

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) CARATELLI	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore FABRIZIO MAIMERI

Seduta del 14/01/2026

FATTO

Con ricorso del 29.8.2025, parte attrice lamenta di essere stata vittima di truffa telefonica a seguito del furto della nuova carta prepagata che avrebbe dovuto esserle spedita al domicilio; In particolare, i truffatori hanno rubato la carta prima che fosse recapitata e poi hanno chiamato l'istante, che, sotto raggiri, ha comunicato il PIN della carta tramite *sms*. Le operazioni sono state effettuate con la carta fisica a Napoli, mentre la cliente si trovava a Roma presso l'ufficio dell'intermediario per bloccare lo strumento. L'intermediario ha riconosciuto un rimborso di € 570,00 a fronte di operazioni disconosciute pari complessivamente a € 1.064,50. Tuttavia, l'istante chiede la restituzione integrale della somma sottratta (dunque, ulteriori € 494,50), poiché «il furto della carta è avvenuto durante la spedizione a cura» dell'intermediario.

In sede di controdeduzioni, l'intermediario espone che il 7.8.2025 alle 15:11 circa, la cliente ha ricevuto una chiamata da un numero di telefono privato, in nessun modo riconducibile all'intermediario; successivamente, sempre da un numero di telefono privato non riconducibile alla resistente, ha ricevuto un *sms* al quale ha risposto comunicando il codice PIN della sua carta di pagamento. La ricorrente, accedendo sulla propria *home banking*, si è avveduta di movimenti presenti sulla sua carta da lei non riconosciuti. L'intermediario, riconoscendo la paritaria responsabilità tra le parti, provvedeva al rimborso parziale dell'importo frodato, per € 570,00. Evidenza che nel caso in esame a parte ricorrente è stato riconosciuto altresì il rimborso di tutte le operazioni autorizzate in NCV, in

adempimento al consolidato orientamento ABF, «cui l'intermediario intende adeguarsi», nei casi di cd “*boxing*” come quello oggetto dell'odierno ricorso: la responsabilità deve essere equamente ripartita tra cliente ricorrente ed intermediario nella misura pari al 50% del pregiudizio economico lamentato». Da un lato, infatti, appare censurabile la condotta negligente con cui la cliente comunica al falso addetto dell'intermediario i propri codici segreti (quali il PIN); dall'altro, deve ascriversi all'intermediario una non corretta gestione dell'operazione di consegna della carta di pagamento, in quanto la posta ordinaria con cui vengono inviate le carte in rinnovo può effettivamente risultare strumento non adeguato ad evitare rischi di furti e accessi non autorizzati. Il PIN associato alla carta rimane il medesimo anche con l'emissione della carta nuova e il primo prelievo sconosciuto è stato autorizzato con la corretta lettura del *chip* della carta e l'immediata e corretta digitazione del PIN; la carta è stata attivata tramite *app*. In materia di *phishing* l'intermediario sta rendendo edotta la propria clientela sui rischi di frode, e richiama i e iniziative assunte al riguardo.

In relazione alle rispettive argomentazioni, la ricorrente chiede all'Arbitro «di rivedere la mia pratica di disconoscimento delle operazioni in quanto vittima di truffa e chiedo il 100% del rimborso in quanto il furto della carta è avvenuto durante la spedizione a cura [dell'intermediario]. E nello stesso giorno. È capitato ad altre 4 persone del mio stesso ufficio (...) con la stessa modalità sempre a Napoli. Essendo stata sia vittima di furto che di *phishing* chiedo cortesemente il 100% del rimborso. La somma delle operazioni sconosciute ammonta a € 1.064,50. Richiedo quindi la restante somma di € 494,50 oltre quella erogata». Dal canto suo, l'intermediario chiede al Collegio «di rigettare la domanda della ricorrente in quanto infondata in fatto e in diritto, stante l'accertata legittima esecuzione delle transazioni sconosciute dalla ricorrente, delle quali è stata accertata l'oggettiva regolarità e l'avvenuta corretta autenticazione e autorizzazione».

DIRITTO

La controversia ha ad oggetto il disconoscimento di cinque operazioni effettuate il 7.8.2025 tra le 15:52 e le 16:08 con una carta – emessa in sostituzione dello strumento di pagamento in scadenza intestato alla ricorrente – verosimilmente intercettata dai frodatori (c.d. *boxing*). L'intermediario afferma di aver rimborsato le transazioni NCV (€ 27,50, € 27,50 ed € 19,50) e il 50% delle restanti operazioni sconosciute: vale a dire, € 27,50 + € 27,50 + € 19,50 + € 495,00 [€ 600,00 + € 390,00 : 2 = € 495,00] = € 570,00.

La ricorrente precisa di non aver mai ricevuto lo strumento di pagamento. Dai *log* si evince che la carta è stata attivata tramite *app* il 7.8.2025; l'intermediario riferisce che le operazioni contestate sono state effettuate con lettura del *microchip* e con digitazione immediatamente corretta del codice PIN. Dalla *legenda* delle evidenze informatiche versate, emerge che «la dicitura “PIN” indicata nella colonna “Dati autenticazione” certifica che al momento della materiale esecuzione delle operazioni i sistemi informativi non hanno rilevato alcuna anomalia o irregolarità, essendo state disposte dietro diretta ed immediata autenticazione da parte della legittima titolare. Si evidenzia che le operazioni autorizzate in modalità NCV sono state rimborsate al 100%, mentre le operazioni autorizzate in modalità PIN al 50%. (...) Si sottolinea che la dicitura “M” nella colonna “Input Mode” identifica operazioni autorizzate con Microchip, la dicitura “C” identifica operazioni autorizzate in modalità *contactless*».

L'intermediario riconduce la fattispecie al *boxing* e al *social engineering*. Ritiene quindi che la carta sia stata intercettata dai frodatori in seguito alla spedizione della nuova tessera in occasione del rinnovo della carta in scadenza. Esso ha, altresì, chiarito che l'attivazione è avvenuta con la digitazione del vecchio PIN. Produce documentazione dalla quale si evince che il PIN non è stato rigenerato, rimanendo il medesimo di quello associato alla carta in fase di prima emissione e quindi noto solo al cliente. La ricorrente ha riferito di essere stata contattata da un sedicente operatore e di aver comunicato il codice PIN tramite *sms*. Come detto, l'intermediario ha riferito di aver già provveduto al

rimborso di € 570,00, pari alle transazioni NCV e al 50% dell'importo delle altre operazioni contestate, conformandosi così, afferma lo stesso intermediario, all'orientamento dei Collegi territoriali ABF che prevede una «ripartizione di responsabilità delle parti», nella misura del 50%, «considerate: - la violazione gravemente colposa dell'obbligo di custodia delle credenziali della carta da parte dell'utente; - la mancata adozione di presidi di sicurezza idonei a evitare l'ingerenza di terzi nella sfera patrimoniale della client+e da parte dell'intermediario, sul quale grava il rischio di impresa derivante dalla spedizione dello strumento». La ricorrente chiede il rimborso integrale della somma sottratta.

Dagli atti emerge che l'istante ha ricevuto una chiamata e poi un *sms* da un numero non riconducibile all'intermediario, sebbene nel corpo del messaggio ne sia stato menzionato il nome. Nei casi di *vishing*, i Collegi ritengono pari la responsabilità delle parti. Cfr., per tutte, Collegio di Napoli, decisione n. 11845 del 14.11.2024, secondo la quale «il caso di specie va inquadrato in una prassi socialmente rilevante cd. di *boxing* e *social engineering*, in cui il contatto telefonico del titolare di uno strumento di pagamento viene raggiunto da un truffatore che si finge falso addetto dell'intermediario e che con comunicazioni provenienti da utenze telefoniche e da *sms* civetta visualizzati in *chat* dall'utente unitamente agli *sms* genuini provenienti dall'intermediario, viene indirizzato verso un sito *internet* del tutto identico o molto simile a quello ufficiale dell'intermediario, con ciò rendendo pressoché impossibile la distinzione (una tecnica di cd. *social engineering* di *vishing* e *spoofing*). In tal modo, il truffatore già in possesso dei dati personali del ricorrente (essendosi appropriato della carta), ottenuta la sua fiducia, gli estorce altri dati tra cui (codice di sicurezza della carta, PIN). Alla luce di tali prassi, può essere valutata la condotta del ricorrente certamente incorso in una colpa grave, considerato che la nuova carta è stata attivata con digitazione del vecchio PIN, evidentemente fornito dal cliente ai truffatori. Peraltro l'intermediario non ha fornito evidenza della consegna della carta al domicilio del cliente, gravando su parte resistente – art. 8, comma 2, d.lgs. n. 11/2020 – i rischi concernenti la spedizione del nuovo strumento di pagamento. Si è determinato, nel caso concreto, un concorso di colpa di talché, considerato il rimborso già effettuato a favore del cliente, null'altro va restituito a suo favore (v. nel medesimo senso, Coll. Napoli, decisione n. 7388/2023)». V. anche nel medesimo senso Collegio di Milano, decisione n. 10877 del 15.10.2024; Collegio di Bologna, decisione n. 11968 del 19.11.2024; Collegio di Torino, decisione n. 11590/2024.

In ogni caso, anche qualora il Collegio volesse dare rilevanza alla menzione del nome dell'intermediario nel testo del messaggio, nelle ipotesi di *spoofing* il Collegio di Roma (decisione n. 6569/2024) esclude la colpa grave dell'utente, salvo la presenza di indizi di anomalia, qui peraltro presenti. Infatti, il messaggio non è inserito nella *chat* con l'intermediario e presenta errori di sintassi («la confermiamo la richiesta»; «per confermare inserisce il suo vecchio PIN»).

Occorre allora concludere che la realizzata divisione al 50% fra le parti della perdita risulta coerente con la fattispecie esaminata, senza che sia necessario disporre ulteriori importi favore della ricorrente.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE