

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) CESARE	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARTOLOMUCCI

Seduta del 13/01/2026

FATTO

Il ricorrente, insoddisfatto degli esiti dell'interlocuzione intercorsa nella fase di reclamo, adiva questo Arbitro deducendo di essere stato contattato, in data 15.01.2025, da un sedicente operatore dell'intermediario B, il quale – tramite artifici e raggiri riconducibili allo smishing e al vishing – lo aveva indotto ad effettuare 12 bonifici istantanei dal conto radicato presso l'intermediario A a favore del conto detenuto presso l'intermediario B, per € 9.680,00.

Faceva presente che il truffatore, ottenuto il pieno controllo dell'account relativo al conto dell'intermediario B, avesse eseguito 44 operazioni dispositive.

Riteneva entrambi gli intermediari responsabili in solido per il nocumento economico subito, dal momento che l'intermediario B non aveva osservato gli obblighi previsti dal d.lgs. 11/2010 in caso di operazioni non autorizzate, mentre l'intermediario A aveva violato i canoni della diligenza professionale ex art. 1176 cod. civ. per non aver impedito l'operatività anomala da cui aveva preso le mosse lo schema fraudolento, non avendo intercettato una fuoriuscita patrimoniale realizzatasi in poco più di un'ora, causando l'azzeramento del saldo disponibile, con operazioni che riportavano una causale quantomeno sospetta ("antifrode").

Dinanzi alla mancata prova della sua "colpa grave", il ricorrente contestava, inoltre, che i sistemi di sicurezza dell'intermediario B si fossero mostrati estremamente carenti.

Chiedeva, pertanto, il rimborso dell'importo complessivo di € 8.587,50, oltre agli interessi e alla rifusione delle spese di assistenza difensiva; domandava pure il risarcimento del danno non patrimoniale per il turbamento subito, da liquidarsi equitativamente.

Si costituivano ritualmente entrambi gli intermediari convenuti.

L'intermediario A rilevava che la carta emessa dall'intermediario B non costituisse in alcun modo un servizio collegato al conto corrente detenuto dal cliente. Osservava che le somme trasferite tramite le operazioni di ricarica non avessero in ogni caso determinato alcuna perdita patrimoniale, trattandosi di trasferimento di fondi tra conti di titolarità del medesimo cliente e che, in ogni caso, queste fossero state disposte personalmente dal cliente, con conseguente esclusione del regime di responsabilità previsto dal d.lgs. n. 11/2010. Evidenziava che l'intermediario B avesse già provveduto a rimborsare parzialmente il cliente prima del reclamo. Eccepiva l'inammissibilità della domanda di risarcimento, che non era stata previamente formulata in sede di reclamo; sottolineava, in ogni caso, che questa risultasse sprovvista di documentazione a supporto. Si opponeva alla richiesta di rifusione delle spese di assistenza difensiva e chiedeva il rigetto del ricorso.

L'intermediario B rilevava di aver già provveduto al rimborso di 4 operazioni per un ammontare di € 996,00, precisando che le restanti 40 operazioni fossero state eseguite mediante procedura conforme alla c.d. Strong Customer Authentication. Sottolineava che il cliente avesse ammesso di aver cliccato su un link decettivo e di aver disposto personalmente le operazioni di ricarica istantanea del proprio conto di moneta elettronica, su indicazione del truffatore. Faceva pure presente che il cliente avesse fornito i codici di sicurezza giunti tramite SMS, consentendo all'interlocutore di accedere al proprio account, associando al profilo un nuovo dispositivo. Osservava di aver attivato, in seguito all'esecuzione di due transazioni di importo rilevante nell'arco di pochi minuti a favore del medesimo esercente, un presidio di sicurezza, impedendo l'esecuzione della terza disposizione ed inviando immediatamente al ricorrente un'opportuna segnalazione per richiedere la conferma dell'autenticità delle operazioni, alla quale egli aveva risposto positivamente. Affermava che controparte avesse pure ricevuto puntuale informativa di esecuzione operazione tramite notifica push istantanea (c.d. servizio di "Memoshop"), contenente il dettaglio delle transazioni eseguite.

Rappresentava, inoltre, di aver messo a disposizione dei clienti un presidio di sicurezza che consente agli stessi di verificare in tempo reale se l'interlocutore telefonico è realmente un operatore bancario oppure no (il cd. bollino di sicurezza). Evidenziava che – nonostante fosse a conoscenza o avrebbe dovuto quantomeno verificare che il recapito non fosse attribuibile al resistente – il cliente avesse ugualmente assecondato le richieste ricevute da un soggetto sconosciuto, circostanza che induce a ritenere che sia stato vittima di colpevole credulità nell'ambito di uno schema di truffa da tempo ormai noto.

Precisava che il ricorrente avesse pure ricevuto gli SMS autentici che lo avevano informato inequivocabilmente dell'associazione di un nuovo dispositivo all'account e del relativo accesso, con evidenza dei codici segreti per finalizzare le operazioni di associazione, che mai gli sarebbero stati richiesti dai veri addetti della banca. Sosteneva di aver da tempo avviato campagne informative nei confronti della clientela per prevenire le truffe informatiche sia attraverso una apposita sezione del proprio sito ufficiale che tramite comunicazioni via e-mail e push, regolarmente ricevute e lette dalla cliente. Contestava la domanda risarcitoria, priva di qualsiasi riscontro probatorio.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni degli intermediari replicava il ricorrente, il quale rammentava che l'SMS decettivo si fosse inserito nella cronologia genuina intrattenuta con l'intermediario (c.d. spoofing), inducendolo a inserire le credenziali su un sito clone e che l'hacker, ottenute le credenziali, avesse associato un nuovo dispositivo, così potendo integrare l'autenticazione a due fattori e operare indisturbato.

Ribadiva di aver risposto "SI" alla richiesta di conferma dell'autenticità delle operazioni inviata dall'intermediario B solo perché sotto pressione psicologica e nella convinzione di interagire con un operatore bancario per bloccare una frode in corso. Lamentava che la condotta omissiva dell'intermediario A avesse permesso la realizzazione successiva della frode, cosicché risultasse palese il nesso causale con la perdita patrimoniale subita, e che l'intermediario B, dal canto suo, avesse permesso che venissero eseguite 41 operazioni in poco più di un'ora. Faceva pure rilevare che la disponibilità massima sul conto radicato presso l'intermediario B, in base al contratto, fosse di €

2.500,00, con un tetto giornaliero di € 1.000,00 per le operazioni di ricarica, e di € 2.500,00 per le medesime operazioni su base mensile; riteneva, pertanto, che tali massimali fossero stati ampiamente superati, avendo ricaricato in totale € 9.583,50. Ribadiva la sussistenza della responsabilità solidale dei resistenti e reiterava la richiesta di restituzione di € 8.587,50, oltre interessi e spese di assistenza difensiva; non veniva, invece, riformulata la richiesta risarcitoria del danno non patrimoniale.

Le repliche del ricorrente venivano riscontrate da entrambi gli intermediari.

L'intermediario A rilevava che l'operazione di ricarica non presentasse alcun nesso causale con la frode denunciata e non potesse neppure qualificarsi come "non autorizzata" ai sensi della PSD2.

Soggiungeva pure che in epoca precedente alla truffa contestata, il cliente operasse regolarmente tramite ricariche verso il conto radicato presso l'intermediario B; pertanto, un eventuale blocco del trasferimento avrebbe esposto la banca a contestazioni di segno opposto, potendo essere considerata responsabile di aver impedito al cliente di disporre liberamente dei propri fondi.

L'intermediario B, dal canto suo, rammentava che in data 04.04.2024 fosse stata inviata una comunicazione di modifica unilaterale del contratto con cui si informava il cliente che i limiti in merito alle ricariche e alla disponibilità massima sul conto sarebbe divenuto "illimitato".

DIRITTO

La domanda del ricorrente è relativa all'accertamento del proprio diritto al rimborso del controvalore di una serie di operazioni, successivamente disconosciute, oltre al risarcimento del danno morale asseritamente subito in conseguenza della truffa.

In relazione a quest'ultima, l'intermediario A ha eccepito in via preliminare l'inammissibilità del ricorso per carenza del preventivo reclamo. L'eccezione è infondata e non merita accoglimento.

Ancorché le stesse Disposizioni della Banca d'Italia che regolano il presente procedimento prevedano 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" (Sez. VI, par. 1), va comunque osservato che nelle contestazioni preliminari contestazioni inviate agli intermediari resistenti, la domanda di risarcimento dei danni risultasse in ogni caso introdotta.

Peraltro la stessa domanda – che non viene reiterata nelle memorie di repliche, potendosi intendere rinunciata – appare pure sfornita del necessario corredo probatorio e dovrebbe essere in ogni caso rigettata: 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 al merito del ricorso, 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 PDS2, 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 contestate consistano in 12 bonifici istantanei effettuati dal conto intrattenuto presso l'intermediario A e in ulteriori 44 bonifici eseguiti dal conto radicato presso l'intermediario B.

Quanto ai primi, emerge *per tabulas* che si tratti essenzialmente di operazioni di giroconto, poiché sono state poste in essere in favore del conto intestato allo stesso cliente presso l'intermediario B, al fine di costituire la provvista necessaria per l'esecuzione dei successivi pagamenti fraudolenti.

Il consolidato orientamento dei Collegi ha stabilito che dette operazioni vadano esenti dall'autenticazione forte; peraltro, nel caso di specie rileva anche la circostanza che lo stesso ricorrente abbia ammesso di averle poste in essere personalmente.

Dalle dichiarazioni rilasciate in sede di denuncia, infatti, alle quali va riconosciuta natura confessoria, emerge che – avendo ricevuto un sms nella chat intrattenuta con l'intermediario B, con il quale veniva informato che la carta di debito sarebbe stata disattivata per presunta frode – il cliente abbia aperto il link inviatogli al fine di impedire la disattivazione, inserendo le credenziali di accesso, il numero di telefono e la mail.

Veniva successivamente chiamato da un presunto operatore dell'intermediario B, che inoltrava la chiamata da un'utenza mobile privata e che gli confermava la presunta attività fraudolenta ad opera di terzi operanti all'estero. Dopo aver affermato di aver bloccato l'operatività fraudolenta e di aver nuovamente reso operativo il conto di moneta elettronica, il truffatore induceva il cliente ad effettuare un primo bonifico dal conto detenuto presso l'intermediario A per verificare l'effettiva operatività del suddetto rapporto.

Parte ricorrente riceveva però un messaggio di storno, alla luce del quale l'operatore lo invitava a ripetere l'operazione, inducendolo così ad effettuare personalmente altri 11 bonifici, per 12 operazioni in totale.

Dal momento che le operazioni non sembravano essere andate a buon fine, il cliente affermava di non essere disposto ad eseguire ulteriori bonifici; il truffatore a quel punto interrompeva la chiamata.

In relazione alle operazioni eseguite personalmente dal cliente si è avuto modo di affermare in molteplici occasioni che debba considerarsi esclusa l'applicabilità della disciplina prevista nelle ipotesi di utilizzi fraudolenti di strumenti di pagamento. Tanto basta perché l'esecuzione dei bonifici istantanei contestati dal ricorrente non possano considerarsi come "operazione non autorizzata", non ricadendo

quindi nell'ambito di applicazione delle norme protettive (artt. 10 e 12 del d. lgs n. 11/2010) richiamate e previste per i casi di utilizzazione fraudolenta degli strumenti di pagamento.

Né tantomeno appaiono sussistenti ulteriori elementi, che possano comunque configurare una responsabilità in capo all'intermediario A ex art. 1176, comma 2, cod. civ., per non aver intercettato una operatività dall'evidente natura "anomala", per importi, frequenza e causale di riferimento; a tale riguardo appare sufficiente richiamare un recente pronunciamento con cui il Collegio di coordinamento, nel ribadire il regime di esenzione dalla SCA per le operazioni di costituzione della provvista, ha pure individuato una possibile responsabilità ascrivibile agli intermediari allorché i pagamenti che siano succeduti alla costituzione della provvista rappresentino conseguenza immediata e diretta di un inadempimento ascrivibile ai prestatori dei servizi di pagamento; a tal fine è stato precisato che "Affinché possano considerarsi tali, occorrerebbe ritenere che sussista un nesso causale immediato e diretto fra l'assenza della SCA – quale prodromo del fatto antigiuridico realizzato dai frodatori ... – e il pregiudizio finale ... subito [dal cliente]" (cfr. Coll. coord. dec. n. 8671/2024). Tale ipotesi è da escludere nel caso di specie, tenuto conto del fatto che tale nesso sia stato interrotto dall'atto del danneggiato, consistente proprio nell'esecuzione personale dei richiamati giroconto.

Con riferimento alle operazioni di pagamenti eseguite sul conto intrattenuto presso l'intermediario B, emerge documentalmente che si tratti di 44 operazioni eseguite il 15.01.2025 tra le ore 19.47 e le ore 22.01; lo stesso ricorrente ha dato atto dell'avvenuto (e documentato) rimborso dell'importo di € 996,00, relativo a quattro di esse, limitando la sua richiesta alla residua somma di € 8.587,50 effettivamente riferibili alle restanti 40 operazioni.

Le tracciature informatiche versate in atti confermano la ricostruzione effettuata dal ricorrente, il quale afferma che il truffatore – avendo già ottenuto il trasferimento dei fondi provenienti dal conto corrente radicato presso l'intermediario A, con le operazioni di ricarica tramite bonifico disposte personalmente dal cliente – ha potuto effettuare in autonomia l'accesso al conto e associare il proprio dispositivo, per poi finalizzare i pagamenti senza alcuna collaborazione ulteriore ad opera del cliente.

In effetti le operazioni contestate sono state precedute da regolare processo di login, il quale – secondo quanto riferito dall'intermediario B – è stato eseguito da un dispositivo mobile differente da quello usualmente utilizzato; secondo quanto riferito dalla banca, il sistema richiede due fattori di autenticazione, costituiti dall'indirizzo e-mail e della password (fattore di conoscenza), oltre al codice OTP SMS inviato al numero di cellulare presente in anagrafica cliente (fattore di possesso).

I log prodotti attestano la ricezione con esito positivo dell'OTP sul dispositivo del cliente, successivamente inserito dal dispositivo in uso ai truffatori (elemento di possesso) e richiamano l'inserimento della password (elemento di conoscenza), con l'indicazione dell'esito positivo.

Una volta eseguita l'associazione al nuovo device, lo stesso intermediario B riferisce che 20 operazioni di e-commerce siano state eseguite con modalità "CHALLENGE" (ovvero doppio fattore conforme a SCA) e altre 20 a mezzo POS, tramite utilizzo del wallet digitale (TOKEN), cui era stata previamente associata la carta di debito.

Con riguardo a queste ultime, l'intermediario afferma che la documentazione in atti attesterebbe che la tokenizzazione sia avvenuta correttamente, mediante l'inserimento di un doppio fattore di autenticazione, costituito dall'accesso al conto tramite dispositivo mobile previamente associato e dall'inserimento della password.

In realtà si evidenzia che, contrariamente a quanto affermato dal resistente, nei log non risulta chiara l'identificazione del dispositivo da cui sarebbe stato effettuato l'accesso e sul quale sarebbe stata effettuata la tokenizzazione dello strumento di pagamento, dal momento che sono presenti informazioni riguardanti solamente il PAN della carta e il nuovo token generato. Pertanto, non è possibile rilevare alcuna evidenza in grado di attestare la verifica di un fattore di possesso.

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 di queste prime 20 operazioni contestate.

Al contrario, le altre 20 operazioni risultano eseguite previa notifica al device corrispondente al dispositivo previamente associato dal truffatore, sul quale veniva effettuata l'azione di "tap" (fattore di possesso) e conseguente autorizzazione tramite l'utilizzo di fattori biometrici (fattore di inerenza). Pertanto, deve ritenersi che tali pagamenti siano sati effettuati in modalità conforme SCA.

Ciò nonostante, il Collegio non può mancare di rilevare l'abnormità delle modalità operative con cui è stata consumata la truffa.

Parte resistente ha allegato e documentato – dinanzi a tre operazioni esecutive effettuate a favore del medesimo beneficiario (dalle 20:15 alle 20:44) – di aver attivato apposito presidio antifrode, domandando al cliente, tramite SMS inviato alle ore 20:45, conferma della genuinità delle operazioni al quale questi ha risposto positivamente alle ore 20:49:45.

Seppur tale sistema ha consentito all'intermediario di andare esente da responsabilità in relazione alle operazioni effettuate in tale arco temporale, risulta tuttavia dalle tracciate informatiche in atti che – dopo la parentesi dei pagamenti eseguiti mediante wallet – siano anche ripresi dalle ore 21:50 e fino alle ore 22:01 quelli tramite POS, palesando l'inefficienza complessiva del sistema di monitoraggio della banca. Deve, quindi essere riconosciuto il diritto del ricorrente ad ottenere la ripetizione del controvalore anche di tali ultimi pagamenti.

Il Collegio dispone che sulle somme così riconosciute vadano computati gli interessi al tasso legale, a far data dal reclamo.

Deve invece essere respinta la domanda di rifusione delle spese di assistenza difensiva, anche alla luce dei principi di diritto di recente affermati dal Collegio di coordinamento, il quale – nel ribadire che essa debba essere qualificata alla stregua di una domanda di risarcimento del danno emergente (in tal senso, cfr. già dec. n. 3498/2012), che può essere presentata per la prima volta nel ricorso – ha affermato 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; in tale prospettiva, può assumere rilievo anche il carattere particolarmente difficile e complesso delle questioni oggetto di controversia" (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.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso nei confronti del primo intermediario; accoglie parzialmente il ricorso nei confronti del secondo intermediario e dispone che quest'ultimo corrisponda alla parte ricorrente la somma di € 6.596,00, oltre interessi legali dal reclamo al saldo.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario soccombente 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