

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

Relatore (MI) BARTOLOMUCCI

Seduta del 03/03/2026

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo che, tra il giorno 1/04/2025 ed il giorno 8/04/2025, fossero stati eseguiti sul suo conto corrente una serie di bonifici per il complessivo importo di euro 148.081,57, oltre ad euro 128,77 a titolo di commissioni, per un totale di euro 148.210,34.

Faceva presente di essersi avveduto di tali operazioni solo in data 10/04/2025 mediante la contabile relativa ai bonifici inviata per posta dall'intermediario e di aver conseguentemente bloccato il conto corrente e presentato denuncia presso le Autorità.

Chiedeva, pertanto, la restituzione dell'importo di euro 148.210,34, oltre al risarcimento dei danni, comprensivi delle spese di assistenza difensiva.

Si costituiva ritualmente l'intermediario convenuto, il quale rilevava che il quadro fornito dal cliente fosse poco contestualizzato e privo di un riscontro probatorio idoneo alla ricostruzione della truffa; sottolineava, comunque, che le sei operazioni effettuate sul conto corrente fossero state autorizzate mediante il doppio fattore di autenticazione.

Richiamava quanto dichiarato nella denuncia in relazione all'attivazione di un nuovo dispositivo su una SIM non di sua appartenenza, osservando che la fase di associazione del nuovo dispositivo richiede le credenziali (username e password) che dovrebbero essere conosciute solo dall'utente, il che significa che esse fossero in possesso dei truffatori.

Riteneva, quindi, che il cliente asserirebbe di essere stato vittima di "SIM SWAP FRAUD", senza aver provato l'interruzione del servizio telefonico dal giorno in cui sono state effettuate le operazioni fraudolente.

Affermava, dunque, che le banche non possono essere ritenute responsabili di disservizi legati a compagnie telefoniche, mentre sottolineava la colpa grave del cliente, il quale aveva ommesso di controllare tempestivamente il conto corrente; aveva sporto denuncia solo dieci giorni dopo il primo bonifico fraudolento e aveva confermato telefonicamente le operazioni, in seguito alla ricezione della e-mail inviata dal Servizio clienti dopo l'esecuzione del secondo bonifico del valore di euro 29.000,00 chiedendo di prendere contatti al fine di confermare le due operazioni di bonifico.

Si opponeva alla richiesta risarcitoria e a quella di rifusione delle spese di assistenza difensiva.

Chiedeva, pertanto, il rigetto del ricorso ovvero – in via subordinata – il riconoscimento di un concorso di colpa ai sensi dell'art. 1227 cod. civ.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale ricostruiva la truffa assumendo che fosse stato inizialmente associato un nuovo dispositivo al suo account di posta elettronica per poi disattivare la sua utenza telefonica e contestualmente cambiare operatore, utilizzando le nuove credenziali e il nuovo numero di telefono per disporre le operazioni fraudolente.

Sottolineava di essere una persona anziana che non usa la tecnologia; riteneva, dunque, contraria a buona fede la contestazione relativa alla sua negligenza per mancata custodia; rilevava pure che un diverso intermediario con il quale intratteneva un altro rapporto di conto corrente su cui pure aveva subito tentativi di truffa, si fosse adoperato ed avesse disposto il blocco del conto stesso.

Soggiungeva di non aver mai confermato telefonicamente la mail e la domanda segreta, in quanto la SIM era già sotto il controllo dei truffatori; ad ogni modo lamentava che l'intermediario, pur ammettendo di aver rilevato anomalie, avesse utilizzato come canale di conferma uno strumento già frodato ed avesse fatto affidamento sull'interlocutore truffatore, senza rilavare l'anomalia di quattro richieste di attivazione del token virtuale, nonostante egli avesse già comunicato di non operare più tramite home-banking.

Rappresentava che la truffa sarebbe stata perpetrata dal finto cliente e dal finto nipote, dal momento che non aveva mai conferito procura ad alcun parente per interagire con gli intermediari bancari; in particolare, riteneva che la telefonata eseguita dai truffatori invalidasse i due fattori di autenticazione in quanto rivelati alla presenza di un terzo estraneo, in violazione della normativa sulla sicurezza dei servizi di pagamento.

Considerava il consenso alle operazioni fraudolente viziato da pressione psicologica che avrebbe inficiato il "collegamento dinamico" (Dynamic Linking) tra la stessa autenticazione e lo specifico importo/beneficiario dell'operazione; la telefonata di conferma, pertanto, non costituirebbe un elemento valido di autenticazione.

Soggiungeva che la circostanza per cui, a seguito dei primi due bonifici e la telefonata di conferma, ne siano stati eseguiti altri quattro di rilevante importo e rivolti all'estero verso conti mai utilizzati prima dal ricorrente, costituisse un evidente fattore di rischio.

In ogni caso, contestava che l'intermediario non avesse fornito prove idonee a dimostrare la corretta autenticazione e la colpa grave del cliente, limitandosi ad addossare la colpa circa la modifica dell'utenza telefonica sul cliente e sull'operatore telefonico; né tanto meno si sarebbe adoperato a garantire la validità dei fattori di autenticazione.

Chiedeva, pertanto, oltre alla domanda restitutoria formulata con il ricorso, anche la rivalutazione monetaria e gli interessi legali.

Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale osservava che il ricorrente non avesse depositato evidenze idonee a dimostrare di non essere più in grado di operare con l'home-banking, né il comportamento tenuto dall'altro intermediario nel bloccare tempestivamente il conto corrente.

Evidenziava che non potesse sapere che l'indirizzo e-mail fosse già stato compromesso; di contro considerava che il fatto stesso che durante la telefonata assieme al sedicente nipote fosse presente anche il finto cliente, avvalorasse nella banca la convinzione della sussistenza del consenso da parte del cliente stesso ad effettuare le operazioni.

Sosteneva pure che la telefonata rappresenta una misura rafforzativa ma non sostituiva del doppio fattore di autenticazione.

Faceva pure presente che il cliente nulla avesse replicato circa l'inserimento delle credenziali per l'associazione del nuovo dispositivo, le quali potevano solo essere in suo possesso e nemmeno circa l'omesso e ritardato controllo del proprio conto corrente.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di alcune operazioni di pagamento, successivamente disconosciute. In sede di repliche il cliente, rispetto alla domanda formulata nel ricorso, ha chiesto altresì la rivalutazione e gli interessi, oltre alla condanna alla rifusione delle spese del procedimento compresi i costi di eventuali consulenze tecniche ulteriori.

Queste ultime domande devono considerarsi inammissibili; va, infatti, ricordato che le Disposizioni della Banca d'Italia che regolano il presente procedimento prevedono che "Il ricorso deve avere ad oggetto la stessa questione esposta nel reclamo; il cliente può chiedere nel ricorso il risarcimento del danno anche quando tale richiesta non sia stata formulata nel reclamo, qualora il danno lamentato sia conseguenza immediata e diretta della medesima condotta dell'intermediario segnalata nel reclamo. Entro il termine perentorio di 25 giorni dalla ricezione delle controdeduzioni, il cliente può trasmettere una memoria di replica. Resta comunque preclusa la possibilità di ampliare la domanda iniziale" (Sez. VI, par. 1).

Sulla scorta di tale previsione, il consolidato orientamento dei Collegi ha affermato che non sono ammissibili quelle modificazioni della domanda che, formulate in atti successivi al ricorso, si concretizzano in una *mutatio libelli* della stessa, poiché volte ad introdurre nel processo un *petitum* diverso e più ampio. Nel caso di specie, dunque, deve concludersi che la richiesta di restituzione degli interessi legali e alla rivalutazione monetaria, in quanto domanda nuova, non è ammissibile in sede di repliche.

Ciò chiarito in premessa e con riguardo al merito del ricorso, mette conto rammentare che 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 sconosciute.

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 le operazioni sconosciute consistono in sei bonifici, tre dei quali esteri, disposti tra il giorno 01.04.2025 ed il 04.04.2025, per il complessivo importo di euro 148.081,57 oltre ad euro 128,77 a titolo di commissioni.

L'intermediario, in via preliminare, afferma che le operazioni contestate sono state precedute dall'attivazione di un nuovo token dispositivo su una SIM, la quale può essere effettuata solo dopo aver operato il LOGIN inserendo entrambe i fattori di autenticazione (user + password e autenticazione con notifica push nella app DB Secure Authenticator).

In particolare, parte resistente riferisce che – dopo l'inserimento delle credenziali utili al login – l'app riconosce l'assenza del secondo fattore di autenticazione costituito dal token virtuale e viene inviata un'email contenente il link per registrare l'app e il codice di registrazione da inserire in essa per scaricare l'app; una volta scaricata l'app, il cliente definisce il PIN per aprire l'app e inserisce il codice di registrazione, in seguito al quale viene inviato un sms al cellulare dell'utente contenente il codice di attivazione per l'associazione univoca dell'app con il dispositivo.

Anche in considerazione di tale processo, l'odierno convenuto precisa inoltre che l'unico modo possibile per creare un nuovo token abbinato alle credenziali del cliente è di disassociare il token dall'utenza e richiedere una nuova associazione, mediante app oppure Online banking (previo inserimento del login di autenticazione) o telefonata al call center della banca, preventivamente ad un rigoroso controllo di identità del chiamante che deve fornire dati segreti e solo a lui noti.

Alla luce di tale descrizione, la documentazione versata in atti evidenzia che è stato effettuato il LOGIN alle ore 12:57 in data 1/04/2025: non vi è, tuttavia, evidenza dell'avvenuto inserimento del PIN (non essendo sufficiente il riferimento a "activation data" e "validated" nel relativo file, che l'intermediario dichiara essere relativo alle credenziali e al secondo fattore). Nessun riscontro documentale emerge, invece, con riguardo alla e-mail contenente un primo codice di attivazione, che la banca assume essere stata inviata all'indirizzo di posta elettronica del cliente, così come in relazione alla disinstallazione del precedente token che dichiara essere condizione essenziale per l'installazione di un nuovo token.

Anche con riguardo alla fase di accesso, le tracciate informatiche in atti non consentono di considerare provata la sussistenza dell'autenticazione forte, che – secondo la ricostruzione dell'intermediario – sarebbe garantito dall'utilizzo di un primo fattore di conoscenza, con la richiesta dell'inserimento nella pagina di LOGIN in web o APP di una USERID univoca e personale ed una PASSWORD definita dal cliente e solo allo stesso nota e di un secondo fattore di possesso, costituito dall'utilizzo di un TOKEN, fisico o virtuale.

Dall'esame dei log, infatti, emerge che tutti i bonifici siano stati preceduti dalla LOGIN e quindi accesso all'home-banking via web; non vi è, tuttavia, evidenza dell'avvenuto inserimento del PIN come dichiarato dall'intermediario (anche in tal caso non essendo sufficiente a tal fine il riferimento "validated" presente nel citato file e che l'intermediario dichiara essere relativo alle credenziali e al secondo fattore).

Conseguentemente, per la fase di autorizzazione delle singole operazioni, non risulta documentato l'inserimento del secondo fattore di autenticazione in concreto utilizzato (di possesso), che l'intermediario affermerebbe essere il token virtuale.

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 delle operazioni contestate.

Va invece respinta la domanda risarcitoria, in assenza di prova circa il pregiudizio asseritamente subito. Al riguardo, appare sufficiente richiamare il principio di diritto espresso dal Collegio di coordinamento, che ha avuto modo di precisare che "spetta al cliente il risarcimento del danno patrimoniale, la cui sussistenza ed entità egli sia in grado di dimostrare, nonché del danno non patrimoniale, la cui sussistenza non è in re ipsa, ma deve essere provata anche facendo ricorso a presunzioni semplici e a nozioni di comune esperienza; in tal caso si potrà ricorrere alla liquidazione equitativa ma rimane onere della parte ricorrente indicare al Collegio idonei elementi di valutazione" (cfr. dec. n. 1642/2019).

Quanto alla componente patrimoniale del danno rappresentata dalle spese di assistenza difensiva, mette conto rilevare che non vi sia prova dell'effettivo esborso da parte del cliente; in ogni caso, anche

alla luce dei principi di diritto di recente affermati sempre dal Collegio di coordinamento, deve essere provato che il pregiudizio patrimoniale lamentato sia comunque soggetto alla prova della sussistenza di un illecito, consistente nel “comportamento gravemente scorretto, oppure significativamente e ingiustificatamente dilatorio od ostruzionistico tenuto dall’intermediario nella gestione della controversia, che abbia reso oggettivamente necessaria la presenza di un professionista (cfr. dec. n. 4580/2025). In mancanza della prova circa la sussistenza di una condotta siffatta da parte dell’odierno resistente, la domanda non può trovare accoglimento.

Quanto al nocumento asseritamente dubito sul piano non patrimoniale, al di là del difetto di prova già evidenziato, va comunque precisato – in coerenza con quanto stabilito anche dalla giurisprudenza di legittimità – che non sono comunque generalmente risarcibili i “pregiudizi consistenti in disagi, fastidi, disappunti, ansie ed ogni altro tipo di insoddisfazione concernenti gli aspetti più disparati della vita quotidiana che ciascuno conduce nel contesto sociale” (Cass., Sez. un., 11 novembre 2008, n. 26972).

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l’intermediario corrisponda alla parte ricorrente la somma di € 148.210,00.

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