

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) SCANNELLA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore VINCENZO MELI

Seduta del 14/05/2026

FATTO

Con ricorso pervenuto il 4.02.2026 il ricorrente riferisce di avere pubblicato su un noto sito di acquisti online un annuncio di vendita di un paio di occhiali. In data 26.01.26 è stato indotto tramite link a inserire i dati della carta su una pagina identica all'originale per "ricevere il pagamento". Nonostante i dubbi, il truffatore e una chat whatsapp lo hanno convinto che l'addebito di € 449,00 fosse una "verifica fake". La banca ha respinto il reclamo per colpa grave. Afferma che l'autorizzazione è stata estorta con dolo e l'operazione verso POS estero era palesemente anomala rispetto al proprio profilo. La banca non ha attivato i sistemi di monitoraggio antifrode necessari per bloccare una transazione palesemente sospetta verso un esercente estero. Il truffatore ha agito simulando un servizio di assistenza clienti, rendendo l'inganno difficilmente distinguibile da una procedura legittima per un utente medio. Nonostante il blocco tempestivo della carta e le numerose chiamate per fermare la transazione, l'assistenza ha imposto di attendere la contabilizzazione senza intervenire proattivamente. Chiede il rimborso di € 484,55.

Con le controdeduzioni, l'intermediario chiede il rigetto del ricorso. Afferma che l'operazione è stata personalmente autorizzata, come confermato dalle dinamiche fattuali e come risulta dalle dichiarazioni di cui al modulo di disconoscimento. Le operazioni sono state correttamente contabilizzate e registrate con sistema SCA *compliant*. Il cliente versa in colpa grave in quanto ha utilizzato canali alternativi alla

piattaforma online ufficiale. Il cliente ha ignorato il contenuto delle *push* che identificavano l'operazione come pagamento.

DIRITTO

La controversia attiene ad una richiesta di rimborso di somme che sono state fraudolentemente sottratte al ricorrente, attraverso un'operazione di pagamento indotta da truffatori.

Da quanto riferito dal ricorrente, anche attraverso la denuncia presentata agli organi di polizia, egli è stato contattato da un potenziale acquirente del paio di occhiali che aveva posto in offerta su un noto sito di acquisti online. Convinto di ricevere il pagamento, ha invece eseguito un'operazione.

Appare pacifico e non contestato che l'operazione, sebbene per via del raggirio operato dai malfattori, sia stata eseguita personalmente da parte ricorrente. Nel modulo di disconoscimento il ricorrente lo afferma espressamente.

Pertanto, è inapplicabile 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).

I Collegi hanno ritenuto, infatti, che, quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2. Rientrano in questa fattispecie anche le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, senza la consapevolezza di disporre una transazione (ad esempio, le c.d. operazioni "sotto dettatura") (si veda, *ex multis*, Collegio di Palermo, dec. n. 2787/2024).

Non potendosi, dunque, applicare la disciplina di favore per il cliente, derivante dalla PSD2, il caso deve essere affrontato valutando, secondo le regole di diritto comune, le condotte delle parti.

Indiscutibile è che la responsabilità per la sottrazione delle somme debba imputarsi al ricorrente, il quale ha inserito i dati della propria carta di credito, ritenendo che ciò servisse a ricevere – e non ad effettuare – un pagamento. Tra l'altro, l'intermediario dà prova della SCA producendo i log dell'operazione contestata, dai quali risulta che la stessa è stata autorizzata tramite fattore di possesso (device in uso abituale al cliente) e fattore di conoscenza (Pin per validare la credenziale dinamica OTP). Dunque, v'erano elementi sufficienti per mettere in allarme l'odierno ricorrente, il quale ha ricevuto anche la notifica push, che lo avvisava dell'operazione di pagamento che stava per effettuare. Parte ricorrente, tuttavia, lamenta una responsabilità dell'intermediario in ordine alla truffa subita. In particolare, afferma che esso non ha attivato i sistemi di monitoraggio antifrode necessari per bloccare una transazione palesemente sospetta verso un esercente estero.

Il Collegio non ritiene condivisibile tale prospettazione. Anche considerando la relativa modestia delle somme oggetto della disposizione, rimasta, peraltro, isolata, non si poteva pretendere dall'intermediario – che nessun ruolo, neanche passivo, ha svolto nella truffa – nulla di più dell'attivazione dell'ordinario sistema di SCA.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE