COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BUTA	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) PANZARINO	Membro di designazione rappresentativa dei clienti

Relatore - CONSIGLIA SILVIA PANZARINO

Seduta del 20/07/2023

FATTO

Parte ricorrente riferisce preliminarmente di essere cointestataria di un c/c acceso presso l'intermediario convenuto e di disporre di abilitazione al servizio di home banking, operante mediante apposita applicazione installata sul proprio device mobile. In merito al servizio di home banking, riferisce che unico presidio di sicurezza per il controllo e la verifica ex post di operazioni effettuate consiste in un sistema di sms alert, trasmessi dall'intermediario, in occasione dell'effettuazione di un'operazione.
In data 22/02/2023, alle ore 17:44, il ricorrente riceveva al proprio recapito mobile una telefonata dal numero fisso dell'intermediario con la quale veniva invitato a disinstallare l'app di home banking per favorirne aggiornamento e procedere alla reinstallazione. Il ricorrente eseguiva quanto richiesto, ricevendo un sms dal medesimo contatto con cui l'intermediario inviava il codice token mobile.
Precisa di aver posto in essere tale attività durante la conversazione telefonica senza peraltro comunicare il codice mobile token ricevuto via sms e inserito dal ricorrente stesso in app; evidenzia inoltre che il codice temporaneo viene utilizzato solo per l'installazione dell'app di home banking ma non anche per confermare le singole operazioni effettuate.
Seguiva ulteriori istruzioni per procedere alla configurazione da remoto del sistema di sicurezza web impartite dall'operatore, il quale illustrava che era necessario un intervallo di tempo compreso tra uno e tre giorni lavorativi; il ricorrente riceveva sempre da un numero dell'intermediario gli sms per dare corso a tale operazione, oltre a un sms di conferma dell'appuntamento telefonico previsto per il giorno seguente. Nei giorni successivi, il ricorrente riceveva ulteriori sms ma la soluzione del problema veniva rinviata

ancora di qualche giorno dall'operatore con cui era in contatto; alle ore 17:30 del 24/02/2023, il ricorrente riceveva quattro sms che lo avvisavano dell'annullamento di quattro bonifici.
Allarmato da tale informativa, in data 25/02/2023 effettuava un'estrazione della lista dei movimenti e apprendeva che erano stati eseguiti n. 6 bonifici del valore complessivo di € 17.918,00.
Ritiene che l'intermediario non abbia adottato un sistema di autenticazione "forte", considerando che, una volta abilitata la funzione Mobile Token, con utilizzo di un codice riservato trasmesso una sola volta a mezzo sms, l'utente può liberamente effettuare, con solo ed esclusivo impiego della propria App mobile, ogni operazione, senza necessità di dover autorizzare ogni operazione tramite altro canale esterno all'applicazione stessa. Osserva altresì che il sistema in questione non rispetta il requisito della non riutilizzabilità di almeno uno dei fattori, dal momento che il PIN dispositivo per accedere all'App mobile è notoriamente una password statica e analogamente anche il codice riservato per attivare il mobile token si sostanzia nell'acquisizione di un unico codice che, una volta digitato abiliterebbe l'utente a operare con la propria applicazione di home banking.
Lamenta la mancata adozione di un sistema di pre-alert che informi l'utente dell'avvenuto accesso all'App, nonché il mancato arresto automatico in caso di accesso da un diverso indirizzo IP.
Infine, lamenta che l'intermediario non ha informato dell'avvenuta effettuazione dei bonifici contestati in modo ingiustificato, considerato che in occasione dell'effettuazione di un precedente bonifico, il ricorrente aveva ricevuto regolare notifica.
Sostiene di aver subito una truffa particolarmente sofisticata e chiede il rimborso delle somme sottratte e la condanna dell'intermediario alla refusione delle spese e competenze legali (richiama la decisione n. 3498/2012 del Collegio di Coordinamento). In via gradata, chiede la condanna dell'intermediario in percentuale all'entità della propria colpa, citando la decisione n. 16405/2021 del Collegio di Bari.
Costituitosi, l'intermediario fa preliminarmente presente che il ricorrente chiede il rimborso di € 17.918,00 relativi a n. 6 bonifici disposti online a valere sul conto corrente a questo cointestato, eseguiti da app dell'intermediario il 22 e 23 febbraio 2023, autorizzati con le credenziali di sicurezza del ricorrente; ulteriori 4 bonifici, inseriti ed autorizzati in data 24/02/2023, sono stati annullati. Al conto corrente in questione è collegato il servizio di home banking, che consente ai clienti di operare sui conti correnti personali a loro riferibili, utilizzando il telefono cellulare o internet; tale servizio si avvale di un sistema di autenticazione "forte". Soggiunge che il cliente ha anche aderito al servizio di SMS alert collegato alla propria utenza.
Precisa al riguardo che, nell'accesso all'home banking da app, per effettuare il login il sistema di autenticazione prevede l'inserimento delle credenziali di sicurezza (numero cliente e PIN) e del codice OTP; mentre per disporre le operazioni, è necessario inserire il PIN e il codice OTP. Il codice OTP viene generato dal mobile token integrato nell'app che il cliente ha attivato sul proprio device.
L'attivazione del mobile token è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente e PIN) e del codice OTP inviato al cliente via SMS al numero di cellulare collegato all'home banking, "indipendentemente dalla attivazione del servizio SMS alert".
Nel caso specifico, l'intermediario riferisce di aver inviato al ricorrente alle ore 17:47:22 del 22.02.2023, una mail contenente la conferma della richiesta di attivazione dell'app dell'intermediario, nonché uno specifico alert che metteva in guardia dal rischio di frodi. In seguito, alle 17:48, l'intermediario inviava al numero di cellulare del ricorrente un sms e la

relativa notifica push contenente il codice OTP necessario per l'attivazione del mobile token, indispensabile per completare l'attivazione dell'app dell'intermediario.
A questo punto, parte ricorrente avrebbe dovuto insospettirsi e rivolgersi al servizio clienti se non aveva effettuato la richiesta di attivazione del mobile token; soprattutto non avrebbe dovuto comunicare a nessuno il codice OTP contenuto nell'sms e neppure inserirlo in un eventuale link o pagina web, come raccomandato nel testo del messaggio.
Soggiunge che il sistema di autenticazione a due fattori adottato dall'intermediario è riconosciuto come un sistema forte anche dall'orientamento diffuso dei Collegi ABF (richiama in proposito la decisione n. 5565/2019 del Collegio di Roma).
In presenza di un sistema in astratto valutabile come sicuro, come quello adottato dall'intermediario e in assenza di particolari anomalie di sistema, presume una negligenza dell'utente nella custodia delle credenziali necessarie per utilizzare i servizi di pagamento.
Al riguardo, evidenzia che al fine di prevenire possibili frodi in danno della clientela, la resistente da tempo raccomanda la massima attenzione e cautela nell'utilizzo dei canali telematici, pubblicando avvisi specifici nella pagina di accesso al portale, in cui avverte la clientela anche del fatto che nessun dipendente dell'intermediario chiederà mai le credenziali di sicurezza che sono strettamente personali e non devono essere comunicate a terzi.
Segnala che il tipo di operatività disconosciuta si rende possibile nei casi in cui il cliente abbocchi a un tentativo di phishing rivelando le proprie credenziali.
Tanto premesso, rileva che nel caso di specie: il ricorrente, come dallo stesso dichiarato, ha disinstallato e reinstallato l'app dell'intermediario; ha scaricato un presunto aggiornamento di sicurezza da un sito per nulla riconducibile all'intermediario; non descrive i passaggi compiuti per scaricare la nuova app; ha assecondato per due giorni consecutivi il falso operatore telefonico, non controllando il proprio conto corrente.
Evidenzia che non si deve riporre troppa fiducia nel "caller ID", in quanto "è risaputo che esso non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul display"; ritiene che tale fattispecie sia riconducibile al tradizionale caso di phishing individuato dalla decisione n. 3498/2012 del Collegio di Coordinamento. Richiama la decisione n. 18731/2021 del Collegio di Milano, la decisione n. 13855/2022 del Collegio di Palermo e la decisione n. 12210/2022 del Collegio di Roma in materia di spoofing.
Riguardo alla colpa grave del ricorrente, ribadisce che la frode si è ripetuta nei 2 giorni successivi (23 e 24 febbraio) con la acritica e colpevole collaborazione del ricorrente, senza alcuna premura da parte sua di controllare il proprio conto corrente; richiama inoltre la sentenza della Cassazione civile sez. I - 13/03/2023, n. 7214.
Rileva che dai log si evince la riconducibilità delle operazioni all'id cliente del ricorrente e che tutte le operazioni, di attivazione di mobile token, di login e di bonifico, sono state correttamente validate con un sistema di autenticazione forte; richiama l'Opinion EBA del 21 giugno 2019.
Con riguardo al sistema di alert, riferisce che l'intermediario ha inviato al cellulare del cliente le notifiche push e gli sms alert che risultano regolarmente consegnati; riferisce che la resistente, venuta a conoscenza del disconoscimento delle operazioni, ha comunque avviato l'attività di recall verso la banca del beneficiario, che non ha avuto esito positivo.
In sede di repliche, il ricorrente disconosce, ai sensi dell'art. 2712 c.c. la documentazione prodotta dall'intermediario con riferimento alle operazioni contestate, precisando di non aver mai ricevuto le notifiche via sms. Contesta la non rilevanza di quanto statuito dalla Suprema Corte di Cassazione con la sentenza n. 7214/2023, considerato che i passaggi citati dall'intermediario attengono allo "svolgimento del processo" e non alle ragioni della decisione.

Nel merito, ribadisce le contestazioni svolte nel ricorso e ritiene di essere stato vittima di una frode denominata "man in the middle"; precisa di non essere in possesso del dispositivo registrato nei log, da cui sarebbero state effettuate le operazioni; che il link era riferibile all'intermediario e inserito nella medesima chat da cui provenivano i messaggi genuini.
Infine, lamenta che l'intermediario non si sarebbe espresso sull'automatico annullamento degli ultimi quattro bonifici; insiste per l'accoglimento.
L'intermediario conferma che i log informatici allegati alle controdeduzioni sono il risultato di una estrazione delle procedure informatiche, trasformati in forma leggibile e non editabile, per dimostrare l'autenticazione a doppio fattore. Ribadisce che il cliente si è autenticato mediante le proprie credenziali e che le notifiche push sono inviate dall'app tramite canale telefonico al device del cliente e non risultano tracciate nei log che tracciano esclusivamente la navigazione del cliente tramite app o sito web.
Con riferimento alla colpa del ricorrente, richiama la decisione n. 2663/23 del Collegio di Bari, ritenendo che nella fattispecie in esame non si configura alcuna azione di man in the middle da parte del truffatore ma la frode è stata portata a termine con la collaborazione del ricorrente.
Per quanto attiene ai bonifici annullati del 24/02/2023, l'intermediario sostiene che lo stesso ricorrente vi abbia provveduto, dal momento che la resistente avrebbe solamente potuto bloccarli e non anche annullarli.
Relativamente alle comunicazioni informative sul rischio di frode, l'intermediario ribadisce di averle rese ripetutamente disponibili, da ultimo nella mail ricevuta il giorno della frode.

DIRITTO

La questione sottoposta all'attenzione del Collegio concerne la richiesta di rimborso di una somma relativa ad operazioni non autorizzate dal ricorrente: trattasi di sei disposizioni di bonifico effettuate il 22 e 23/03/2022, per un importo complessivo di € 17.918,00.
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 ha allegato in atti un estratto dei log, con la relativa legenda, a supporto della corretta autenticazione, registrazione e contabilizzazione delle operazioni. Tali documenti sono stati contestati e disconosciuti dal ricorrente sulla base del fatto che non ne è stata attestata l'autenticità. Sul punto, il Collegio rileva che il procedimento ABF non prevede la possibilità di disporre delle CTU, né richiede particolari formalità per la documentazione interna che l'intermediario produca con le proprie difese. Per consolidato orientamento dei Collegi, inoltre, le dichiarazioni e le allegazioni degli intermediari sono considerate in linea generale genuine, tenuto conto del dovere in capo a questi ultimi di cooperazione al funzionamento della procedura (cfr. Collegio di Bari, dec. n. 4772/22).
L'intermediario afferma, in via generale, che l'attivazione del Mobile Token è stata resa possibile attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente tramite SMS al numero di cellulare certificato.
Nel caso di specie, specifica anzitutto che in data 22/02/2022, alle ore 17:46 vi è stato un tentativo di accesso propedeutico all'attivazione del Mobile Token mediante inserimento di PIN da parte di un certo device.
L'intermediario precisa poi che alle ore 17:48 dallo stesso indirizzo IP è stata effettuata l'attivazione del Mobile token tramite l'inserimento del PIN (fattore di conoscenza) e della

OTP trasmessa via sms (fattore di possesso) ed eseguito l'accesso "con verifica a 2 fattori, utilizzando l'OTP (*****018) generato dal Mobile Token".
L'intermediario produce, inoltre, la schermata del sms inviato al ricorrente contenente il codice per attivare il Mobile Token; il numero di cellulare al quale è stato trasmesso il messaggio coincide con quello indicato dal ricorrente nel modulo di ricorso. Nella suddetta schermata viene indicata la data e ora di consegna del sms al cliente (22/02/2023 alle ore 17:48) nonché il testo del messaggio.
Sulla base delle dichiarazioni dell'intermediario, per l'esecuzione delle operazioni di bonifico il sistema ha richiesto, quindi, l'utilizzo utilizzo del PIN (fattore di conoscenza) e dell'OTP generato da mobile token (fattore di possesso) ed infatti dai log prodotti dall'intermediario risulta l'inserimento di sei bonifici, che sono stati autenticati mediante inserimento del codice PIN e dall'OTP generata dal mobile Token. Emerge, inoltre, che l'indirizzo IP utilizzato durante le operazioni coincide con quello associato al device del ricorrente.
Ciò premesso, il Collegio rileva che tanto la preventiva configurazione del Mobile Token, quanto le operazioni contestate sono state autenticate mediante elementi che, in base agli standard tecnici fissati dall'EBA nell'Opinion del 21 giungo 2019, risultano riconducibili alle categorie della conoscenza (PIN per accedere all'home banking, nonché per generare le OTP) e del possesso e che dunque sia stata fornita la prova da parte dell'intermediario dell'autenticazione forte (cfr. Collegio di Bari, decisione n. 2663/23).
Il soddisfacimento dell'onere probatorio gravante sull'intermediario resistente in ordine alla natura "forte" dell'autenticazione e all'assenza di anomalia consente - in conformità alla normativa vigente e secondo la giurisprudenza di consolidata - di analizzare la sussistenza o meno di profili di dolo o colpa grave nella condotta del ricorrente.
Sulla base di quanto prospettato e della documentazione agli atti, il Collegio osserva che nel caso di specie le operazioni non autorizzate sono avvenute tramite frode con sms spoofing.
Al riguardo, il ricorrente ha allegato copia dei messaggi civetta - preceduti dalla telefonata del sedicente operatore - ricevuti da un mittente con denominazione dell'intermediario, all'interno della medesima chat in cui risulta ricevuto il messaggio relativo all'ultimo bonifico del 17/03/2022. Per contro, la resistente mette in luce che il link ricevuto dal ricorrente negli sms allegati non conteneva alcun riferimento all'intermediario e che si trattava di link non sicuro in quanto non contenente il protocollo di sicurezza https (dove "s" sta per sicuro). Aggiunge, poi, che in data 24/02/2023, il ricorrente riceveva sms relativi all'annullamento di bonifici a seguito di richiesta del cliente.
Ebbene, sulla base di quanto prospettato e della documentazione agli atti, è indubitabile che la truffa sia stata perpetrata anche tramite la condotta attiva del ricorrente, il quale - come dallo stesso ricostruito in atti - prima veniva contattato tramite telefonata e poi riceveva un sms con un link per installare sul telefono una nuova app per accedere ai servizi bancari.
È altrettanto vero, però, che la ricostruzione delle modalità della truffa subita dal ricorrente – come possibile dalla documentazione in atti – ne evidenzia i caratteri dell'insidiosità e della sofisticatezza (cfr. Collegio di Bari, dec. n. 1690/2023).
Con riguardo alle operazioni contestate, il Collegio rileva altresì che il numero e l'importo delle suddette operazioni è decisamente anomalo in quanto difforme da quelle usualmente poste in essere dal ricorrente.
Alla luce di quanto sopra, attesa anche la peculiarità del caso in esame legata all'anomalia di numero e importo delle operazioni contestate, il Collegio rileva quindi che possa ritenersi sussistente un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa e, dall'altro, alle criticità

organizzative dell'intermediario, che giustifica l'accoglimento parziale della domanda di restituzione, nella misura dell'70% per cento.
Pertanto, il Collegio, nel caso di specie, riconosce un concorso di colpa tra le parti e, riconosce dovuta alla parte ricorrete la somma di € 12.543,00.
Il Collegio riconosce a titolo di refusione delle spese di assistenza professionale l'importo di € 200,00.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 12.543,00. Il Collegio dispone, inoltre, che l'intermediario corrisponda al ricorrente l'importo di € 200,00 a titolo di refusione delle spese di assistenza professionale.
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