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) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - FABIO GIROLAMO PORTA

Seduta del 26/05/2025

FATTO

Insoddisfatto dell'esito del reclamo, il ricorrente, contitolare con la moglie di un conto corrente (n. ***279) abilitato all'operatività on-line intrattenuto presso l'intermediario convenuto, chiede il rimborso della somma fraudolentemente sottratta da terzi a conclusione di una operazione di pagamento, a mezzo bonifico bancario, dal medesimo asseritamente non autorizzata.
In particolare, il ricorrente espone: di avere ricevuto, alle ore 12:58 del 19/12/2024, uno SMS, apparentemente proveniente dall'intermediario, recante la segnalazione di scadenza del questionario di "adeguata verifica" e l'invito a contattare il numero 06***; di avere interloquito con il presunto operatore, contattato sull'utenza indicata nel messaggio, il quale rappresentava che nelle ore successive avrebbe comunicato gli esiti delle opportune verifiche; di avere ricevuto la telefonata dal falso operatore, alle ore 16:52 dello stesso giorno, il quale confermava "*il corretto inserimento del questionario*" e chiedeva di disinstallare l'APP di *homebanking* per un aggiornamento, nonché di installare l'applicazione "*Token APP*"; di avere accolto la richiesta, seguendo le istruzioni impartite dal chiamante, e di essere stato nuovamente contattato dallo stesso individuo, alle ore 08:10 del 20/12/2024, il quale riferiva che avrebbe fornito aggiornamenti nel pomeriggio; di essersi tuttavia avveduto - in mancanza dell'atteso riscontro da parte del (falso) operatore - che i numeri dai

quali era stato in precedenza raggiunto fossero inesistenti e di avere appreso dal servizio clienti dell'intermediario (contattato alle ore 18:00 circa) di essere rimasto vittima di una truffa. A tale ultimo riguardo, il ricorrente afferma: di non avere rivelato a terzi il proprio codice cliente e "*i codici PIN*"; che la mattina del 19/12/2024, il conto (n. ***279) evidenziava un saldo attivo superiore a € 25.000,00, mentre alle 09:19 del 21/12/2024, risultava pari a € 8.001,44, per via di un bonifico in uscita di € 16.000,00, eseguito alle ore 17:23 del 19/12/2024, in favore di un soggetto sconosciuto; che il sistema di *alert* non era funzionante; di avere sporto denuncia presso le autorità competenti e chiesto il rimborso dell'operazione disconosciuta alla banca convenuta, ricevendo riscontro negativo.

Tanto premesso in fatto, il ricorrente, ascrivendo all'intermediario la responsabilità dell'evento dannoso per non avere approntato idonei presidi di sicurezza nell'erogazione dei servizi di cui trattasi, invoca la tutela dell'Arbitro affinché disponga il rimborso del controvalore della transazione non autorizzata, pari a € 16.000,00.

Instaurato il contraddittorio, l'intermediario si oppone alla domanda del ricorrente rilevando che dalle verifiche effettuate non è emerso alcun malfunzionamento o compromissione dei sistemi utilizzati. In proposito, precisa che il servizio di home banking da App prevede l'utilizzo di un sistema di autenticazione *forte*, sin dalla fase di accesso all'area riservata; in particolare, per le operazioni di *login* e *inquiry*, il sistema richiede l'inserimento delle credenziali di sicurezza (numero cliente e PIN) e del codice OTP generato dal Mobile Token; per le operazioni dispositive è necessario l'inserimento del PIN e del codice OTP. Specifica che il codice OTP viene generato in modo "*silente*" dal mobile token integrato nell'App, e che la notifica inviata sul device del pagatore – la quale presuppone il *tap* dell'utente per l'autorizzazione – indica chiaramente l'operazione che si sta approvando. L'intermediario soggiunge che l'attivazione del *Mobile Token* avviene attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato via sms al numero di cellulare collegato all'home banking, indipendentemente dall'attivazione del servizio di sms Alert.

Nella fattispecie, la resistente afferma che la transazione controversa è stata correttamente autenticata, registrata e contabilizzata, secondo quanto evincibile dai log prodotti, i quali documentano l'esecuzione di un bonifico bancario impartito a distanza (home banking) dal correntista, in data 19/12/2024, per l'importo di € 16.000,00, mediante addebito sul c/c n. ***279, con la digitazione dei codici statici e della password dinamica generata dal Mobile Token integrato nell'App precedentemente attivata sul device dell'ordinante. Deduce altresì che, contrariamente a quanto sostenuto dal cliente, contestualmente all'esecuzione dell'operazione ha inviato a quest'ultimo un alert via SMS e via *push*. Osserva di essersi prontamente attivata per il richiamo della somma trasferita, in riscontro alla segnalazione del cliente ricevuta due giorni dopo la frode, seppure con esito negativo.

Nel descritto contesto, la resistente sostiene che in presenza di un sistema valutabile in astratto come sicuro, debba presumersi che l'utente, rimasto vittima di una truffa non sofisticata, sia incorso in colpa grave contravvenendo agli obblighi di custodia dei codici e delle credenziali associate al conto in suo possesso. Sul punto rileva che: il ricorrente non ha allegato alcuna evidenza in ordine al messaggio che sostiene di avere ricevuto, ha ammesso di avere seguito le istruzioni del frodatore e installato un APP non a sé riconducibile, al pari del numero indicato come contenuto nel messaggio truffaldino. Soggiunge di avere avviato da tempo una campagna informativa in favore della clientela per favorire la massima attenzione e cautela nell'utilizzo dei canali telematici. Pertanto, escludendo profili di responsabilità alla medesima ascrivibili in relazione alla vicenda che occupa, la resistente chiede all'Arbitro la declaratoria di rigetto del ricorso in quanto infondato.

DIRITTO

Il ricorrente rivendica il diritto al rimborso dell'importo di euro 16.000,00, pari al controvalore di un bonifico bancario eseguito a distanza, in data 19 dicembre 2024, utilizzando il sistema di internet banking, mediante addebito sul conto corrente n. ***279 al medesimo cointestato, successivamente disconosciuto.

La materia, sulla quale è imperniato il ricorso, è regolata dalle disposizioni del d.lgs. 27 gennaio 2010, n. 11, di recepimento della direttiva 2007/64/CE, come modificato dal d.lgs. 218/2017 (che ha attuato la Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno), secondo cui il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricade, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme illecitamente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore (v. combinato disposto degli artt. 7 e 12, comma 4, d.lgs. n. 11/2010; Provvedimento Banca d'Italia 5.7.2011, Sez. IV, § 2). In particolare, a mente dei commi 1 e 2 dell'art. 10 (d.lgs. n. 11/2010, cit.): "Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti. Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".

Nel caso in esame, dalla documentazione in atti consta l'esecuzione a distanza di un bonifico ordinario disposto alle ore 17:08 del 19/12/2024, per l'importo di euro 16.000,00 addebitato sul conto corrente n. ***279 cointestato al ricorrente e al coniuge. A fronte del disconoscimento operato dal ricorrente, la convenuta ha negato il rimborso, ritenendo il cliente unico responsabile della frode subita, sul rilievo che l'operazione sarebbe stata correttamente conclusa attraverso una procedura di accesso all'area di home banking, di autenticazione e autorizzazione nel complesso conforme ai requisiti di Strong Customer Authentication, combinando più elementi di sicurezza indipendenti tra loro: uno statico (il PIN, quale fattore di conoscenza) e uno dinamico (OTP, quale fattore di possesso).

A sostegno della formale regolarità della procedura illustrata, la resistente allega talune evidenze estratte dai propri sistemi informatici onde ricostruire le operazioni di login, di autenticazione ed esecuzione dell'ordine di bonifico impartito alle ore 17:08 del 19/12/2024. In particolare, con riferimento alla fase di accesso all'area riservata, il log prodotto dall'intermediario documenta: alle 17:05:56 l'inserimento di Id Utente e Pin (PIN) da indirizzo IP 2.195.240.194 con il dispositivo M2103K19PG e verifica a 2 fattori con OTP generato dal Mobile Token; in relazione alla fase dispositiva, risulta che dal medesimo dispositivo e indirizzo IP è stato inserito il bonifico alle 17:08:10 firmato con Strong Customer Authentication, attraverso la digitazione del Pin (PIN) e della OTP generata da Mobile Token. Ora, per quanto il sistema di autenticazione innanzi descritto preveda l'utilizzo di un doppio fattore di sicurezza, nel caso di specie non constano allegazioni specifiche in ordine al device sul quale è stato installato il Mobile Token che ha generato le OTP; più in particolare: l'intermediario non precisa quando è stato installato il Mobile Token sul device adoperato

per l'operazione disconosciuta né se tale installazione sia avvenuta a ridosso dell'operatività contestata o se sia risalente nel tempo; ancorché dai log prodotti si evinca l'utilizzo dei medesimi device e indirizzi IP anche per attività svolte antecedentemente quella contestata, gli stessi registrano attività svolte a partire dalle ore 13:08 del 19/12/2024, successive al messaggio civetta ricevuto dal ricorrente alle 12:58. Assume inoltre rilievo decisivo la circostanza, evincibile dagli stessi tracciati in esame, che in corrispondenza delle attività di "*accesso con Id Utente e Pin con verifica a due fattori con OTP da Mobile Token*", registrata alle ore 17:04:58, e di "*accesso con Id Utente e Pin con verifica a due fattori con OTP da Mobile Token*" registrata alle ore 17:05:56 risulti utilizzata la stessa OTP (77337988) malgrado tra le due operazioni consti l'"Uscita dall'App" alle ore 17:05:44.
Tali significativi elementi inducono il Collegio a ritenere che le evidenze prodotte non costituiscano prova esaustiva e concludente idonea a dimostrare la conformità delle procedure adottate dal PSP (nell'erogazione dei servizi telematici) alle regole di strong customer authentication imposte dalla normativa di settore, in tutti i passaggi illustrati dalla convenuta. Simili lacune depongono per il non corretto assolvimento dell'onere probatorio gravante sull'intermediario, ai sensi degli artt. 10, 10-bis, d. lgs. n. 11/2010, cit. (cfr. ABF Coll. Bari, Dec. n. 11625/2024), la cui valutazione, in aderenza al dato normativo, costituisce un prius logico-giuridico rispetto all'esame di eventuali profili di colpa ascrivibili al titolare del conto abilitato all'operatività on line, ovvero all'utilizzatore nella gestione degli strumenti di pagamento (cfr. ABF Coll. Napoli, Dec. n. 6124/2024).
Tanto induce a concludere che l'ordine di bonifico in questione sia stato perfezionato in un ambiente non conforme agli standard di sicurezza definiti dalla regolamentazione vigente in materia, come declinati dall'EBA negli orientamenti del 21 giugno 2019. Pertanto, assorbita ogni altra questione, il Collegio accerta il diritto del ricorrente al rimborso del controvalore dell'operazione disconosciuta, pari a euro 16.000,00.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 16.000,00.
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