

## COLLEGIO DI MILANO

composto dai signori:

|                |                                                           |
|----------------|-----------------------------------------------------------|
| (MI) TINA      | Presidente                                                |
| (MI) MODICA    | Membro designato dalla Banca d'Italia                     |
| (MI) RIZZO     | Membro designato dalla Banca d'Italia                     |
| (MI) FORMAGGIA | Membro di designazione rappresentativa degli intermediari |
| (MI) AFFERNI   | Membro di designazione rappresentativa dei clienti        |

Relatore (MI) FORMAGGIA

Seduta del 05/02/2026

## FATTO E DIRITTO

Il ricorrente afferma che in data 29/09/2025 veniva contattato dal numero 011\*\*\*311, riconducibile all'intermediario; che l'interlocutore, presentatosi come operatore dell'Ufficio Antifrode, gli riferiva di un tentativo di accesso in APP tramite un Samsung S24 Ultra, confermando tutti i suoi dati (PIN, numero carta e CVV) senza che gli venissero comunicati; che poco dopo riscontrava un'operazione non autorizzata di € 796,00 verso "P\* P\* Srl"; che contattava subito il Servizio Antifrode ufficiale, che gli confermava la validità del numero; che nonostante la sua buona fede, la Banca respingeva il disconoscimento ravvisando inosservanza nella custodia delle credenziali; che in data 04/10/2025 sporgeva denuncia ai Carabinieri per frode informatica.

Ciò premesso, chiede di ordinare alla banca il rimborso dell'importo di € 796 relativo all'operazione non autorizzata effettuata il 29/09/2025 e il riconoscimento della responsabilità della banca per la mancata protezione dei propri sistemi di sicurezza e per non aver garantito un'adeguata tutela del cliente da frodi telefoniche.

L'intermediario, nelle controdeduzioni, afferma che il cliente era titolare della carta di debito n. 5167\*\*\*6384, abilitata al servizio di Internet banking; che in data 04/10/2025 il ricorrente presentava formale disconoscimento; che l'operazione disconosciuta è stata realizzata in modalità commercio

elettronico sicuro, in completa assenza di anomalie e con inserimento del CVV; che l'utilizzo contestato è stato reso possibile esclusivamente a causa dell'inosservanza con colpa grave degli obblighi di custodia delle carte e delle credenziali di sicurezza da parte del ricorrente; che infatti se il ricorrente non avesse comunicato al terzo il codice OTS, essenziale per l'*enrollment* del nuovo dispositivo, compreso il codice CVV l'operatività truffaldina non si sarebbe realizzata; che il codice necessario per l'*enrollment* del nuovo dispositivo è stato inviato al cellulare certificato del ricorrente (riportato anche in denuncia), per cui non vi è stato alcun dubbio circa la riconducibilità dell'esecuzione dell'*enrollment* al cliente; che il ricorrente non fornisce alcun elemento probatorio a supporto delle proprie dichiarazioni, omettendo di dimostrare la ricezione della telefonata dal numero indicato, nonché la circostanza che il truffatore fosse già in possesso dei suoi dati bancari senza che gli venissero comunicati; che del resto era logico pensare che, se il terzo fosse stato in possesso di tutte le credenziali necessarie a perfezionare l'operazione di pagamento, non avrebbe contattato il ricorrente; che se il ricorrente avesse prestato attenzione agli *alert* inviati in fase di effettuazione dell'*enrollment* (SMS e push "parlante") ne avrebbe evitato l'esecuzione, impedendo così ai terzi di disporre l'operazione contestata; che il suo intervento di blocco della carta ha evitato che venissero realizzate ulteriori operazioni, tentate tra le ore 13:05 e le 13:10; che l'Arbitro, in casi simili, ha riconosciuto in capo ai ricorrenti "auto-responsabilità per l'operazione disconosciuta", rigettando i ricorsi.

Ciò posto, ha concluso chiedendo di rigettare il ricorso in quanto infondato in fatto ed in diritto.

Il cliente, richiamati i propri scritti, replica che la truffa, tutt'altro che "banale", si è svolta con tecniche ingannevoli ed altamente persuasive; che l'SMS e la PUSH citate dalla Banca non erano affatto chiare, non menzionavano alcun rischio reale ed immediato, non spiegavano come riconoscere se la richiesta fosse fraudolenta e, per di più, venivano ricevuti in una condizione di pressione psicologica, nel corso di una telefonata con quello che pareva essere un operatore Antifrode della Banca; che la presenza di un *alert* non esclude l'inganno psicologico, né dimostra dolo o colpa grave; che il fatto che la Banca ammetta di aver bloccato successive operazioni dimostra come il sistema antifrode avesse riconosciuto delle anomalie e che, dunque, la Banca fosse consapevole del rischio.

L'intermediario, riportandosi alle conclusioni in atti, controreplica che la truffa in cui è caduto il ricorrente non è affatto equiparabile al "*social engineering* avanzato" come esso asserisce, ma è una truffa molto comune; che le affermazioni riportate dal cliente circa la mancata comunicazione del PIN non sono supportate da alcun elemento probatorio; che il contenuto del messaggio SMS inviato sul *device* certificato del ricorrente (dal testo "*NON CEDERE IL CODICE. Se qualcuno te lo chiede E' UNA FRODE! Per attivare l'App su SM-G960F, solo se in tuo possesso, usa il codice 838649*") è più che lapalissiano nella sua chiarezza e non lascia adito a nessun dubbio interpretativo; che il blocco di sicurezza disposto poco dopo l'avvenuta effettuazione dell'operazione in oggetto, evidenzia la correttezza del proprio comportamento.

In fatto, si osserva che oggetto del presente ricorso è una operazione dell'importo complessivo di € 796,00, effettuata il 29/09/2025 alle ore 12:59.

Dalle dichiarazioni rese dal ricorrente nel ricorso e nella denuncia risulta che il frodatore, sedicente operatore dell'Ufficio Antifrode, fosse già in possesso dei dati del cliente (PIN dell'APP di Banca, numero della carta e CVV), senza che questi gli venissero comunicati.

Per contro, l'intermediario resistente ritiene illogico pensare che il terzo, pur essendo già in possesso di tutte le credenziali necessarie a perfezionare l'operazione di pagamento – circostanza, peraltro, in alcun modo dimostrata in atti – abbia comunque contattato il ricorrente; ritiene invero a questo proposito ragionevole desumere che il cliente, con colpa grave, abbia comunicato telefonicamente al frodatore il codice OTS necessario per l'*enrollment* del nuovo *device*, oltre che gli estremi della carta di pagamento, compreso il codice CVV. Ciò avrebbe permesso il verificarsi dell'operatività truffaldina.

In diritto, si osserva che, alla data dell'operazione contestata, 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 fonti normative regolanti la materia 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).

Secondo il consolidato orientamento dei collegi, solo nel caso in cui risulti pacifico o dimostrato che le operazioni contestate siano state compiute direttamente e interamente dal cliente (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), l'intermediario è esonerato dalla prova di autenticazione. Diversamente, ove vi siano operazioni non compiute interamente dal cliente, ed il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale, 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 dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP.

Occorre pertanto l'accertamento della sussistenza della SCA (*Strong Customer Authentication*), con riferimento alle singole operazioni e ad ogni fase attraverso cui si sono realizzate, sempre con onere della prova a carico dell'intermediario. Infatti, secondo l'orientamento consolidato dei collegi, l'autenticazione forte è richiesta 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 prova di autenticazione delle operazioni, a carico dell'intermediario, rappresenta, in aderenza al dato normativo, un *prius* logico rispetto ad ogni ulteriore accertamento, compreso quello sulla colpa grave del cliente.

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. In caso di difetto di piena prova sull'autenticazione, per ogni fase, delle transazioni disconosciute, la domanda deve essere accolta, posto che la mancanza anche parziale della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente.

Resta il fatto che, comunque, non è configurabile una responsabilità oggettiva a carico dell'intermediario, sicché spetta al Collegio verificare se, in concreto, vi sia stata una responsabilità concorrente del PSP secondo le norme di diritto comune, qualora emerga dalla documentazione in atti

un apporto causale dell'intermediario alla frode (ad esempio, la mancanza o temporanea indisponibilità del numero verde del PSP, o il mancato rilievo di indici di frode).

Resta in ogni caso ferma la possibilità di valutare in concreto se l'utente abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave agli obblighi di cui all'art. 7 ai sensi dell'art. 12 D.Lgs. 11/2010.

Occorre dunque che si proceda all'esame sulla sussistenza della prova di autenticazione per ogni fase della sua realizzazione.

Dalle evidenze prodotte risulta dimostrata la sussistenza della SCA sia per le azioni antecedenti all'esecuzione dell'operazione contestata sia per l'operazione stessa.

Infatti, quanto alla fase di *enrollement* del nuovo dispositivo, l'*enrollement*, avvenuto alle ore 12:51:06, risulta autorizzato con PIN, quale fattore di conoscenza, e con codice OTS inviato via SMS, quale fattore di possesso.

Quanto alla operazione contestata, essa risulta autorizzata mediante ricorso a un elemento di conoscenza, il PIN, e a un elemento di possesso, la notifica push sul dispositivo precedentemente registrato dal truffatore.

A ciò va aggiunto, che, comunque, le affermazioni del ricorrente, compresa quella sul ricevimento della chiamata iniziale ricevuta dal truffatore, restano indimostrate, non avendo al riguardo il ricorrente prodotto alcuna evidenza, con conseguente impossibilità di stabilire se la chiamata in questione fosse riconducibile all'intermediario resistente.

Per tutto quanto considerato il ricorso va rigettato.

### **PER QUESTI MOTIVI**

**Il Collegio non accoglie il ricorso.**

IL PRESIDENTE