avvenute a distanza di un minuto, tempo che non può esser considerato sufficiente per estrarre il codice segreto dalle carte attraverso procedure tecniche di alta sofisticazione;

- grava sul cliente l'obbligo di custodire la propria carta e il relativo codice segreto PIN, impedendone l'acquisizione da parte di soggetti non autorizzati;
- alla luce di quanto precede, è da respingere l'affermazione che la banca non abbia attivato adeguati controlli antifrode sulle due operazioni;
- peraltro, proprio il giorno prima, il cliente aveva attivato il profilo "MONDO", a riprova della sua volontà di utilizzare la carta all'estero;
- l'invio di un sms alert sarebbe stato del tutto influente, trattandosi di operazioni effettuate a breve distanza di tempo l'una dall'altra;
- le operazioni si collocano nell'alveo del plafond di spesa della carta nel pieno rispetto dei massimali contrattualmente previsti.

L'intermediario convenuto domanda, quindi, il rigetto del ricorso in quanto infondato; in via subordinata, domanda di ripartire il danno secondo le rispettive responsabilità delle parti ex art. 1227 c.c.

DIRITTO

Oggetto della presente controversia sono due operazioni contestate, per un importo complessivo di € 1.228,90, poste in essere il 26/07/2025. Alla data delle operazioni trovava applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018.

È agli atti la denuncia del cliente presentata in data 8/08/2025.

Quanto all'autenticazione forte, corretta registrazione e contabilizzazione delle operazioni contestate, dall'esame dei log informatici prodotti agli atti dall'intermediario convenuto emerge che le operazioni contestate sono state, correttamente, autenticate mediante i fattori del possesso (la carta) e della conoscenza (il codice PIN).

Valutando la condotta delle parti e i profili rilevanti per la valutazione di sussistenza della colpa, rileva questo Collegio come l'intermediario convenuto, oltre a contestare al cliente l'assenza di coerenza espositiva circa l'asserita molteplicità dei tentativi di pagamento, evidenzi poi, quale elemento dirimente della vertenza, il fatto che il cliente fosse presente al momento dei pagamenti e che l'attività fraudolenta sia avvenuta in sua presenza, risultando pertanto ravvisabile a suo carico una colpa grave per omessa vigilanza delle credenziali a lui affidate o per utilizzo incauto dello strumento di pagamento. Ad avviso di parte resistente, risulta chiaro che se il ricorrente non avesse incautamente digitato il PIN davanti all'esercente "infedele", le due operazioni non si sarebbero mai verificate. A conferma della sussistenza di grave colpa in capo al ricorrente, l'intermediario esclude, poi, la natura sofisticata della truffa, invocata in sede di repliche al fine di escludere negligenza e distrazione; non vi sarebbe, infatti, alcuna prova circa l'asserita manipolazione del POS, potendo al massimo ravvisarsi una modifica dell'importo da parte dell'ambulante. Al contrario, l'intermediario ritiene che il contesto (pagamento eseguito per strada, presso un esercente ambulante occasionale, all'estero, in un paese che rinomatamente ha una criminalità e microcriminalità diffusa) costituisca un aggravante e non già un esimente.

Nello medesimo senso, il Collegio deve rilevare come lo stesso ricorrente, in sede di repliche, ammetta, tra l'altro, il senso di "disorientamento" sperimentato in quei momenti. D'altra parte, l'intermediario

evidenza come il cliente, proprio il giorno precedente alla truffa, avesse attivato il profilo “MONDO”, a riprova della sua volontà di utilizzare la carta all'estero.

Considerato quanto prodotto agli atti e la scarna rappresentazione dei fatti offerta dal ricorrente, questo Collegio ritiene raggiunta la prova dell'efficacia causale determinante, nella produzione dell'evento dannoso, della colpa grave del ricorrente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE