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 ESTERNI - MICHELE GRAZIADEI

Seduta del 22/06/2022

FATTO

Il ricorrente ha affermato con riferimento al reclamo di essere titolare di conto corrente n. *****491, acceso presso la resistente; in data 13/10/2021 riceveva un sms apparentemente proveniente dalla banca con cui veniva avvisato di un accesso anomalo al suo conto; contestualmente veniva invitato a collegarsi ad una pagina web, cliccando su un link, indicato nello stesso sms, per fornire alcuni dati personali; il giorno successivo riceveva un altro sms da un tale M. N., il quale, qualificatosi come operatore della banca, lo informava che un ordine di bonifico online per € 18.650,00 era stato annullato. Non avendo mai disposto detto bonifico, in data 15/10/2021 si recava presso la banca per avere spiegazioni in merito; in tale occasione veniva a conoscenza dell'effettuazione di due bonifici non autorizzati dal suo conto nei due giorni precedenti per gli importi di € 7.000,00 e di € 18.650,00; la frode patita è imputabile esclusivamente ai sistemi informatici della banca, che hanno consentito a terzi malintenzionati di disporre operazioni dal suo conto, eludendo anche la protezione rappresentata dall'impronta digitale; di non aver ricevuto alcun sms di *alert* in ordine alle operazioni fraudolentemente disposte, nonostante si trattasse di pagamenti anomali.

L'intermediario, nelle controdeduzioni, ha rappresentato che il ricorrente è titolare di conto corrente n. *****491, cui è collegato il servizio di internet banking; di aver inviato al ricorrente la proposta di modifica unilaterale del contratto in data 12/03/2018, con riguardo alle nuove disposizioni introdotte dalla PSD2; che per accedere ai servizi online della banca è richiesto l'inserimento di password statiche (codice titolare e PIN) e della password dinamica (codice OTP); che a seguito dei fatti dichiarati dal ricorrente, è stato disposto un tentativo di *recall* delle somme, non andato a buon fine; sia dalle dichiarazioni rese nella denuncia dal cliente sia dalle evidenze informatiche risulta che il ricorrente ha cliccato sul link, disinstallato l'applicativo della banca, digitato le sue credenziali (codice utente, password, numero di telefono) e comunicato a terzi estranei il codice OTP, necessario per effettuare le operazioni di bonifico. La documentazione informatica dimostra la corretta, autenticazione, registrazione e contabilizzazione delle operazioni contestate; dai log allegati risulta che, a seguito dell'accesso all'*home banking*, è stata effettuata l'installazione dello smart OTP su un nuovo dispositivo (con disinstallazione di quello sul dispositivo del cliente), sono quindi state fatte delle interrogazioni sul profilo del cliente e quindi sono state inserite le operazioni di bonifico; per le singole operazioni, oltre all'inserimento delle credenziali di accesso e dell'OTP, è stata inserita anche un'ulteriore password dinamica OTS inviata via sms al numero del ricorrente, in ragione del rischio frode dell'operazione. Il sistema della banca non è stato violato da parte dei malfattori; la truffa perpetrata ai danni del cliente si è potuta perfezionare unicamente grazie alla collaborazione del medesimo, nell'ambito di un fenomeno di *phishing*. Come ritenuto dalla Polizia postale, i furti di identità sono ascrivibili a condotte esterne ai sistemi di sicurezza e di autenticazione forte adottati dalle banche; nel caso di specie infatti il cliente è stato vittima di *phishing* e *vishing*.

Nel replicare alle controdeduzioni, il ricorrente, ripercorrendo i fatti, pacifici tra le parti, ha precisato: che non è sufficiente per la banca dimostrare che i bonifici contestati siano stati autenticati correttamente, dovendo altresì provare come dette operazioni siano riconducibili alla frode, al dolo o alla colpa grave del ricorrente; che alcuna colpa è rilevabile nel caso di specie, avendo egli ricevuto un sms dalla banca, identico a quelli che era solito ricevere e avendo immediatamente disconosciuto i bonifici; di non aver ricevuto alcun sms alert né per la modifica dell'utenza associata alla banca, né per il cambiamento del profilo biometrico né per le disposizioni; che secondo gli orientamenti dell'arbitro, la mancata attivazione del servizio di sms alert costituisce una disfunzione organizzativa, imputabile alla banca; che la colpa grave dell'intermediario è riscontrabile anche nell'inadeguatezza dei sistemi impiegati per rilevare gli indici di anomalia delle operazioni disconosciute, l'elevata entità dei bonifici e l'impiego di un IP e di un browser mai utilizzati in precedenza; che i Collegi ABF hanno rilevato che un sistema che richieda la digitazione di un'ulteriore password dinamica trasmessa per sms alla stessa utenza telefonica del ricorrente sia sostanzialmente inadeguato; che la banca è consapevole delle vulnerabilità del proprio sistema, dato che, nella medesima data in cui avveniva la frode, inviava ai propri clienti un'email con cui li avvisava di diversi tentativi di truffa.

L'intermediario, nelle controrepliche ha evidenziato come le operazioni disconosciuta sia scaturita da un fenomeno di "*SMS Spoofing*"; ha sottolineato che tale messaggio truffaldino non era contenuto nella medesima chat dei messaggi genuini provenienti dalla banca; ha eccepito che dal testo del messaggio civetta era possibile comprenderne il carattere anomalo dal momento che il link non era in alcun modo riconducibile alla banca; ha ribadito come la banca abbia adottato un sistema di autenticazione forte, come risulta dalle ulteriori evidenze allegate; ha riferito che il cliente in sede di sottoscrizione del contratto ha rifiutato di aderire al sistema di sms alert; ha affermato che alcuna responsabilità può essere addebitata alla banca per l'importo elevato dei bonifici, dal

momento che il massimale è stato impostato dal ricorrente.
La parte ricorrente domanda il rimborso della somma di € 25.650,00, oltre interessi legali dalle date delle operazioni al saldo.
L'intermediario resistente chiede il rigetto del ricorso.

DIRITTO

Le operazioni contestate sono disciplinate 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. Più precisamente si tratta di due bonifici, di cui uno di € 18.650,00 e uno di € 7.000,00, disposti rispettivamente in data 13/10/2021 e in data 14/10/2021 (sulla data e sull'orario si vedano i log dell'intermediario).
Tali operazioni risultano dai moduli di disconoscimento e dall'estratto conto, oltreché dalla denuncia. L'intermediario ha riferito che le operazioni contestate sono state autenticate, previo *enrollment* del software token sul cellulare del malfattore, tramite accesso all'home banking e inserimento del codice OTP virtuale e del codice OTS inviato via sms al numero di cellulare del ricorrente. In particolare, ha precisato che l'*enrollment* sarebbe avvenuto tramite inserimento delle credenziali statiche e OTP inviato via sms al numero del ricorrente.
Il sistema di autenticazione dell'intermediario risulta basato sui seguenti fattori: per l'accesso al sistema di internet banking, l'elemento di conoscenza è codice titolare e PIN; l'elemento di possesso è l'OTP. Per l'*enrollment* della App, l'elemento di conoscenza è il codice titolare e PIN; l'elemento di possesso è l'OTP via SMS. Tuttavia, sebbene l'intermediario descriva compiutamente il sistema di autenticazione e i fattori impiegati per l'accesso e per l'*enrollment* del software token Smart OTP, le evidenze versate in atti non documentano espressamente l'inserimento dei codici OTP che sarebbero richiesti, affinché operi effettivamente un'autenticazione a doppio fattore. Per le singole operazioni l'autenticazione risulta dall'uso di un elemento di conoscenza: codice titolare e PIN (credenziali statiche per il login); un elemento di possesso: OTP generata via software token. L'intermediario ha dichiarato che sarebbe stato richiesto anche un ulteriore elemento di possesso, quale un codice OTS, inviato via sms. Nei log prodotti non compare tuttavia la dicitura OTP virtuale, ma la voce "Autorizza", né è stata prodotta evidenza della trasmissione dell'ulteriore OTS via sms al numero del ricorrente.
Considerato il quadro così ricostruito, il Collegio ritiene che l'intermediario non abbia offerto piena prova della regolare autenticazione registrazione e archiviazione delle operazioni contestate, ai sensi della disciplina applicabile, sopra richiamata. Pertanto, in presenza delle lacune probatorie in questione, l'intermediario è tenuto a corrispondere alla parete ricorrente la somma domandata, pari a € 25.650,00, oltre agli interessi legali dal reclamo al saldo.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 25.650,00, 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