

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

La ricorrente, insoddisfatta dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di essere stata vittima di un complesso raggiro basato sull'installazione dell'applicazione anydesk sul proprio cellulare e sulla simulazione di assistenza da parte di finti consulenti finanziari. In particolare, la ricorrente, ultraottantenne e priva di alfabetizzazione informatica, faceva presente di essere stata indotta a consentire l'accesso remoto credendo di ricevere supporto tecnico in materia di investimenti per poi ravvisare sul conto in essere presso l'intermediario convenuto che fossero stati disposti tre bonifici di € 10.000,00 ciascuno ad un soggetto sconosciuto, di cui solo uno andato a buon fine.

Precisava che le operazioni fossero state disconosciute tempestivamente con trasmissione del modulo di disconoscimento, denuncia alle autorità competenti e diffida inviata a marzo 2024.

Riteneva che la banca resistente fosse responsabile per aver rilevato l'anomalia della ripetizione di due di tre bonifici identici in tempi ravvicinati, e che l'operazione andata a buon fine dovesse quindi imputarsi a difetto di diligenza dell'istituto.

Contestava la violazione dell'obbligo di trasparenza bancaria di cui all'art. 119 t.u.b., stante l'assenza dell'IBAN del beneficiario nell'estratto conto; lamentava pure che la banca fosse tenuta ad assicurare un sistema di sicurezza informatica adeguato ai rischi attuali e ad adottare misure di prevenzione efficace, come gli alert in tempo reale, il blocco di operazioni anomale, la verifica dell'identità dei beneficiari.

Considerava, quindi, l'intermediario responsabile – ai sensi del d.lgs. n. 11/2010 – per la sicurezza, integrità e tracciabilità delle operazioni di pagamento, sottolineando pure che l'art. 97 della direttiva PSD2 impone autenticazione forte del cliente e meccanismi di monitoraggio in tempo reale del rischio transazionale.

Soggiungeva, peraltro, che controparte avesse violato gli obblighi di diligenza professionale qualificata ai sensi dell'art. 1176, comma 2, cod. civ., non avendo dimostrato (i) di aver adottato un sistema sufficientemente evoluto di rilevazione delle anomalie, (ii) di aver correttamente informato la cliente circa i rischi derivanti da accessi remoti non autorizzati, (iii) di aver attivato procedimenti interni tempestivi di contestazione e blocco.

Sottolineava che, in caso di operazioni non autorizzate, grava sull'intermediario l'onere di dimostrare che l'operazione è stata autorizzata dall'utente e che non vi è stata frode o malfunzionamento; richiamava pure la giurisprudenza di questo Arbitro, che ha affermato che la semplice dimostrazione dell'uso delle credenziali corrette non è sufficiente a provare che l'utente abbia autorizzato l'operazione.

Osservava che, nel caso di specie, l'intermediario non avesse fornito alcuna prova concreta dell'origine dell'accesso, né dei dispositivi utilizzati, né della provenienza dell'indirizzo IP, non ha dimostrato che il sistema di sicurezza fosse in grado di impedire attacchi via software remoto e non ha attivato misure di verifica aggiuntive, nonostante l'anomalia delle operazioni eseguite.

Evidenziava che l'abusiva installazione ed uso remoto di sistemi di captazione fraudolente non esime dalla responsabilità l'istituto, ove ricorra l'omesso immediato riconoscimento di operazioni anomale per importo, beneficiario, dispositivi di accesso e inusitata frequenza di ripetizione.

Peraltro, faceva presente che fossero tutte ultraottantenni e prive di formazione informatica specifica, che le aveva resa vittima di un inganno telefonico sofisticato, con utilizzo di social engineering, con una manipolazione fraudolenta della volontà della cliente, tali da non potersi ritenere sussistente la sua colpa grave in relazione alla sola installazione di un software di accesso remoto.

Considerava, invece, l'intermediario responsabile per non aver rilevato l'anomalia dell'esecuzione di 3 bonifici estremamente ravvicinati verso lo stesso beneficiario, nel giro di poche ore; per non aver verificato l'identità dei beneficiari che risultano sconosciuti alla ricorrente e per non averla informata del rischio; per non aver posto in essere alcun tentativo di tracciamento tempestivo delle somme e per non aver disposto la verifica multifattoriale dell'operazione disconosciuta.

Chiedeva, pertanto, il rimborso dell'importo complessivo di € 10.000,00, oltre interessi e rivalutazione monetaria, nonché la rifusione delle "spese vive sostenute", tra cui quelle di assistenza difensiva.

Costitutosi ritualmente, l'intermediario rilevava che la ricorrente fosse stata vittima di un attacco di social engineering, truffa nota e diffusa, tanto da non poter essere più ritenuta una frode sofisticata.

Affermava che la banca, periodicamente, invia comunicazioni volte a mettere in guardia i clienti da rischi legati a questo tipo di truffa; evidenziava che, dalla descrizione dei fatti, emergesse che la cliente,

dopo aver installato l'app che permette il controllo a distanza di terzi, avesse effettuato l'accesso ai propri conti correnti, permettendo così ai terzi di venire a conoscenza dei codici segreti di accesso. Precisava che l'esecuzione dell'operazione contestata fosse stata preceduta dall'enrollment dell'app di homebanking su altro dispositivo e che fosse stata eseguita con doppio fattore di autenticazione alle ore 10:23 del 22/11/2024, così come gli ulteriori due bonifici eseguiti il 23 e 25 novembre 2025, questi ultimi stornati a seguito della ricezione della denuncia.

Riteneva sussistente la colpa grave della cliente che aveva scaricato sul proprio cellulare un programma in grado di consentire ai terzi estranei di prendere il controllo del dispositivo su cui tale software era stato installato; soggiungeva che ella, nonostante fosse stata avvisata dalla dipendente di un'altra banca, avesse continuato a dare credito ai malfattori, eseguendo ogni attività dagli stessi richiesta, senza effettuare alcun controllo o approfondimento.

Evidenziava che non risultasse che, dopo la ricezione dell'sms che la avvisava di aver preso in carico il bonifico di € 10.000,00, la cliente avesse contattato il servizio clienti per segnalare quanto occorso e chiedere lo storno del bonifico disconosciuto.

Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava la ricorrente, la quale contestava che l'intermediario non avesse prodotto i contratti sottoscritti con le clienti per l'abilitazione al servizio di internet banking, né avesse fornito la prova di aver previamente impartito alle clienti, ultra ottantenni e prive di adeguata alfabetizzazione informatica, istruzioni chiare e complete in ordine all'utilizzo consapevole dello strumento e dei rischi connessi.

Osservava che il ricorso a canali digitali non possa tradursi in una deresponsabilizzazione del professionista e in abnorme aggravio di rischio in capo al consumatore; al contrario, la normativa vigente prevede precisi obblighi di diligenza, informazione e correttezza in capo al prestatore di servizi di pagamento.

Lamentava che, in mancanza della prova contrattuale, non potesse sostenersi che la ricorrente avesse accettato condizioni che non erano state debitamente allegate; soggiungeva, comunque, che anche laddove il contratto fosse stato prodotto, l'intermediario avrebbe dovuto dimostrare di aver personalizzato l'informativa in ragione della particolare condizione delle clienti, adottando strumenti compensativi, come alert telefonici e warning a sportello.

Affermava che l'intermediario non avesse assolto l'onere probatorio circa l'avvenuta consegna di istruzioni precise e di un adeguato *caveat* circa i rischi di frode, ma si fosse limitato a produrre dei tracciati in cui mancava la prova che le fossero stati mostrati l'importo e l'IBAN del beneficiario e che il codice OTP fosse specificamente generato per autorizzare quella precisa transazione.

Peraltro sottolineava che gli sms prodotti riportassero un pin generico, privo di qualsiasi riferimento al contenuto dell'operazione e del dynamic linking; soggiungeva che l'installazione dell'app di controllo da remoto avesse compromesso l'indipendenza dei canali di autenticazione e il PSP non avesse dimostrato di aver adottato misure idonee a neutralizzare tale rischio.

Riteneva l'intermediario responsabile per l'inefficacia del suo sistema di monitoraggio del rischio transazionale, in violazione dell'art. 18 RTS e dell'obbligo di diligenza professionale qualificata.

Rilevava che i tracciati prodotti evidenziassero anomalie, quali (i) l'accesso da dispositivo sconosciuto, (ii) l'accesso da geolocalizzazioni anomalie, (iii) sostituzione del token software, (iv) disposizione di un bonifico di importo rilevante verso un beneficiario sconosciuto; soggiungeva che la prova definitiva

dell'inadeguatezza del sistema risiedesse nella incontestabile evidenza che la banca aveva bloccato due successivi tentativi di bonifico, identici per importo e beneficiario, ma aveva colpevolmente lasciato passare il primo.

Contestava la tesi difensiva della banca che fondava la colpa grave della cliente nell'aver scaricato l'app di controllo remoto any desk, omettendo di considerare il contesto fraudolento – simulazione di assistenza bancaria/finanziaria - nonché le condizioni soggettive della cliente, ultraottantenne e priva di adeguata alfabetizzazione informatica.

Le repliche della ricorrente venivano riscontate dall'intermediario, il quale faceva presente di inviare periodicamente comunicazioni volte a mettere in guardia i correntisti dai rischi legati alle truffe a cui si è esposti; rammentava pure che, all'atto della sottoscrizione del modulo di apertura del conto corrente, alla ricorrente fosse stata consegnata anche una copia delle norme contrattuali, contenenti specifico riferimento alla possibilità di svolgere le operazioni tramite internet banking nonché all'obbligo di custodire i codici segreti necessari per poter operare.

Rappresentava che la stessa descrizione dei fatti fosse contraddittoria e contrastasse con la definizione della cliente come un soggetto privo di adeguata alfabetizzazione informatica, evidenziando che – in seguito alla lettura della pagina riepilogativa generata in seguito al dynamic linking – fosse stato inserito l'OTP e che l'art. 18 RTS (Reg. Delegato UE 2018/389) si limitasse a precisare i casi in cui la SCA non è necessaria, in presenza di un "basso livello di rischio".

Ribadiva che sussistesse la colpa grave della cliente e precisava che i successivi due bonifici disconosciuti fossero stati richiamati dalla banca non già perché presentassero elementi di anomalia, ma solo a seguito della segnalazione fornita dalla cliente, accompagnata dalla denuncia in un momento in cui i due bonifici non risultavano ancora eseguiti alla data di ricezione della segnalazione.

DIRITTO

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

Per mera completezza, il Collegio rileva altresì che nelle repliche questa muova una ulteriore contestazione che, tuttavia, non viene espressa in termini di nuova domanda; in particolare, essa lamenta la mancata produzione della documentazione contrattuale relativa all'attivazione del servizio di internet banking, al fine di dimostrare l'inadempimento della banca nel fornire istruzioni adeguate alla sua età avanzata.

La doglianza in parola sembrerebbe mirare alla nullità del contratto sottoscritto; essa, dunque, appare inammissibile sotto un duplice profilo: da un alto in quanto avanzata per la prima volta in sede di repliche, contravvenendo a questo previsto nelle Disposizioni della Banca d'Italia che regolano il presente procedimento, le quali non ammettono ampliamenti del *petitum* in sede di repliche; dall'altro, in quanto esulta dalla competenza temporale dell'Arbitro, poiché – come riferito dall'intermediario (pur non producendone evidenza) – il contratto in questione risulta essere stato sottoscritto nel 2003 (circostanza non specificamente contestata).

Così individuato l'oggetto del ricorso, va rammentato 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 l'operazione contestata consiste in un bonifico eseguito il 22/11/2025, per un importo di € 10.000,00.

Dai log informatici versati in atti emerge che l'accesso all'home banking della ricorrente (prodromica all'esecuzione del bonifico), sia stato effettuato mediante digitazione di un OTP inviato al suo numero di cellulare; non è tuttavia possibile ricavare evidenza di un ulteriore fattore di autenticazione utilizzato per l'accesso. La stessa colonna "SCA_TYPE" è valorizzata con una dicitura non spiegata dall'intermediario.

Alle medesime conclusioni deve pervenirsi con riferimento al successivo enrollment dell'app sul nuovo device; parte resistente fa riferimento al solo "PIN" (peraltro più correttamente qualificabile come OTP), di cui tuttavia non vi è prova dell'inserimento nei log dallo stesso prodotti ma risulta solo l'SMS inviato sul numero di telefono certificato del cliente. Anche con riguardo a tale fase, dunque, manca la prova del secondo fattore utilizzato ai fini della SCA; anche volendo considerare a tal fine la telefonata di

conferma dal numero di cellulare certificato, non v'è alcuna evidenza al riguardo se non il messaggio inviato al numero del cliente.

Peraltro, anche con riguardo all'operazione contestata non è possibile riscontrare evidenza di quali siano i fattori di autenticazione utilizzati per l'autorizzazione.

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 alla 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.

Non può essere accolta, invece, la domanda relativa alla rivalutazione monetaria, in conformità con i principi che governano le obbligazioni pecuniarie (art. 1277 cod. civ.), trattandosi di debito di valuta.

Neppure può trovare accoglimento la domanda di refusione delle spese vive, in quanto non provate; quanto alla rifusione delle spese di assistenza difensiva, deve essere richiamato il principio di diritto di recente affermato 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 stabilito 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 accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 10.000,00 oltre interessi legali dal reclamo al saldo.

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