

## COLLEGIO DI MILANO

composto dai signori:

|                         |                                                           |
|-------------------------|-----------------------------------------------------------|
| (MI) TINA               | Presidente                                                |
| (MI) BARTOLOMUCCI       | Membro designato dalla Banca d'Italia                     |
| (MI) DELL'ANNA MISURALE | Membro designato dalla Banca d'Italia                     |
| (MI) SANTARELLI         | Membro di designazione rappresentativa degli intermediari |
| (MI) AFFERNI            | Membro di designazione rappresentativa dei clienti        |

Relatore (MI) DELL'ANNA MISURALE

Seduta del 15/07/2025

### FATTO

Il cliente, con ricorso del 24 marzo 2025, espone quanto segue:

- è cointestatario con la moglie del conto corrente \*6709 acceso presso l'intermediario convenuto;
- nel mese di novembre 2024 si avvedevano della presenza sul conto di operazioni eseguite tra il 10.10.2024 e il 5.11.2024 verso IBAN esteri non riferibili e mai autorizzate dagli stessi;
- le dette operazioni venivano effettuate mediante due carte di credito aventi come beneficiari piattaforme di *trading online*, connesse al conto corrente e di cui non è mai stata chiesta l'emissione e, pertanto, oggetto di conseguente restituzione;
- alla carta \*9871 erano riferibili 8 operazioni eseguite tra il 11.10.2024 e il 5.11.2024 per un importo complessivo di € 6.745,00;
- alla carta \*1062 erano riferibili 6 operazioni effettuate tra il 17.10.2024 e il 3.11.2024 per un importo complessivo di € 6.895,00;
- tali operazioni esulano dalla normale operatività dei coniugi sia per ammontare degli importi sia per essere state effettuate verso conti esteri;
- procedeva in data 25.11.2024 a sporgere denuncia presso le Autorità, oggetto di successiva integrazione in data 30.11.2024;
- procedeva in data 26.11.2024 a disconoscere le operazioni presso la banca convenuta;
- in data 29.11.2024 la banca comunicava l'esito negativo del rimborso;

- si avvedeva, successivamente, che era stato sottoscritto a sua insaputa e a suo nome un contratto di finanziamento n. \*6436 di € 10.000,00, a lui in alcun modo riferibile;
- si avvedeva nel mese di dicembre 2024 che era stato trattenuto un importo sul suo conto corrente a titolo di rata mensile;
- presentava reclamo all'intermediario in data 28.01.2025, che veniva riscontrato negativamente.

Chiede, pertanto, il rimborso delle somme relative alle operazioni disconosciute, nonché la risoluzione del contratto di finanziamento.

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

- il ricorso è irricevibile in quanto la richiesta di risoluzione del contratto di finanziamento, avendo natura costitutiva, esula dalle competenze dell'Arbitro;
- l'operatività contestata non è in alcun modo riferibile alla banca, in quanto in sede di denuncia il ricorrente dichiara di aver eseguito le operazioni dopo aver ricevuto una telefonata da una persona che lo istigava ad effettuarle e il cui numero non è riconducibile a quello della banca;
- le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto realizzate con il corretto inserimento delle credenziali;
- sussiste la colpa grave del cliente in quanto ha scaricato sul proprio dispositivo, su indicazione dei presunti truffatori, App che ne consentono il controllo da remoto dagli operatori, permettendo così che questi ultimi fossero in condizione di poter effettuare operazioni per suo conto;
- adotta tutte le misure volte a garantire agli utilizzatori la sicurezza dei servizi offerti dalla banca;
- non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.

Chiede, pertanto, dichiararsi la domanda di risoluzione inammissibile e comunque rigettarsi il ricorso.

## DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto il disconoscimento di n. 14 operazioni, per un importo complessivo di € 13.640,00.

Si tratta di operazioni eseguite con due diverse carte.

Le operazioni sono avvenute nelle date e per gli importi seguenti:

operazioni con carta \*9871:

- 1) 10.10.2024 ore 13:23 € 500,00
- 2) 10.10.2024 ore 13:56 € 500,00
- 3) 10.10.2024 ore 13:58 € 1.000,00
- 4) 10.10.2024 ore 14:00 € 300,00
- 5) 17.10.2024 ore 11:12 € 500,00
- 6) 17.10.2024 ore 11:15 € 500,00
- 7) 4.11.2024 ore 10:21 € 2.445,00
- 8) 4.11.2024 ore 10:23 € 1000,00

operazioni con carta \*1062:

- 1) 16.10.2024 ore 15:15 € 600,00
- 2) 16.10.2024 ore 15:42 € 1.500,00
- 3) 16.10.2024 ore 15:46 € 200,00

- 4) 16.10.2024 ore 15:55 € 1.150,00
- 5) 17.10.2024 ore 11:20 € 100,00
- 6) 1.11.2024 ore 10:40 € 3.345,00

Sono in atti le denunce presentate in data 25/11/2024 e in data 30/11/2024.

Viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate.

Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27.1.2010, n. 11. In particolare, le fonti normative applicabili alla fattispecie 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). Nello specifico è richiesta l'autenticazione forte (SCA) quando il cliente 1. accede al suo conto di pagamento *online*; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. 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.

Al riguardo, giova precisare che l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.

Ciò premesso, per quanto attiene al primo profilo sopra individuato, vale a dire l'onere di provare la SCA, l'intermediario fornisce dettagliata ricostruzione, confortata da documenti, dell'autenticazione delle operazioni.

Preliminarmente deve osservarsi che, al contrario di quanto rileva il cliente con le repliche, la documentazione informatica prodotta dall'intermediario, analoga a quella usualmente presentata per controversie simili, è ritenuta pacificamente adeguata a fornire la prova.

L'intermediario in merito al funzionamento del servizio di internet *banking* riferisce, in generale, che per accedere al servizio *online* della banca è richiesto l'inserimento simultaneo di *password* statiche (codice titolare e PIN) e *password* dinamiche (codice OTP) e che, una volta collegati i codici online, per autorizzare le operazioni dispositive è necessario il codice dinamico OTP.

Ha poi precisato che tale codice OTP può essere generato via *software* dalla App o inviato via SMS.

Ha specificato ulteriormente che, nel caso in cui il cliente usi la App, i codici OTP vengono generati a seguito della selezione della notifica sul *device* su cui è attivato il servizio o attraverso la digitazione su tale dispositivo del PIN o, se abilitato, all'apposizione dell'impronta digitale o del riconoscimento facciale.

Ebbene dall'analisi dei *login* propedeutici all'esecuzione dei pagamenti è possibile ricavare l'autenticazione forte. In particolare, per quanto riguarda la fase di accesso all'APP l'intermediario afferma e prova che il cliente si è connesso prevalentemente usando uno *smartphone* del tipo IOS (tracciato come "Canale 8") identificato con un codice univoco ed uno *smartphone* di tipo android (tracciato come "Canale 9") identificato con un altro codice univoco, impiegati per compiere l'operatività disconosciuta.

Anche con riferimento alle operazioni contestate sono agli atti i *log* che attestano la presenza del doppio fattore di autenticazione. In particolare, l'elemento del possesso (OTP generato su *device* certificato) e l'elemento dell'inerenza (il fattore biometrico).

Valutato positivamente assolto l'onere della prova relativo alla sussistenza della SCA, deve procedersi nell'esame del profilo della colpa, incombendo sull'intermediario l'ulteriore onere di provare la colpa grave del cliente.

Vale la pena riepilogare quanto rappresentato in denuncia essendo in questa sede il cliente più prodigo di informazioni sulle modalità di svolgimento della truffa perpetrata ai propri danni. In particolare, si evince che:

- il 7 ottobre veniva contattato sul suo telefono da un operatore di A\*, il quale gli chiedeva se fosse interessato ad investire € 250,00 sui titoli A\*;
- dopo aver accettato l'offerta veniva contattato da un consulente per fornirgli le istruzioni su come procedere;
- veniva indotto a scaricare sul suo cellulare due applicazioni; la prima consentiva l'accesso di terzi da remoto, la seconda, denominata B\*, era funzionale all'esecuzione degli investimenti;
- l'operatore procedeva ad entrare sul suo cellulare effettuando l'accesso all'*home banking*;
- successivamente procedeva ad autorizzare gli investimenti disposti dall'operatore tramite l'App installata sul suo *device*;
- l'operatore, in seguito, effettuava la richiesta di diverse carte di credito intestate al ricorrente;
- venivano disposti diversi pagamenti tra il periodo del 10.10.2024 e il 17.10.2024, durante il quale il ricorrente veniva contatto;
- nello stesso periodo veniva indotto a scaricare sul proprio *device* una terza applicazione denominata C\* per effettuare passaggi di denaro da un App all'altra;
- una volta effettuati questi investimenti per un importo totale di € 6.850 l'operatore non lo contattava più, ma veniva contattato da un altro operatore che lo induceva ad effettuare altri investimenti sull'App B\*, assicurandogli che avrebbe ricevuto nelle successive 24/48h le somme sul suo conto corrente;
- si avvedeva della presenza di un bonifico di € 3.500,00 del quale però la banca non sapeva dare spiegazioni;
- provava a contattare il numero del sedicente operatore, ma risultava irreperibile.

Con l'integrazione alla denuncia specifica altresì che:

- i truffatori attivavano le carte di credito a suo nome sul suo conto corrente ed effettuavano ulteriori pagamenti, oltre a quelli già denunciati;
- le due carte di credito non sono state da lui mai richieste e quindi, una volta ricevute, sono state prontamente restituite;
- è stato vittima di una truffa telefonica mediante la quale i malfattori sono riusciti a richiedere le carte di credito a suo nome e sono riusciti ad eseguire le operazioni fraudolente.

Il cliente non produce evidenza in merito alla chiamata ricevuta dal sedicente operatore A\*. Secondo l'orientamento dei Collegi la mancata allegazione, da parte del cliente, della chiamata di abboccamento (o del messaggio civetta) determina il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario e pertanto possibile un legittimo affidamento dell'utente circa la genuinità del messaggio. Per giunta, pur avendo riferito di essere stato contattato più volte anche da un preteso consulente non produce evidenza in merito alle successive chiamate o ai messaggi ricevuti e quindi non è possibile verificare l'eventuale riconducibilità di questi all'intermediario convenuto.

Si aggiunga che il cliente afferma di aver provveduto, su indicazione del sedicente operatore, a scaricare due applicazioni sul proprio dispositivo. La prima funzionale a consentire l'accesso di terzi sul telefono del ricorrente; la seconda, denominata B\*, funzionale ad effettuare gli investimenti.

Ed ancora il cliente afferma che il sedicente operatore procedeva ad entrare nel suo *home banking* e a disporre i pagamenti, che ammette di avere egli stesso autorizzato.

Il ricorrente afferma, inoltre, che il sedicente operatore provvedeva a richiedere diverse carte di credito a lui intestate e lo induceva a scaricare un'ulteriore app sul suo dispositivo denominata "C\*", funzionale ai passaggi di denaro tra B\* e C\*.

Il tutto si svolgeva in un arco temporale che rende ancor più evidente la colpa grave del cliente, il quale avrebbe avuto tutto il tempo per controllare l'identità del sedicente operatore A\*. Il cliente avrebbe dunque dovuto accorgersi o quanto meno controllare, anche grazie alle comunicazioni ricevute dalla banca, gli accessi al servizio online e l'esecuzione delle operazioni da parte di ignoti.

La condotta negligente e imprudente è peraltro testimoniata dalla circostanza che lo stesso cliente afferma, nel crociare i relativi spazi nel modulo di disconoscimento, di avere disposto personalmente le operazioni oggetto di disconoscimento dopo essere stato convinto da terzi ad effettuare i pagamenti. Nella realtà il suo contributo causale nell'esecuzione delle operazioni, pur se decisivo, è stato parziale essendosi svolte azioni concorrenti dei truffatori.

Per ciò che attiene al profilo di responsabilità dell'intermediario riconducibile alla violazione di regole di controllo e vigilanza sulle operazioni concluse dalla clientela si osserva quanto segue.

Sono presenti notifiche *push* con riferimento a tutte le operazioni con carta.

Sussiste, tuttavia, un indice di frode e specificamente quello previsto dall'art. 8, lett. a, punto 2, D.M. 30 aprile 2007, n. 112 (tre o più richieste di autorizzazione sulla stessa carta effettuate nelle 24 ore, presso un medesimo punto vendita), di talché deve concludersi per la sussistenza di un profilo di responsabilità concorrente dell'intermediario sul quale grava l'obbligo di approntare adeguati sistemi di monitoraggio delle operazioni che potrebbero configurarsi come fraudolente.

Come noto, la necessità che gli intermediari operanti nel settore si dotino di sistemi di monitoraggio capaci di intercettare elementi sintomatici di un rischio di frode rispetto a operazioni c.d. sospette si evince dalle indicazioni contenute nel D.M. n. 112 del 2007, adottato in attuazione della legge 17 agosto 2005, n. 166 (recante "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento"). In particolare, l'art. 8 del D.M. 112/2007 identifica i casi di frode che, ai fini della normativa stessa, vanno segnalati all'Ufficio Centrale Antifrode dei Mezzi di Pagamento del Ministero dell'Economia e delle Finanze (UCAMP) per consentire un monitoraggio del mercato delle carte di pagamento. Secondo le posizioni condivise dell'Arbitro, le relative disposizioni non hanno un valore precettivo, ma rappresentano comunque utili indicatori per identificare anomalie e scenari

di frode anche ai sensi dell'art. 2 del Regolamento EBA n. 2018/389, in base al quale gli intermediari sono tenuti a predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente.

Conseguentemente, in linea con i Collegi territoriali, deve reputarsi sussistere un profilo di responsabilità concorrente dell'intermediario.

Ebbene, nel caso di specie, sia a mezzo della carta n. \*9871 che della carta n. \*1062, vi sono state richieste di pagamento presso uno stesso punto vendita in numero superiore a tre; devono dunque essere rimborsate operazioni per un ammontare complessivo di € 3.250,00 (€ 1.800,00 per le operazioni eseguite con la carta n. \*9871 ed € 1.450,00 per quelle eseguite con la carta n. \*1062).

In ultimo deve rilevarsi la inammissibilità della domanda di risoluzione del contratto di finanziamento. Al riguardo, il Collegio rileva che pacificamente le azioni di risoluzione del contratto presentano natura costitutiva, non estrinsecandosi nella declaratoria circa la esistenza di un diritto o di una pretesa, bensì comportando la emanazione di un provvedimento capace di modificare la realtà giuridica. Ed è altrettanto pacifico che rendere pronunce costitutive esula dalla competenza di questo Arbitro (v. le "Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari", che - Sez. I, § 4 circoscrivono la competenza dell'ABF alle questioni "aventi ad oggetto l'accertamento di diritti, obblighi e facoltà"). Sul punto, è superfluo riportare un orientamento assolutamente univoco presso i Collegi territoriali, solo a titolo esemplificativo v. Collegio Bologna, decisione n. 15423 del 02 dicembre 2022).

### **PER QUESTI MOTIVI**

**Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 3.250,00.**

**Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura, e alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.**

IL PRESIDENTE

Firmato digitalmente da  
ANDREA TINA