COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) BARENGHI	Membro designato dalla Banca d'Italia
(TO) FERRANTE	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) D'ANGELO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MAURILIO D'ANGELO

Seduta del 24/01/2024

FATTO

Con ricorso depositato il 20.09.2023, la parte ricorrente ha lamentato di essere stato vittima di una frode informatica. Nello specifico, ha rilevato di aver ricevuto, in data 8.07.2023 alle ore 13:46, un sms inseritosi nella chat dei messaggi provenienti dall'intermediario, che le riferiva di un presunto accesso da un nuovo dispositivo e la invitava, nel caso disconoscesse tale accesso, a cliccare su un link. Eseguita la suddetta operazione, veniva reindirizzata ad una pagina ove le veniva chiesto di reimpostare la password ed al cui interno erano previsti alcuni campi da compilare (i) nome; ii) cognome; iii) numero della carta; iv) soldi sullo strumento di pagamento).
Non appena inseriti i dati, riceveva una chiamata dal numero 320xxxxx67 da parte di una persona che, qualificatasi come operatore dell'intermediario, lo invitava a recarsi ad uno sportello automatico per effettuare una operazione. Avendo compreso che si trattava di una truffa, si rifiutava di eseguire quanto richiesto e tentava di contattare l'intermediario, senza successo. Tuttavia, nonostante l'avvenuto blocco della carta, ignoti sono riusciti ad effettuare due pagamenti di € 790,00 e € 100,00 (quest'ultimo rimborsato).
Nel costituirsi per il tramite di apposite controdeduzioni, l'intermediario ha rappresentato che
verosimilmente la truffa ai danni del Ricorrente si è verificata secondo una delle ormai note pratiche adottate in occasione di "phishing/vishing", in quanto il Ricorrente ha dato seguito

sia ad informazioni ricevute tramite SMS che a quelle fornite telefonicamente da un presunto operatore, permettendo così di portare a termine un'operazione di pagamento. Nel caso di specie l'operazione di pagamento è stata autenticata mediante i fattori di sicurezza stabiliti dalla Strong Customer Authentication (SCA) tramite validazione della notifica push ricevuta in app. Peraltro, il comportamento del cliente integra i connotati della colpa grave in quanto questi ha: i) cliccato su un link ricevuto tramite SMS; ii) assecondato le richieste ricevute da un soggetto sconosciuto che l'ha contattato da un riferimento telefonico non riconducibile alla banca; iii) presumibilmente fornito tutti i codici di sicurezza giunti tramite SMS, così permettendo all'interlocutore di accedere al proprio account in "strong log in" associando un nuovo dispositivo. Ha, poi, rilevato che la parte ricorrente non ha prodotto il messaggio spoofed ma, come confermato dalla visione dello stesso nella fase antecedente alla proposizione del ricorso, lo stesso presentava chiari ed evidenti errori grammaticali, un utilizzo non corretto nelle lettere maiuscole, nonché un inconferente utilizzo dei tempi verbali nonché della punteggiatura. Inoltre, il link in esso contenuto, non poteva considerarsi affidabile poiché non è neppure lontanamente riconducibile al dominio della parte resistente. Sul punto, l'orientamento dei collegi dell'Arbitro Bancario Finanziario è quello di ritenere che nelle ipotesi di spoofing si ravvisi la colpa grave della Ricorrente se si rinvengano indici di inattendibilità (quali ad esempio errori grammaticali o sintattici) o di anomalia (quali ad esempio l'invito a selezionare un link in nessun modo riferibile all'intermediario). L'intermediario, consapevole che le truffe perpetrate tramite furto di strumenti di pagamento sono purtroppo in costante aumento, ha avviato una campagna di rafforzamento del proprio piano di comunicazione all'intera clientela con l'intento di sollecitare l'adozione di azioni tempestive di autotutela per evitare queste spiacevoli situazioni. Non fosse sufficiente, al ricorrente sono state inviate anche comunicazioni via push e via sms al fine di metterlo in guardia da tale genere di truffe.
Nella circostanza, la chiamata ricevuta dal cliente è pervenuta da un'utenza in alcun modo riconducibile all'intermediario (peraltro, ad una ricerca online, tale numero viene indicato come truffaldino) ed in forza anche delle condizioni contrattuali sottoscritte dal ricorrente, all'articolo rubricato "*Estraneità della Banca ai rapporti sottostanti al trasferimento di denaro*" la banca è estranea ai rapporti e alle controversie relative ai beni e/o servizi acquistati per i quali il Cliente dovrà rivolgersi esclusivamente alla propria controparte in caso di contestazione
In virtù di ciò, ha richiesto il rigetto del ricorso.
In sede di repliche il ricorrente, dopo avere negato di avere fornito informazioni al sedicente operatore, ha contestato qualsivoglia sua negligenza, addebitando al sistema dell'intermediario le responsabilità della subita truffa.
Nelle controrepliche, a propria volta, l'intermediario ha chiarito come le evidenze prodotte smentiscono gli assunti di parte ricorrente e che ogni contestazione appare priva di fondamento.

DIRITTO

Come noto, l'utilizzo fraudolento è disciplinato dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

Appare, quindi, preliminare e pregiudiziale chiarire come il dettato normativo impone all'intermediario provare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata (art. 10, D. Lgs. 11/10).
In merito a ciò, va chiarito che l'operazione contestata consiste in un pagamento di € 790,00 eseguito da terzi in data 8.07.2023 tramite la piattaforma R.
La parte ricorrente ha riferito che le operazioni fraudolentemente autorizzate sono state due, una di € 790,00, oggetto del presente procedimento, e una di € 100,00, già rimborsata dall'intermediario e, pertanto, estranea al ricorso
In ordine alla prova di autenticazione, l'intermediario ha riferito che "l'operazione contestata dal Ricorrente è stata autenticata mediante i fattori di sicurezza stabiliti dalla Strong Customer Authentication (SCA) prevista dalla direttiva (UE) 2015/2366: invero, tramite la notifica push autorizzativa giunta sullo smartphone a qual momento collegato all'account e ove l'applicazione [nome intermediario] è in uso, e tramite un'azione volontaria ("tap") eseguita sulla medesima notifica, il soggetto disponente si è "loggato" e fatto accesso all'interno dell'applicazione [nome intermediario] con i propri riferimenti personali identificativi, autorizzando di conseguenza l'operazione posta in essere".
Inoltre, ha prodotto specifiche evidenze per provare la corretta autenticazione (schermate e log informatici) da cui parrebbe doversi desumere che le operazioni siano state autorizzate direttamente dal malfattore tramite il proprio device a seguito di enrollment
Il Collegio rileva che a fronte di evidenze documentali analoghe prodotte dallo stesso intermediario in controversie anaoghe, l'ABF ha ritenuto provata l'autenticazione delle operazioni contestate e compliant con la SCA il sistema di pagamento adottato dall'intermediario resistente, tenuto conto dell'utilizzo dei seguenti fattori di autenticazione per le operazioni e-commerce: 1. elemento di possesso: notifica alla app nel device del ricorrente; 2. elemento di inerenza: riconoscimento biometrico.
A fronte di evidenze documentali di questo tenore deve giudicarsi dimostrata la corretta contabilizzazione, registrazione e autenticazione delle operazioni disconosciute, lungo tutto l'iter del loro compimento, ai sensi e per gli effetti dell'art. 10 D.Lgs. n. 11/2010.
Operata la superiore ed ineludibile verifica, va riferito dalla documentazione agli atti emerge che le operazioni contestate sono scaturite da un fenomeno di spoofing realizzato ai danni di parte ricorrente, in quanto l'SMS allegato dalla stessa, sebbene non riporti il mittente, risulta inserito nella medesima chat contenente gli sms genuini provenienti dalla resistente. La ricorrente con il ricorso ha riferito di aver ricevuto anche una telefonata (vishing) dal numero dell'intermediario, da un presunto operatore, ma di non avergli comunicato alcun dato e/o codice dispositivo.
Dalla denuncia allegata, tuttavia, non è possibile ricostruire esattamente la vicenda fraudolenta, in quanto la ricorrente si è limitata a dare atto dell'effettuazione di un prelievo non autorizzato dal suo conto. Né è stata prodotta, inoltre, alcuna evidenza in merito al lamentato vishing.
In relazione all'SMS civetta allegato, si dà atto altresì che lo stesso riporta un link non riferibile all'intermediario convenuto e che la punteggiatura presente nel testo del messaggio non risulta corretta.
Operata la superiore ed ineludibile verifica, si rileva che dalla documentazione agli atti sembra che le operazioni contestate siano scaturite da un fenomeno di *vishing e spoofing* realizzato simultaneamente ai danni di parte ricorrente. In particolare la ricorrente afferma di aver ricevuto un SMS inserito nella chat abitualmente utilizzata dall'intermediario per le comunicazioni, nella quale veniva invitata a contattare un'utenza telefonica fissa, se l'operazione indicata nel messaggio non fosse stata da lei richiesta.
L'intermediario, a sua volta, contesta espressamente come il numero di telefono indicato nel messaggio civetta non sia a sé riconducibile e come la ricorrente avrebbe potuto

contattare il numero verde della banca o il numero degli sportelli, aperti quel giorno, ed evitare così la frode.
Orbene, va specificato che l'SMS allegato dalla ricorrente, riporta un link non riferibile all'intermediario convenuto e che la punteggiatura presente nel testo del messaggio non risulta corretta.
Né la denuncia allegata ricostruisce esattamente la vicenda fraudolenta; tantomeno risulta prodotta dall'istante una qualsivoglia evidenza in merito al lamentato vishing.
Secondo l'orientamento condiviso dei Collegi ABF, nelle fattispecie di spoofing non è generalmente ravvisabile la colpa grave del ricorrente, data l'insidiosità del meccanismo di aggressione.
Tuttavia, qualora il testo del messaggio civetta presenti indici di evidente inattendibilità (quali ad esempio errori grammaticali o sintattici) o di anomalia (quali ad esempio l'invito a selezionare un link in nessun modo riferibile all'intermediario) che dovrebbero far allertare l'utente avveduto, è stato ritenuto che si possa ravvisare un concorso di colpa tra le parti, in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario.
In tale direzione, nel caso di specie, l'orientamento della giurisprudenza consolidata dei Collegi ABF (cui codesto Collegio intende uniformarsi) ravvisa un concorso di colpa tra le parti in ragione delle circostanze che hanno reso possibile la frode (ex multis, Collegio di Torino, decisione n. decisione n. 12856/2022 e decisione n. 9547/2021; Collegio di Milano, decisione n. 6472/2021).
Il ricorso va pertanto parzialmente accolto e, in assenza della prova di una diversa ripartizione della colpa tra le parti, le conseguenze dell'evento dannoso vanno ripartite fra la ricorrente e l'intermediario nella misura del 50%.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 395,00.
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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
EMANUELE CESARE LUCCHINI GUASTALLA