COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) VITERBO	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 ESTERNI - GRAZIA BUTA

Seduta del 21/12/2023

FATTO

Il ricorrente premette che: è titolare del conto corrente n. 121 2015-5 aperto presso l'intermediario convenuto, a cui risulta collegata la carta di debito n. 5321********2471; in data 22/03/2023, alle ore 14:16, riceveva sul suo cellulare un primo S.m.s. con cui l'emittente della carta lo informava di aver "limitato la sua carta/conto per mancata verifica di sicurezza web. Riattivala ora"; provvedeva a seguire il link riportato nel predetto messaggio, il quale lo conduceva ad un sito "assolutamente sovrapponibile" a quello utilizzato nei precedenti accessi ed in cui gli veniva richiesto di inserire le credenziali di accesso al conto corrente; non ricordando le predette credenziali, le aveva inserite errate; aveva ricevuto un secondo S.m.s. con cui sarebbe stato "contattato da un nostro operatore in merito alla nuova sicurezza web, la invitiamo ad attendere"; era stato contattato telefonicamente da un operatore tramite l'utenza fissa n. 080****611, riconducibile alla banca, comunicandogli che era necessario "resettare le password di accesso on line" e, una volta eseguita tale operazione, gli era stato richiesto di inviare un codice pervenuto "dapprima a mezzo sms e successivamente tramite mail"; il sedicente operatore lo invitava a disinstallare dal suo smartphone l'App e reinstallarla il giorno successivo, al fine di "ottenere un corretto funzionamento"; aveva ricevuto un terzo S.m.s. con cui gli veniva comunicato "aggiornamento eseguito con successo, la invitiamo ad attendere 1-3 giorni lavorativi un nostro sms di conferma prima di poter utilizzare tutti i nostri servizi online"; in data 23/03/2023, alle ore 14:27, veniva contattato dalla banca per comunicargli che dal suo conto corrente erano stati effettuati due bonifici di € 5.300,00 ed

€ 4.700,00, per un ammontare complessivo di € 10.000,00; aveva disconosciuto "immediatamente" i predetti bonifici e si era recato in filiale per bloccare l'accesso ai servizi di home banking, apprendendo in tale occasione che era stato inviato un "recall" per tali operazioni; in data 28/04/2023 gli veniva comunicato informalmente dalla banca che la richiesta di "recall" aveva avuto esito negativo.

Ciò premesso, richiama un costante orientamento giurisprudenziale secondo cui, in caso di operazioni effettuate a mezzo di strumenti di pagamento elettronici, la sicurezza del sistema va ricondotta nell'area di rischio professionale del prestatore di servizi, di modo che grava sulla banca una responsabilità di tipo oggettivo a meno che questi non provi il dolo o la colpa grave del cliente (cita Cass. Civ., ordinanza n. 9158/2018, Cass. Civ., sentenze n. 2950/2017, 10638/2016, Trib. di Parma, sentenza n. 1268/2018, Trib. di Napoli, sentenza n. 2470/2023).

Soggiunge che la banca è tenuta al monitoraggio delle operazioni effettuate dai correntisti al fine di segnalare tempestivamente anomalie e conseguentemente bloccare operazioni non autorizzate.

Evidenzia che i "pirati informatici" avevano utilizzato numeri riconducibili alla banca a mezzo Sms e chiamata telefonica. Precisa che il testo dell'Sms ricevuto non presenta errori o anomalie tali da poterlo indurre a dubitare della sua autenticità.

Conclude richiamando una comunicazione inviata via e-mail dalla banca in data 09/05/2023, con cui veniva avvertito della modifica della "propria sicurezza bancaria passando ad un nuovo sistema informatico" e che "non ti verranno mai richiesti [dalla banca] dati personali, credenziali e password di accesso al tuo internet banking".

Il ricorrente chiede che "la Banca […] corrisponda al [ricorrente], la somma di €. 10.000,00=, pari all'importo sottratto dal suo conto corrente, oltre interessi e spese della presente procedura".

Costituitosi, preliminarmente l'intermediario illustra in generale: le modalità di accesso all'home banking tramite App; le modalità di disposizione di un bonifico tramite il predetto canale; 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.

Nel merito, fa presente che l'oggetto della controversia concerne la restituzione della somma complessiva di € 10.000,00, relativa a due operazioni di bonifico di € 5.300,00 ed € 4.700,00, effettuate in data 22/03/2023.

Ricostruisce la vicenda mediante i fatti esposti dal ricorrente in sede di reclamo, denuncia e ricorso. Rappresenta in particolare che in data 22/03/2023, alle ore 14:16, il cliente aveva ricevuto un S.m.s. con cui veniva invitato a riattivare la carta per un "fantomatico blocco intervenuto per una presunta mancata verifica di sicurezza", seguendo un link che riportava un "insolito e anonimo indirizzo". Precisa che il predetto messaggio si accodava ai precedenti messaggi inviati dalla "società di emissione e gestione di carte di credito" e che, pertanto, trattasi di un tentativo di frode effettuata mediante la tecnica dello "smishing", utilizzata congiuntamente a quella dello "SMS spoofing".

Evidenzia come il ricorrente medesimo, aprendo il link riportato nel messaggio in questione, aveva inserito le proprie credenziali di accesso (codice utente e password), così comunicandole ai truffatori. Successivamente il cliente aveva ricevuto un secondo S.m.s. e, alle ore 14:30, una telefonata da un numero coincidente con quello di una delle sue filiali, in quanto i criminali "avevano evidentemente manipolato il numero telefonico del chiamante", realizzando un "call ID spoofing". Sottolinea che durante tale conversazione telefonica, "durata ben 27 minuti", il truffatore chiedeva al ricorrente il codice che gli era stato inviato "dapprima a mezzo sms e successivamente tramite email", codice che il

cliente stesso aveva comunicato allo sconosciuto interlocutore e che era necessario per l'attivazione di un nuovo Token Software.
In particolare, ritiene che i truffatori stavano procedendo, grazie ai codici comunicati dal ricorrente, ad attivare l'App con il Token Software sul proprio smartphone, impostando il relativo PIN, chiedendo contemporaneamente al ricorrente di disinstallare l'App. Precisa che i truffatori, una volta completata l'installazione del Token, avevano effettuato l'accesso tramite App alle ore 14:51 ai servizi di internet banking.
Riferisce che, una volta ottenuto l'accesso all'internet banking, i truffatori avevano modificato alle 14:52 l'indirizzo e-mail collegato a tale servizio, precisando che tale operazione era stata resa possibile dalla previa attivazione dell'App sul device dei truffatori. Fa presente che, ad ogni modo, il ricorrente aveva ricevuto alle ore 14:52 un Alert relativo alla modifica dell'indirizzo mail associato al conto.
Alle successive ore 15:00 e 15:01 i truffatori avevano potuto autorizzare i due bonifici fraudolenti in questione via App, senza che i suoi sistemi di sicurezza potessero rilevare alcuna anomalia.
Tutto ciò narrato, sostiene che le operazioni siano state autenticate, correttamente registrate e contabilizzate con un sistema a doppio fattore e senza alcuna anomalia, come confermato dai log informatici allegati. Sostiene che nel caso in esame sussiste la colpa grave del ricorrente che, con il suo comportamento imprudente, aveva consentito ai truffatori di poter perpetrare la frode, in contrasto con quanto previsto dall'art. 7, comma 2°, del D.Lgs. n. 11/2010. In particolare, evidenzia che gli Sms ricevuti sembravano provenire dalla "società emittente di carte di credito/debito", mentre il cliente era stato invitato ad inserire la password del servizio di internet banking della banca (richiama plurimi Precedenti ABF).
Rileva di aver pubblicato sul proprio sito web e di inviare periodicamente alla propria clientela comunicazioni finalizzate ad avvertirla delle frodi informatiche, fornendo specifiche informazioni sulle varie tipologie di truffa perpetrate e sulle modalità con cui difendersi. Precisa che tale circostanza è confermata dalla e-mail del 09/05/2023 prodotta in atti da controparte, e che la variazione "dell'Outsourcer informativo" non riguarda presunte esigenze di maggiore sicurezza della piattaforma di internet banking, ma è connessa ad una operazione di natura strategica.
Pertanto, l'intermediario chiede:
- in via principale, di "rigettare integralmente la domanda di parte ricorrente in quanto infondata";
- in via subordinata, "nella denegata e non creduta ipotesi che siano ravvisati profili di responsabilità attribuibile alla Banca, considerare il peso dei comportamenti colposi assunti dal ricorrente e determinanti per il verificarsi della frode".
In sede di repliche, il ricorrente ribadisce di aver inserito in maniera errata le proprie credenziali di accesso sul sito civetta, e che tale circostanza era stata regolarmente comunicata in sede di denuncia, ma non era stata verbalizzata dagli agenti "perché per loro non rilevante ai fini della denuncia stessa".
Sostiene di non aver tenuto alcun comportamento fraudolento o gravemente colposo, posto che la truffa subita era stata posta in essere mediante diverse tecniche fraudolente.
Soggiunge che nel messaggio ricevuto e sul sito cui rinviava il relativo link non erano presenti errori grammaticali che avrebbero potuto far riconoscere la truffa in atto, e che anche la successiva chiamata ricevuta era stata effettuata da un'utenza riconducibile a quella di una delle filiali della banca (cita Collegio di Roma, decisione n. 5481/2021, Collegio di Milano, decisione n. 22556/2019, Collegio di Roma, decisione n. 511/2015, Collegio di Coordinamento, decisione n. 3498/2012).

Fa presente che la banca, oltre a non aver provato la sussistenza di un sistema di autenticazione forte che potesse prevenire le truffe on line, aveva deciso di cambiare nel mese di maggio 2023, quindi poco dopo la truffa subita, il proprio sistema di sicurezza, rendendolo più forte e preavvertendo la propria clientela di "diffidare da contatti telefonici di chi richiedeva credenziali o codici on line".
Conclude insistendo per l'accoglimento delle domande formulate nel ricorso.
In sede di controrepliche, l'intermediario produce in atti un ulteriore log ricevuto dal suo "outsourcer informativo pro tempore", il quale integra i log già allegati in sede di controdeduzioni.
Conclude insistendo per l'accoglimento delle conclusioni formulate in sede di controdeduzioni.

DIRITTO

Il ricorrente invoca il rimborso dell'importo di euro 10.000,00 corrispondente a due operazioni di bonifico eseguite da terzi malfattori a valere sul proprio conto corrente.
La materia oggetto di ricorso trova specifica regolamentazione nelle 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 recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno (PSD2). Le operazioni controverse risultano poste in essere anche sotto la vigenza del Regolamento Delegato (UE) n. 2018/389 della Commissione che definisce i requisiti per l'autenticazione forte previsti dalla citata direttiva. La disciplina richiamata prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore, ai sensi del combinato disposto degli artt. 7 e 12, comma 4, d.lgs. 27 gennaio 2010 n. 11, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011. In particolare, ai sensi dell'art. 10 del d.lgs. n. 11/2010, cit., "qualora l'utilizzatore dei 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 dei 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". Ai sensi del comma 2, "quando l'utilizzatore di servizi di pagamento neghi di avere 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'art. 7" del medesimo decreto legislativo. Da ultimo, il d.lgs. n. 218/17 ha introdotto nell'art. 10, co. 2, d.lgs. n. 11/2010 la precisazione secondo cui "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".
Al riguardo, il Collegio di Coordinamento ha, in più occasioni, precisato che la disciplina in esame istituisce "un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle

procedure esecutive o ad altri inconvenienti del sistema […]. Neanche l'apparentemente corretta autenticazione dell'operazione è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art.7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 50 euro). La ratio di tale scelta legislativa è fin troppo notoriamente quella […] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (Coll. Coord., decisione n. 3947 del 24.6.2014. In senso conforme: Coll. Coord. Decisione n. 3498/2012; Coll. Coord., decisione n. 991 del 21.2.2014. Da ultimo, cfr. Coll. Coord., decisione n. 22745/19, per quanto riguarda, in particolare, l'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, ex art. 10, co. 2, d. lgs. n. 11/2010).

L'orientamento di questo Arbitro ha trovato riscontro nella sentenza della Corte di Cassazione, 3.2.3017, n. 2950, la quale ha statuito che la disciplina speciale, in tema di strumenti di pagamento, ha esplicitato il principio generale, in tema di onere probatorio a carico del debitore professionale, nelle azioni di risoluzione contrattuale, risarcimento del danno o adempimento, "in quanto si è ritenuto che non può essere omessa la verifica dell'adozione da parte dell'istituto bancario delle misure idonee a garantire la sicurezza del servizio […]; infatti la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi come parametro la figura dell'accorto banchiere" (Cass., n. 2950/17, sulla scia di Cass., 12.6.2007, n. 13777. In senso conforme, cfr. Cass.,12.4.2018, n. 9158; Cass., 26 novembre 2020, n. 26916, anche per l'importante statuizione, secondo cui "al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento -prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente - la possibilità di un'utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo").

Tanto premesso in termini generali, rileva il Collegio che, nella specie, oggetto di disconoscimento sono due operazioni di bonifico online di € 5.300,00 ed € 4.700,00 compiute da sconosciuti malfattori alle ore 15:00 e 15:01 del 22/03/2023.

Quanto alle modalità della truffa, il ricorrente, in sede di denuncia ricostruiva i fatti oggetto di controversia affermando che in data 22/03/2023 alle ore 14:16 riceveva sulla sua utenza un S.m.s. con cui gli veniva comunicato che "era stato limitato il [suo] conto/carta per mancanza di verifica sicurezza" e che doveva seguire il link ivi riportato; aveva seguito tale link, visualizzando una pagina web in cui gli veniva richiesto di inserire "utente e password"; aveva effettuato tale operazione e veniva contattato da un operatore tramite l'utenza fissa n. 080****611, con cui gli veniva richiesto di disinstallare l'App; alle successive ore 14:27 era stato contattato dalla filiale della banca per chiedergli se avesse effettuato due di € 5.300,00 ed € 4.700,00 e che si era recato "subito" in filiale per bloccare i servizi di home banking.

Per contro, l'intermediario resistente afferma che le transazioni sono state eseguite con sistema di autenticazione forte.
All'uopo, l'intermediario descrive in termini generali le modalità di accesso, affermando che per l'accesso tramite App è necessario l'uso congiunto di: smartphone con App token software installata (elemento di possesso); credenziali userid-password e codice PIN (elemento di conoscenza). Ricostruisce, del pari, la modalità di enrollment del Token software su un nuovo device, affermando che è richiesto l'uso congiunto di: credenziali userid-password (elemento di conoscenza); codice OTP, inviato esclusivamente all'indirizzo e-mail dell'utente (elemento di possesso).
Quanto al caso di specie, l'intermediario sostiene che in data 22/03/2023: i truffatori stavano procedendo, grazie ai codici comunicati precedentemente dal ricorrente durante una chiamata ricevuta alle ore 14:30 (codice utente e password + OTP), ad attivare l'App con il Token Software sul proprio smartphone, impostandone il relativo PIN; i truffatori, una volta completata l'installazione del Token, avevano effettuato l'accesso tramite App alle ore 14:51 ai servizi di internet banking e che alle ore 14:52 avevano modificato l'indirizzo e-mail collegato a tale servizio.
Tanto premesso, l'intermediario allega i relativi log in sede di controdeduzioni, corredati dalle legende esplicative (file log "NXG" e file log "Hub").
Il Collegio rileva che, dall'esame dei predetti log, manca qualsiasi riferimento all'operazione di enrollment del Token Software sul device dei truffatori, verificatasi verosimilmente nell'intervallo temporale 14:30 – 14:50. Da ultimo, in sede di controrepliche, la banca ha prodotto un ulteriore log ricevuto dal suo "outsourcer informativo pro tempore", il quale integra i log già allegati in sede di controdeduzioni e dal cui esame si dovrebbero evincere: i vari collegamenti effettuati dalle ore "14:37 in poi", mediante inserimento per ciascuno di essi del codice userid e password, nonché della seconda credenziale "OTP PIN"; le fasi di enrollment del nuovo device, ovvero la fase di attivazione del nuovo Token Software mediante l'invio dell'e-mail contenente il codice OTP e conseguente scelta del PIN, utilizzando la seconda credenziale "OTP PIN" in fase di enrollment; file log "IHB".
Con riferimento invece alla ricezione dell'OTP sul device del cliente, utile per l'installazione del Mobile Token, l'intermediario ha prodotto uno specifico log. Si precisa che, dall'esame di quest'ultima evidenza, si evince che l'oggetto del predetto messaggio è "Attivazione token software", anche se non è riportato il relativo contenuto.
Ora, sebbene in termini generali, il sistema approntato dall'intermediario per l'accesso alla piattaforma di home banking e l'autorizzazione delle operazioni di pagamento on line appaia conforme ai requisiti di "Strong Customer Authentication", il Collegio non può non rilevare che la documentazione prodotta e, segnatamente, gli articolati tracciati informatici forniti, non consentono l'individuazione chiara, certa e inequivoca dei presidi di sicurezza adottati in concreto nelle varie fasi del processo di installazione e di configurazione dispositiva dell'App descritto dalla resistente (cfr., nei confronti dello stesso intermediario, Collegio di Bari, n. 11082/2023; nonché Collegio di Bari, n.. 9919/2023, 9570/2023, 9425/2022). A tale ultimo riguardo, si osserva che l'allegazione della resistente, secondo cui il ricorrente avrebbe comunicato ai truffatori i codici ricevuti (codice utente e password nonché OTP) per procedere ad attivare l'App Token sul dispositivo dei truffatori, sembra basarsi su una valutazione di mera probabilità e verosimiglianza, evidentemente svolta dalla banca, non sorretta da evidenze concludenti, gravi, precise e concordanti (cfr., per un caso analogo, Collegio di Bari, n. 11082/2023).
Difettando la dimostrazione chiara ed oggettiva della procedura di autenticazione e autorizzazione che la banca sostiene avere adottato 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".
Tanto premesso, questo Collegio – ribadendo quanto già affermato in alcuni precedenti relativi a fattispecie analoghe (cfr. Collegio di Bari, nn. 9919/2023, 9570/2023, 9425/2022) – ritiene che l'intermediario non abbia assolto l'onere probatorio.
Per le suesposte ragioni, il ricorso è meritevole di accoglimento.

P.Q.M.

Il Collegio, in accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 10.000,00, 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