Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) MEZZACAPO	Membro designato dalla Banca d'Italia
(RM) SICA	Membro di designazione rappresentativa degli intermediari
(RM) VARDI	Membro di designazione rappresentativa dei clienti

Relatore NOAH VARDI

Seduta del 28/01/2026

FATTO

1. Nell'atto introduttivo la rappresentante legale della società ricorrente riferisce di essere titolare di una carta di debito emessa dalla convenuta. In data 09.06.2025, alle ore 16:52, il socio (aderente al ricorso nonché marito), riceveva sulla propria utenza una chiamata apparentemente proveniente dal numero associato al servizio clienti della citata carta; in tale sede un sedicente operatore gli segnalava l'esecuzione di un'operazione sospetta per 100,00 USD, notificata tramite *app* che il cliente "verbalmente" disconosceva. Subito dopo, lo stesso operatore gli segnalava un'altra operazione sospetta di euro 1.900,00 e gli chiedeva di accadere all'*app* per confermare il disconoscimento. Il cliente seguiva le istruzioni impartite ma immediatamente riceveva la notifica relativa all'addebito del medesimo importo oggetto di disconoscimento; chiamava, quindi, il servizio clienti per bloccare il pagamento (che risultava in pre-autorizzazione) e la carta. Tuttavia, nonostante la tempestiva richiesta, dopo tre giorni la banca autorizzava l'addebito. Parte ricorrente, ritenendo di essere rimasta vittima di una truffa sofisticata, chiede il rimborso dell'importo complessivamente sottratto per euro 1.900,00.
2. In sede di controdeduzioni l'intermediario resistente rileva quanto segue. Come confermato dai log (allegati), il ricorso concerne n. 1 transazione effettuata con la carta di pagamento n. ****9059 alle ore 17:04 del 09.06.2025 per l'importo di euro 1.900,00. La transazione contestata è avvenuta prima del blocco della carta disposto alle ore17:15:35 della medesima giornata; nonostante si tratti di una sola transazione, la resistente deduce e documenta di aver inviato l'*sms alert* della transazione eseguita al cellulare indicato dalla ricorrente n. +39 *531 (perfettamente valido e funzionante in quanto dalla

ricorrente inserito in sede di attivazione del servizio *PUSH* e confermato in denuncia e ricorso). In sede di denuncia, la ricorrente ha ammesso di aver autorizzato la transazione pur nell'errata convinzione di bloccare la truffa in atto con conseguente inapplicabilità della disciplina relativa alle disposizioni non autorizzate. Rileva che è evidente che la ricorrente (anche se lo omette) ha comunicato i dati della propria carta e successivamente, circostanza ammessa, ha ricevuto sul *device* il messaggio autorizzativo della transazione; invero, come documentalmente provato, il 09.06.2025, sul dispositivo in possesso della ricorrente sul quale era installata l'*app* utilizzata come canale di SCA da oltre due anni (22.08.2023) giungeva il messaggio *push* con la richiesta di autorizzare la transazione *online* avviata dai truffatori successivamente autenticata con inserimento del fattore biometrico (*FaceID*/*FingerPrint*). La transazione, pertanto, è stata consapevolmente autorizzata dalla ricorrente, omettendo negligentemente di leggere il contenuto del messaggio autorizzativo ove era espressamente riportato trattarsi di un pagamento. Dai LOG allegati, che i Collegi hanno già ritenuto idonei a comprovare la corretta autenticazione (cfr. decisione Collegio di Milano n. 2372/25), si evince che la truffa in esame non ha comportato alcuna clonazione o sottrazione di credenziali né l'*enrollment* della carta sul *device* del truffatore. Da quanto ricostruito se ne deduce l'evidente colpa grave della ricorrente per aver eseguito pedissequamente le istruzioni di un truffatore sconosciuto tramite una telefonata proveniente da un numero solo apparentemente riconducibile alla resistente. La truffa, dunque, risulta realizzata secondo uno schema tipico e ampiamente noto, consistente nell'indurre il titolare dello strumento a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, o (come in questo caso) direttamente ad autorizzare le transazioni, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza, e nel caso in esame, precisamente mediante cd. *social hacking.*

L'intermediario afferma che per sensibilizzare i clienti rispetto a tali tipologie di truffe, ha da tempo avviato una campagna di informazione tramite i propri canali ufficiali; la ricorrente, peraltro, è una società commerciale e la sua rappresentante legale, di giovane età, che utilizza da anni l'*App* sul suo *device* avrebbe potuto facilmente avvedersi della truffa. La resistente eccepisce, infine, la mancanza di anomalie e la mancanza di indici di rischio di cui al DM 112/2007, atteso che si è trattato di una sola transazione con una carta che non ha esaurito il plafond. Del tutto prive di fondamento, da ultimo, sono le considerazioni della ricorrente relativamente al fatto che al momento del blocco della carta la transazione risultava ancora in pre-autorizzazione, atteso che le transazioni con le carte di pagamento, una volta autenticate sono irrevocabili e non è consentito alcun annullamento ancorché risultanti in pre-autorizzazione (definizione meramente contabile). Conclude per il rigetto del ricorso.

3. In sede di repliche la ricorrente insiste per l'accoglimento delle richieste formulate aggiungendo la domanda di "interessi e spese". Richiama quanto già affermato nel ricorso introduttivo, precisando che l'interlocutore telefonico era già a conoscenza dei nominativi e della numerazione della carta mai forniti a terzi dalla ricorrente che, peraltro, non ha mai perso il possesso della tessera; dagli estratti conto emerge che la carta veniva raramente utilizzata motivo per il quale l'importo dell'operazione costituiva un'anomalia facilmente rilevabile, tale da imporre all'intermediario un controllo rafforzato; nonostante la transazione risultasse ancora in pre-autorizzazione al momento del blocco la resistente non impediva

la contabilizzazione definitiva dell'addebito. Richiama normativa a giurisprudenza a supporto di quanto sostenuto.

4. In sede di controrepliche l'intermediario richiama quanto già affermato nelle precedenti difese rinnovando la richiesta di accoglimento delle conclusioni ivi rassegnate. Precisa, inoltre, che dalla documentazione prodotta e dalle dichiarazioni rese dalla ricorrente è possibile presumere che anche i dati della carta siano stati forniti nel corso della telefonata, non risultando diversi modi di apprensione degli stessi; la carta è intestata a una società commerciale che la utilizza per la propria attività imprenditoriale. Peraltro, trattandosi di un'unica transazione eseguita entro il plafond, non ricorreva alcun elemento per ritenere la transazione anomala. La ricorrente dichiara di aver bloccato la carta dopo aver eseguito ed autenticato la transazione. Come noto le transazioni online con carte di pagamento, una volta eseguite mediante l'autenticazione, non sono revocabili; ciò che può fare l'intermediario, una volta ricevuta la richiesta del titolare, è il blocco della carta per le transazioni successive, cosa puntualmente avvenuta nel caso in esame. La circostanza che la transazione risultasse in cd. "pre-autorizzazione", come sostiene la ricorrente, oltre a non esser provato, è irrilevante, atteso che trattasi di indicazione meramente contabile che nulla ha a che vedere con l'intervenuto perfezionamento e conseguente irrevocabilità della transazione.

DIRITTO

1. Il ricorso ha ad oggetto la richiesta di rimborso della somma fraudolentemente sottratta alla ricorrente all'esito di una truffa perpetrata ai suoi danni tramite la tecnica del *vishing*. La ricorrente disconosce un'operazione online per l'importo di euro 1.900,00 disposta in data 9.6.2025 tramite carta di debito emessa dalla resistente. L'operazione contestata è stata effettuata sotto la vigenza del d.lgs. 11/2010, così come modificato dal d.lgs. 218/2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2). Ai sensi dell'Art. 12, comma 1 del d.lgs 11/2010, salvo il caso in cui abbia agito in modo fraudolento, l'utente non sopporta alcuna perdita derivante dall'utilizzo di uno strumento di pagamento smarrito, sottratto o utilizzato indebitamente intervenuto dopo la comunicazione di smarrimento, furto o utilizzo non autorizzato dello strumento; mentre ai sensi dell'art. 12, comma 2-*bis* del d.lgs. n. 11/2010, a fronte della disposizione di un'operazione di pagamento online, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte, salvo il caso in cui abbia agito in modo fraudolento.

Nel caso di specie, l'intermediario deduce che il pagamento debba considerarsi alla stregua di un'operazione autorizzata dalla stessa ricorrente e, in quanto tale, estranea all'ambito di applicazione del d.lgs. 11/2010. A tal proposito evidenzia che il pagamento è stato autorizzato dall'*app* installata sul *device* della cliente, a seguito della *push* autorizzativa ricevuta; richiama inoltre quanto emerge dalle dichiarazioni confessorie rese dalla ricorrente in denuncia.

Nella denuncia, la ricorrente riferiva che, in data 09.06.2025, alle ore 16:52, il socio (aderente al ricorso nonché marito), veniva contattato telefonicamente da un soggetto qualificatosi come operatore della banca che lo informava dell'esecuzione di un'operazione sospetta notificata tramite *app* che il cliente " verbalmente" disconosceva. Subito dopo, lo stesso operatore gli segnalava un'altra operazione sospetta di euro 1.900,00 e gli chiedeva di accedere all'*app* per confermare il disconoscimento.

Trattandosi di chiamata apparentemente proveniente da un'utenza telefonica associata al servizio clienti della carta, il ricorrente riponeva affidamento circa la genuinità delle richieste, eseguendo le istruzioni impartite. Immediatamente riceveva la notifica relativa all'addebito del medesimo importo oggetto di disconoscimento avvedendosi della truffa subita. La ricorrente produce evidenza della chiamata ricevuta nella quale compare il numero riferibile all'assistenza clienti per la carta.
Si osserva, sul punto, che sebbene la stessa ricorrente ammetta di aver fatto accesso all'*app* al fine di eseguire le istruzioni dell'operatore, nell'errata convinzione di bloccare l'operazione sospetta, non pare trattarsi di un'operazione eseguita per intero dal pagatore. Secondo l'orientamento condiviso dei Collegi territoriali ABF, l'applicazione del regime di responsabilità per le operazioni disconosciute, previsto dalla normativa del citato d.lgs 11/2010, è escluso solo quando l'operazione sia stata eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione). Quando invece, come nel caso di specie, il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad esempio con l'inserimento di uno dei fattori di autenticazione), la transazione non deve, per ciò solo, ritenersi autorizzata (cfr. ad es. Collegio di Bologna, dec. 8882/2025).
2. Appare pertanto necessario verificare la sussistenza del sistema di autenticazione delle operazioni previsto dal d.Lgs. 11/2010 al fine di poter accertare eventuali profili di responsabilità delle parti.
L'intermediario afferma che l'operazione di pagamento risulta correttamente autenticata, registrata e contabilizzata e che non è emerso alcun malfunzionamento o compromissione dei sistemi. Afferma, in particolare, che l'*app* non ha subito *enrollment* su altri dispositivi: è stato infatti lo stesso Titolare tramite l'*app* installata sul proprio dispositivo con *DeviceId*= 79441CAB8DF145D0A729B370B651**** sin dal giorno 22.08.2023 e già utilizzata per autorizzare accessi e operazioni, ad aver utilizzato la medesima *app* ed il medesimo *device* per autorizzare ed autenticare la transazione contestata. L'intermediario versa in atti i log relativi alla sua autenticazione, dai quali si evince l'utilizzo dell'*app* della ricorrente (*push* autorizzativa come fattore di possesso) installata sul *device* e del fattore biometrico (fattore di inerenza). In punto di colpa grave, l'intermediario evidenzia altresì che parte ricorrente ha ignorato la *p ush* autorizzativa relativa all'operazione. Appurata la conformità del sistema di autenticazione dell'intermediario, vanno prese in considerazione le ulteriori circostanze fattuali in cui l'operazione contestata è stata posta in essere.
3. La ricorrente riferisce innanzitutto di essersi avveduta della truffa a seguito della ricezione del messaggio di *alert.* Dichiara di aver contattato il servizio clienti per bloccare il pagamento (che risultava in pre-autorizzazione) e la carta. Agli atti risulta evidenza del tempestivo blocco della carta, intervenuto alle ore 17:15 della medesima giornata di esecuzione dell'operazione (disposta alle ore 17:04). La ricorrente lamenta che, nonostante la richiesta tempestiva di blocco e nonostante, in quel frangente, la transazione risultasse ancora in pre-autorizzazione, la resistente non abbia impedito la contabilizzazione definitiva dell'addebito. Secondo l'intermediario, la circostanza che la transazione risultasse in cd. "*pre-autorizzazione*", oltre a non essere provata, sarebbe irrilevante, atteso che trattasi di indicazione meramente contabile che nulla ha a che vedere con l'intervenuto perfezionamento e conseguente irrevocabilità della transazione.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

4. È da ritenersi rilevante invece, la tipologia di truffa messa in atto, utilizzando la tecnica di *vishing caller ID* che integra la fattispecie dello *spoofing.* In presenza di tale insidiosa fattispecie fraudolenta, l'orientamento di codesto Collegio è che vi sia un concorso di colpa tra le parti, sul presupposto che all'intermediario debba essere addossato il rischio d'impresa relativo alla modalità di comunicazione adottata, propedeutica all'operazione di disposizioni poi avvenute. Alla luce della ricostruzione delle circostanze di fatto in cui l'operazione fraudolenta è stata messa in atto, il Collegio ritiene che possa riconoscersi un concorso di colpa tra le parti e che alla ricorrente possa, di conseguenza, essere riconosciuto il rimborso della somma di euro 1000,00, determinata in via equitativa.

PER QUESTI MOTIVI

Il Collegio dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 1.000,00, determinata in via equitativa.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE