

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) PERON	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) RIZZO

Seduta del 31/03/2026

FATTO

Il cliente, nel ricorso, afferma quanto segue:

- subiva il furto del cellulare da parte di ignoti e sporgeva denuncia;
- sul cellulare era installata l'app Apple Wallet, contenente la carta dell'intermediario; il cellulare era provvisto di codice di sblocco e risultava attivato il riconoscimento biometrico;
- scopriva in seguito che tramite la carta dematerializzata erano state effettuate numerose operazioni fraudolente;

- i ladri avevano effettuato prelevamenti e pagamenti; per fare ciò avevano anche aperto due conti correnti;
- provvedeva a sporgere nuova denuncia, che successivamente integrava;
- presentava all'intermediario il modulo di disconoscimento degli importi;
- l'intermediario negava il rimborso; di conseguenza il cliente trasmetteva apposito reclamo con cui contestava il diniego ed evidenziava le anomalie della fattispecie; con questo sottolineava anche che i ladri erano riusciti a modificare la risposta segreta da fornire all'apposita domanda per autorizzare le operazioni;
- l'intermediario riscontrava il reclamo negativamente in quanto le operazioni risultavano correttamente autorizzate;
- tale diniego è contrario alla normativa vigente;
- l'intermediario non ha dato prova della SCA;
- sussiste responsabilità dell'intermediario, in quanto colpevole di non aver adottato appositi sistemi di monitoraggio e di prevenzione delle frodi; infatti, le transazioni sono anomale per frequenza ed importi.

Il ricorrente domanda, quindi, il rimborso della somma di € 11.237,41 oltre agli interessi legali dalla data dei singoli addebiti al saldo effettivo, e alle spese del presente procedimento.

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

- il cliente contesta 29 transazioni eseguite con due diverse carte (***7350 e ***7066)
- tutte le operazioni sono state correttamente registrate ed autenticate;
- ogni operazione eseguita con Apple Pay richiede riconoscimento biometrico (tramite impronta o riconoscimento del volto) o la conoscenza del codice di accesso/sblocco;
- il codice di sblocco è fondamentale perché consente di accedere al cellulare e perché è anche richiesto per completare la procedura di salvataggio e uso del riconoscimento biometrico;
- senza di esso non è, dunque, possibile modificare la biometria;
- ne deriva che si può escludere che le operazioni siano state effettuate in modo fraudolento o senza accesso ai codici o agli elementi per il riconoscimento biometrico;
- dalle denunce emerge la colpa grave del cliente in quanto ha lasciato il proprio cellulare a una sconosciuta di cui ignorava le generalità e non ha adottato nessuna azione tempestiva; non ha contattato il servizio clienti e ha iniziato ad avere i primi sospetti solamente il giorno seguente;
- il cliente non ha nemmeno disposto il blocco delle carte, che è stato invece operato dall'intermediario in via cautelativa;
- non sono state registrate anomalie nell'associazione all'app di un nuovo dispositivo, né nell'accesso all'home banking, né nelle modifiche dei limiti operativi;
- chi ha perpetrato il furto ha eseguito prelievi, un prelievo smart e pagamenti;
- per prelievi e pagamenti tramite wallet è necessario essere a conoscenza del codice di sblocco del telefono e del Pin della carta;
- per il Prelievo Smart, serve essere a conoscenza sia del codice di accesso all'app che del codice MPIN (Mobile Code) per prenotare l'importo, ed è anche necessario il telefono per sbloccare l'importo inquadrando il QR code davanti all'ATM;
- per gli accessi all'app bisogna essere a conoscenza del codice di accesso all'app, codice adesione e PIN;
- per le attivazioni di ulteriori carte tramite app, di cui solamente una utilizzata fraudolentemente, serve essere a conoscenza sia del codice di accesso all'app che del codice MPIN (Mobile Code);

- non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici;
- ha inviato al cliente apposite notifiche che lo avvisavano del compimento delle operazioni;
- appare evidente che un'intrusione di tale portata non può che avvenire attraverso la cooperazione, seppur involontaria di parte ricorrente con la mancata custodia dei codici dei dispositivi di autenticazione ovvero nella trasmissione degli stessi a terzi.

L'intermediario convenuto domanda, quindi, il rigetto integrale del ricorso in quanto infondato.

DIRITTO

Oggetto della presente controversia sono ventinove operazioni contestate, per un importo, comprensivo delle commissioni addebitate, di € 11.237,41. 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.

Sono presenti agli atti la denuncia del cliente presentata il 09/08/2025 per il furto del cellulare; la denuncia del 12/08/2025 per l'indebito uso della carta; l'integrazione alla seconda denuncia, datata 19/08/2025.

Dalle evidenze riportate si evince che la vicenda descritta si colloca in un arco temporale di 10 giorni, ovverosia dal 09/08/2025, giorno del furto del cellulare, al 19/08/2025, giorno dell'ultimo contatto con le forze dell'ordine e di ultimo aggiornamento dell'importo delle operazioni fraudolente.

Con la carta ***7350 sono state eseguite 22 operazioni, che consistono in prelievi e in pagamenti contactless. Dall'esame dei log informatici prodotti agli atti dall'intermediario convenuto, risulta che: le operazioni consistono tutte in addebiti, come provato dal codice PRESENTMENT; le operazioni sono avvenute in modalità CONTACTLESS con lettura del chip, come indica il codice M nella colonna ENTRY MODE; per svolgere le operazioni è stata usata una carta tokenizzata su apposito wallet, come indicato dalla spunta nel campo TOKEN. Quanto alle due operazioni di pagamento di € 2,50 ed € 9,00, le stesse ricadono nell'ambito dell'applicazione dell'esenzione dall'autenticazione forte a doppio fattore prevista dall'art. 11 del Regolamento delegato. Non ricade, invece, nella citata esenzione l'operazione di pagamento di € 1.320,00, in riferimento alla quale non sussiste evidenza dell'inserimento del fattore di conoscenza, ma solo della presenza della carta in modalità contact-less. Il costo di tale operazione, che non risulta autenticata correttamente, dovrà gravare sul prestatore dei servizi di pagamento.

Con riferimento alle operazioni poste in essere con la carta ***7066, attivata dai malviventi con contratto sottoscritto digitalmente, dall'esame dei log informatici prodotti agli atti dall'intermediario resistente risulta che l'operazione di pagamento del 09/08/2025, h. 10:01, di € 1.989,00 non è stata correttamente autenticata, rinvenendosi soltanto la prova dell'utilizzo del fattore di possesso ma non anche quello di conoscenza (il PIN); quanto all'operazione di pagamento del 09/08/2025, h. 13:30, di € 511,01 manca, del pari, la prova dell'inserimento del fattore di conoscenza (il PIN). Con riferimento, invece, alla quattro operazioni di prelievo poste in essere con la medesima carta, manca la prova dell'autenticazione forte in relazione alle fasi prodromiche al compimento delle stesse. In particolare, dai log prodotti agli atti non è possibile ricavare evidenza dei fattori di autenticazione prodromici all'enrollment della carta. Ne consegue che il costo di tutte le operazioni poste in essere con la carta ***7066 dovrà gravare sul prestatore dei servizi di pagamento.

Diversamente, risulta compliant alla SCA l'operazione di prelievo smart per l'importo di € 1.000,00, autenticata attraverso i fattori del possesso, dato dalla disponibilità materiale del telefono, e della conoscenza, rappresentato dal PIN.

Analizzando la condotta delle parti e i profili rilevanti per la valutazione di sussistenza della colpa, emerge una condotta gravemente colposa del ricorrente, che però – sulla base delle regole poste dalla PSD2 – non può certo superare la (parziale) mancata prova dell'autenticazione forte delle operazioni contestate, incombente sull'intermediario convenuto. In particolare, il cliente ha affermato che il cellulare gli è stato rubato da una donna in tarda serata ma di non avere dato peso all'accaduto, in quanto il dispositivo era protetto dal riconoscimento facciale. Attenendosi a quanto riportato nelle controdeduzioni della parte resistente, sembrerebbe, poi, che il cliente non abbia neppure proceduto a bloccare la propria carta, mentre vi avrebbe provveduto l'intermediario in autonomia.

Sulla base delle evidenze agli atti, risulta la sussistenza dei seguenti indici di anomalia/rischio frode di cui al D.M. 112/2007: sette o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore (art. 8, lett. b, punto 1); tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita (art. 8, lett. a, punto 2). Più specificamente, rileva il Collegio come nove operazioni di prelievo abbiano avuto luogo presso il medesimo esercizio commerciale ("Tabaccheria J**).

In presenza di tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita, il Collegio, infatti, riconosce in capo al prestatore di servizi di pagamento la sussistenza di un obbligo di protezione nell'interesse del cliente, che avrebbe dovuto portarlo all'interdizione dell'operatività anomala realizzatasi e che, pertanto, risulta inadempito, con la nascita del conseguente obbligo risarcitorio a carico del medesimo prestatore, nell'ipotesi, come l'attuale, in cui l'adempimento del predetto obbligo non abbia avuto luogo. Ne consegue che il costo di tali operazioni, a partire dalla terza compresa, poste in essere nell'arco delle 24 ore presso il medesimo esercizio commerciale ("Tabaccheria J**), dovrà gravare sul prestatore dei servizi di pagamento.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 9.480,00, oltre interessi legali dal reclamo al saldo.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00, quale contributo alle spese della procedura e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE