

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) SICA	Membro di designazione rappresentativa degli intermediari
(RM) NOTARO	Membro di designazione rappresentativa dei clienti

Relatore DANIELA CONCETTA NOTARO

Seduta del 10/04/2026

FATTO

Con ricorso del 20.11.2025 (preceduto da rituale reclamo, negativamente riscontrato dall'intermediario) l'istante si è rivolto a codesto Collegio rappresentando che in data 12/11/2025, alle ore 14:09 riceveva una chiamata da un numero di telefono, durante la quale l'interlocutore lo informava della sostituzione della carta in scadenza.

Durante il contatto telefonico il frodatore, a conoscenza di tutti i suoi dati, induceva il ricorrente ad entrare nella propria app e provvedeva ad attivare la carta sostitutiva.

Parte ricorrente successivamente controllava tramite app la propria carta di pagamento e si avvedeva di operazioni in addebito non riconosciute effettuate tra le 14:23 e le 14:37, consistenti in Un prelievo di euro 600,00, una ricarica di euro 391,00 ed un pagamento di euro 130,00, per un totale di 1.125 €.

Il 19/11/2025 l'intermediario rimborsava il 50% (560 €) dell'importo.

Con l'odierno ricorso, pertanto, l'istante ha richiesto il rimborso delle somme residue.

Nel costituirsi con apposite controdeduzioni, l'intermediario ha rilevato che, relativamente alle modalità di autenticazione, le operazioni sono state autorizzate mediante CHIP e PIN inserito al primo tentativo, senza la rilevazione di alcuna anomalia.

Per quanto concerne la dinamica della frode, ritiene che si possano riscontrare elementi di "social engineering" e di "boxing". In base a tali circostanze, sostiene che la responsabilità sia da attribuirsi in misura condivisa: da un lato, la cliente avrebbe comunicato il proprio codice segreto a un falso operatore; dall'altro, l'intermediario non avrebbe gestito correttamente la consegna della carta.

Il blocco della carta in questione è avvenuto alle ore 09:17 del giorno 18/11/2025 e, pertanto, successivamente alle operazioni per cui è controversia: il cliente non ha adempiuto ai propri doveri di

tempestiva informativa all'intermediario dell'accaduto, permettendo l'esecuzione delle operazioni e di conseguenza le stesse non sono imputabili all'Intermediario.

Tuttavia, riconoscendo la paritaria responsabilità tra le parti, l'intermediario provvedeva in fase di riscontro al reclamo al rimborso del 50% dell'importo frodato, riaccreditando la somma di Euro 560.

Conclude chiedendo il rigetto del ricorso, precisando che il servizio di sms alert era attivo di default sull'app della ricorrente.

DIRITTO

Nel merito, va chiarito che la parte ricorrente disconosce n. 3 operazioni per l'importo complessivo di € 1.125,00, eseguite tramite una carta emessa in sostituzione di altra carta scaduta a lei intestata.

L'intermediario ha provveduto al rimborso parziale dell'importo sottratto, pari ad € 560,00, come da evidenze prodotte in atti.

In ordine alle modalità di autenticazione, l'intermediario sostiene che le operazioni contestate sono state perfezionate tramite il riconoscimento del microchip (fattore di possesso) ed il corretto inserimento del PIN (fattore di conoscenza) conformemente ai requisiti normativi previsti dalla "SCA - *Strong Customer Authentication*".

Al riguardo, produce le seguenti evidenze informatiche, al fine di fornire informazioni tecniche circa le modalità di esecuzione.

In particolare, all'interno dell'apposito allegato alle controdeduzioni, la dicitura "PIN" nella colonna "Dati Autenticazione" certifica che non sono state riscontrate anomalie o irregolarità nelle transazioni, poiché disposte a seguito di diretta autenticazione della titolare. Difatti, i prelievi sono avvenuti con la digitazione immediatamente corretta del PIN così come evidenziato dalla presenza del codice 0 nella sezione "action code".

L'intermediario sostiene che per autorizzare i prelievi è stato utilizzato il medesimo codice segreto della carta scaduta, atteso che i sistemi aziendali, che di norma tracciano le eventuali modifiche o rigenerazioni del PIN, nel caso di specie non hanno generato alcuna richiesta in tal senso.

Rispetto agli elementi rilevanti dell'evento presuntivamente fraudolento, si precisa che dalla denuncia versata in atti emerge che il 12.11.2025, alle ore 14:09 il ricorrente riceveva una chiamata da un numero privato, con cui un sedicente operatore riusciva a ottenere l'attivazione della carta intercettata a seguito dell'accesso all'app da parte del cliente.

Orbene, sebbene l'intermediario abbia riconosciuto una sua parziale responsabilità per l'accaduto e si sia attivato per il rimborso del 50% dell'importo sottratto – in linea con gli ormai consolidati orientamenti ABF - contesta alla ricorrente una colpa grave per aver comunicato il PIN del suo mezzo di pagamento. Ciò nonostante il ricorrente agisce per la ripetizione integrale della somma fraudolentemente sottratta, negando la propria implicazione causale nella vicenda.

Tanto premesso, la fattispecie appare riconducibile all'ipotesi di *boxing*.

In particolare, in tali circostanze il Collegio è solito ravvisare un concorso di colpa tra le parti, rinveniente - da un lato dalla violazione da parte del cliente, degli obblighi di custodia dello strumento di pagamento e delle relative credenziali (ex art. 7 D.Lgs. 11/2010) e, dall'altro lato, dalla violazione del "*dovere dell'intermediario di porre il massimo livello di attenzione nella scelta del metodo di spedizione dello strumento di pagamento*" (ex art. 8, comma 2 del d.lgs. 11/2010, in base al quale "*I rischi derivanti dalla spedizione di uno strumento di pagamento o delle relative credenziali di sicurezza personalizzate sono a carico del prestatore di servizi di pagamento*", e dalle corrispondenti disposizioni di attuazione del D.Lgs. 11/2010, contenute nel regolamento della Banca d'Italia del 5.07.2011) (ex multis Collegio di Roma, decisione n. 8860 del 07.06.2022).

Nello specifico, secondo l'orientamento consolidato dei Collegi, nei casi in cui la frode viene realizzata con l'utilizzo delle tecniche del c.d. boxing (i truffatori intercettano e rubano la carta di pagamento spedita dall'emittente al titolare unitamente ai suoi dati personali), risulta ravvisabile una ripartizione di responsabilità delle parti, considerate la mancata adozione di presidi di sicurezza idonei a evitare l'ingerenza di terzi nella sfera patrimoniale del cliente da parte dell'intermediario, sul quale grava il rischio di impresa derivante dalla spedizione dello strumento (cfr. infra art. 8, comma 2, D.Lgs. n. 11/2010); la violazione degli obblighi posti a carico dell'utente dei servizi di pagamento in relazione alla custodia delle credenziali di sicurezza personalizzate. E per analoghe fattispecie questo Arbitro, valorizzando anche altri elementi di fatto (quali l'omesso invio di sms alert e, in generale, la presenza di criticità organizzative nel servizio di pagamento offerto dall'intermediario), ha accertato il concorso di colpa tra le parti, disponendo una ripartizione delle responsabilità in misura pari a 1/3 a carico del ricorrente e di 2/3 a carico dell'intermediario (cfr. Collegio di Roma, decisione n. 1585/2023).

Si evidenzia, poi, che non sono agli atti evidenze della telefonata ricevuta dal falso operatore, che, tuttavia, per ammissione di parte ricorrente, proveniva da un'utenza privata, non riferibile alla banca. Ebbene, in virtù della ricostruzione fattuale nonché della documentazione prodotta dalle parti si evince la presenza di un concorso di colpa rispetto al quale l'adempimento spontaneo dell'intermediario (ai sensi dell'articolo 1227 c.c.) è ampiamente soddisfattivo delle pretese del ricorrente.

A ciò consegue la cessazione della materia del contendere.

PER QUESTI MOTIVI

Il Collegio dichiara cessata la materia del contendere.

IL PRESIDENTE