Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	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 10/02/2026

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 30.06.2025, una telefonata da un'utenza apparentemente riconducibile all'intermediario, nel corso della quale un operatore segnalava presunte operazioni fraudolente sul conto e la necessità di procedere al blocco e richiedeva le credenziali di accesso all'home banking.
Faceva presente di aver fornito i dati richiesti, confidando nella genuinità dell'interlocuzione, dopo aver verificato che l'utenza telefonica fosse riconducibile all'intermediario e di aver successivamente ricevuto una nuova telefonata che confermava il blocco delle operazioni sospette.
Evidenziava che, nei giorni 30.06.2025 e 01.07.2025, fossero pervenuti due SMS relativi all'esecuzione di due bonifici istantanei non autorizzati per importi pari ad € 1.498,00 e ad € 1.499,00 verso soggetto sconosciuto; soggiungeva, tuttavia, che in data 03.07.2025, non riuscendo ad accedere all'home banking, si fosse recato presso la filiale dell'intermediario e fosse venuto a conoscenza dell'esecuzione di ulteriori tre bonifici ordinari non autorizzati, disposti anche su altro conto cointestato, per un importo complessivo pari ad € 38.397,00.
Affermava di aver presentato reclamo e sporto denuncia-querela presso l'autorità competente; riteneva che la frode fosse riconducibile a un caso di vishing con caller id spoofing, particolarmente sofisticata poiché realizzata mediante manipolazione dell'identità del chiamante, idonea a generare un legittimo affidamento sull'autenticità dell'interlocuzione, ed agevolata dall'assenza di adeguati sistemi di

prevenzione, monitoraggio e blocco delle operazioni anomale, nonché dall'inefficacia del sistema di autenticazione forte adottato dall'intermediari.
Lamentava anche l'assenza di notifiche SMS per alcune operazioni e il mancato blocco cautelativo del conto, che costituirebbero ulteriori criticità organizzative imputabili all'intermediario ed imputabili alla sua responsabilità.
Chiedeva, pertanto, il rimborso delle somme fraudolentemente sottratte.
Costituitosi ritualmente, l'intermediario convenuto rilevava che il numero indicato dal cliente fosse stato utilizzato unicamente per mascherare il numero reale del chiamante e non gli fosse in alcun modo riconducibile, essendo operante solo in ambiti territoriali diversi da quello associato al prefisso telefonico indicato. Precisava che il numero in questione risultasse riferibile esclusivamente a un servizio di assistenza dedicato alle carte di pagamento e non al servizio di home banking né ad altri servizi dell'intermediario. Sottolineava che la documentazione contrattuale consegnata al cliente e sottoscritta includesse una specifica informativa sulla sicurezza dei pagamenti, nella quale era espressamente indicato che l'intermediario non richiede mai telefonicamente, via e-mail o tramite SMS la comunicazione delle credenziali di accesso; specificava di aver pure inviato al cliente, nel periodo 2024-2025, numerosi messaggi informativi, ricevuti e letti, volti a sensibilizzare sui rischi di frode e sull'obbligo di non condividere le credenziali personali.
Rappresentava che dalla documentazione prodotta dallo stesso cliente emergesse un comportamento negligente e imprudente idoneo a consentire la realizzazione della frode; in particolare, dagli screenshot allegati risultava la ricezione di messaggi contenenti avvisi espliciti a inserire i codici esclusivamente nell'applicazione ufficiale e a diffidare di qualsiasi richiesta alternativa, ai quali non aveva gatto seguito alcun contatto da parte del cliente.
Osservava, peraltro, che le verifiche effettuate dall'ufficio antifrodi del gruppo di appartenenza avessero accertato che i bonifici fossero stati disposti tramite accesso regolare al servizio di home banking mediante l'utilizzo delle credenziali corrette e l'autorizzazione SCA dal dispositivo associato al cliente, senza anomalie tecniche, bypass dei protocolli di sicurezza, intrusioni, spoofing di sistema, malware o deviazioni di traffico e che le operazioni fossero state precedute dal censimento dei beneficiari e successivamente autorizzate attraverso l'inserimento del PIN sul dispositivo del cliente, secondo procedure ordinarie e conformi alla normativa vigente.
Rilevava che i sistemi antifrode non avessero rilevato comportamenti anomali rispetto allo storico operativo del cliente né nella fase di accesso né in quella dispositiva.
Sosteneva che il monitoraggio delle operazioni di pagamento, ai sensi della normativa europea e degli orientamenti richiamati, non richiedesse necessariamente un controllo in tempo reale preventivo, potendo operare anche *ex post*.
Riteneva che il ritardo nella segnalazione delle anomalie integrasse una grave violazione degli obblighi di diligenza e avesse contribuito in modo determinante all'entità del danno, oltre ad integrare una violazione degli obblighi di custodia delle credenziali e di immediata comunicazione dell'uso non autorizzato, previsti dalla normativa di settore e dalle condizioni contrattuali.
Concludeva precisando che la colpa grave del ricorrente escludesse il diritto al rimborso delle somme contestate, ai sensi della normativa applicabile.
Chiedeva, pertanto, il rigetto del ricorso.
Alle controdeduzioni dell'intermediario replicava il ricorrente, evidenziando che l'intermediario si fosse limitato a negare la riconducibilità dell'utenza telefonica utilizzata per la chiamata fraudolenta senza spiegare come un terzo fosse riuscito a utilizzare una numerazione riferibile ai propri servizi di assistenza. Ribadiva che sul display del telefono fosse comparsa una denominazione completa e corretta riconducibile al gruppo bancario dell'intermediario, circostanza mai adeguatamente chiarita dalla resistente, che aveva assunto una posizione contraddittoria, negando il collegamento del numero telefonico per il solo prefisso e ammettendo al contempo che i propri servizi di assistenza utilizzano numerazioni con il medesimo prefisso. Contestava l'affermazione secondo cui i sistemi antifrode non

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

avessero rilevato anomalie comportamentali, tenuto conto che dagli estratti conto prodotti emergesse che le operazioni contestate costituissero le uniche movimentazioni anomale rispetto all'uso storico del rapporto.
Riteneva sussistente una ulteriore contraddizione nella ricostruzione di parte resistente, che da un lato affermava la normalità delle operazioni e dall'altro lo aveva convocato urgentemente in filiale proprio per la loro anomalia.
Precisava che la procedura di registrazione del nuovo dispositivo si fosse conclusa immediatamente prima dell'esecuzione del primo bonifico fraudolento e che tutte le operazioni fossero state disposte in sequenza ravvicinata, con causali e importi del tutto estranei alla normale operatività del conto, pertanto l'intermediario avrebbe dovuto attivare presidi di alert e di blocco cautelativo.
Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale reiterava le proprie deduzioni in merito alla estraneità dell'utenza telefonica.
Soggiungeva che nessun nuovo dispositivo fosse stato registrato e che l'unico device associato al cliente fosse rimasto quello già censito per l'autenticazione forte, sottolineando che i sistemi antifrode non avessero rilevato anomalie né nella fase di accesso né in quella dispositiva.
Ribadiva che le operazioni di bonifico fossero state eseguite tramite accesso regolare, utilizzando credenziali e SCA rilasciate dal dispositivo in possesso del cliente, sul quale erano stati indirizzate le notifiche SMS relative ai primi bonifici, senza che questi avesse contattato tempestivamente la filiale o il servizio di blocco
Osservava che la condotta del cliente integrasse negligenza grave per cessione delle credenziali e autorizzazione delle operazioni.

DIRITTO

La domanda proposta dalla ricorrente è relativa all'accertamento del diritto alla restituzione del controvalore di alcune operazioni, successivamente disconosciute.
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

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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 consistono in cinque bonifici eseguiti tra il 30.06.2025 e l'01.07.2025, per un importo complessivo di € 37.697,00.
Secondo la ricostruzione fornita dall'intermediario, a supporto della documentazione tecnica e dalle risultanze informatiche versate in atti, il processo di accesso all'home banking prevede l'inserimento di codice utente e password su home banking, con successiva richiesta di accesso che genera una notifica push in app sul device del cliente, da approvarsi con digitazione del Pin conosciuto dal cliente stesso.
Orbene, dall'analisi dei log forniti risulta la notifica push in APP sul device riferibile al cliente, ma non vi è evidenza né dell'inserimento della password richiesta per accedere all'home banking, né del PIN da inserire in APP con la push autorizzativa per completare l'autenticazione.
Il cliente, tuttavia, nel ricorso e in denuncia, ammette di aver fornito i codici di accesso al proprio home banking; pertanto, in presenza di una dichiarazione di natura confessoria, deve ritenersi che il login sia avvenuto tramite inserimento della password (elemento di conoscenza) e con validazione di una push ricevuta su device del cliente (elemento di possesso) a seguito dell'inserimento del PIN.
Parte resistente dà pure atto della circostanza che, in data 30.06.2025, sarebbe anche avvenuto un enrollment del dispositivo, specificando che il telefono enrollato sarebbe diventato "l'unico device ad operare la SCA"; le tracciature informatiche versate in atti, tuttavia, evidenziano che il device su cui è stata reinstallata l'App è il medesimo già in uso al cliente.
Con riguardo alla fase dispositiva dei bonifici, dalla descrizione dei passaggi fornita dall'intermediario emerge che il processo autorizzativo si sarebbe svolto integralmente sull'App, mediante l'autorizzazione dell'operazione attraverso l'inserimento del PIN (fattore di conoscenza) e la successiva ricezione della notifica push in App (fattore di possesso); tuttavia, pur a fronte dell'indicazione secondo cui la SCA sarebbe stata correttamente eseguita (in base ai riferimenti presenti nella legenda), dalle tracciature risulta la sola evidenza della push, mentre non emerge alcuna traccia dell'inserimento del PIN.
Né tantomeno può ipotizzarsi il riutilizzo del fattore di accesso all'area riservata (che il cliente ha pure ammesso di aver fornito al truffatore); va, infatti, rammentato che la European Banking Authority ammette la possibilità di un impiego del fattore già utilizzato in fase di accesso, purché l'operazione avvenga nell'ambito della medesima sessione (Q&A EBA 2018_4141). Nel caso di specie, il login via web risale alle ore 15:53 (quindi entro un lasso temporale superiore a 20 minuti); inoltre, la mancata evidenza dell'inserimento della password ai fini dell'apertura della sessione – elemento che costituirebbe il fattore di conoscenza – lascia presumere che la procedura di autenticazione descritta dall'intermediario sia distinta e autonoma rispetto a quella effettuata tramite il canale web.
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.

PER QUESTI MOTIVI

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 37.697,00.
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