COLLEGIO DI BARI

composto dai signori:

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

Relatore - FILIPPO BOTTALICO

Seduta del 29/01/2024

FATTO

Il ricorrente, contitolare assieme all'aderente al ricorso di due conti correnti accesi presso l'intermediario odierno resistente, riferisce di aver ricevuto in data 08/03/2023 un SMS da altro intermediario, partner commerciale del resistente e gestore delle carte, con il quale veniva richiesto di effettuare aggiornamenti di sicurezza sul conto corrente, con indicazione di un link.
Afferma che, poco dopo avere effettuato tali aggiornamenti, veniva contattato da un numero riconducibile ad una filiale dell'odierno intermediario e che un operatore gli prestava assistenza, data la complessità della procedura, chiedendogli alcune informazioni tra cui i numeri generati dall'app.
Rappresenta di aver ricevuto un ulteriore SMS dall'intermediario, gestore delle carte, a conferma della procedura e con il quale veniva fissato un appuntamento telefonico per il giorno successivo con il medesimo operatore, al fine di verificare il buon esito dell'aggiornamento.
Come preannunciato, in data 09/03/2023 riceveva una nuova telefonata, sempre da un numero riconducibile alla filiale della resistente, e un operatore lo guidava nel completamento della procedura di aggiornamento, chiedendo di volta in volta informazione sui numeri generati dall'app e raccomandandogli di accedere alla stessa soltanto decorsi due/tre giorni.
Fa presente di essere stato contattato in data 13/03/2023 alle ore 09.00 dalla vera filiale della resistente, la quale lo avvertiva della presenza di bonifici sospetti.

Riferisce di essersi recato personalmente in filiale, ove apprendeva che erano stati effettuati in data 09/03/2023 due bonifici di € 10.000,00 ciascuno e in data 10/03/2023 due ulteriori bonifici, rispettivamente di € 4.978,00 e di € 4.998,00 da un conto, nonché una operazione di € 2.500,00 dall'altro conto in data 13/03/2023.
Evidenzia, quindi, che in tali giorni gli sono stati sottratti in totale € 32.476,00 mediante bonifici mai autorizzati e senza ricevere alcun avviso sulla propria utenza telefonica.
Riscontrata tale situazione, provvedeva a sporgere due querele in data 13/03/2023 e 14/03/2023, allegando copia degli estratti conto; nonché a presentare formale reclamo, riscontrato negativamente dall'intermediario.
Lamenta il superamento del limite giornaliero contrattualmente previsto, fissato in € 5.000,00, a fronte del quale l'intermediario non ha adottato misure adeguate.
Ritiene di essere stato vittima di una truffa particolarmente insidiosa, come confermato dalla circostanza che lo stesso intermediario, a partire dal mese di agosto 2023, abbia predisposto dei messaggi di avviso all'apertura dell'app, fornendo informazioni contro tali tipologie di truffe.
Chiede, dunque, di:
1) "condannare la Banca alla refusione di € 32.476,00, oltre interessi fino al soddisfo;
2) in subordine, condannare la Banca alla refusione di tutte le somme che eccedono il limite giornaliero contrattualmente previsto (€ 5.000,00);
3) condannare la Banca al pagamento delle spese legali e della procedura".
Costituitosi, preliminarmente l'intermediario illustra in generale le modalità di accesso all'home banking sia tramite app sia tramite pc; le modalità di disposizione di un bonifico tramite app; come eseguire l'enrollment di un token software su nuovo device; come modificare i dati personali a sistema.
Osserva che ognuna delle citate operazioni è eseguita in conformità con i requisiti in materia di SCA previsti dalla direttiva PSD2.
In merito al superamento dei limiti operativi contestato dal ricorrente, evidenzia che, dal giorno di sottoscrizione del contratto di internet banking (18/04/2017), la piattaforma si è evoluta con la previsione di nuovi limiti, attualmente portati ad € 10.000,00 per quello giornaliero e ad € 50.000,00 per quello mensile.
Precisa che, in occasione di tali aumenti, sulla piattaforma è stata inviata alla clientela, che aveva già sottoscritto il servizio, una notifica pop up con presa visione obbligatoria.
In tal modo, la clientela è stata messa a conoscenza della variazione dei massimali, peraltro con la possibilità di stabilire limiti di importo differente, ove necessario.
Ciò premesso, ricostruisce la vicenda, rappresentando in particolare che il ricorrente è stato vittima di un tentativo di frode realizzato attraverso la tecnica del c.d. SMS spoofing.
Evidenzia come nessun reale messaggio contiene un link informatico con invito ad accedervi ed inserire le proprie credenziali e che il ricorrente medesimo, cliccando sul link ricevuto, ha inserito i dati richiesti.
Subito dopo ha ricevuto un secondo SMS, in coda a quello precedente, dove gli è stata preannunciata la chiamata da parte di un operatore telefonico.
Successivamente, è stato contattato da un numero coincidente con quello di una delle sue filiali, in quanto i criminali avevano manipolato il numero telefonico del chiamante, realizzando un call ID spoofing.
Sottolinea che durante tale conversazione telefonica il truffatore ha chiesto al ricorrente e questi ha riferito, come si evince dal ricorso, "talune informazioni" e i "numeri generati dall'app", invitandolo poi a cancellare l'applicazione dal telefono.
Osserva che il truffatore, ormai in possesso delle credenziali di accesso fornite dal ricorrente "dopo aver cliccato sul link fraudolento" e utilizzando il "numero generato dall'app" (codice OTP generato dal token software), ha fatto accesso all'home banking

tramite browser alle ore 15:46; successivamente, è stata inviata esclusivamente all'email del ricorrente la password dinamica-codice OTP, necessaria per l'attivazione del nuovo dispositivo.
Afferma che, in tal modo, il truffatore ha completato l'installazione del Token Software sul cellulare ed ha fatto accesso all'home banking tramite app alle ore 15:50 per poi procedere alle successive ore 15:51 a modificare l'indirizzo email collegato al rapporto, al fine di impedire che gli alert sull'esecuzione dei bonifici arrivassero al cliente.
Precisa che a fronte di tale modifica, il ricorrente ha ricevuto una comunicazione di alert.
Rappresenta che immediatamente dopo, alle ore 16.00, il truffatore ha autorizzato via app il primo bonifico, utilizzando le corrette modalità di autenticazione, senza che i sistemi di sicurezza potesse rilevare alcuna anomalia; mentre i successivi bonifici sono stati autorizzati nei giorni successivi (9,10 e 13 marzo) con le stesse modalità.
Tutto ciò narrato, sostiene che le operazioni disconosciute siano state correttamente autenticate, registrate e contabilizzate, senza alcuna anomalia, come confermato dai log informatici allegati.
Ritiene, dunque, che sussista la colpa grave del ricorrente, il quale ha collaborato alla realizzazione della truffa con il suo comportamento imprudente, dapprima facendo accesso al link fraudolento e poi comunicando al truffatore i codici OTP necessari per l'accesso e per l'attivazione dell'app con il token software integrato sul device dei truffatori, in violazione dell'obbligo di custodia previsto dall'art. 7, co. 2 d.lgs. n. 11/2010.
Rileva che il ricorrente è stato vittima della ormai nota truffa dello smishing, e di aver posto in essere campagne informative nei confronti della propria clientela al fine di evitare simili truffe, richiamando l'attenzione dei clienti soprattutto sull'obbligo di custodia dei codici di accesso che consentono l'utilizzo del servizio online.
Evidenza che il ricorrente non ha dato rilevanza alla circostanza che gli SMS provenivano da un intermediario diverso dall'attuale resistente; così come ha ignorato l'alert relativo all'avvenuto cambio di indirizzo email.
Sottolinea poi che il ricorrente ha comunicato a terzi i codici OTP riservati, sia quelli generati dal proprio token software, sia quello pervenuto via email.
Conclude dunque rappresentando che va esclusa la responsabilità della banca nell'ipotesi in cui il ricorrente comunichi imprudentemente le credenziali di accesso all'home banking a terzi, versando così in colpa grave.
Infine, contesta la richiesta relativa alla rifusione delle spese di assistenza difensiva, atteso che è stata formulata unicamente in sede di ricorso e inoltre "la natura alternativa del procedimento comporta […] che lo stesso [sia] instaurabile senza il ministero di un difensore".
Chiede, quindi, il rigetto del ricorso.
In sede di repliche, il ricorrente ribadisce anzitutto la tardività dell'intermediario nell'informare la clientela sulle frodi particolarmente sofisticate, come quella subita.
Ritiene che "il sistema è risultato fallace" dal momento che è stato escluso dallo stesso dopo aver fornito un solo numero OTP, ovvero quello per l'attivazione di un nuovo token software.
Evidenzia, difatti, che con la nuova piattaforma ogni operazione deve essere autorizzata dal cliente anche con il proprio pin personale che, al contrario, non era previsto nella precedente versione, oggetto di numerosi tentativi di frode; così come era previsto l'invio delle notifiche solo via email e non sul dispositivo mobile.
Aggiunge che l'intermediario non ha dato rilevanza alle movimentazioni anomale, avvisandolo soltanto dopo quattro giorni dalla truffa.
Infine, con riferimento al limite dei bonifici, contesta le modalità con cui l'intermediario avrebbe modificato unilateralmente le pregresse condizioni contrattuali.

In particolare, sostiene che la notifica pop up non fornisce prova del fatto che sia stata visualizzata o correttamente intesa; inoltre, afferma che la stessa non ha indicato che il limite contrattuale sarebbe stato variato automaticamente.
Insiste, quindi, per l'accoglimento delle proprie richieste.

DIRITTO

Premesso che 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 13/01/2018, la modalità della truffa sono ricostruite dal ricorrente nella denuncia-querela in atti e nella successiva integrazione in termini analoghi a quanto esposto nel ricorso.
Il ricorrente, dunque, disconosce cinque operazioni di bonifico disposte tramite app nelle date 9, 10 e 13 marzo 2023 di importo complessivamente pari a € 32.476,00.
L'intermediario sostiene che tali bonifici, impartiti mediante app, sono stati validati attraverso un sistema di autenticazione forte a due fattori.
In particolare, 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;
- enrollment del token software su un nuovo device: è necessario l'utilizzo congiunto della userId-password e del codice OTP, inviato a mezzo email;
- modifica dei dati personali: l'utilizzo congiunto di smartphone con app token sofwtare installata (fattore di possesso) e codice pin (fattore di conoscenza).
Specifica altresì che password e pin vengono scelti dai clienti; in particolare, il pin viene scelto in fase di installazione del token software.
Tanto ricostruito, l'intermediario sostiene che in data 08/03/2023:
- alle ore 15:46 i truffatori hanno effettuato un primo accesso al servizio di internet banking tramite browser/pc, inserendo le credenziali di accesso previamente fornite dal ricorrente (il quale aveva cliccato sul link contenuto nel messaggio civetta, ricevuto nella medesima giornata) ed utilizzando il codice OTP generato dal token software, comunicato dallo stesso durante la telefonata;
- i medesimi truffatori necessitavano poi del codice OTP per l'installazione del mobile token sul loro device, ricevuto dal ricorrente via email alle ore 15:49 (14.49 GMT) e comunicato anche esso durante la telefonata;
- una volta completata l'installazione del token software sul loro device, i truffatori hanno effettuato l'accesso tramite app alle ore 15:50 al servizio di internet banking ed hanno modificato l'indirizzo email collegato al rapporto con altro di natura fraudolenta, di cui il ricorrente riceveva comunicazione alert;
- a tal punto, i truffatori avrebbero impostato un nuovo pin e alle ore 16:00 hanno autorizzato via app il primo bonifico fraudolento, mentre gli ulteriori bonifici sono stati effettuati nei successivi giorni 9, 10 e 13 marzo.
A supporto di quanto affermato, produce in atti i log del proprio sistema informatico relativi al periodo 08/03/2023 – 13/03/2023.

Allega, inoltre, ulteriori log volti a provare l'invio della notifica di modifica dei dati personali alla email del ricorrente.
Tuttavia, si deve evidenziare che l'intermediario resistente non offre alcuna prova in ordine ai fattori di sicurezza utilizzati in fase di login, per l'attivazione del token software, e infine nella successiva fase di autorizzazione delle operazioni di bonifico.
La documentazione prodotta e innanzi menzionata, difatti, attesta gli accessi e le disposizioni effettuate nell'arco temporale considerato, ma non contiene alcun riferimento esplicativo alla conformità ai requisiti normativamente previsti in tema di SCA.
Ciò posto, conformemente a quanto prescritto dall'art. 24 del Regolamento Delegato (UE) 2018/389 in tema di associazione all'utente dei servizi di pagamento (in particolare, il secondo comma, lett. b), la giurisprudenza arbitrale – nell'ipotesi di esecuzione delle operazioni con l'utilizzo di app sul device del frodatore – impone di verificare se vi sia stato l'impiego della SCA nella fase di installazione e di configurazione del nuovo dispositivo in questione.
La mancanza di allegazioni in merito non consente di ritenere assolto l'onere probatorio gravante sull'intermediario, secondo quanto statuito da questo Collegio con orientamento meritevole di adesione: "alla stregua delle prescrizioni di cui all'art. 24 del Regolamento Delegato (UE) 2018/389, della Commissione del 27 novembre 2017 - che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri - in tema di associazione all'utente dei servizi di pagamento (v. comma 2, lett. b), nell'ipotesi di esecuzione delle operazioni con l'utilizzo dell'app sul device del frodatore, occorre accertare se nel caso concreto vi sia stato l'impiego della SCA nella fase di installazione e di configurazione del dispositivo utilizzato. Nel caso di specie, la mancanza di puntuali allegazioni fornite dal PSP in merito a tali fasi dell'attività a distanza non consente di ritenere assolto l'onere probatorio sull'autenticazione forte gravante sull'intermediario, ai sensi degli artt. 10, 10-bis, d.lgs. n. 11/2010, cit. (cfr. ABF Coll. Bari, Dec. nn. 3749/2023; 787/2023)" (Collegio di Bari, decisione n. 8597/23; conformi Collegio di Bari, decisioni nn. 787/23 e 14699/22; Collegio di Napoli, decisione n. 14619/22; Collegio di Bologna, decisione n. 13282/22).
Per effetto del mancato assolvimento dell'onere probatorio incombente in capo all'intermediario, che risulta prodromico e assorbente rispetto ad ogni altra valutazione (autorevolmente, Collegio di Coordinamento, decisione n. 22745/19), il ricorso è meritevole di accoglimento con riferimento alla richiesta di rimborso della somma sottratta, considerato che – proprio per effetto dell'enrollment del dispositivo dei frodatori – risulta verosimile che l'operazione contestata, eseguita su tale ultimo device, non abbia presentato indici di anomalia (in senso adesivo, si richiama la decisione n. 11082/23 di questo Collegio resa nei confronti del medesimo intermediario odierno resistente, a mente della quale: "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 le operazioni di pagamento in questione siano state compiute 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"; conformi e sempre nei confronti dello stesso intermediario, Collegio di Bari, decisioni nn. 9919/23 e 9570/23).
Difatti, secondo l'appena menzionato orientamento del Collegio di Coordinamento, la mancanza della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente; la prova di autenticazione rappresenta infatti,

in aderenza al dato normativo, un prius logico rispetto alla prova della colpa grave dell'utente.
Il mancato assolvimento del prodromico onere probatorio in capo all'intermediario assorbe, dunque, la disamina di ogni altro profilo di merito del ricorso sul punto.
Inammissibile è la richiesta di corresponsione degli interessi legali, attesa che tale domanda è stata formulata solo in sede di ricorso e non anche all'atto del preventivo reclamo.
Difatti, a mente della Sez. VI, Par. 1) delle disposizioni ABF, "il ricorso deve avere ad oggetto la stessa questione esposta nel reclamo".
In ordine al concetto di medesimezza della questione, si è espresso il Collegio di Coordinamento, precisando che: "Come è noto, il "ricorso", con il quale è formulata la domanda all'Arbitro Bancario, è preceduto necessariamente da una fase interlocutoria diretta tra le parti, attivata da un atto di contestazione denominato reclamo, che integra una vera e propria condizione di procedibilità. Tale fase preliminare non condiziona solo formalmente l'avvio del procedimento avanti all'ABF, ma refluisce e influisce anche sulla decisione del merito della controversia, giacché il ricorso deve avere ad oggetto la stessa "questione" esposta nel reclamo, il quale dunque diventa utile strumento interpretativo della domanda presentata col ricorso e flessibilmente qualificata dal Collegio" (decisione n. 7716/17).
Sulla scorta di questa decisione, questo Collegio ha chiarito che: "Invero, l'art. 4 della del. Cicr del 29 luglio 2008, n. 275 e il punto 1, sezione VI, delle Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari della Banca d'Italia prevedono che «Il ricorso all'ABF è preceduto da un reclamo preventivo all'intermediario. Il reclamo è effettuato secondo le modalità previste dalla disciplina di trasparenza dei servizi bancari e finanziari. Il ricorso deve avere ad oggetto la stessa questione esposta nel reclamo; …» (sez. VI, § 1). Secondo le medesime Disposizioni è previsto, altresì, che per reclamo si deve intendere «ogni atto con cui il cliente, chiaramente identificabile, contesti in forma scritta all'intermediario un suo comportamento o un'omissione» (sez. I, § 3). Dette previsioni vincolano il ricorrente a rendere preventivamente edotto l'intermediario della contestazione sollevata, in modo da offrire la possibilità a quest'ultimo di poter interloquire sul punto e, per questa via, di migliorare i rapporti con la clientela, prevenendo, se del caso, una probabile lite. Per costante orientamento dell'Arbitro, ancorché sia generalmente ammesso che il reclamo non debba essere inteso in senso formale, la ratio sottesa a tale formulazione precettiva si raccorda all'esigenza di prevenire l'insorgere di controversie e di risolvere in codesta fase preliminare le situazioni di potenziale insoddisfazione del cliente, assicurando, per tal via, il contenimento dei rischi legali e di reputazione degli intermediari e l'efficiente funzionamento del sistema di definizione stragiudiziale di situazioni contenziose. Da ciò discende che non solo il ricorso deve essere preceduto da reclamo, ma che vi deve essere simmetria tra l'oggetto del reclamo e quello del ricorso, il quale è ammissibile solo se l'intermediario è stato posto preventivamente a conoscenza della lagnanza del cliente e quindi nella possibilità di risolvere bonariamente la questione insorta (cfr., in tal senso, Collegio di Milano, decisione n. 4800 del 2014, Collegio di Bologna, decisione n. 5235 del 12 maggio 2017, Collegio di Bari, decisioni n. 8352/2018 e n. 14858/2017)" (decisione n. 21129/18; in senso conforme, la successiva decisione n. 14802/2020).
Non meritevole di accoglimento, infine, è la richiesta di rifusione delle spese legali, del tutto sprovvista di qualsivoglia supporto probatorio.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 32.476,00.
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