

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) PERON	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 31/03/2026

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 12/05/2025, una chiamata da un numero apparentemente riferibile all'intermediario, nel corso della quale gli veniva comunicato che il suo conto fosse bloccato; insospettito dalla chiamata, riferiva di non aver fornito alcuna informazione e di aver chiamato il suo istituto bancario affinché mettesse in sicurezza il suo conto corrente.

Faceva, tuttavia, presente di aver ricevuto, in data 19/05/2025, un'ulteriore telefonata truffaldina, che interrompeva tempestivamente; in seguito, si accorgeva che fosse stato disposto un bonifico istantaneo di € 1.999,00 da lui non autorizzato alle ore 21:12 del 19/05/2025.

Sosteneva di aver presentato quindi denuncia presso le Autorità competenti e disconosciuto l'operazione contestata.

Chiedeva, pertanto, il rimborso dell'importo di € 1.999,00.

Si costituiva l'odierno resistente il quale rilevava che l'operazione fosse stata correttamente autorizzata, contabilizzata e registrata e non avesse subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; precisava, peraltro, che essa fosse stata preceduta dall'installazione dell'app sul device del truffatore, tramite inserimento dei dati personali del cliente (codice cliente + data di nascita + PIN + OTP ricevuto via SMS sul suo numero di cellulare) che quindi aveva prestato la sua cooperazione alla truffa.

Sottolineava che la modifica del dispositivo fosse avvenuta senza anomalie e nel rispetto della "Strong Customer Authentication" (c.d. SCA) che non sarebbe stata possibile senza una collaborazione da

parte della vittima; soggiungeva che il cliente avesse ricevuto la notifica alert dell'installazione dell'app (laddove non fosse stata fatta da lui), a seguito della quale avrebbe potuto e dovuto prendere immediati contatti con la propria banca, impedendo così il procrastinarsi della truffa in proprio danno.

Riteneva, quindi, sussistente la colpa grave del cliente, il quale aveva colposamente seguito le istruzioni dei frodatori; affermava pure di aver tentato, in data 20/05/2025, il recall del bonifico che non aveva avuto alcun esito.

Da ultimo, rappresentava di aver avviato una campagna anti frode per sensibilizzare la propria clientela sulle truffe.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale sosteneva che controparte non avesse fornito prova della propria colpa grave; di contro, evidenziava che il bonifico fraudolento fosse stato disposto alle ore 21:12 mentre la chiamata truffaldina fosse stata disposta alle ore 21:16, dovendosi escludere alcuna cooperazione con il truffatore nell'esecuzione dell'operazione disconosciuta.

Precisava di aver ricevuto solamente una notifica di avvenuto pagamento ma non anche l'email avente ad oggetto l'alert relativo all'installazione dell'app su un altro dispositivo, così come sms ovvero push nel corso della truffa.

Riteneva che la sua fiducia fosse stata carпита dal fatto che il numero dal quale perveniva la chiamata fosse riconducibile al servizio assistenza dell'intermediario e il falso operatore fosse a conoscenza del numero di telefono del cliente e di alcuni movimenti del suo estratto conto.

Contestava la genericità delle schermate contenute nel corpo delle controdeduzioni, inidonee a dimostrare la condotta negligente del cliente.

Considerava l'operazione del tutto anomala, atteso l'importo abnorme non in linea con l'ordinaria operatività del cliente.

Da ultimo, affermava che non vi fosse prova che le campagne antifrode promosse dall'intermediario avessero raggiunto specificatamente il cliente.

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale ribadiva che – immediatamente dopo l'installazione dell'app su un altro dispositivo – fosse stata inviata una e-mail all'indirizzo di posta elettronica del cliente.

Evidenziava che il codice OTP necessario per installare l'app e l'alert relativo all'installazione dell'app fossero stati inviati presso dei recapiti indicati nell'anagrafica del cliente.

Sosteneva di non aver bloccato la truffa in quanto non vi è un obbligo di monitoraggio delle operazioni in capo all'intermediario.

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 istantaneo effettuato il 19/05/2025, per l'importo di € 1.999,00.

Quanto al processo di autenticazione, l'odierno convenuto chiarisce che le operazioni contestate sono state precedute, alle ore 16:33, dall'installazione dell'app della banca su un nuovo device, descrivendo i singoli passaggi dell'iter: in particolare afferma che alle ore 16:31 il truffatore ha digitato il Codice Cliente e la propria data di nascita e conferma cliccando sul bottone "Continua", per poi digitare (alle ore 16:31:01) le tre cifre del PIN richieste e confermare cliccando sul bottone "Continua".

Ottenuto riscontro positivo dal sistema, alle ore 16:31:05, è stato scelto il codice segreto (Smart Code) ed è stata effettuata la scelta se utilizzare o meno i propri dati biometrici per accedere all'app e

autorizzare le operazioni. Alle ore 16:31:19 la banca ha inviato un sms OTP al numero di telefono che corrisponde a quello dichiarato dal cliente in sede di denuncia.

Da ultimo, è stato inserito il Codice OTP ricevuto via SMS che ha ottenuto la validazione della banca alle ore 16:33. All'esito di tali passaggi, la banca ha completato l'attivazione dell'APP sul nuovo dispositivo e ha inviato la relativa e-mail di notifica.

Sulla scorta di tali risultanze documentali, deve ritenersi che l'accesso all'area riservata sia avvenuto in modalità conforme a SCA, mediante l'utilizzo dei due fattori di autenticazioni: il PIN (fattore di conoscenza) e l'SMS OTP (fattore di possesso).

Dalle tracciate informatiche emerge poi che, nel giorno della truffa, sia stato effettuato un accesso all'App scaricata sul nuovo device precedentemente enrollato; tale accesso risulta eseguito in modalità conforme a SCA, tramite l'applicazione (fattore di possesso) e la digitazione dello Smart Code (fattore di conoscenza).

Con riferimento alla fase dispositiva, risulta *per tabulas* che anche il bonifico sia stato predisposto ed eseguito in modalità conforme a SCA, mediante l'utilizzo dell'app (fattore di possesso) e l'inserimento del codice segreto (fattore di conoscenza).

Attesa la conformità a SCA dell'operazione contestata, 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 avere ricevuto una chiamata da un numero apparentemente riconducibile all'intermediario e di essere stato informato dall'operatore del blocco del proprio conto corrente. Ciò nonostante, ancorché risulti documentalmente che il numero di telefono sia effettivamente riconducibile all'intermediario resistente, dall'analisi dello screen shot versato in atti emerge che la chiamata in entrata da tale numero (della durata di un minuto e 56 secondi) sia pervenuta in data 19/05/2025 alle ore 21:16, mentre il bonifico è stato disposto alle ore 21:12.

Il ricorrente non riferisce null'altro in relazione alla truffa a suo danno, se non di non aver comunicato alcun dato personale al truffatore nel corso delle chiamate; di contro, l'intermediario ha allegato e dimostrato di aver inviato tanto una e-mail di notifica dell'avvenuta installazione dell'app su un altro dispositivo, quanto una e-mail di conferma dell'operazione eseguita.

Non vi sono, pertanto, elementi che consentano di accogliere il ricorso.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso

IL PRESIDENTE