COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) GRAZIADEI	Membro designato dalla Banca d'Italia
(TO) COTTERLI	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) DE FRANCESCO	Membro di designazione rappresentativa dei clienti

Relatore - FABRIZIO DE FRANCESCO

Seduta del 22/06/2022

FATTO

La parte ricorrente ha affermato:

- di essere titolare di un conto corrente con servizio di *home banking* presso l'intermediario resistente;
- di essersi avveduta, in data 18/02/2022, che ignoti avevano disposto a valere sul suo conto e a sua insaputa un bonifico di € 14.871,00 in favore di soggetto del tutto sconosciuto;
- di aver rappresentato le modalità di svolgimento della truffa subita nelle denunce presentate all'Autorità;
- che, in particolare, rappresentava: (i) di aver ricevuto in data 17/02/2022 un SMS dal numero dell'intermediario resistente con cui veniva informato che la sua carta e il suo conto erano stati limitati per "*mancata verifica della sicurezza web*" più altri SMS dal contenuto simile; (ii) di aver cliccato sul *link* contenuto nel messaggio e di aver inserito nel sito cui veniva rimandato – identico a quello di accesso all'*home banking* – le credenziali di accesso e il proprio numero di telefono; (iii) di essere poi stata contattata da un sedicente operatore della banca – dal numero verde ufficiale – il quale riferiva che occorreva aggiornare i sistemi di sicurezza; (iv) in quel frangente riceveva sul suo telefono un file che apriva su suggerimento del suo interlocutore; (v) l'interlocutore riferiva a quel punto che l'operazione di aggiornamento era in corso e che lo avrebbe ricontattato il giorno successivo;

- di non aver mai ricevuto alcun codice OTP per autorizzare l'operazione;
- che il giorno 18/02/2022, non avendo ricevuto alcuna chiamata, controllava il suo conto e realizzava che ignoti avevano disposto il menzionato bonifico, dallo stesso mai autorizzato;
- che l'intermediario rifiutava il rimborso della somma fraudolentemente prelevata, affermando che l'operazione risultava correttamente autorizzata;
- che deve in ogni caso escludersi la sua colpa grave, trattandosi di un caso di c.d. *spoofing*.

Dopo aver vanamente esperito la fase del reclamo, parte ricorrente chiede pertanto il rimborso della somma di € 14.871,00, indebitamente sottratta, oltre agli interessi legali dal giorno dell'addebito sul conto e la rifusione delle spese di procedura.

Con le proprie controdeduzioni, l'intermediario resistente ha rappresentato che:

- il ricorrente è titolare di un conto corrente al quale è collegato il servizio di *home banking* che consente ai clienti di effettuare le operazioni di *inquiry* e dispositive, utilizzando il telefono cellulare o *internet*;
- il ricorrente aveva altresì attivato il servizio SMS *alert* collegato al suo numero di telefono cellulare;
- il sistema di sicurezza predisposto adotta un sistema di autenticazione "forte" per l'accesso alle funzioni di *inquiry* o dispositive, in conformità a quanto previsto dalla Direttiva PSD2;
- in particolare, nell'*home banking* da App, il sistema di autenticazione prevede: (i) per effettuare il *login* e le operazioni di *inquiry*, l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) + codice OTP dinamico generato da *Mobile Token*; (ii) per disporre le operazioni, dopo avere effettuato il *login* come sopra e inserita l'operazione, la stessa deve essere confermata mediante l'inserimento del PIN + codice OTP generato da *Mobile Token*;
- il tipo di operatività disconosciuta dal ricorrente si rende possibile solo nel caso in cui sia stato il cliente stesso a rivelare in qualche modo le proprie credenziali di sicurezza, via *e-mail*, SMS o via telefono o abbia abboccato ad un SMS *phishing*, solitamente contenente un *link* che, se cliccato ed inserite le credenziali di accesso, permette a soggetti estranei al titolare di accedere alle informazioni personali del titolare del conto corrente;
- ciò è confermato dalle stesse dichiarazioni del ricorrente, il quale ha ammesso di aver cliccato un *link* ricevuto via SMS e di aver inserito nel sito civetta le proprie credenziali dell'*home banking*;
- il comportamento tenuto dall'odierno ricorrente è stato pertanto gravemente colposo;
- la tipologia di frode subita è infatti ormai molto diffusa e pertanto riconducibile a un *phishing* classico;
- il ricorrente ha inoltre dichiarato di aver aperto un file ricevuto nel corso della chiamata con il sedicente intermediario: nonostante la carenza di dettagli su tale file, è plausibile ritenere che il ricorrente, sotto la guida del suo interlocutore, o abbia scaricato un'applicazione non riferibile in alcun modo alla banca (es. TeamViewer) - che ha consentito al terzo di assumere il controllo del *device* del cliente - oppure che, sotto dettatura, sia stato lo stesso cliente ad inserire il bonifico e ad autorizzarlo di suo pugno;
- in ogni caso il ricorrente ammette di avere seguito le istruzioni che il terzo gli ha fornito al telefono senza porsi alcun dubbio;
- la banca ha fornito ampia informativa alla propria clientela in merito alle più diffuse tiptologie di truffa e ai modi per evitarle;

- dai "*Log*" dell'operazione controversa si evince, oltre all'adozione di un sistema di autenticazione "forte", che non vi è stata alcuna attivazione di un nuovo *mobile token* su diverso *device* e che l'operatività disconosciuta risulta effettuata direttamente dal *device* del cliente;
- il cliente ha ricevuto un SMS e una notifica *push* di *alert*;
- l'odierno ricorrente ha disconosciuto l'operazione controversa soltanto a distanza di due giorni dal suo perfezionamento.

L'intermediario chiede pertanto il rigetto del ricorso.

Le parti hanno fatto pervenire memorie di replica e controreplica, insistendo per le proprie difese e richieste e contestando le avverse argomentazioni.

DIRITTO

Il Collegio, rilevato che il caso di specie riguarda un bonifico *on line* di € 14.871,00 disposto da App in data 17/02/2022 a favore di un terzo, nominativamente individuato, che la parte ricorrente dichiara di non conoscere; ricordato che detta operazione contestata e disconosciuta è disciplinata dal D.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13 gennaio 2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (cd. PSD2); considerato che nel caso di specie, l'intermediario non ha fornito adeguata prova della corretta autenticazione, registrazione e contabilizzazione dell'operazione di pagamento contestata, in relazione a tutti i passaggi esecutivi della medesima (accesso all'area personale del cliente, *enrollment* dell'app ed esecuzione del pagamento); rilevato infatti, da un lato, che i cd. "*Log*" prodotti in atti dall'intermediario sono incomprensibili ed incompleti; ricordato inoltre, dall'altro lato, che, al fine dell'autenticazione con cd. "doppio fattore", i PIN e le credenziali statiche non soddisfano i requisiti previsti dalla normativa di settore, così come precisati dall'EBA (*European Banking Authority*) nella sua *Opinion* del 21/06/2019, recepita da Banca d'Italia con comunicato dell'agosto del 2019 in cui si precisa "*l'immediata applicabilità delle regole di imputazione delle responsabilità, in caso di frodi, alle transazioni prive dei requisiti di sicurezza richiesti dalla normativa*" (si vedano sul punto, le decisioni di questo Collegio di Torino nn. 2129/2021, 6835/2021, 5074/2021 e 6689/2021); preso dunque atto del costante orientamento dei Collegi ABF, a mente del quale, ai sensi dell'art. 10 del citato D.lgs. 27 gennaio 2010, n. 11, è onere dell'intermediario provare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata, in ogni sua fase, con la conseguenza che, in mancanza di detta prova, l'intermediario sopporta in ogni caso ed integralmente le conseguenze del disconoscimento delle operazioni di pagamento, senza applicazione della franchigia (si vedano, fra le tante, le decisioni Collegio di Torino n. 3464/2018; Collegio di Torino n. 6454/2018; Collegio di Torino n. 2408/2018; Collegio di Torino n. 27616/2018; Collegio di Torino n. 5642/2018; Collegio di Milano n. 1588/2017; Collegio di Bologna n. 6837/2017; Collegio di Milano n. 7131/2017; Collegio di Milano n. 5206/2016); considerato pertanto che il ricorso va accolto per l'intero importo richiesto da parte ricorrente, pari ad € 14.871,00.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 14.871,00, oltre interessi legali dal 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 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