

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) RUSSO	Membro designato dalla Banca d'Italia
(PA) IMBURGIA	Membro di designazione rappresentativa degli intermediari
(PA) PLATANIA	Membro di designazione rappresentativa dei clienti

Relatore VINCENZO MELI

Seduta del 14/04/2026

FATTO

Con ricorso pervenuto il 9.12.2025 il ricorrente riferisce di aver messo in vendita su un noto sito e-commerce una stampante e di essere stato contattato da un asserito compratore. Nel corso della trattativa, in data 8.12.2025, ha ricevuto un messaggio contenente un *link*. Cliccando su tale *link* è stato riportato ad una pagina apparentemente riconducibile al sito, nella quale ha inserito i propri dati personali e quelli relativi alla propria carta, al fine di ricevere il pagamento. Inizialmente ha inserito i dati riferiti ad una carta riconducibile ad un intermediario terzo nel presente procedimento, ma poi, visto il mancato perfezionamento della procedura, ha inserito i dati riferiti ad una diversa carta, collegata alla resistente. In realtà, si trattava di una truffa, attraverso la quale gli è stata sottratta la somma di € 496,00, della quale chiede il rimborso.

Con le controdeduzioni, l'intermediario chiede il rigetto del ricorso. Argomenta che le operazioni del caso di specie non possono considerarsi non autorizzate, in quanto sono state poste in essere dal ricorrente, seppur sulla base di un consenso viziato. In ogni caso, risultano correttamente autenticate, registrate e contabilizzate con un sistema di autenticazione forte. Sostiene che il ricorrente ha ignorato gli *alert* del sistema antifrode e ha tenuto una condotta gravemente negligente.

Con le repliche e le controrepliche, le parti hanno sostanzialmente ribadito le proprie conclusioni.

DIRITTO

La controversia attiene ad una richiesta di rimborso di somme che sono state fraudolentemente sottratte al ricorrente, attraverso due operazioni poste in essere in data 8.12.2025, ciascuna per l'importo di € 248,00.

L'intermediario sostiene che tali operazioni non possono considerarsi come non autorizzate, giacché poste in essere da parte ricorrente, seppur sulla base di un consenso viziato. Richiama, a tale proposito, il contenuto della denuncia in atti, dalla quale emerge che è il ricorrente stesso ad avere inserito sull'apparente sito della piattaforma i dati delle proprie carte.

Si fa in proposito presente che i Collegi territoriali hanno statuito che le operazioni integralmente effettuate dal cliente (che ha cioè personalmente inserito la disposizione di pagamento e tutti i fattori di autenticazione), seppure sulla base di un consenso viziato per un raggirio subito dal terzo ignoto, non possono configurarsi come non autorizzate (si veda, *ex plurimis*, Collegio di Palermo, dec. n. 2787/2024) e ad esse non si applica, quindi, la disciplina di cui al D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II). Disciplina che, si applica, invece, alle operazioni per le quali il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione).

Nel caso all'esame, quanto affermato dal ricorrente non vale a dimostrare univocamente che le operazioni contestate siano state direttamente ed esclusivamente poste in essere da lui. Egli afferma, infatti, di avere comunicato i dati delle carte, ma non di avere personalmente effettuato, sia pure a seguito della truffa subita, le operazioni dispositive. Tuttavia, dalle circostanze riferite e documentate dall'intermediario con le controdeduzioni, in sede di dimostrazione dell'esistenza della SCA, appare evidente che, sia pure su indicazione del truffatore, sia stato proprio l'odierno ricorrente ad operare, attraverso l'app, effettuando i pagamenti attraverso l'utilizzo del proprio *device* registrato. Ne deriva che non può trovare applicazione del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2). Infatti, in casi simili, in modo assorbente, i Collegi territoriali hanno statuito che le operazioni integralmente effettuate dal cliente (che ha cioè personalmente inserito la disposizione di pagamento e tutti i fattori di autenticazione), seppure sulla base di un consenso viziato per un raggirio subito dal terzo ignoto, non possono configurarsi come non autorizzate (si veda, *ex plurimis*, Collegio di Palermo, dec. n. 2787/2024).

In tali ipotesi, i Collegi ritengono che, esclusa l'applicabilità della disciplina di favore derivante dalla PSD II, la responsabilità del cliente che ha effettuato l'operazione non possa essere esclusa, salvo prova contraria, del quale egli è onerato, ed egli sia tenuto a sopportare la perdita subita. Detta responsabilità può, tuttavia, concorrere con quella dell'intermediario, ancorché non si rilevino gli indici di anomalia previsti dal D.M. n. 112/2007, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode come, ad esempio, nei casi di:

- mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore;
- mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, nel caso in cui il pagatore si sia rivolto esponendo le richieste del frodatore;
- mancato rilievo di indici di frode nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere (si vedano, ad es., Collegio di Palermo, dec. n. 9829/2023; Collegio di Milano, dec. n. 8435/2023).

Nel caso di specie, dall'analisi della denuncia risulta:

- che il ricorrente ha messo in vendita una stampante su una nota piattaforma di e-commerce;
- che è stato contattato da un potenziale acquirente che, al termine del contatto, gli inviava una asserita evidenza dell'avvenuto pagamento;

- che il frodatore chiedeva all’odierno ricorrente di confermare la vendita, per potere poi ricevere l’importo sulla carta intesta al padre;
- in ragione di ciò, il ricorrente cliccava su un *link* contenuto in un messaggio inviato dal frodatore e, successivamente, inseriva i dati della carta;
- tale operazione non andava a buon fine, per cui il ricorrente era costretto ad inserire i dati di un’altra carta di pagamento.

L’intermediario sostiene che il ricorrente ha tenuto una condotta negligente per i seguenti motivi:

- il tipo di truffa che lo stesso ha subito non può dirsi “sostificata”;
- ha colpevolmente cliccato il link inviatogli dal frodatore;
- ha ignorato il messaggio inviatogli dal sistema antifrode dell’intermediario (circostanza documentata e non smentita dal ricorrente);
- non ha avuto sospetti quando, nell’ambito della vendita di un bene, gli è stato richiesto di effettuare dei pagamenti.

L’intermediario evidenzia che, successivamente alle operazioni fraudolente (sia quelle delle quali oggi il ricorrente chiede il rimborso sia quella oggetto di storno) ha inviato al ricorrente delle notifiche *push* di riepilogo delle operazioni.

Alla luce delle superiori circostanze, ritiene il Collegio che non sussistano ragioni per configurare un concorso di colpa dell’intermediario.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso

IL PRESIDENTE