

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) BARTOLOMUCCI

Seduta del 23/06/2026

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 11/11/2025, molteplici chiamate dal numero verde corrispondente a quello dell'assistenza clienti; avendo verificato la genuinità del numero, provvedeva a richiamare ed entrava in contatto con il sedicente operatore della banca che, essendo a conoscenza di tutti i suoi dati, lo guidava nella disinstallazione e installazione dell'App, operazione necessaria per l'aggiornamento dell'*home banking*.

Faceva presente che, una volta conclusa l'operazione, fosse stato informato che sarebbe stato ricontattato dopo un paio di giorni per completare il procedimento di aggiornamento; soggiungeva che, nell'attesa, non avesse riscontrato alcun movimento anomalo.

Rappresentava che, in data 14/11/2025, fosse stato ricontattato per eseguire la medesima operazione di disinstallazione ed installazione senza fornire alcun codice; il sedicente operatore predisponendo un bonifico di prova, inserendo importo, causale e beneficiario con la promessa che poi sarebbe stato stornato.

Affermava di non aver mai fornito alcun codice e/o credenziale all'operatore, in quanto l'App era stata sbloccata con la propria impronta digitale; riteneva, dunque, che il truffatore gli aveva fatto installare un App malevola per avere accesso agli SMS e alle notifiche *push*.

Sosteneva di aver sporto denuncia alle Autorità competenti e di aver proceduto al disconoscimento dell'operazione.

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

Si costituiva l'odierno resistente, il quale rilevava che la denuncia e le dichiarazioni contenute nel ricorso contenessero la dichiarazione, di natura confessoria, per cui fosse stato lo stesso cliente ad effettuare le operazioni seguendo le istruzioni del frodatore, con conseguente inapplicabilità della disciplina di cui al D.lgs n. 11/2010.

Riteneva pure sussistente la colpa grave del cliente in quanto la sua condotta si collocava al di là degli standard di diligenza media.

Sottolineava che non fosse possibile verificare se la truffa presentasse degli indizi di sofisticatezza in quanto il cliente non aveva allegato *screenshot* del registro chiamate; soggiungeva, peraltro, che il cliente avesse risposto ad un numero che – pur sembrando riconducibile al numero verde dell'assistenza clienti – fosse abilitato solo a ricevere ma non a chiamare.

Rilevava che tutte le operazioni fossero state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali, senza aver riscontrato malfunzionamenti o intrusioni nei propri sistemi informatici.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale ribadiva che l'operazione fosse stata disposta senza il proprio consenso, essendosi limitato a seguire le indicazioni del truffatore per scaricare l'App.

Affermava di non aver mai ricevuto le notifiche *push* né alcun SMS di *alert*.

Allegava evidenze del registro chiamate già depositate in filiale il giorno in cui si era recato per denunciare le anomalie, evidenziando che dalla documentazione prodotta dalla banca si deducesse un'attività del tutto anomala rispetto al proprio ordinario, in quanto nel giro di 7 minuti erano stati eseguiti tre bonifici a favore beneficiari diversi e tutti recanti la stessa causale.

Riteneva che l'intermediario fosse tenuto, in relazione all'obbligo di buona fede oggettiva nell'ambito del rapporto contrattuale di cui all'art. 1175 c.c. e nell'esecuzione in buona fede del contratto ai sensi dell'art. 1375 c.c., ad attivarsi in caso di operazioni sospette.

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale evidenziava che la produzione del registro chiamate non fosse idonea a provare la riconducibilità delle stesse all'intermediario né la sussistenza di una truffa telefonica.

Ribadiva che il cliente avesse disposto personalmente l'operazione sbloccando l'App, sottolineando che non vi fossero riscontri probatori circa il fatto che il truffatore gli avesse fatto scaricare un'App malevola.

Rilevava, peraltro, che dalle evidenze prodotte dal cliente, si evincesse che lo stesso avesse intrattenuto anche una corrispondenza su Whatsapp con il truffatore, denotando una condotta imprudente e negligente.

Di contro non considerava ravvisabili indizi di anomalia in quanto era stata disposta una sola operazione, rispetto alla quale affermava che non sussiste un obbligo *ex ante* di blocco.

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 bonifico effettuato il 14/11/2025, per l'importo di € 5.990,00.

L'intermediario afferma che l'operazione sia stata eseguita personalmente dal ricorrente e che, pertanto, non dovrebbe trovare applicazione la disciplina di cui all'art. 11 D.lgs. 11/2010. Invero, dalle dichiarazioni rese dal cliente nella denuncia e nel ricorso risulta che il cliente abbia autorizzato un bonifico tramite App dopo che il truffatore ne aveva predisposto l'importo e il beneficiario, previa comunicazione dei codici di accesso all'*home banking*; tale bonifico sarebbe servito, a detta del sedicente operatore, a verificare l'operatività dell'App (oggetto di un attacco hacker) e sarebbe stato successivamente stornato.

Con riferimento a fattispecie analoghe l'orientamento uniforme dei Collegi ha chiarito che se 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 prestatore dei servizi di pagamento.

Laddove, invece, l'operazione di pagamento *online* sia stata preparata dal truffatore che ha a disposizione i codici dispositivi del cliente, questa non può ritenersi eseguita per intero dal pagatore, e quindi non può considerarsi sussistente il requisito necessario per escludere il regime di responsabilità previsto dalla PSD2.

Ciò rilevato, le tracciate informatiche versate in atti mostrano che, in data 10/11/2025 (e quindi prima dell'esecuzione dell'operazione di pagamento disconosciuta) sia stato effettuato un *reset* della password dell'*home banking* tramite accesso via web; tale modifica, a detta dell'intermediario, può avvenire mediante digitazione del codice PIN a sei 6 cifre scelto in fase di *enrollment* ovvero fattore biometrico (elemento di conoscenza/inerenza), con l'utilizzo di un *device* univocamente riconducibile al cliente (elemento di possesso).

Dalla lettura dei log prodotti, tuttavia, si ravvisa unicamente l'elemento di possesso costituito dal *device* del ricorrente, ma non del secondo fattore indicato dall'intermediario come PIN (elemento di conoscenza) o fattore biometrico (elemento di inerenza). Anche la legenda allegata alle stesse evidenze non riporta riferimenti ad alcun elemento di conoscenza.

La medesima carenza documentale si ravvisa anche per tutti gli ulteriori passaggi, dall'*enrollment* del dispositivo, all'accesso finalizzato all'esecuzione dell'operazione sia all'autenticazione di quest'ultima. La mancanza anche parziale della prova del rispetto dei presidi di sicurezza in tutte le fasi dell'operazione di pagamento, e quindi sin da quella di accesso al sistema, è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente, costituendo, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente (cfr. Coll. coord., dec. n. 22745/2019).

Deve, pertanto essere riconosciuto il diritto del ricorrente ad ottenere il rimborso del controvalore dell'operazione contestata.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 5.990,00.

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