

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) BARTOLOMUCCI

Seduta del 01/09/2026

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 14/10/2025, una notifica di tentativo di accesso al proprio *Internet banking*, che rifiutava prontamente.

Faceva presente che, in seguito, fosse stato contattato telefonicamente da un soggetto che si qualificava come operatore antifrode dell'intermediario, il quale gli aveva comunicato che vi fossero in corso delle operazioni fraudolente; precisava di avergli riferito il codice OTP ricevuto tramite SMS in quanto ritenuto necessario per mettere in sicurezza il conto, senza tuttavia aver indicato la password, lo User ID o i dati della carta.

Sottolineava di essersi avveduto di essere stato vittima di una truffa in quanto era stata eseguita un'operazione con carta di credito di € 531,36 da lui disconosciuta; riteneva, quindi, di essere stato vittima di *spoofing* e contestava la sussistenza di colpa grave.

Chiedeva, pertanto, il rimborso dell'importo complessivo fraudolentemente sottratto.

Si costituiva l'odierno resistente il quale rilevava che l'operazione di pagamento *E-commerce* si fosse perfezionata attraverso il servizio di 3D Secure, senza che si fossero riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.

Si considerava, dunque, estraneo alla causazione degli eventi che avevano determinato il danno lamentato dal ricorrente, che peraltro non aveva fornito prova che l'episodio fosse da ricondurre alla sua responsabilità; chiariva, infatti, che l'operazione non presentasse indici di anomalia.

Al contrario, considerava sussistente la colpa grave del cliente in quanto questi aveva provveduto in autonomia a dissociare il suo smartphone dall'utenza *Internet banking* ed aveva rivelato al truffatore le proprie credenziali di accesso al suo *Internet banking* (Codice Utente e password per effettuare il primo accesso in App e il codice OTP ricevuto tramite SMS consentendo l'*enrollment* del dispositivo del truffatore).

Chiedeva, pertanto, il rigetto del ricorso ovvero – in caso di riconoscimento di profili di responsabilità – di accertare l'eventuale concorso di colpa con la condotta del cliente; da ultimo domandava l'applicazione della franchigia come per legge.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale contestava l'affermazione dell'intermediario secondo cui sarebbero state comunicate a terzi le credenziali di accesso (User ID e password).

Rappresentava che, in una precedente occasione relativa alla richiesta della carta di credito, gli era già stato richiesto dall'intermediario di comunicare telefonicamente un codice ricevuto via SMS per finalità di verifica; tale circostanza aveva quindi contribuito a rendere credibile la richiesta avanzata dal truffatore.

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale si riportava ai propri scritti difensivi.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di un'operazione di pagamento, successivamente disconosciuta.

La materia, come noto, è regolata dal D. lgs. n. 11/2010 come modificato dal D. lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/UE (c.d. PSD2 - Payment Services Directive 2).

Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d. *Strong Customer Authentication* SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.

Con riferimento alla c.d. SCA gli artt. 97 e 98 della direttiva PSD2, nonché l'articolo 10 bis del D. lgs. n. 11/2010, oltre che le norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato UE 2018/389 della Commissione Europea e i criteri interpretativi adottati dalla stessa Autorità (cfr. in particolare il parere dell'EBA del 21 giugno 2019), hanno stabilito che essa 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. In relazione a tutte le predette fasi, la SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori, che devono essere reciprocamente indipendenti e appartenere a categorie diverse: conoscenza; inerenza; possesso.

Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa de qua prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.

Risulta documentalmente che l'operazione in parola consista in un pagamento eseguito in data 14/10/2025, per un importo di € 531,36.

Parte resistente afferma che alle 18:23 il cliente ha fatto accesso all'App installata sul suo dispositivo (fattore di possesso) utilizzando il riconoscimento facciale (fattore di inerenza). Le tracciate informatiche versate in atti evidenziano che lo User ID utilizzato per effettuare il log-in in App prima dell'operazione contestata è il medesimo di quello presente nel dettaglio dell'*enrollment* del cliente.

Il relativo log-in, infatti, pur non riportando un codice identificativo del dispositivo raffrontabile con l'evidenza relativa al dispositivo associato all'utenza, riporta in chiaro il medesimo userID cui risulta abbinato un unico dispositivo sin dal 27/11/2022.

Peraltro non va sottaciuto che lo stesso cliente ha dichiarato di avere, su indicazione dell'interlocutore, "dissociato tutti i dispositivi dalla [propria] App". Inoltre, dalle medesime evidenze documentali emerge che la SCA è stata eseguita correttamente: il login, infatti, è avvenuto tramite l'App installata sul suo dispositivo (fattore di possesso) utilizzando Face ID (fattore di inerenza).

Sempre con riferimento alla fase prodromica al compimento dell'operazione contestata, l'intermediario afferma che il ricorrente ha provveduto autonomamente a dissociare il suo smartphone dall'utenza *Internet banking*, utilizzando il fattore biometrico (Face ID), che ha generato un codice "OTP silente" che è stato inviato direttamente dalla APP sullo smartphone al server del PSP. Secondo la ricostruzione dell'odierno convenuto, il de-*enrollment* del dispositivo ha comportato anche la "dissociazione" dello stesso quale *device* di riferimento dell'autorizzazione con SCA delle operazioni eseguite online con le carte di pagamento intestate al cliente. Saggiunge pure che, non appena completata la dissociazione del proprio dispositivo, il cliente deve aver necessariamente comunicato ai malfattori il proprio Codice Utente unitamente alla password necessaria per effettuare il primo accesso in App, e il codice OTP trasmesso a mezzo SMS al suo numero di telefono certificato al fine di consentire l'associazione di un nuovo dispositivo alla sua utenza *Internet banking* (c.d. *enrollment*) e la creazione di un nuovo "SmartPIN", per il quale il ricorrente ha anche ricevuto un SMS informativo di conferma dell'avvenuta creazione.

A tale riguardo, risulta *per tabulas* che l'accesso in App necessario al fine di procedere con la fase di *enrollment* di un nuovo dispositivo è avvenuto con il medesimo User ID utilizzato in precedenza dal ricorrente; non pare, invece, potersi rinvenire l'impostazione del riconoscimento biometrico. Ciò

nonostante è verosimile che in fase di creazione dello smartPIN sia stata selezionata l'opzione per memorizzarlo nel dispositivo e sostituirne l'inserimento manuale con un fattore biometrico.

Con riferimento alla fase di autenticazione, invece, dall'analisi dei log prodotti risulta che l'operazione – avvenuta mediante applicazione del protocollo 3D Secure – sia stata resa possibile dalla contemporanea presenza dell'elemento di possesso, rappresentato dalla notifica *push* inviata all'ultimo dispositivo associato (fattore di possesso) e da quello di inerenza, coincidente con il fattore biometrico. Attesa la conformità a SCA delle operazioni contestate, non resta che verificare se – dalla condotta tenuta dal ricorrente – siano evidenziabili profili di colpa grave, rispetto alla quale la prova di autenticazione rappresenta, in aderenza al dato normativo, un *prius* logico (cfr. Coll. coord., dec. n. 22745/2019).

A tale proposito, il cliente riferisce di aver ricevuto una chiamata da un numero riconducibile all'odierno resistente. Di tali circostanze, tuttavia, non fornisce alcuna prova documentale.

Secondo il consolidato indirizzo di questo Collegio, la mancata allegazione, da parte del cliente, del registro delle chiamate non consente di verificare se il numero da cui la telefonata truffaldina sarebbe partita possa essere riconducibile all'intermediario e, pertanto, se sia configurabile un legittimo affidamento dell'utente circa la sua genuinità.

Trattandosi di un'unica operazione, non assume rilievo la mancata evidenza relativa all'attivazione di un servizio di SMS *alert*, a prescindere dalla prova dell'invio della notifica *push*, che – in seguito all'*enrollment* dell'App sul *device* dei truffatori – è stata inviata a questi ultimi, rendendo impossibile al ricorrente di avvedersi del compimento delle operazioni fraudolente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE