COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(BA) VITERBO	Membro designato dalla Banca d'Italia
(BA) COSTANTINO	Membro di designazione rappresentativa degli intermediari
(BA) ROBUSTELLA	Membro di designazione rappresentativa dei clienti

Relatore CARMELA ROBUSTELLA

Seduta del 29/11/2023

FATTO

Parte ricorrente, in persona del rappresentante legale, riferisce che sul proprio conto corrente è stato effettuato un bonifico non autorizzato tramite App, per € 4.999,00; afferma di aver denunciato la circostanza alla competente Autorità. Chiede pertanto il rimborso dell'importo sottratto.
Costituitosi ritualmente, l'intermediario eccepisce preliminarmente la genericità e indeterminatezza del ricorso, carente di motivazione e di prova a supporto della richiesta economica e, pertanto, implicante lo svolgimento di un'attività di carattere consulenziale da parte dell'ABF.
Illustra, in via generale, le modalità di accesso all'home banking, sia tramite App sia tramite pc, le modalità di disposizione di un bonifico tramite i predetti canali e le modalità di *enrollment* di un token software su un nuovo device. Osserva che ognuna delle citate operazioni avviene in conformità con i requisiti in materia di SCA previsti dalla direttiva PSD2.
Nel merito, conferma che l'oggetto della controversia concerne la restituzione della somma di € 4.999,00, relativa a un'operazione di bonifico effettuata il 14/03/2023.
Rappresenta che né in sede di reclamo né di ricorso, parte ricorrente riferisce le modalità di svolgimento dei fatti occorsi e che l'unica documentazione allegata è la denuncia alle Autorità, da cui si evince che la ricorrente avrebbe ricevuto, in data 14/03/23, alle ore 12:00 circa, una prima telefonata da un numero riconducibile all'intermediario resistente, da parte di un sedicente operatore di un diverso intermediario, seguita da una seconda telefonata,

durante la quale avrebbe comunicato i dati relativi alla società; infine, con sms delle 14:10 parte ricorrente avrebbe ricevuto un codice di attivazione del token software e un messaggio di conferma dell'avvenuto aggiornamento.
Ribadisce che, in mancanza di prove, non è possibile una ricostruzione puntuale di quanto avvenuto.
L'intermediario reputa riscontrabile solamente la circostanza dell'invio di un sms e di una mail contenenti i codici per l'attivazione del token software, rispettivamente al numero di cellulare del cliente e all'indirizzo mail della società ricorrente. Ritiene quindi che la vicenda rientri nello schema dello "smishing" e del "vishing" evidenziando, peraltro, che parte ricorrente non ha fornito alcuna evidenza per comprovarlo.
Soggiunge che dai log si evince: un accesso tramite web browser il giorno 14/03/23, alle ore 12:11; un accesso da App, alle ore 14:11, eseguito con il codice di attivazione di un nuovo token software, inviato al cliente un minuto prima; la disposizione del bonifico contestato, da tale App, alle ore 14:15.
Evidenzia che, a fronte della disposizione di bonifico, il cliente ha ricevuto una mail di alert alle ore 14:15; ritiene pertanto che l'operazione sia stata correttamente autenticata e non sia riconducibile a una frode.
Fa presente che lo stesso ricorrente nella denuncia ammette di aver comunicato i propri dati ai presunti truffatori nel corso della telefonata; inoltre precisa che per installare il nuovo token software su un nuovo device era necessario disporre della password dinamica OTP, inviata alle ore 14:10 via mail e via sms, esclusivamente ai recapiti intestati a parte ricorrente.
A conferma della leggerezza di parte ricorrente, rileva che, come dalla stessa affermato, gli sms ricevuti sembravano apparentemente provenire da altro intermediario, emittente di carte di pagamento e soggetto terzo rispetto alla resistente.
Soggiunge di aver periodicamente informato i propri clienti per metterli in guardia dai tentativi di frode e che il cliente ha ignorato la mail di alert prontamente inviata dalla resistente, non consentendo di bloccare il bonifico denunciato come fraudolento. Chiede pertanto il rigetto del ricorso.

DIRITTO

Preliminarmente, si osserva che l'intermediario eccepisce l'inammissibilità del ricorso, rilevando che parte ricorrente non specifica la *causa petendi* del ricorso e non allega prove a supporto della richiesta di rimborso dell'operazione contestata.
Si osserva che effettivamente nel modulo di ricorso l'odierno istante, in persona del legale rappresentante, non assistita da un procuratore, si limita a contestare l'effettuazione di un bonifico non autorizzato sul proprio conto corrente, chiedendone il rimborso. Al riguardo, si osserva che in generale parte ricorrente è tenuta a formulare una domanda articolata nel *petitum* e nella *causa petendi*, che non si risolva in una mera richiesta di verifica della legittimità della condotta tenuta dalla banca (cfr. *infra*, *ex multis*, Collegio di Coordinamento, decisione n. 10929/16).
In varie occasioni, tuttavia, i Collegi hanno affermato che la valutazione sulla indeterminatezza della domanda deve essere fatta tenendo conto del contenuto complessivo del ricorso e dei documenti ad esso allegati (cfr. ex multis per il Collegio di Bari, decisione n. 7704/22, in linea con la sentenza della Corte di Cassazione n. 1681/2015).
Inoltre, in conformità con la giurisprudenza di legittimità, molti Collegi hanno affermato che l'onere di determinazione dell'oggetto della domanda è validamente assolto anche quando l'attore ometta di indicare esattamente la somma pretesa dal convenuto, a condizione che abbia però indicato i titoli posti a fondamento della propria pretesa, ponendo in tal modo il convenuto in condizione di formulare le proprie difese.

Nel caso di specie, è in atti la denuncia presentata in data 15/03/2023, nella quale il legale rappresentante riferisce di essere stato contattato da un numero di telefono apparentemente riconducibile all'intermediario resistente, da un sedicente operatore di un diverso intermediario, che lo avvisava della necessità di aggiornare i dati antiriciclaggio.
Precisa che alle ore 14:09 veniva ricontattato dallo stesso numero e che nel corso di tale telefonata forniva alcuni dati relativi alla società ricorrente.
Alle ore 14:10 riceveva un sms contenente un codice di attivazione token da lui mai richiesto, seguito da due sms informativi, sul numero di telefono dell'intermediario terzo, dell'avvenuto aggiornamento. In data 15/03/2023, alle ore 10:15, parte resistente contattava il cliente per comunicare di aver riscontrato un tentativo di frode, mediante disposizione di un bonifico per l'importo di € 4.999,00. Pertanto, il Collegio, accogliendo anche il principio sancito dalla Corte di Cassazione (sentenza n. 1681/2015), in virtù del quale la valutazione deve essere fatta caso per caso, e considerato quanto risulta dalla documentazione agli atti, ritiene che l'oggetto della domanda possa essere ricavato dalla suddetta documentazione.
Nel merito, l'operazione contestata è stata eseguita 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.
Il ricorrente disconosce un'operazione di bonifico disposta tramite App il 14/03/2023 di importo pari a € 4.999,00. L'intermediario eccepisce che l'ordine di bonifico per cui vi è contestazione, impartito mediante App, era stato validato attraverso un sistema di autenticazione forte a due fattori. In particolare, questi ricostruisce le modalità di:

- accesso: tramite App è necessario l'utilizzo congiunto dell'App/Token Software installata sullo smartphone e delle credenziali statiche (userid-password e pin), mentre tramite browser/pc è necessario l'utilizzo congiunto della userid-password e del codice OTP generato dal Token Software, previa digitazione del PIN;
- disposizione di un bonifico: tramite App è necessario l'utilizzo congiunto dell'App/Token Software installata sullo smartphone e del codice PIN, mentre tramite browser/pc è necessario l'utilizzo congiunto della lettura a video, tramite App, del QR code riferito alla singola operazione e del codice OTP generato dal Token Software, previa digitazione del PIN;
- enrollment del Token Software su un nuovo device: utilizzo congiunto della userid-password e del codice OTP, inviato a mezzo e-mail.

A supporto di quanto affermato:

- produce in atti i *log* del proprio sistema informatico relativi al periodo 04/03/2023 – 14/03/2023;
- allega evidenza del sms e della mail, inviati ai recapiti di parte ricorrente e coincidenti con quelli riportati in denuncia, contenenti il codice (OTP) per poter attivare un nuovo token software.

Dall'esame dei predetti log si evincono gli accessi (login) intervenuti da web browser e da App (rispettivamente, ore 12:11 e 14:11), l'autorizzazione avvenuta il 14/03/2023 per la predisposizione del bonifico in questione (ore 14:15), emerge inoltre un'autorizzazione per la modifica dei dati personali nei minuti successivi all'operazione di bonifico (ore 14:25).
Sulla base di quanto denunciato da parte ricorrente, la resistente ipotizza che in occasione della prima telefonata c'è stato un accesso via web, mentre, durante la seconda telefonata c'è stato un nuovo accesso dall'App attivata con il codice inviato al cliente.
Dalla documentazione versata in atti si evince che l'operazione di bonifico è stata disposta tramite App, quindi durante il secondo accesso a seguito di enrollment del Token, eseguito alle ore 14:11 del 14/03/2023, ma non risulta presente in atti alcun riferimento all'operazione di enrollment del Token Software sul device dei truffatori, nonché alcuna indicazione su quali

siano stati i fattori di sicurezza richiesti, sia in fase di login, sia nella successiva fase di autorizzazione delle operazioni di bonifico.
Difettando la dimostrazione oggettiva della procedura di autenticazione e autorizzazione che la banca sostiene avere adottata nella fattispecie in esame, non è possibile ritenere che l'operazione di pagamento in questione sia stata compiuta all'interno di un sistema adeguatamente presidiato, secondo gli standard di sicurezza definiti dalla regolamentazione pro tempore vigente in materia, come declinati dall'EBA negli orientamenti del 21 giugno 2019 elaborati sull'autenticazione forte.
Alla luce di queste evidenze, deve, pertanto, essere riconosciuto il diritto del ricorrente ad ottenere la ripetizione del controvalore dell'operazione disconosciuta.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 4.999,00.
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