Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BARTOLINI	Membro designato dalla Banca d'Italia
(BA) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) SIVIGLIA	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCA VESSIA

Seduta del 01/12/2025

FATTO

Il ricorrente, titolare del rapporto di conto corrente n. ***975, riferisce di aver subito una truffa sofisticata il 26/02/2025 e di essere stato convinto da presunti operatori dell'intermediario a fornire le proprie credenziali di accesso al conto corrente e scaricare un'applicazione fraudolenta sul proprio dispositivo mobile.
In particolare, sono stati effettuati due bonifici non autorizzati per un importo complessivo di € 29.700,00 e € 14.900,00, per un totale di € 44.600,00.
Il cliente riferisce che la truffa è stata resa possibile poiché le chiamate ricevute risultavano apparentemente provenienti dal contatto ufficiale dell'intermediario.
Afferma di aver esposto le proprie doglianze sul sistema di sicurezza adottato dalla convenuta con diffida rimasta prova di riscontro, nel mese di aprile 2025.
Richiama l'art. 10 del D.Lgs. n. 11/2010, lamentando in particolare che la resistente non abbia tempestivamente bloccato il conto corrente del cliente dopo aver rilevato operazioni e modifiche anomale all'utenza del cliente.
Chiede pertanto di condannare l'intermediario: al rimborso dell'importo complessivo di € 44.600,00, oltre interessi legali sulle somme sottratte, "dalla data di ciascun addebito sino al saldo"; "al risarcimento del danno per il disservizio subito e per l'aggravamento derivante dalla mancata risposta alla diffida, da liquidarsi in via equitativa in euro 2.000"; al rimborso delle spese del procedimento.
Costituitosi, l'intermediario fa preliminarmente presente che il ricorrente ha chiesto il rimborso della somma di € 44.600,00, oltre interessi legali, relativa a due bonifici disposti online il giorno 26/2/2025, a

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

valere sul conto corrente n. ***975, oltre ad € 2.000,00 quale risarcimento del danno e "aggravamento" derivante dalla mancata risposta alla diffida e la refusione delle spese del procedimento.
Afferma che, dal mese di febbraio 2021, è collegato al conto corrente il servizio di home banking, scollegato in occasione della truffa e poi riattivato; tale servizio consente ai clienti di effettuare le operazioni di inquiry e dispositive su tutti i conti correnti personali a loro riferibili utilizzando il telefono cellulare o Internet.
Evidenzia che il ricorrente ha dichiarato in denuncia: di aver ricevuto un sms con l'invito a contattare un numero per disconoscere degli SDD; di aver, successivamente, ricevuto un SMS con denominazione dell'intermediario nel mittente, che lo invitava a contattare un numero non riconducibile alla resistente; di aver chiamato il numero contenuto nell'SMS; di aver intrattenuto una conversazione telefonica con un presunto operatore della resistente; di aver seguito le istruzioni fornite dal sedicente operatore, installando un'app non riconducibile a quelle ufficiali dell'intermediario e rilasciato delle autorizzazioni, ignorando il contenuto delle stesse.
Evidenzia che il ricorrente non ha assolto all'onere di provare la frode, non avendo depositato in atti alcuna evidenza del download dell'app esterna scaricata, registro chiamate in entrata, link dell'app malevola.
Riporta evidenza del servizio di home banking collegato al conto corrente in questione e intestato al cliente, il quale prevede l'accesso alle funzioni di inquiry e dispositive mediante un sistema di autenticazione "forte": - in fase di accesso all'home banking, il sistema di autenticazione prevede, per effettuare il login e le operazioni di inquiry, l'inserimento del numero cliente + PIN (codice statico noto solo al cliente) e del codice OTP (One Time Password), generato da Mobile Token; per disporre le operazioni, dopo avere effettuato la login e inserita l'operazione, la stessa deve essere confermata mediante l'inserimento del PIN + codice OTP (One Time Password), generato da Mobile Token.
Nel caso di specie, la disposizione è occorsa dallo smartphone del ricorrente il cui device name "diting" così come lo userAgent non hanno cambiato nomenclatura nei giorni antecedenti e successivi alla frode.
Per le operazioni dispositive inserite, l'intermediario ha inviato SMS alert, così come riportato dalle schermate interne; per contro, il cliente ha notiziato la banca circa l'evento ed il conseguente disconoscimento delle operazioni solo il giorno successivo.
Rappresenta che da tempo raccomanda la massima attenzione e cautela nell'utilizzo dei canali telematici, pubblicando ricorrenti avvisi specifici nella pagina di accesso al proprio portale, sulla App e sugli schermi degli ATM, nei quali si avverte la clientela anche del fatto che le credenziali non devono mai essere comunicate a terzi.
Con riferimento alla colpa grave, l'intermediario afferma che utilizzare le proprie credenziali per accedere a link di cui non si sia preventivamente verificata l'attendibilità, per poi accedere al proprio home banking con le proprie e riservate credenziali d'accesso (finger print nel caso di specie), configura un incauto comportamento del titolare degli strumenti di pagamento e una condotta gravemente colposa.
Con riguardo alla richiesta di risarcimento del danno da disservizio e mancato riscontro al reclamo, rileva che il ricorrente non offre la prova dello specifico pregiudizio subìto e ritiene priva di pregio l'asserzione afferente il mancato riscontro al reclamo.
Soggiunge di aver richiesto il recall delle operazioni non ottenendo esito positivo e di aver verificato la presenza di un accredito sul conto corrente del ricorrente del 12/03/2025 di € 14.700,00, relativo ad un bonifico con causale "return payment dated 2025-02-27"; volendo escludere un intento speculativo, invita il ricorrente a rettificare le richieste (da quantificare in € 29.890,00).
L'intermediario chiede il rigetto del ricorso.
In sede di repliche, parte ricorrente osserva che, le difese della resistente non considerano né la natura sofisticata della frode né i precisi obblighi di sicurezza e di prova che la normativa e la giurisprudenza consolidata pongono a carico dell'intermediario.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Sostiene che la resistente si sia limitata a registrare le operazioni fraudolente senza attivare un sistema di allarme.
Quanto all'eccezione dell'intermediario sul parziale accredito ricevuto dal ricorrente, precisa che la richiesta di rimborso è da intendersi per l'importo residuo effettivamente sottratto e non recuperato, pari a € 29.900,00, oltre interessi legali dalla data dell'addebito al saldo effettivo.
Insiste per l'accoglimento della domanda risarcitoria pari a € 29.900,00.

DIRITTO

La questione sottoposta al Collegio concerne due operazioni di bonifico online non autorizzate, disposte il giorno 26/2/2025, per un importo complessivo di € 29.700,00 e € 14.900,00, per un totale di € 44.600,00.
Dalla denuncia versata in atti, si sarebbe trattato di una truffa descritta in modo analogo al ricorso, piuttosto sofisticata e articolata in plurimi passaggi, oltre che durata due giorni. In primo luogo il ricorrente ha ricevuto due sms il giorno 26/2/2025, uno da un terzo intermediario e uno da mittente con denominazione della resistente, con invito a contattare due diversi numeri telefonici. A seguire il ricorrente ha contattato il secondo numero telefonico e, seguendo le indicazioni del finto operatore, ha prima fornito il saldo del proprio conto corrente e poi l'invito a installare un'app per proteggere i clienti dalle frodi informatiche. Alle 16:30 ha ricevuto una chiamata da un contatto apparentemente appartenente all'intermediario (06***60) e un SMS con un link per installare l'app, procedendo pertanto all'installazione, acconsentendo alle richieste di permessi e immettendo la propria impronta digitale. Il giorno successivo ha ricevuto un'ulteriore chiamata dal presunto operatore e posto in essere nuovamente tutti i passaggi richiesti fino a che, insospettitosi, accedeva al proprio home banking e riscontrava che erano stati eseguiti due bonifici non autorizzati, che provvedeva a disconoscere.
In sede di controdeduzioni, l'intermediario evidenzia che il ricorrente ha ottenuto sul proprio conto il rimborso di € 14.700,00 da parte del presunto beneficiario dell'operazione e allega la seguente evidenza del rimborso ricevuto dal ricorrente in data 12/03/2025. Nelle repliche, il ricorrente rettifica la richiesta restitutoria per l'importo di € 29.900,00. Alla luce delle evidenze in atti, l'importo sottratto al ricorrente sarebbe pari a € 29.890,00.
Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/1/2018.
L'intermediario afferma che le operazioni contestate sono state eseguite mediante l'utilizzo di due fattori, come richiesto dalla normativa in tema di autenticazione forte, ai sensi dell'art. 10 d.lgs. n. 11/2010, commi 1 e 2, ossia il PIN (fattore di conoscenza) e l'OTP generato da mobile token (fattore di possesso). Precisa che il codice OTP è una password temporizzata valida per un solo utilizzo, in particolare solo per l'operazione richiesta, che viene generata in modo silente dal Mobile Token integrato nell'App che il cliente ha attivato sul device che sta utilizzando. Evidenzia che il testo della notifica, che appare sul dispositivo e sul quale l'utente deve fare "tap" per autorizzare, indica in chiaro quale operazione/attività si sta autorizzando. L'intermediario aggiunge che, nel caso di specie, non è stato attivato alcun secondo fraudolento Mobile Token il giorno della frode, confermando quindi la tesi della disposizione/autorizzazione occorsa dallo smartphone del ricorrente il cui Device name "diting" così come lo userAgent non hanno cambiato nomenclatura nei giorni antecedenti e successivi alla frode. A tal scopo fornisce la descrizione dell'attività eseguita dal 12/02/2025 al 26/02/2025, giorno della frode. Dalle evidenze versate in atti si rileva che in data 26/02/2025 alle ore 17:49:51 è stato effettuato il login mediante inserimento di ID utente e PIN (Impronta Digitale) da indirizzo IP ***11.54, tramite il dispositivo diting (***2UG), nonché utilizzando l'OTP generato dal Mobile Token; alle ore 17:52:05 è stato inserito un bonifico di importo € 29.700,00 in favore dell'IBAN IT***319 e con causale "finanziamento ing", firmato con PIN (Impronta Digitale) e OTP generato dal Mobile Token, da indirizzo

IP ***11.54, tramite il dispositivo diting (***2UG); alle ore 17:54:27 è stato inserito un bonifico di importo € 14.890,00 in favore dell'IBAN IT***600 e con causale "paga straordinaria", firmato con PIN (Impronta Digitale) e OTP generato dal Mobile Token, da indirizzo IP ***11.54, tramite il dispositivo diting (***2UG). Inoltre, dal 27/02/2025 e fino al 03/03/2025, si registrano tentativi di accesso mediante inserimento di ID utente e PIN da diversi indirizzi IP e tramite un diverso dispositivo (***639).
Dai log informativi forniti dall'intermediario risulta che le attività svolte dal 12/02/2025 al 26/02/2025, giorno della truffa, risultano eseguite dal medesimo device impiegato per l'autenticazione delle operazioni oggetto di ricorso. Infine, sempre dai log informatici forniti, risulta che le notifiche push risultano consegnate in app, fino alle ore 17:54 del 26/02/2025, su un telefono avente modello uguale a quello che emerge dai log (cfr. 22***2UG, colonna descrizione device); successivamente, le notifiche risultano non consegnate al cliente.
Tanto permesso, il Collegio ritiene, in conformità con l'orientamento dell'Arbitro in casi analoghi, che la documentazione allegata dall'intermediario nel caso di specie, sia idonea a fornire la prova dell'adozione della SCA nelle operazioni disconosciute, ritenendo conforme il predetto sistema di autenticazione a garantire l'adozione di un doppio fattore di autenticazione, uno di possesso e l'altro di conoscenza.
Quanto invece alla prova della colpa grave o dolo del cliente, il Collegio rammenta che secondo l'orientamento del Collegio di coordinamento (decisione n. 22745/2019) "[…] la previsione di cui all'art. 10, comma 2, del d. lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l' "autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente".
A tale riguardo, l'intermediario adduce che il ricorrente in denuncia ammette di aver installato sul proprio cellulare un'app estranea alla banca, su indicazione di un sedicente operatore, ammettendo di aver concesso i permessi e immesso la propria impronta digitale, e riscontrando soltanto il giorno seguente gli addebiti delle operazioni contestate. Ritiene plausibile che, tramite l'installazione di suddetta app, di cui il ricorrente non ha depositato evidenza, il ricorrente abbia consentito al terzo di assumere il controllo del dispositivo. Inoltre, il ricorrente non produce alcuna evidenza tratta dal proprio registro chiamate. Secondo la prassi di questo Collegio di Bari è stato ritenuto, anche recentemente, gravemente colposo il comportamento dell'utente quando, autorizzando l'installazione di un'applicazione la cui funzionalità risiede nel permettere l'accesso e il controllo di pc e smartphone, consente al truffatore di agire indisturbato e disporre i pagamenti (Collegio di Bari, decisioni nn. 9200/25 e 5283/25). Si deve tuttavia tenere conto di un elemento indiziario di un possibile concorso di colpa dell'intermediario. Si è trattato, infatti, di una truffa piuttosto sofisticata ed insidiosa, che ha visto, tra le altre cose, la telefonata di phishing provenire dallo stesso numero di telefono dell'intermediario, in specie del suo servizio clienti.
Tale dinamica evidenzia, pertanto, l'agevole vulnerabilità organizzativa dei canali di comunicazione adottati dall'intermediario come per altro questo Collegio ha già sostenuto in altri casi simili (Collegio di Bari, decisione n. 9071/22; decisione n. 284/22; decisione n. 7685/2024).
Per contro, assume minore (se non anche nessuna) rilevanza la circostanza contestata dal ricorrente della presenza di alcuni indici di frode, alla luce dell'art. 8, lett. b), del D.M. 112/2007, ai quali l'intermediario non ha dato seguito. In verità, l'unico dato significativo è l'importo delle operazioni di bonifico superiore a € 1.000,00 (€ 14.890,00 e € 29.700,00), che potrebbero avere rilievo se le stesse fossero anomali rispetto all'andamento delle abituali operazioni disposte sul conto corrente del ricorrente. Nel caso di specie, il ricorrente non ha fornito specifiche prove a supporto di quale sia la normale movimentazione del proprio conto, avendo versato in atti soltanto un estratto conto trimestrale

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

dall'01/04/2022 al 30/06/2022, troppo risalente nel tempo per poter dimostrare che, ad oggi, le somme oggetto di disposizione siano anomale e non siano usuali.
L'insieme delle circostanze riferite inducono a ritenere che l'intermediario abbia dato la prova della colpa grave del ricorrente il quale non ha adottato la cautela dovuta al fine di riconoscere il phishing posto in essere ai suoi danni e ha dato seguito alle richieste dei truffatori, installando un'app malevola che ha consentito il perpetrarsi della truffa senza prima effettuare le doverose verifiche presso l'intermediario; ma, al contempo, vi sia stato un concorso di colpa dell'intermediario, quanto meno per la vulnerabilità organizzativa dei suoi canali di comunicazione con i clienti, e quindi per la facile replicabilità da parte dei truffatori del numero del proprio servizio clienti.
Per queste ragioni, il Collegio ritiene che in forza di un concorso di colpa tra ricorrente e convenuto, si debba riconoscere in via equitativa all'intermediario l'obbligo di corresponsione di una somma pari a € 6.000,00 in favore del ricorrente.
Infine, quanto alla richiesta di risarcimento del danno formulata dal ricorrente per il disservizio subito e per l'aggravamento derivante dalla mancata risposta alla diffida, con richiesta di liquidazione in via equitativa in euro 2.000, il Collegio rileva che nessuna prova di un danno concreto e attuale è stata fornita in atti, essendosi limitato il ricorrente a sostenere l'illegittimità della condotta dell'intermediario. A tale riguardo, il Collegio rammenta che in conformità con l'orientamento espresso dalla giurisprudenza di legittimità, non è sufficiente allegare l'illegittimità di una condotta per poter ottenere la condanna al risarcimento, non essendo configurabile nel nostro ordinamento il danno *in re ipsa*. Per contro il ricorrente è tenuto a fornire la prova sia dell'*an* che del *quantum* della pretesa risarcitoria (cfr. Collegio di coordinamento, decisione n. 1642/19), con specifica indicazione, ai sensi dell'art. 2697 c.c., degli elementi costitutivi del pregiudizio patito sia esso patrimoniale o non patrimoniale (cfr. Collegio di coordinamento, decisione n. 3089/12). Pertanto, la richiesta di ulteriore risarcimento del danno non può essere accolta.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 6.000,00.
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 al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
ANDREA TUCCI