

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) NASO	Membro di designazione rappresentativa dei clienti

Relatore DOMENICO NASO

Seduta del 04/12/2025

FATTO

Con ricorso introduttivo del presente giudizio preceduto da reclamo del 03/06/2025, parte ricorrente esponeva che, a seguito della registrazione su una nota applicazione per la compravendita tra privati, in data 03/06/2025 riceveva un messaggio relativo ad un capo da lei messo in vendita, ove risultava la richiesta di acquisto di un capo da parte di un utente, in forza della quale la predetta avrebbe dovuto registrare i suoi dati al fine di ottenere il relativo pagamento.

La ricorrente seguiva le indicazioni fornite dalla chat e, alla ricezione dell'e-mail, attivava la funzione di acquisto e conferma della vendita, attraverso inserimento dei dati bancari della propria carta.

L'operatore del supporto tecnico della chat dell'app comunicava la presenza di anomalie, che rendeva necessario il versamento di ulteriori somme da corrispondere; la ricorrente eseguiva pertanto cinque operazioni di pagamento, per un importo complessivo di euro 1.252,00, del quale chiedeva l'immediata restituzione in quanto oggetto di truffa.

Si costituiva in giudizio l'Intermediario resistente, il quale rilevava l'esecuzione delle operazioni da parte della ricorrente personalmente, che autorizzava le notifiche *push* ricevute nell'applicazione dell'Intermediario.

Rilevava la Banca che il *device* utilizzato per autorizzare le operazioni era il medesimo in uso della ricorrente e che pertanto non poteva ascriversi alcuna responsabilità in capo all'Intermediario, tenuto conto della condotta negligente e gravemente colposa della ricorrente, la quale aveva cliccato sul link ricevuto da un indirizzo email non riconducibile all'app di compravendita e, a seguito del reindirizzamento sul sito, inseriva le credenziali della sua carta e autorizzava le operazioni di pagamento.

L'Intermediario insisteva pertanto per il rigetto del ricorso.

DIRITTO

Parte ricorrente chiede la restituzione della somma complessiva di euro 1.252,00 relativa a cinque operazioni di pagamento eseguite in data 03/06/2025 e disconosciute, di importo pari rispettivamente ad euro 195,00, euro 99,00, euro 299,00, euro 499,00 e euro 160,00.

Le operazioni contestate sono state effettuate dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (cosiddetta PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15/12/2017, entrato in vigore in data 13/01/2018, che modifica in più punti il d.lgs. n. 11 del 2010.

In particolare, ai fini della verifica del rispetto della Strong Customer Authentication (c.d. SCA), affinché l'Intermediario possa andare esente da responsabilità dovrà fornire prova, oltre che

dell'insussistenza di malfunzionamenti, dell'adozione di un sistema di sicurezza adeguato e della corretta registrazione, autenticazione e contabilizzazione delle operazioni contestate.

Come sancito dal Collegio di Coordinamento con la decisione n. 22745/19: *<<...la previsione di cui all'art. 10, comma 2, del D.lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'Intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente>>.*

Con riferimento alle modalità di autenticazione dell'operazione di pagamento, la ricorrente stessa afferma di aver inserito i dati della carta e di aver confermato le transazioni mediante conferma di notifica *push* ricevuta.

Secondo l'orientamento consolidato dell'Arbitro, quando l'operazione è eseguita per intero dal pagatore – con inserimento della disposizione di pagamento e dei fattori di autenticazione – deve considerarsi autorizzata e dunque non soggetta al regime di responsabilità di cui alla PSD2.

Pur tuttavia, può residuare una responsabilità a carico dell'Intermediario in presenza di un apporto causale alla frode, sussistente in presenza di alcuni indici:

- 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, 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.

Nel caso di specie, l'Intermediario ha dimostrato che il processo di autenticazione delle operazioni è stato spontaneamente eseguito dalla ricorrente.

Avuto riguardo all'apporto causale alla frode da parte dell'Intermediario – quale elemento da valutare ai fini dell'eventuale individuazione di una responsabilità concorrente della Banca – si rileva che la truffa non si è svolta attraverso i canali ufficiali della Banca, tenuto conto che le transazioni eseguite sono riconducibili ad un'applicazione estranea all'Intermediario.

Secondo il consolidato orientamento di questo Arbitro, in ipotesi di “sito clone”, non può essere ravvisata la responsabilità della Banca in quanto <<[...] *non sono stati tuttavia veicolati messaggi truffaldini apparentemente provenienti dalla banca; infatti, nello specifico, il ricorrente pare aver inserito i dati della carta e le credenziali per il pagamento sul sito clone della piattaforma di compravendita, quindi al di fuori dei canali ufficiali della banca.* [...]>> (Collegio di Roma, decisione n. 6534/2024).

Nella fattispecie in oggetto, l'Intermediario ha peraltro inviato alla ricorrente degli alert ove la informava dei pagamenti in corso verso un'applicazione esterna, che è stata sbloccata manualmente dalla ricorrente.

Tenuto conto della grave negligenza della ricorrente, alla quale è esclusivamente ascrivibile la condotta colposa consistita nell'esecuzione e autorizzazione delle operazioni di pagamento oggetto di truffa, il ricorso non merita accoglimento.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE