COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(BA) SEMERARO	Membro designato dalla Banca d'Italia
(BA) STEFANELLI	Membro di designazione rappresentativa degli intermediari
(BA) POSITANO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - PIERFRANCESCO BARTOLOMUCCI

Seduta del 07/04/2022

FATTO

Il ricorrente, titolare di un conto corrente abilitato al servizio di *home banking* fornito da una società terza, insoddisfatto dell'interlocuzione intrattenuta con l'intermediario nella fase del reclamo, adiva questo Arbitro con il ministero di un legale di fiducia, affermando di aver ricevuto, in data 30 settembre 2021, un SMS da un mittente apparentemente riconducibile all'intermediario, recante la richiesta di cliccare sul link ivi contenuto al fine di evitare la sospensione dell'utenza a causa di un mancato aggiornamento; veniva così reindirizzato ad una pagina web identica a quella della resistente, ove inseriva le proprie credenziali di accesso.
Nei minuti immediatamente successivi, perveniva una chiamata da un numero di cellulare durante la quale l'interlocutore, qualificatosi come un operatore della banca, lo invitava a completare l'operazione di recupero dei dati di accesso al fine di scongiurare il blocco della piattaforma bancaria; in tale occasione comunicava il codice di attivazione dell'APP e il "*codice ***y dell'app*", entrambi pervenuti tramite SMS alle ore 20:17.
Poco tempo dopo, recatosi presso l'intermediario, si avvedeva che, a distanza di ben cinque giorni dal suddetto contatto telefonico, erano stati effettuati quattro bonifici di euro 2.000,00, euro 1.985,00, euro 1.991,00 ed euro 1.994,00, rispettivamente il 5, il 6, il 7 e l'8 ottobre 2021.

Riteneva che l'intermediario non avesse assicurato un livello di protezione idoneo a scongiurare e/o minimizzare i rischi derivanti dalle truffe online. Nel caso di specie, infatti, i frodatori avevano creato un'ulteriore utenza che aveva consentito di disporre in maniera autonoma i bonifici, senza che fosse necessario l'invio di un codice OTP sull'utenza telefonica certificata del cliente; lamentava dunque l'assenza di un sistema di autenticazione forte, nonché la mancanza del "collegamento dell'operazione per uno specifico importo al beneficiario specifico"; contestava la condotta della resistente per non aver comunicato l'inserimento delle disposizioni di bonifico contestate, diversamente da quanto accaduto in precedenti occasioni e per non aver fornito specifiche raccomandazioni in merito agli attacchi informatici da parte dei truffatori.
Qualificava la frode perpetrata ai propri danni come "SMS spoofing" che, lungi dall'essere equiparata all'ordinario *phishing*, sarebbe stata resa possibile anche da una "colpevole vulnerabilità organizzativa del sistema di comunicazione adottato dall'intermediario".
Chiedeva, dunque, il rimborso della somma complessiva di euro 7.970,00, fraudolentemente sottratta, oltre alle spese legali.
Costituitosi ritualmente, l'intermediario convenuto rappresentava che il "doppio controllo" per l'autenticazione e il monitoraggio delle transazioni della clientela venisse effettuato da una società terza, fornitrice del servizio di *outsourcing* informatico.
Eccepiva che, nel caso di specie, le operazioni contestate fossero state correttamente registrate e contabilizzate e disposte mediante un sistema di autenticazione forte.
Evidenziava che lo stesso ricorrente avesse dichiarato di aver cliccato sul link contenuto nel messaggio truffaldino e di aver fornito le informazioni richieste al sedicente operatore, comunicando i dati riservati e sensibili; al riguardo osservava come il contratto relativo al sistema di *virtual banking* sottoscritto dal cliente prevedesse, all'art. 5, la responsabilità dell'utente per la custodia e il corretto utilizzo delle credenziali e per qualsiasi conseguenza dannosa derivante dall'utilizzo illegittimo e/o dallo smarrimento e dalla sottrazione delle medesime.
Chiedeva pertanto il rigetto del ricorso.
Alle controdeduzioni dell'intermediario replicava il ricorrente, che ribadiva la mancata predisposizione di un sistema adeguato a tutelare i dati anagrafici e telefonici degli utenti, essendo pacifico che il messaggio truffaldino fosse pervenuto nella medesima chat usata dalla banca per l'invio delle comunicazioni genuine. Riteneva che la resistente non avesse dimostrato il meccanismo di autenticazione con cui erano stati disposti i bonifici in questione, per la cui autorizzazione era stato richiesto l'inserimento dei codici OTP mai ricevuti sul proprio telefono; riteneva che ciò fosse stato reso possibile dall'abbinamento dell'utenza ad un altro numero di cellulare e/o applicativo non autorizzato e non approvato dall'intermediario. Rappresentava, infine, di non aver ricevuto alcuna notifica relativa alle operazioni contestate e, pertanto, di non essere stato messo nelle condizioni di revocare o, quantomeno, di prevenire i bonifici fraudolenti eseguiti successivamente al primo.
Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale affermava che, contrariamente a quanto asserito da controparte, il messaggio pervenuto sul suo cellulare fosse stato inviato da un falso operatore, che aveva simulato il servizio di *virtual banking* creando un apposito link fraudolento, come avviene in tutti i tentativi di *phishing*.
Precisava che il truffatore, dopo aver ottenuto i dati necessari direttamente dal ricorrente tramite la tecnica del *vishing*, avesse modificato il numero di telefono al quale inviare "i messaggi da autorizzare tramite OTP e veicolati tramite notifica nell'app"; per tale motivo, il cliente non aveva ricevuto i messaggi autorizzativi né nell'app né sulla sua utenza telefonica.
Affermava infine che, contrariamente a quanto asserito da controparte, non si fosse verificata alcuna violazione, da parte della banca, nella custodia dei dati sensibili, atteso che per ottenere tali informazioni il frodatore aveva dovuto ricorrere al *phishing* e al *vishing*.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di una molteplicità di operazioni *online*, successivamente disconosciute.
La materia, come noto, regolata dal d. lgs. n. 11/2010 come modificato dal d. lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/Ue (c.d. PSD2- *Payment Services Directive 2*).
Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante – introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori, nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.
Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa *de qua* prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento.
Orbene, risulta *per tabulas* che le operazioni contestate consistano in quattro bonifici di euro 2.000,00, euro 1.985,00, euro 1.991,00 ed euro 1.994,00 (comprensivi della relativa commissione), eseguiti rispettivamente il 5, il 6, il 7 e l'8 ottobre 2021.
Secondo quanto riferito dallo stesso ricorrente, la truffa avrebbe preso le mosse dal c.d. 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.
Tale circostanza sembra confermata dallo *screenshot* della schermata del telefono del ricorrente, da cui si evince la ricezione del messaggio truffaldino in data 30 settembre 2021 alle ore 11:14, nella medesima chat in cui sono pervenuti gli SMS genuini dell'intermediario; tra questi ultimi, vi sono anche i messaggi delle ore 20:17 contenenti il codice di attivazione dell'APP e il "codice ***y dell'app".
Ciò nonostante, assume rilievo assorbente la circostanza per cui l'intermediario si sia limitato a produrre il riscontro fornito dalla società responsabile del servizio di *virtual banking* alla richiesta di informazioni sulle modalità autorizzative dei bonifici in questione, nel quale vengono indicati alcuni estratti dei log registrati nei sistemi da cui si evincerebbe l'invio, veicolato mediante notifica su APP, e l'inserimento dei codici OTP, con conseguente inoltro dei bonifici.
Parte resistente, tuttavia, non ha illustrato il meccanismo di funzionamento dell'app, né ha versato in atti documentazione sul punto; secondo il consolidato orientamento di questo Arbitro, l'assenza di allegazioni relative all'installazione e alla configurazione dispositiva dell'App non consente di ritenere raggiunta la prova dell'autenticazione forte, in conformità

all' "*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*" del 21.06.2019, ove sono presi in considerazione esempi di soluzioni tecniche e chiarito quali elementi possono considerarsi *compliant* in ciascuna delle tre categorie (inerenza, possesso e conoscenza), precisando che i dati identificativi della carta e il codice di sicurezza stampati sulla stessa non possono costituire un elemento affidabile di cui l'utilizzatore abbia il possesso o la conoscenza (cfr. *ex multis* Coll. Bari, dec. n. 26084/2021).
Dalle deduzioni di entrambe le parti sembra che fosse attivo un servizio di alert; tuttavia, a seguito dell'installazione dell'app e della variazione dell'utenza telefonica, le notifiche di alert sono state verosimilmente ricevute dal frodatore.
Alla luce del complessivo quadro probatorio e delle dichiarazioni delle parti, tenuto conto della mancata prova acquisita in relazione all'adozione di un sistema di autenticazione forte, deve essere riconosciuto il diritto del ricorrente ad ottenere il rimborso del controvalore delle operazioni fraudolente, per il relativo importo di euro 7.970,00.
Deve invece essere respinta la domanda di ristoro delle spese di assistenza difensiva, in assenza della preventiva specifica richiesta nel reclamo e di idonea documentazione al riguardo.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 7.970,00.
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