Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) BALDINELLI

Seduta del 10/02/2026

FATTO

Il cliente afferma quanto segue:

- il 29/09/2025 riceveva una chiamata che sembrava provenire dal servizio clienti (*800) della banca B*(non convenuta);
- con la chiamata gli veniva comunicato che erano presenti dei movimenti anomali sulla carta di credito, della quale venivano riportati anche i dati;
- il fatto stesso che il truffatore sapesse esattamente i dati della carta ha rafforzato in lui l'idea che si trattasse realmente del servizio clienti dell'intermediario;
- a questo punto un sedicente operatore dell'intermediario gli forniva un codice pratica al fine di procedere allo storno di presunte operazioni fraudolente;
- seguendo le indicazioni dell'operatore, provvedeva a confermare tramite app dell'intermediario B* lo storno delle suddette operazioni, a seguito delle quali veniva inviato un sms di conferma dello storno al suo numero di cellulare;
- il truffatore lo avvisava inoltre che la carta era stata bloccata e che avrebbe ricevuto una nuova carta di credito direttamente a casa tramite raccomandata;
- dopo la chiamata, controllando l'app dell'intermediario B* verificava che la carta non era stata bloccata e che risultavano le operazioni eseguite al telefono con il truffatore;
- realizzando di essere stato vittima di una truffa, chiamava il numero del servizio clienti, il quale lo

informava che non risultava alcuna pratica di storno e che probabilmente era stato vittima di una truffa;

- procedeva a bloccare la carta e compilare il modulo di disconoscimento dei movimenti, poi rifiutata.

Il cliente chiede il disconoscimento dei movimenti fraudolenti e ne chiede il rimborso.

L'intermediario, riportato il fatto, afferma quanto segue:

- la documentazione allegata e quella presentata dal cliente confermano che le operazioni oggetto di contestazione sono tre, avvenute in data 29/09/2025 per un totale di euro 1.484,88;
- le operazioni sono avvenute prima del blocco della carta, che è avvenuto secondo i documenti allegati, solo dopo sette ore circa dalla chiamata;
- si evidenzia che il sistema di messaggistica alert fosse correttamente attivato sul numero di cellulare del cliente e, contrariamente a quest'ultimo, produce gli sms alert relativi alle transazioni;
- il cliente non ha fornito alcuna prova circa le chiamate e gli sms ricevuti dal truffatore, questi ultimi peraltro provenienti da un cellulare sconosciuto (*446) e inseriti in una chat diversa da quella originale della resistente;
- tale condotta attesta che le transazioni effettuate sono state realizzate in piena consapevolezza dal cliente, il quale ha autorizzato le suddette mediante accesso all'app tramite impronta;
- pertanto, il ricorso è inammissibile in quanto la denuncia presentata dal cliente contiene la dichiarazione, di natura confessoria, per cui è stato lo stesso cliente ad effettuare le operazioni seguendo le istruzioni del frodatore;
- alla luce della dichiarazione confessoria contenuta nella denuncia, la resistente si considera esonerata dalla prova di contabilizzazione, registrazione e autenticazione;
- di conseguenza, non è applicabile la disciplina cui alla PSD2 e al D. Lgs n. 11 del 27/01/2010;
- tuttavia, ferma restando l'inapplicabilità della predetta disciplina, l'operazione è stata comunque correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali;
- la mancata produzione documentale da parte del cliente unitamente al fatto che la telefonata e i messaggi ricevuti avrebbero dovuto destare sospetto circa la truffa in atto, evidenziano come la condotta del cliente sia da inquadrare nella colpa grave;
- si evidenzia infine che tali episodi di truffe sui servizi di pagamento (cd. Social hacking) sono note al pubblico, tanto che lo stesso cliente ha qualificato in autonomia l'episodio come truffaldino.

In conclusione, l'intermediario chiede, in via preliminare, di respingere il ricorso in quanto le transazioni contestate effettuate con la carta di pagamento sono state autorizzate dal ricorrente. In subordine, nel merito, chiede di respingere il ricorso per indeterminatezza, mancanza di prove ed allegazioni in ordine

alla presunta frode e/o per infondatezza in fatto ed in diritto e per colpa grave di parte ricorrente anche per aver ignorato gli SMS alert. In via ulteriormente subordinata, chiede che l'Arbitro definisca la ripartizione in misura proporzionale alle effettive responsabilità delle parti, con applicazione della franchigia di legge.

DIRITTO

Alla data delle operazioni trovava applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018.

Le operazioni disconosciute sono 3 per un importo complessivo di 1.484,88 euro, effettuate il 29/09/2025:

1) operazione di € 780,00 delle ore 13:29;
2) operazione di € 260,00 delle ore 13:35;
3) operazione di € 44,88 delle ore 13:44.

Con riferimento alla strong customer authentication (cd. SCA) le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019). La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Malgrado l'intermediario deduca che le operazioni risulterebbero eseguite interamente dal cliente, dalle dichiarazioni dallo stesso rese nella denuncia e nel ricorso risulta che egli, su indicazione del sedicente truffatore, abbia soltanto autorizzato le suddette operazioni fraudolente tramite l'app dell'intermediario banca B* installata sul suo device, laddove i dati di tali operazioni sembrerebbero essere stati materialmente predisposti dal truffatore. In particolare, come risulta dalla documentazione fornita dall'intermediario N*, il cliente avrebbe inserito il fattore biometrico (FINGERPRINT_FACEID) a seguito di ricezione di notifica push.

In linea generale, i Collegi ABF escludono l'applicazione del regime di protezione previsto dal d.lgs. n. 11 del 2010 in caso di operazioni disposte ed autorizzate personalmente dal titolare dello strumento di pagamento, sebbene sulla base di un consenso viziato dagli artifizi e raggiri posti in essere da un truffatore.

Nel caso in esame, in base alla documentazione in atti, le operazioni parrebbero predisposte materialmente dal truffatore e autenticate grazie alla cooperazione del ricorrente che avrebbe fornito entrambi i fattori di autenticazione (device certificato a cui è stata inviata la notifica push e fattore

biometrico). Secondo l'orientamento dei Collegi, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo deve essere prestato nella forma convenuta tra il pagatore stesso e il PSP.

Pertanto, si rende necessario procedere all'esame della prova di autenticazione delle operazioni ai sensi del D.Lgs. 11/2010. Sulla base delle evidenze prodotte, risulta che le tre operazioni sono state correttamente autorizzate ed autenticate tramite:

- notifiche push arrivate sul device (possesso);
- fattore biometrico (elemento di inerenza).

In merito alla condotta delle parti e ai profili rilevanti per la valutazione di sussistenza della colpa, il Collegio osserva che il cliente non produce evidenza in merito alle chiamate ricevute; pertanto, non è possibile stabilire se le chiamate in questione fossero riconducibili alla banca del cliente, comunque non convenuta nel presente procedimento, e se la fattispecie sia qualificabile come ID caller spoofing. Anche per quanto riguarda gli sms di conferma delle operazioni di storno, il cliente non produce evidenze, ma si limita ad indicare che si tratta di un numero di cellulare privato (*446).

Al riguardo si osserva che il ricorrente si è limitato a un non circostanziato (né tantomeno documentato) riferimento a una frode, senza tuttavia fornire al Collegio elementi dai quali accertare la sussistenza di una truffa particolarmente sofisticata. D'altro canto, l'intermediario resistente ha offerto la prova dell'autenticazione delle transazioni disconosciute, il sistema di pagamento risulta conforme alla SCA e non risultano indici di anomalia delle operazioni e/o ulteriori elementi a questi assimilabili (vd. ABF-Coll. Milano n. 2863 del 4 febbraio 2021). Il comportamento tenuto dal ricorrente integra, pertanto, una condotta gravemente colposa, con la conseguenza che il ricorso non può essere accolto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE