

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) PICARO	Membro designato dalla Banca d'Italia
(RM) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) NOTARO	Membro di designazione rappresentativa dei clienti

Relatore DANIELA CONCETTA NOTARO

Seduta del 13/02/2026

FATTO

Con ricorso del 6 settembre 2025 (preceduto da regolare reclamo, negativamente riscontrato dall'intermediario) l'istante si è rivolto a codesto Collegio, rappresentando di essere titolare di una carta di pagamento, emessa dall'intermediario X e gestita dal resistente in qualità di licenziatario del circuito internazionale, collegata al conto corrente radicato presso l'intermediario X.

In data 21/08/2025, ha ricevuto un SMS da un numero di telefono mobile in chiaro con il quale le veniva comunicato che era stato sospeso un bonifico di € 1.786,00 e che per disconoscerlo era necessario contattare un numero di telefono.

Contattava il numero riportato e l'interlocutore si presentava come agente della sezione antifrode dell'intermediario resistente, al quale la ricorrente ha riferito di non aver disposto lei il bonifico; costui le confermava che il conto corrente della ricorrente era stato violato ed erano in atto pagamenti ordinati da Lugano.

Il sedicente operatore, inoltre, consigliava alla ricorrente di bloccare la carta, il conto corrente e far transitare il denaro in un altro conto, che avrebbe attivato direttamente al telefono.

Non confidando nella bontà delle informazioni ricevute dal presunto operatore, comunicava l'intenzione di interrompere la chiamata in attesa di essere ricontattata dalla propria banca.

Pochi istanti dopo, riceveva una chiamata da un numero riconducibile all'intermediario X di radicamento del conto (non convenuto nell'odierno ricorso) ed ha creduto alla genuinità di quanto le veniva riferito.

Su richiesta dell'interlocutore, comunicava i dati personali, i dati del conto necessari per accedere all'assistenza clienti ed i dati per accedere alla banca online.

Avvedendosi della esecuzione di tre transazioni per un valore complessivo di € 1.988,00 (di cui chiede il rimborso nel ricorso), sporgeva denuncia presso i carabinieri.

Nel costituirsi con apposite controdeduzioni, l'intermediario eccepiva la propria carenza di legittimazione passiva in quanto non è né emittente né collocatore dello strumento di pagamento ma mero licenziatario del circuito internazionale ed in tale veste si limita a svolgere talune attività relative all'operatività della carta.

La banca X è deputata alla gestione dei rapporti con la clientela; tuttavia il resistente ha riscontrato il reclamo in qualità di mero fornitore del servizio di gestione delle contestazioni per conto della Banca X, indicando altresì la possibilità di rivolgersi direttamente alla Banca X.

Nel merito ha chiarito che in data 21.08.2025 la ricorrente ha ricevuto un messaggio SMS proveniente da un numero di telefonia mobile a lei sconosciuto, nel quale le veniva segnalata l'esecuzione di un bonifico fraudolento.

L'istante, dando seguito alle istruzioni contenute nel messaggio, ha contattato un ulteriore numero di cellulare non riconducibile né al resistente né alla banca X e ha interloquito con un presunto operatore antifrode.

Successivamente è stata contattata da un numero riconducibile alla banca X e nel corso della conversazione ha fornito i dati della propria carta di debito.

Peraltro, il contenuto dell'SMS, relativo a un presunto "bonifico" non eseguibile tramite una carta di debito, avrebbe dovuto rivelare la natura fraudolenta dello stesso.

La ricorrente si avvedeva tardivamente, dopo le attività espletate, di essere rimasta vittima di un raggiro e, sempre in data 21 agosto 2025, ha contattato il servizio clienti per richiedere il blocco della carta.

A seguito della contestazione, l'intermediario resistente ha effettuato il rimborso della prima transazione, pari a € 990,00, tenuto conto del fatto che la chiamata ricevuta dalla Cliente proveniva da un numero che poteva apparire riconducibile alla Banca emittente.

Per le operazioni successive alla prima, la richiesta di rimborso è stata respinta in quanto la ricorrente ha ricevuto l'SMS alert di addebito dell'operazione e da ciò ella avrebbe dovuto desumere la frode.

Nonostante ciò, la Cliente ha proseguito nell'esecuzione di ulteriori operazioni, seguendo pedissequamente le istruzioni dei truffatori e ciò denota la colpa grave della stessa.

In ordine alle operazioni contestate, le stesse sono avvenute con positiva validazione dei codici OTP SMS inviati sul numero di cellulare della ricorrente e positiva validazione del codice segreto K** che deve essere digitato nella pagina di autenticazione dei pagamenti online, in aggiunta all'inserimento del codice OTP che l'utente riceve via SMS sul cellulare certificato.

A tal proposito, l'intermediario ha evidenziato che non si sono verificati accessi all'aera personale di App o portale; pertanto, non vi è stata alcuna intrusione o visualizzazione codice K** nella data dell'evento oggetto del ricorso.

Pertanto, la resistente ha richiesto la declaratoria di carenza di legittimazione passiva. In subordine, chiede il rigetto del ricorso e la rideterminazione del *petitum* in € 998,00.

DIRITTO

Come noto, l'utilizzo fraudolento è disciplinato dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento

delle disposizioni interne al regolamento (UE) n. 751/2015 correlata alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Sul punto si rammenta che, secondo la posizione consolidata dell'ABF, la disciplina sopra citata prevede un regime probatorio di favore per l'utente di strumenti e servizi di pagamento, essendo *"ispirata al principio del "rischio d'impresa", e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi"* (così Collegio di coordinamento, decisione n. 3498/2012).

In particolare, l'art. 10 del d.lgs. 11/2010 (*infra* riportato) prevede, in merito all'onere della prova gravante sul prestatore dei servizi di pagamento (PSP), una precisa e graduata sequenza, in base alla quale il PSP è tenuto a dimostrare:

A. l'autenticazione, la corretta registrazione e contabilizzazione della o delle operazioni contestate e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

Nello specifico, secondo gli orientamenti condivisi dei Collegi, la prova di autenticazione rappresenta, in aderenza al dato normativo l'antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente;

B. il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

Preliminarmente, si rileva che nelle controdeduzioni l'intermediario eccepisce la carenza di legittimazione passiva in quanto mero licenziatario del circuito internazionale, privo tanto della qualifica di emittente, quanto della qualifica di collocatore della carta utilizzata per eseguire le transazioni in contestazione. Afferma, dunque, che unica legittimata passiva sia la banca X, emittente dello strumento di pagamento.

A supporto di tale eccezione, l'intermediario riporta nel corpo delle controdeduzioni uno stralcio della Convenzione stipulata con la banca X di radicamento del conto.

Peraltro, il resistente non ha prodotto la copia della Convenzione, sicché non è dato comprendere il riparto dei compiti tra l'odierna resistente e la banca di radicamento del conto.

Dalla documentazione in atti, poi, risulta che l'intermediario è entrato nel merito delle contestazioni: ha riscontrato il reclamo e ha prodotto i LOG relativi all'autenticazione delle operazioni.

Nel fare ciò, la banca resistente ha precisato che la resistente ha assunto la gestione della richiesta di disconoscimento in qualità di fornitore delegato dalla Banca.

In tale direzione, dalla documentazione allegata dall'intermediario sembrerebbe emergere che esso sia entrato nel merito delle contestazioni, rilevando che l'operazione era stata correttamente autenticata.

Peraltro, il processo di autenticazione è un elemento a difesa riproposto nelle controdeduzioni. Ciò appare confermare che l'intermediario sia deputato a gestire non solo il processo di autenticazione, ma anche le controversie discendenti dalla contestazione delle operazioni.

Sul punto, occorre specificare che i Collegi territoriali hanno affrontato eccezioni di carenza di legittimazione passiva simili a quella oggetto dell'odierno ricorso e la gran parte delle pronunce affermano la legittimazione dell'intermediario che ha curato la gestione della pratica di contestazione riscontro nel merito la richiesta di rimborso; la conclusione è avvalorata quando l'intermediario, costituendosi nella procedura ABF, ha prodotto la documentazione tecnica relativa al processo di

autenticazione delle transazioni impugnate. Questi criteri depongono nel senso della legittimazione passiva dell'odierna resistente (cfr. Collegio di Roma, decisione n. 10549 del 28.10.2025).

Nel merito, si evidenzia che la ricorrente richiede il rimborso di € 1.988,00, sottratti mediante tre operazioni fraudolente.

In particolare, sono oggetto di contestazione le seguenti operazioni:

- un pagamento di € 990,00 eseguito con carta di debito in data 21.08.2025 alle ore 14:33;
- un pagamento di € 499,00 eseguito con carta di debito in data 21.08.2025 alle ore 14:36;
- un pagamento di € 499,00 eseguito con carta di debito in data 21.08.2025 alle ore 14:38.

Tuttavia, l'intermediario resistente fa presente di aver rimborsato la prima operazione disconosciuta, ovvero il pagamento di € 990,00 eseguito in data 21.08.2025 alle ore 14:33.

Si fa presente, infatti, che l'intermediario ha inizialmente accreditato al ricorrente le tre operazioni fraudolente e, dopo aver svolto verifiche, ha riaddebitato le due operazioni da € 499,00 ciascuna effettuate dopo le 14:34. Non ha invece stornato l'accredito di € 990,00 che risulta dunque confermato. Ne consegue che il *petitum* è da rideterminarsi in € 998,00.

In tale contesto, la controversia riguarda specificamente il disconoscimento di n. 2 pagamenti con carta di debito eseguiti in data 21.08.2025, rispettivamente alle ore 14:36 e 14:38, per un totale di € 998,00. In base a quanto emerge dalla denuncia e dalle ulteriori evidenze in atti si rileva che in data 21.08.2025, alle ore 12:18, la ricorrente ha ricevuto un SMS proveniente da un numero di telefono mobile a lei sconosciuto, nel quale le è stata segnalata l'esecuzione di un presunto bonifico ed indicato un secondo numero di cellulare da contattare per ulteriori verifiche.

L'SMS appare provenire da un'utenza non riconducibile alla banca resistente; sembrerebbe trattarsi infatti del primo messaggio incanalatosi nella chat.

Nell'intestazione del messaggio è riportato il nominativo dell'intermediario resistente e non sembra presentare gravi errori grammaticali.

Parte ricorrente, dando seguito alle istruzioni contenute nel messaggio, ha contattato il numero di telefono cellulare indicato, anch'esso non riconducibile alla banca resistente né all'emittente.

Alla chiamata ha risposto un soggetto che si è presentato come agente della sezione antifrode dell'intermediario resistente, al quale la ricorrente ha comunicato di aver ricevuto l'SMS.

l'interlocutore, in tale circostanza ha confermato che il conto corrente della ricorrente era stato violato e che erano in atto pagamenti ordinati da Lugano.

Inoltre, il sedicente operatore ha consigliato alla ricorrente di bloccare la carta, il conto corrente e far transitare il denaro in un altro conto, che avrebbe attivato al telefono.

Non confidando nella bontà delle informazioni ricevute dal presunto operatore, la ricorrente ha comunicato l'intenzione di interrompere la chiamata in attesa di essere ricontattata dalla propria banca. Pochi istanti dopo ha ricevuto una chiamata da un numero riconducibile all'intermediario X, emittente della carta di pagamento, e il medesimo interlocutore l'ha invitata ad effettuare un controllo della genuinità del numero su internet; fatti tali controlli la ricorrente ha pertanto ritenuto genuina la chiamata ricevuta.

Su richiesta dell'interlocutore, ha comunicato i dati personali, i dati del conto necessari per accedere all'assistenza clienti ed i dati per accedere alla banca online.

Successivamente, resasi conto di esser stata vittima di truffa, ha contattato il servizio clienti dell'intermediario resistente per chiedere il blocco della carta.

L'intermediario ha fornito evidenza dell'avvenuto blocco della carta, avvenuto in data 21.08.2025 alle ore 16:06.

Dalle evidenze in atti, risulta che la ricorrente abbia ricevuto l'SMS alert relativo alle operazioni online oggetto di ricorso.

Quanto all'autenticazione delle operazioni, l'intermediario ha prodotto i LOG relativi alle operazioni fraudolente.

Dalle evidenze in atti sembrerebbe che l'autenticazione sia avvenuta da browser (cfr. la voce "Dispositivo" che riporta la risultanza "02- BRW") mediante inserimento del codice OTP ricevuto via SMS sul numero di telefono della ricorrente (fattore di possesso) e inserimento del codice segreto K*** (fattore di conoscenza).

In tale contesto, va precisato che dalla documentazione agli atti, si evince la ricezione di un sms da un numero di cellulare sconosciuto alla ricorrente contenente un link.

Dunque, la truffa è stata perpetrata mediante il fenomeno del c.d. *smishing*, tipo particolare di *phishing*, caratterizzato dalla ricezione del messaggio ingannevole tramite SMS.

Il phishing operato tramite e-mail o sms è ritenuto fenomeno diffusamente noto, che quanto meno qualunque utente dotato di normale avvedutezza e prudenza, come si ritiene siano quelli avvezzi all'uso dell'home banking, dovrebbero conoscere.

L'orientamento cristallizzato nelle pronunce dei Collegi Territoriali (e dello stesso Collegio di Coordinamento) evidenzia che soltanto il ricorrente vittima di truffe particolarmente insidiose e difficili da individuare è esente da colpa grave.

Viceversa, il ricorrente vittima di truffe tramite phishing o, come nel caso di specie, smishing, è gravemente negligente nella custodia dei codici di accesso, circostanza questa che comporta la responsabilità dell'utilizzatore ai sensi dell'art. 12, comma 3, D.Lgs. n. 11/2010, e non consente di accogliere la richiesta di rimborso delle somme indebitamente sottratte.

Il Collegio osserva altresì che, nel caso di specie, la ricorrente ammette di aver dato seguito alle istruzioni contenute nel messaggio ricevuto sulla propria utenza telefonica, che erroneamente credeva provenire dall'intermediario resistente.

Stante quanto sopra, il Collegio ritiene sussistente, nel comportamento della ricorrente, la colpa grave che non consente di accogliere la richiesta di rimborso della somma indebitamente sottratta.

Ne consegue che, ritenendosi congruo il rimborso relativo alla prima operazione, la restante parte della domanda debba essere rigettata.

PER QUESTI MOTIVI

Il Collegio, ritenuto congruo il rimborso effettuato dall'intermediario, respinge il ricorso nel resto.

IL PRESIDENTE