COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) SIVIGLIA	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCA VESSIA

Seduta del 22/04/2024

FATTO

Il ricorrente afferma che in data 28/06/2023 è stato vittima di una "truffa informatica". In particolare, asserisce di avere ricevuto, da un intermediario diverso dal resistente, diversi Sms con cui veniva informato che la propria carta di credito "era stata limitata per mancata verifica della sicurezza web", cui seguiva un invito a cliccare su un link per la riattivazione. Precisa che i predetti Sms confluivano nella cronologia dei messaggi con cui tale intermediario terzo lo avvertiva abitualmente di tutte le operazioni bancarie effettuate sul proprio conto e/o carta.
Osserva che nella stessa giornata, dopo la ricezione degli Sms, alle ore 13:28 riceveva una chiamata proveniente da un'utenza fissa riconducibile ad una filiale della banca resistente. Precisa che durante tale chiamata l'interlocutore si qualificava come operatore di quest'ultima e lo informava dell'esistenza di problematiche legate ai sistemi informatici, invitandolo a non aprire l'home banking per due giorni.
Soggiunge che il giorno successivo (29/06/2023), alle ore 9:00 circa, contattava la banca per chiedere di verificare le movimentazioni bancarie del proprio conto corrente, apprendendo dell'esistenza di una operazione in corso relativa ad un bonifico di € 600,00, che non aveva autorizzato e di cui non aveva ricevuto alcun avviso o richiesta di autorizzazione tramite App.
Precisa che alle successive ore 11:00 circa, si recava presso la sede della banca per accertarsi che l'operazione fosse stata effettivamente bloccata, e che dopo aver sottoscritto un modulo per richiedere la revoca del bonifico, il personale gli comunicava che l'operazione

in questione difficilmente poteva essere bloccata, adducendo motivazioni "tutt'altro che circostanziate".
Rileva che le modalità con cui la truffa si è svolta evidenziano le carenze organizzative della banca, per l'assenza di un adeguato livello di sicurezza dei sistemi informatici (il frodatore era a conoscenza dei suoi dati personali, come il numero di conto corrente e gli estremi della carta di credito) e per l'intempestivo riscontro alle "innumerevoli" telefonate da lui effettate nel tentativo di mettersi in contatto con la banca.
Ritiene che dalle citate carenze organizzative e dalla mancata revoca del bonifico bancario, richiesta a poche ore dall'operazione illecita, discenda la responsabilità della banca.
Il ricorrente chiede, pertanto, il rimborso della somma di € 600,00.
L'Intermediario, costituitosi, precisa preliminarmente che l'operazione oggetto di ricorso è stata eseguita utilizzando il nuovo sistema di internet banking adottato a seguito del cambio di outsourcer informatico avvenuto in data 08/05/2023.
Illustra quindi l'operatività di tale sistema, chiarendo che per eseguire l'accesso tramite APP occorre l'utilizzo di uno smartphone con l'APP di token software installata (elemento di possesso) e l'inserimento dello UserId, della password e del codice *Pin (elementi di conoscenza), e che per disporre un bonifico tramite APP, dopo l'accesso, occorre l'utilizzo dello smartphone con l'APP di token software installata (elemento di possesso) e l'inserimento del codice *Pin (elemento di conoscenza). Soggiunge che per eseguire l'enrollment del token software su un nuovo device occorre l'inserimento dello UserId e della password (elementi di conoscenza), nonché l'inserimento del codice OTP inviato via Sms al numero di telefono dell'utente, precisando che in caso di attivazione con contestuale disattivazione del vecchio token software viene prima inviato un ulteriore codice OTP di sicurezza al numero telefonico dell'utente.
Rappresenta che a seguito dell'accesso all'APP e della disposizione di bonifico viene inviato un messaggio di alert via email.
Rileva che un sistema di autenticazione basato sull'uso di due fattori è notoriamente ritenuto dai Collegi ABF e dall'EBA conforme ai requisiti previsti dalla direttiva PSD2 per l'autenticazione forte del cliente (SCA) basata sull'uso di almeno due elementi di autenticazione tra loro indipendenti.
Tanto premesso, ripercorre le vicende occorse evidenziando che, come risulta dal contenuto del reclamo e della denuncia, il ricorrente, già in data 27/06/2023, alle ore 15:13, riceveva, da un mittente che si spacciava per una società emittente le carte di credito/debito, un Sms che lo invitava a riattivare la carta o il conto, seguendo un link che non era riconducibile in alcun modo alla banca resistente; inoltre, nella stessa giornata, alle ore 17:23 il ricorrente riceveva un secondo Sms, che preannunciava una telefonata da un operatore.
Ritiene che il secondo Sms, relativo all'appuntamento telefonico, viene indirizzato solo a coloro che seguono il link riportato nel primo messaggio e, pertanto, il truffatore, al momento della telefonata era già in possesso dei dati inseriti dal cliente.
Chiarisce che tali messaggi sono tentativi di frode attuati con la tecnica dello "smishing", utilizzato congiuntamente con la tecnica dello Sms Spoofing e che la clientela è periodicamente oggetto di campagne informative sul tema delle frodi informatiche, con particolare riguardo al fatto che la banca non chiede codici di accesso tramite Sms o chiamate; quanto alla telefonata, richiama la truffa del falso numero chiamante nota come "call ID spoofing".
Fa quindi presente che, durante la conversazione telefonica del giorno 27, circostanza confermata dal ricorrente in denuncia, alle ore 17:45 e 17:46 sono stati inviati al numero telefonico del ricorrente i due Sms contenenti i codici OTP necessari per disattivare il vecchio token software e attivarne uno nuovo. Precisa che, in assenza di tali codici, non sarebbe stato possibile procedere all'attivazione di un nuovo Token Software.

Soggiunge che, una volta scaricata ed installata l'App, i truffatori hanno potuto effettuare l'accesso al servizio di Internet Banking del ricorrente, alle ore 17:44:59, effettuando alle ore 17:46:32 l'attivazione del Token Software sul loro device mediante il codice di attivazione inviato via Sms al ricorrente, in seguito al reset del vecchio Token alle ore 17:45:19.
Rileva che il 28/06/2023, previa telefonata delle ore 13:18, in cui invitavano il ricorrente a non aprire la propria App per "due giorni", i truffatori, in possesso delle credenziali di accesso al servizio e dell'App con Token Software regolarmente installato e nuovo codice *Pin impostato, hanno potuto disporre alle ore 15:57:24 il bonifico di € 600,00. Rimarca che a seguito della disposizione di bonifico, è stato inviato il relativo alert alla mail del ricorrente.
Precisa che quindi solo nella giornata del 29/06/2023 il ricorrente si è reso conto della truffa e ha chiesto il blocco del bonifico.
Afferma quindi che l'operazione disconosciuta è stata correttamente autenticata, registrata e contabilizzata con un sistema a doppio fattore senza alcuna anomalia e soggiunge che i propri sistemi non sono stati violati e non hanno presentato anomalie.
Ribadisce che la truffa è stata portata a termine solo grazie alla totale, seppur inconsapevole, collaborazione del cliente che ha violato con colpa grave gli obblighi di cui all'art. 7, comma 2, del d.lgs n. 11/2010 (cita plurimi precedenti ABF in materia di phishing e spoofing).
Il ricorrente. In sede di repliche, eccepisce l'insidiosità della truffa subita, dimostrata dall'assenza di anomalie nei messaggi inviati dal "phisher", dall'apparente provenienza degli Sms esca dalla società emittente le carte di credito e dalle telefonate ricevute da una utenza riconducibile alla banca resistente. Pertanto, emerge con chiarezza che le modalità messe in atto dai truffatori potevano essere tutt'altro che "facilmente riconoscibili".
Ritiene, inoltre, che la banca non abbia provato la sua colpa grave.
L'intermediario, in sede di controrepliche, evidenzia in relazione alla colpa grave la macroscopica incongruenza, di cui il ricorrente non si sarebbe accorto, di ricevere Sms da un intermediario diverso rispetto a quello da cui provenivano le telefonate.
Sottolinea le contraddizioni del ricorrente tra quanto dichiarato in denuncia e quanto riportato in ricorso, ove omette di riferire della telefonata ricevuta il giorno 27/6/2023 e omette di allegare gli Sms ricevuti dalla banca, nella predetta giornata, contenenti i codici OTP per disattivare il vecchio Token e attivare quello nuovo.
Insiste per il rigetto della domanda, e in subordine, chiede di considerare il peso dei comportamenti colposi assunti dal ricorrente, determinanti per il verificarsi della frode.

DIRITTO

La domanda sottoposta al Collegio riguarda la richiesta di rimborso di € 600,00 per un bonifico disconosciuto dal ricorrente eseguito online ma non autorizzato, dovuto ad una truffa perpetrata ai suoi danni mediante la tecnica congiunta dello Sms Spoofing e smishing, nonché di chiamata apparentemente proveniente da un numero dell'intermediario, qualificabile come call ID spoofing.
Il ricorrente ha dichiarato, infatti, di aver ricevuto nella mattina del 28/06/2023 diversi SMS da un'utenza riconducibile a quella dell'intermediario resistente (stessa chat dell'intermediario) con cui veniva informato che la propria carta di credito "era stata limitata per mancata verifica della sicurezza web", e seguiva un invito a cliccare su un link per la riattivazione. Il ricorrente, pur non avendo dichiarato e ammesso di aver seguito le istruzioni ricevute e di essersi collegato al link ricevuto, circostanza che invece è stata dichiarata e provata dall'intermediario, ha sostenuto di aver successivamente ricevuto alle ore 13:28 una chiamata proveniente da un'utenza fissa riconducibile ad una filiale della banca resistente, durante la quale l'interlocutore, qualificatosi come operatore di quest'ultima, lo informava

dell'esistenza di problematiche legate ai sistemi informatici, invitandolo a non aprire l'home banking per due giorni. Soggiunge che il giorno successivo (29/06/2023), alle ore 9:00 circa, contattava la banca per chiedere di verificare le movimentazioni bancarie del proprio conto corrente, apprendendo dell'esistenza di una operazione in corso relativa ad un bonifico di € 600,00, che non aveva autorizzato e di cui non aveva ricevuto alcun avviso o richiesta di autorizzazione tramite App.

L'intermediario non concorda sulla ricostruzione dei fatti, affermando che, dal contenuto del reclamo e della denuncia, risulta che il ricorrente già in data 27/06/2023, alle ore 15:13, riceveva, da un mittente che si spacciava per una società emittente le carte di credito/debito, un Sms che lo invitava a riattivare la carta o il conto, seguendo un link che non era riconducibile in alcun modo alla banca resistente; inoltre, nella stessa giornata, alle ore 17:23 il ricorrente riceveva un secondo Sms, che preannunciava una telefonata da un operatore. Ritiene che oltre alle contraddizioni del ricorrente tra quanto dichiarato in denuncia e quanto riportato in ricorso, il ricorrente abbia anche omesso di allegare gli Sms ricevuti dalla banca.

Il Collegio rileva preliminarmente che l'operazione contestata è stata eseguita 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.

Altresì il Collegio constata che il ricorrente in sede di denuncia, presentata alle competenti autorità in data 29/06/2023, alle ore 15:10, ricostruiva i fatti oggetto di controversia in maniera parzialmente diversa rispetto a quanto riportato nel ricorso, ed in specie omettendo di aver ricevuto gli Sms dai truffatori già in data 27/06/2023, contenente l'informazione della limitazione della sua carta di credito e l'invito a seguire un link per la riattivazione. Asserisce di non avere seguito il predetto link, ma di essere stato contattato telefonicamente dall'utenza fissa riconducibile alla banca resistente, sia il giorno 27/06/2023 (alle ore 17:25), per essere informato dell'esistenza di problematiche legate ai sistemi informatici, sia il giorno 28/06/2023 (ore 13:18), ed essere invitato a non aprire l'home banking per due giorni. Precisa che durante entrambe le conversazioni non sono stati chiesti "codici e credenziali". Conferma che la mattina del 29/06/2023 contattava telefonicamente la banca, venendo a conoscenza sul suo conto corrente era stato addebitato in bonifico di € 600,00.

Nel merito il Collegio osserva che, ai fini dell'accertamento dell'autenticazione forte (SCA) alle operazioni di pagamento elettronico, qual è il bonifico bancario di € 600,00 oggetto di disconoscimento, disposto da home banking il 28/03/2023, alle ore 13:57:24 (GMT), ai sensi degli artt. 10-*bis* e 12, D.lgs. 27 gennaio 2010, n. 11 e ss.mm.ii., risulta determinante l'insieme delle prove prodotte in atti dall'intermediario. Innanzitutto, l'intermediario ha dimostrato che durante la conversazione telefonica del giorno 27, circostanza confermata dal ricorrente in denuncia, alle ore 17:45 e 17:46 sono stati inviati al numero telefonico del ricorrente i due Sms contenenti i codici OTP necessari per disattivare il vecchio token software e attivarne uno nuovo, producendone evidenza in atti. L'intermediario sostiene e dimostra mediante i log informatici che, in assenza di tali codici, non sarebbe stato possibile procedere all'attivazione di un nuovo Token Software e alla contestuale disattivazione del *device* del ricorrente. Difatti, una volta scaricata ed installata l'App, l'intermediario ha fornito la prova che i truffatori hanno potuto effettuare l'accesso al servizio di Internet Banking del ricorrente, alle ore 17:44:59, effettuando alle ore 17:46:32 l'attivazione del Token Software sul loro device mediante il codice di attivazione inviato via Sms al ricorrente, in seguito al reset del vecchio Token alle ore 17:45:19, sempre esibendo i log informatici.

Anche in relazione all'operazione di bonifico eseguita il giorno successivo in data 28/06/2023, previa telefonata delle ore 13:18, in cui invitavano il ricorrente a non aprire la propria App per "due giorni", l'intermediario ha fornito prova mediante log informatici del fatto

che i truffatori, in possesso delle credenziali di accesso al servizio e dell'App con Token Software regolarmente installato e nuovo codice *Pin impostato, hanno potuto disporre alle ore 15:57:24 il bonifico di € 600,00. Tanto si evince dalla dicitura "/securesca/otp-transaction" dei log informatici.
Pertanto, alla luce di tali elementi forniti dall'intermediario il Collegio ritiene di poter valutare i log informatici prodotti in atti come elementi complessivamente idonei a provare la SCA, in continuità con una decisione recente assunta in un caso simile nei confronti dello stesso intermediario (Collegio di Bari, decisione n. 1998/2024).
Una volta raggiunta la conclusione sulla prova dell'autenticazione forte, il Collegio passa a valutare i profili di dolo o colpa grave dell'utente. A tale riguardo rileva la circostanza che gli Sms ricevuti dal ricorrente provengano dalla chat di un intermediario finanziario sebbene non si tratti dell'intermediario resistente, come dichiarato dal ricorrente, bensì di altro intermediario, il quale si occupa di emettere e gestire carte di debito/credito, come risulta dagli *screenshot* esibiti in atti. Rileva, altresì, la circostanza che la telefonata ricevuta dal ricorrente sembrava provenire da un numero che coincide con quello di una delle filiali dell'intermediario, in quanto i criminali avevano posto in essere una truffa telefonica con falso numero chiamante, nota come "*call ID spoofing*".
Alla luce del quadro complessivo delle circostanze, il Collegio ritiene di trovarsi in una fattispecie di truffa piuttosto insidiosa in cui se, per un verso, è innegabile che il ricorrente versi in colpa grave, essendosi fidato di chi l'ha contattata prima via sms e poi telefonicamente e comunicando i propri codici di accesso all'home banking, per altro verso, emerge un difetto nell'organizzazione del servizio offerto dall'intermediario, atteso che il numero dal quale è partita la telefonata dei truffatori era comunque riconducibile all'intermediario. Non rilevante, invece, è la mancata ricezione dell'sms alert da parte dell'utente, che in ogni caso a fronte di una sola operazione fraudolenta risulta essere inidoneo ad incidere sull'iter causale della truffa. Pertanto, il Collegio reputa che la condotta negligente dell'intermediario abbia avuto un peso eziologicamente rilevante nella commissione dell'illecito rispetto a quello del ricorrente e che, pertanto, la perdita vada distribuita tra le parti nella misura rispettivamente del 60% per l'intermediario e del 40% per il cliente.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 360,00.
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