COLLEGIO DI BARI

composto dai signori:

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

Relatore DAMIANO LIPANI

Seduta del 06/02/2023

FATTO

Il ricorrente riferisce di essere cointestatario, unitamente alla coniuge, di un conto corrente presso l'intermediario convenuto, sul quale è stata addebitata la somma complessiva di Euro 49.563,52 a seguito dell'esecuzione di un bonifico fraudolento.
In particolare, afferma:
- di avere ricevuto, alle ore 16:27 del 29/03/2022, una chiamata da un numero riconducibile alla resistente, nel corso della quale un sedicente operatore lo invitava a disinstallare l'app di mobile banking e ad installarne una nuova in quanto, come comunicato in un SMS pervenuto alle ore 14:27 nella chat ufficiale della banca, erano stati riscontrati alcuni problemi di sicurezza che avevano determinato la limitazione dell'operatività del conto;
- di avere ricevuto, insieme alla cointestataria del conto, alle ore 16:29 dello stesso giorno, un secondo SMS, apparentemente proveniente dall'intermediario e contenente il link per scaricare la nuova applicazione;
- di aver cliccato sul link e di essere stato reindirizzato ad una pagina del tutto identica a quella dell'intermediario, nella quale non inseriva dati personali o credenziali di accesso; precisa di non aver comunicato tali informazioni neppure nel corso dell'interlocuzione telefonica;
- che, a conferma dell'operazione di disinstallazione/installazione della nuova app, la moglie riceveva un SMS in cui veniva comunicata la presa in carico della procedura da parte di un operatore e veniva preannunciato un contatto telefonico di quest'ultimo per il giorno successivo, in modo da "finalizzare l'accesso";

- di avere risposto, il giorno seguente, alla suddetta chiamata in occasione della quale l'operatore gli forniva spiegazioni in merito all'installazione della nuova applicazione e che, nel frattempo, giungeva sul cellulare della moglie un messaggio di alert, che la informava dell'avvenuto inserimento di un bonifico di Euro 18.560,23;
- di avere chiesto spiegazioni all'interlocutore, il quale riferiva che avrebbe provveduto al blocco immediato dell'operazione di cui sopra, la quale era stata il frutto di un errore tecnico di un'impiegata;
- di avere contattato direttamente l'intermediario e di avere appreso in tale occasione che il giorno precedente era stato eseguito sul conto corrente un altro bonifico non autorizzato di Euro 49.563,52, di cui non aveva avuto notizia in quanto non aveva ricevuto il relativo messaggio di alert; al contempo, l'operatrice provvedeva ad annullare la disposizione di bonifico di Euro 18.560,23;
- di avere sporto denuncia alle autorità competenti e di essere stato informato, una volta recatosi in filiale, del fatto che gli uffici centrali della banca avevano avviato la procedura di richiamo del bonifico di Euro 49.563,52;
- di avere presentato, in data 05/04/2022, formale reclamo all'intermediario, il quale, tuttavia, forniva una risposta insoddisfacente "nonostante quanto ulteriormente precisato ed annotato anche per il tramite del […] difensore".

Tanto premesso, il ricorrente ritiene che la responsabilità per l'operazione in questione sia imputabile all'intermediario, il quale non avrebbe adottato misure idonee a proteggere i propri clienti da illegittimi ed illegali "hackeraggi" del proprio sistema informatico e, inoltre, non avrebbe garantito presidi rafforzati per le operazioni bancarie effettuate on-line.

Evidenzia, inoltre, che la convenuta avrebbe consentito l'utilizzo fraudolento, da parte di terze persone, dei propri canali di comunicazione, così determinando l'affidamento degli utenti circa la genuinità dell'interlocuzione con la banca.

Individua poi, quali ulteriori profili di responsabilità della resistente, le seguenti circostanze:

- il mancato potenziamento delle campagne informative, nonostante la diffusione di tali fenomeni criminosi;
- il mancato funzionamento del servizio di SMS alert in occasione dell'esecuzione del bonifico contestato, nonostante tale servizio fosse configurato a far data dal 22/11/2019; ritiene che la ricezione di un messaggio di alert avrebbe consentito di avvedersi fin da subito della frode e di agire tempestivamente per ottenere la revoca dell'operazione;
- la natura anomala dell'operazione di Euro 49.563,52 (oltre che di quella di Euro 18.560,23 eseguita successivamente e poi stornata), tenuto conto delle seguenti circostanze: (a) rilevanza dell'importo; (b) provenienza della disposizione da un indirizzo IP diverso da quello riconducibile al cliente; (c) inusualità della transazione rispetto alla normale operatività del conto corrente; (d) assenza di operazioni di rilievo nella storia del conto corrente; (e) anomalia della causale.

Rappresenta, infine, che l'intermediario non ha dato seguito alla richiesta di richiamo del bonifico di Euro 49.563,52.

Sulla base di quanto sopra, il ricorrente chiede la restituzione della somma illecitamente sottratta e il risarcimento dei danni ex art. 26 del D.Lgs. 27 gennaio 2010, n. 11, nonché il rimborso delle spese e delle competenze della presente procedura, maggiorate di rimborso forfetario del 15%, IVA e CPA.

Costituitosi, l'intermediario spiega che, per effettuare il login e le operazioni di inquiry, è richiesto l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) e del codice OTP e che per disporre le operazioni, dopo avere effettuato il login, è prevista la conferma con codice PIN e OTP.

Specifica, poi, che il codice OTP viene generato in modo silente dal mobile token integrato nell'app dell'intermediario e attivato sul device utilizzato dal cliente.

Soggiunge che l'attivazione del mobile token è resa possibile attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare collegato all'home banking.
Riporta, poi, i log relativi all'operatività disconosciuta dal cliente, da cui si evince che in data 29/03/2022, alle ore 16:40, è stato attivato il mobile token su un nuovo dispositivo attraverso l'inserimento del PIN e del codice OTP inviato tramite SMS e che, dopo l'accesso eseguito con verifica a due fattori, è stato inserito, alle ore 16:42, il bonifico contestato, finalizzato con PIN e OTP generato dal mobile token.
Con specifico riferimento alle modalità della frode e alla colpa grave, l'intermediario rappresenta che non è dimostrata la circostanza che il frodatore abbia acquisito dalla banca i numeri di cellulare dei clienti; inoltre, secondo il resistente, il contenuto del primo SMS, alquanto generico, avrebbe dovuto insospettire il ricorrente, non essendo stato preceduto da altre richieste/comunicazioni dell'intermediario e i link – dei quali solo uno riportava nella sua estensione un riferimento alla banca – non contenevano il protocollo di sicurezza "https".
Ritiene plausibile che, per accedere al link riportato nel messaggio, il ricorrente abbia inserito le credenziali di sicurezza dell'home banking e abbia anche inserito o comunicato il codice OTP ricevuto via sms, necessario per attivare il mobile token, per poi seguire le indicazioni fornite dal sedicente operatore e installare una nuova applicazione non riconducibile all'intermediario.
Considera, dunque, raggiunta la prova della colpa grave del ricorrente, il quale ha seguito le istruzioni fornite telefonicamente dal sedicente operatore, omettendo di adempiere con la dovuta diligenza ai propri obblighi di custodia e protezione delle credenziali di sicurezza personalizzate.
Rappresenta, inoltre, di aver inviato al numero di cellulare del cliente le notifiche push e gli sms alert che risultano regolarmente consegnati, compreso il messaggio contenente il codice OTP necessario per l'attivazione del mobile token che non avrebbe dovuto essere comunicato a nessuno.
Soggiunge che il 30/03/2022, quando è venuto a conoscenza del disconoscimento dell'operazione inserita ed autorizzata il giorno precedente, erano decorsi i termini per bloccare il bonifico prima che entrasse nel circuito interbancario, diversamente dall'operazione di Euro 18.560,23.
Eccepisce, infine, l'infondatezza della domanda di risarcimento dei danni e di rimborso delle spese legali.

DIRITTO

Sulla base di quanto prospettato e della documentazione agli atti, il Collegio osserva che la questione in esame attiene la richiesta di rimborso della somma di Euro 49.563,52, oltre interessi legali dal 29/03/2022 al saldo, e la richiesta di risarcimento danni ex art. 26 D.lgs. 27/01/2010, n. 11, nonché la rifusione delle spese legali e delle competenze della procedura, oltre IVA, CPA e rimborso spese generali.
In via preliminare, il Collegio rileva che le operazioni contestate sono state eseguite sotto la vigenza 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.
In punto di prova di autenticazione e di esecuzione delle operazioni di pagamento, il Collegio, innanzitutto, ritiene di dovere superare le contestazioni del cliente relative all'inattendibilità del file excel prodotto dall'intermediario, contenente le tracciature

informatiche, in quanto – secondo la tesi del ricorrente – questo sarebbe inidoneo a dimostrare con certezza la provenienza, il contenuto e la riferibilità delle informazioni riportate al conto corrente del ricorrente.
Infatti, la giurisprudenza costante dell'ABF è nel senso di considerare genuine le informazioni estratte dall'intermediario dai propri sistemi informativi, tenuto conto del dovere in capo a quest'ultimo di cooperazione al funzionamento della procedura e stante, in ogni caso, l'impossibilità nel procedimento ABF di disporre delle CTU per acquisire i dati in questione (cfr. Collegio di Bari, decisione n. 13929/22 e Collegio di Roma, decisione n. 4772/22).
Ciò posto, in ordine alla questione inerente l'attivazione del mobile token, l'intermediario afferma che essa è resa possibile dalla digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente tramite SMS.
In proposito, produce (a) la schermata che riproduce il log relativo all'attivazione del mobile token avvenuta in data 29/03/2022 alle ore 16.40, con la legenda esplicativa da cui si evincerebbe l'inserimento del PIN (fattore di conoscenza) e della OTP ***29 (fattore di possesso), nonché (b) la schermata del messaggio inviato all'utenza certificata contenente il codice per attivare il mobile token.
Dalla sopra citata schermata risulta che il messaggio contenente il codice per attivare il mobile token è stato effettivamente inviato al numero di cellulare della coniuge - nel quale era attivo il servizio di notifiche dei movimenti del conto corrente – coincidente con quello indicato nella denuncia.
Circa la questione del login e dell'esecuzione dell'operazione contestata, l'intermediario afferma che, alle ore 16:40 del 29/03/2022, è stato registrato un login con "verifica a due fattori", mediante inserimento del codice OTP generato dal Mobile Token.
Come visto sopra, per l'esecuzione dell'operazione di bonifico delle ore 16:42 il sistema ha richiesto l'utilizzo del PIN (fattore di conoscenza) e del codice OTP generato da mobile token (fattore di possesso).
Ciò posto, il Collegio rileva che – conformemente ai propri precedenti (tra le altre, Collegio di Bari, decisione n. 32/2023) - il sistema di autenticazione adottato dall'intermediario è idoneo a soddisfare i requisiti dell'autenticazione forte (SCA) richiesti dalla normativa vigente.
Rispetto al profilo della prova del dolo o della colpa grave del ricorrente, questo Collegio ritiene doveroso ricordare che sul punto il Collegio di Coordinamento, con la pronuncia n. 22745 del 10/10/2019, ha affermato che "[…] 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".
Il Collegio rileva che è in atti copia dei messaggi truffaldini (con cui il ricorrente veniva invitato a scaricare la nuova app e veniva preannunciata la chiamata di un operatore) ricevuti nella stessa chat in cui sono pervenuti anche messaggi genuini dell'intermediario; si precisa che anche la cointestataria del conto, che ha aderito al presente ricorso, ha ricevuto sul proprio cellulare messaggi sostanzialmente analoghi a quelli pervenuti sul dispositivo del ricorrente.
Quanto alla telefonata del sedicente operatore, il ricorrente non ha prodotto copia dello screenshot del registro chiamate.

Il ricorrente, dunque, sembra essere stato vittima della truffa denominata "SMS spoofing" che consiste nella manipolazione dei dati relativi al mittente di un messaggio per far sì che quest'ultimo appaia provenire da un soggetto differente, rimpiazzando il numero originario con un testo alfanumerico (ossia quello utilizzato dall'intermediario per i propri messaggi genuini); in tal modo, il truffatore può inviare SMS civetta che sembrano provenienti da numeri o contatti legittimi.

Nel caso di specie, è indubitabile che le modalità di ricostruzione della truffa subita dal ricorrente – come possibile dalla documentazione in atti - ne evidenziano i caratteri della insidiosità e della sofisticatezza. Difatti, il primo SMS civetta veniva ricevuto dal ricorrente nella chat utilizzata dall'intermediario resistente per l'invio, fino al momento della truffa, di comunicazioni genuine; tra l'altro, l'SMS in questione non conteneva errori grammaticali o altre anomalie che potessero evidenziarne la non genuinità. Per tale motivo, verosimilmente il cliente veniva ingannato in ordine a quanto stava accadendo, anche a fronte delle rassicurazioni ottenute dal truffatore nella telefonata.

Tuttavia, è da riconoscere che la truffa è stata perpetrata anche tramite la condotta attiva del ricorrente che, come da lui stesso affermato nel ricorso, ha cliccato sul link contenuto nell'SMS civetta e ha scaricato un'app sostitutiva di quella ufficiale dell'intermediario.

Riguardo ai sistemi di allerta, l'intermediario allega le tracciature informatiche attestanti l'invio e la consegna al numero di cellulare certificato, in data 29/03/2022 alle ore 16:42, del messaggio di alert relativo all'inserimento dell'ordine di bonifico contestato; risulta anche l'invio di una notifica push di identico tenore.

Secondo quanto affermato nel ricorso e nelle repliche, tale messaggio non sarebbe pervenuto sul dispositivo della cointestataria.

Tenuto conto delle modalità della frode sopra descritte, il messaggio di alert relativo al bonifico di Euro 49.563,52 potrebbe essere stato "dirottato" sul device del truffatore (come anche, verosimilmente, il messaggio contenente il codice OTP per l'attivazione del mobile token).

In relazione alla contestazione relativa alla mancata predisposizione, da parte dell'intermediario, di adeguati presidi di sicurezza a fronte di operazioni connotate da indici di anomalia, questo Collegio ritiene di aderire all'orientamento espresso più volte da questo Arbitro secondo cui "il Regolamento n. 389/2018 (riguardante le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri previsti dall'articolo 98, paragrafo 4, della direttiva 2015/2366/UE - PSD2), in vigore dal 14 settembre 2019 prevede soltanto meccanismi di monitoraggio ex post, non essendo previsto un obbligo di monitoraggio delle operazioni in tempo reale (se non nei casi in cui l'intermediario voglia avvalersi della esenzione SCA), di talché tali indici di anomalia non possono essere valorizzati per desumerne una concorrente responsabilità della resistente" (ex multis, Collegio di Roma, decisione n. 8530/21).

Quanto alla contestazione relativa alla mancata revoca dell'operazione contestata, si rammenta che l'art. 5, comma 4, del D.lgs. 11/2010 prevede che: "Il consenso ad eseguire un'operazione di pagamento o una serie di operazioni di pagamento può essere revocato in qualsiasi momento, nella forma e secondo la procedura concordata nel contratto quadro o nel contratto relativo a singole operazioni di pagamento, purché ciò avvenga prima che l'ordine di pagamento diventi irrevocabile ai sensi dell'articolo 17", e cioè prima che esso venga "ricevuto dal prestatore di servizi di pagamento del pagatore".

Al riguardo, la resistente eccepisce che erano decorsi i termini per bloccare il bonifico in quanto ormai entrato nel circuito interbancario e che il tentativo di recall dei fondi ha dato esito negativo.

Alla luce della normativa e della giurisprudenza richiamate, nonché in relazione alle modalità della vicenda come ricostruibile dalla documentazione in atti, aderendo ad un orientamento già espresso dalla giurisprudenza di questo Collegio (cfr. Collegio di Bari, decisione n. 32/2023), appare equo riconoscere una corresponsabilità dell'intermediario resistente (derivante dall'utilizzo, da parte del truffatore, di canali di comunicazione analoghi a quelli ufficiali, sintomatico di una sua criticità organizzativa) e del ricorrente (che ha comunque dato corso alle richieste fraudolente, consentendo l'esecuzione delle operazioni fraudolente in un arco temporale di due giorni), ripartendo le conseguenze patrimoniali delle operazioni contestate nella misura del 70% a carico del primo e del 30% a carico del secondo.
Entro questi limiti, il Collegio ritiene che le domande di restituzione delle somme e di corresponsione degli interessi legali vadano accolte.
La domanda di risarcimento del danno ex art. 26 D.lgs. 11/2010, invece, andrà rigettata in quanto non supportata da allegazioni documentali specifiche.
Il ricorrente chiede inoltre la rifusione delle spese legali senza, tuttavia, versare in atti una fattura emessa dall'Avvocato suo difensore; senonché, a fronte della mancanza di documentazione a supporto della domanda, nonché in ragione della parziale soccombenza, tale richiesta non può essere accolta.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 34.694,00 oltre gli interessi legali dalla data del reclamo al saldo.
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