

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) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore MASSIMO CARATELLI

Seduta del 13/03/2026

FATTO

1. La controversia attiene alla contestazione di alcuni addebiti, operati attraverso il servizio di *home banking* a valere su di una carta di debito rilasciata dalla convenuta e intestata alla proponente.
2. In particolare, in base alla dinamica riferita da parte attrice, l'istante – in data 6 maggio 2023, alle ore 17.30 – riceveva sulla propria utenza cellulare un SMS apparentemente proveniente dall'intermediario resistente, con il quale veniva invitata ad aggiornare le credenziali di accesso "*nell'area a lei riservata sul sito*" dell'istituto di credito. Ritenendo il messaggio genuino, la ricorrente procedeva al cambio delle credenziali. Subito dopo, riceveva due telefonate nel corso delle quali un soggetto, qualificatosi come addetto dell'ufficio antifrode, le rappresentava la presenza di due operazioni anomale, provenienti dalla Svizzera, sulla sua carta di debito. A seguito di ciò, la proponente contattava il servizio clienti della banca, apprendendo che ignoti avevano disposto – in data 6 maggio 2023 – due operazioni non autorizzate, rispettivamente di euro 391,00 e di euro 381,00, entrambe eseguite alle ore 17.39 in favore di un beneficiario a lei sconosciuto. Alla luce delle modalità con cui si sono svolti i fatti, l'istante deduce che il sistema di autenticazione e protezione adottato

dall'intermediario non risulta conforme ai requisiti della *strong customer authentication (SCA)*, atteso che – in caso contrario – il danno si sarebbe potuto evitare. Tanto premesso, parte attrice chiede il rimborso integrale delle somme sottratte, pari a euro 772,00.

3. Con le controdeduzioni, parte convenuta rileva che la ricorrente, titolare di una carta di debito, richiede il rimborso di due operazioni di ricarica disposte *online* ed eseguite in data 6 maggio 2023 mediante l'utilizzo delle proprie credenziali di sicurezza. La resistente precisa che l'istante è stata verosimilmente vittima di una truffa riconducibile al cd. "phishing", evidenziando tuttavia che non è stata allegata alcuna documentazione idonea a dimostrare l'accaduto, quale, ad esempio, l'SMS ricevuto o il registro delle chiamate. Rappresenta, inoltre, che la cliente ha provveduto al disconoscimento delle operazioni solo in data 8 maggio 2023. L'intermediario evidenzia che le operazioni risultano approvate correttamente mediante sistema di autenticazione forte, nel rispetto dei requisiti della SCA e in assenza di anomalie. Sottolinea, altresì, che non risultano modifiche del *device* utilizzato poco prima della disposizione delle operazioni, circostanza che induce a ritenere che le stesse siano state eseguite dal medesimo cellulare della ricorrente. La convenuta osserva, inoltre, che parte attrice non ha fornito elementi idonei a dimostrare la natura fraudolenta delle operazioni, richiamando sul punto l'orientamento consolidato dei Collegi ABF, secondo cui grava sul ricorrente l'onere di fornire "*elementi utili a provare che l'operazione sia stata realmente fraudolenta*" (cfr. Collegio di Coordinamento, decisione n. 897/2014). Evidenzia, infine, che la stessa proponente ha ammesso di aver inserito le proprie credenziali e i dati della carta su un *link* fraudolento e di aver successivamente comunicato i codici di sicurezza ricevuti sul proprio telefono, consentendo così al truffatore – seppure inconsapevolmente – di disporre le operazioni oggetto di contestazione. Alla luce di quanto sopra, la banca deduce che la condotta della ricorrente sia connotata da "colpevole credulità", in una fattispecie estranea alla sfera di controllo dell'intermediario. Richiama, al riguardo, l'orientamento secondo cui tali forme di raggiro risultano ormai note anche all'utente medio, con conseguente configurabilità di una negligenza inescusabile (cfr. Collegio di Coordinamento, decisione n. 3498/2012). Alla luce di quanto precede, l'intermediario chiede il rigetto del ricorso, in quanto infondato in fatto e in diritto.

4. In sede di repliche, l'istante afferma che – anche alla luce delle controdeduzioni – risulta evidente come sia stata vittima di un fenomeno di *vishing* e *spoofing*. A riguardo, precisa che l'intermediario ha contestato la riconducibilità all'istituto di credito del numero di telefono indicato nel messaggio civetta, ma richiama l'orientamento prevalente dei Collegi ABF, secondo cui nelle ipotesi di *spoofing* – non è generalmente ravvisabile la colpa grave del ricorrente, in ragione dell'elevato grado di insidiosità del meccanismo fraudolento. Riferisce, altresì, di aver sporto denuncia, pur senza produrre il testo del

messaggio, in quanto non richiesto in tale sede; aggiunge che non poteva ragionevolmente prevedere la necessità di conservarlo, non avendo conoscenze specifiche in materia.

5. Con le controrepliche, la resistente richiama quanto già affermato nelle precedenti difese ribadendo i profili di colpa grave dell'utente.

DIRITTO

1. Ebbene, ad avviso di questo Arbitro, la ricorrente non offre elementi utili a ricostruire la frode, limitandosi a riferire – genericamente – di aver proceduto al cambio delle credenziali a seguito della ricezione, sulla propria utenza cellulare, di un SMS apparentemente proveniente dall'intermediario resistente. Osserva, peraltro, il Collegio che non è presente in atti il testo del messaggio civetta, il quale – alla luce delle deduzioni formulate in sede di repliche – non risulta essere stato conservato dalla proponente.

2. Sul punto si osserva che, secondo l'orientamento condiviso dai Collegi territoriali, le mancate allegazioni del cliente sulle circostanze di fatto della frode rappresentano un elemento da cui l'Arbitro può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente (cfr. Collegio di Roma, decisione n. 11050/2024).

3. A tale riguardo, si osserva che la banca ha fornito evidenza della mancata modifica del *device* utilizzato per l'esecuzione delle operazioni, le quali risultano, pertanto, verosimilmente disposte mediante il *mobile token* della cliente. Tale circostanza, peraltro, non è stata oggetto di contestazione in sede di repliche.

4. Tanto premesso, in assenza di elementi idonei a contestualizzare l'evento truffaldino, questo Collegio ritiene di dover respingere la richiesta restitutoria del proponente, desumendone la colpa grave, in linea con quanto già espresso con la decisione n. 23474/2021, per cui *“[l']assoluta carenza di allegazione da parte del cliente rende eccessivamente generica la rappresentazione del fatto costitutivo della pretesa restitutoria, che legittima la veridicità dell'ipotesi dell'utilizzo dello strumento di pagamento imputabile per colpa grave al titolare”*).

5. In relazione a quanto precede, il ricorso non può, pertanto, essere accolto.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE