Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) GRAZIADEI	Membro designato dalla Banca d'Italia
(TO) BATTELLI	Membro designato dalla Banca d'Italia
(TO) DALMOTTO	Membro di designazione rappresentativa degli intermediari
(TO) CATTALANO	Membro di designazione rappresentativa dei clienti

Relatore EUGENIO DALMOTTO

Seduta del 09/06/2021

FATTO

La parte ricorrente ha in sintesi affermato:

- di essere titolare del conto corrente n. xxx954, accesso presso una filiale dell'intermediario resistente e a cui è collegato il servizio di *home banking*;
- che, come dichiarato nella denuncia alle Autorità allegata al ricorso, a partire dall'8 giugno 2020, subiva l'indebita sostituzione della SIM associata alla propria utenza telefonica nr. xxx384, a sua volta collegata al servizio di *internet banking*;
- che tra l'8 giugno 2020 e il 12 giugno 2020 venivano effettuati tramite il proprio servizio di *home banking* quattro bonifici mai autorizzati per un importo complessivo di € 30.270,00;
- che, dalle verifiche svolte, apprendeva di aver subito una c.d. *sim swap fraud,* a mezzo della quale terzi malfattori sostituivano l'identità associata alla sua SIM allo scopo di utilizzarla per ricevere i codici dispositivi necessari a eseguire operazioni di pagamento da *internet banking*;
- che ha sempre custodito correttamente le proprie credenziali di accesso al servizio di *home banking*, senza mai comunicarle ad alcuno;
- che, in base al D.Lgs. 11/2010, come modificato in seguito al recepimento della direttiva PSD2, sul prestatore di servizi di pagamento incombe l'onere di provare sia la corretta autenticazione delle operazioni non autorizzate sia la colpa grave dell'utente che le disconosca;

- che, in tal senso, si è chiaramente espresso il Collegio di Coordinamento ABF, con la decisione n. 22745 del 10 ottobre 2019, nonché lo stesso Collegio ABF di Torino e la giurisprudenza di legittimità;
- che, in base al condiviso orientamento dell'ABF, la particolare insidiosità della *sim swap fraud* esclude in capo a chi la subisce la sussistenza della colpa grave;
- che il cliente, infatti, non è in grado di collegare immediatamente il malfunzionamento del telefono con l'esecuzione di operazioni bancarie non autorizzate;
- che l'intermediario ha omesso di predisporre sistema di controllo e sicurezza idonei a prevenire truffe del tipo di quella subita nel caso di specie (quali, ad esempio, la previsione di una conferma a mezzo *e-mail* o di ulteriori OTP specifiche);
- che l'intermediario avrebbe, inoltre, dovuto intercettare le anomalie dell'operatività controversa rispetto al *plafond* e al dispositivo utilizzato per effettuarle;
- che le truffe del tipo di quella subita normalmente presuppongono attacchi mirati a soggetti di cui si conoscono i dati personali e che, per svolgere ulteriori approfondimenti in questa direzione, intende richiedere all'intermediario *ex* art. 119 TUB di consegnarli i *log* di sistema riferiti ai 60 giorni precedenti il compimento della prima operazione disconosciuta;
- che la responsabilità dell'intermediario è aggravata dal fatto di non aver diffuso, presso la propria clientela, specifici avvisi relativi alla truffa perpetrata a mezzo di *sim swap*;
- che la *sim swap fraud* vanifica l'efficacia di qualsiasi eventuale sistema di *SMS alert.*

Pertanto domanda (i) che l'intermediario venga condannato a pagare al ricorrente l'importo di € 30.270,00, o di altra somma anche maggiore accertanda, a titolo di rimborso delle operazioni di pagamento disconosciute e comunque a titolo di risarcimento del danno subito per i fatti di cui è controversia, oltre interessi legali dal dovuto al saldo e al pagamento delle spese legali e di procedura; (ii) che l'intermediario, anche ai sensi dell'art. 119 TUB, venga condannato a consegnargli e/o a produrre in atti, la documentazione relativa ai *log* informatici di sistema relativi all'accesso al rapporto di conto corrente ed *home banking* oggetto di controversia, compiuto nei 60 giorni precedenti all'8 giugno 2020.
L'intermediario, nelle controdeduzioni, ha invece rappresentato:

- che il servizio di *internet banking* collegato al c/c bancario del ricorrente prevede l'accesso alle funzioni di *inquiry* e dispositive mediante un sistema di autenticazione «forte», in linea con la normativa europea PSD2, che prevede per il *login* e le operazioni di *inquiry*, l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) + codice OTP (*One Time Password*), codice dinamico generato da *mobile token* e per disporre le operazioni, dopo avere effettuato la *login*, la conferma con inserimento del PIN + codice OTP (*One Time Password*), generato da *mobile token*;
- che il codice OTP (*One Time Password*) è una password temporizzata valida per un solo utilizzo che viene generata in modo silente dal *mobile token* integrato nell'*App* che il cliente ha attivato sullo strumento/device che sta utilizzando;
- che nell'operatività dal sito il codice OTP deve essere autorizzato dal cliente tramite notifica *push* che riceve sul dispositivo mobile e sulla quale dovrà cliccare inserendo il suo codice PIN o *touchID o faceID*;
- che l'attivazione del *mobile token* è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare collegato all'*home banking*;

- che ha diffuso avvisi specifici di sicurezza nella pagina di accesso al portale, sull'*App* e sugli schermi ATM, nei quali si avverte espressamente la clientela che la banca non chiederà mai le credenziali di sicurezza, le quali sono personali e non devono mai essere comunicate a terzi;
- che ha altresì inviato *e-mail* di analogo contenuto a tutta la clientela;
- che constano numerosi precedenti, anche del Collegio di Torino, in base ai quali, in presenza di un sistema di autenticazione forte, si deve presumere che ci sia stata una negligenza dell'utente nella custodia delle credenziali necessarie per utilizzare i servizi di pagamento;
- che, nel caso di specie, il 9 e il 12 giugno 2020, ignoti malfattori chiamavano il servizio clienti dell'operatore telefonico dell'odierno ricorrente e ottenevano il blocco della sua scheda SIM;
- che, nelle stesse giornate, allorquando all'odierno ricorrente era inibito l'uso del telefono cellulare, i truffatori eseguivano le operazioni oggetto di controversia;
- che, per attivare il *mobile token*, è necessario digitare il numero cliente e il codice PIN associato, e che quindi si deve presumere che il ricorrente abbia comunicato tali credenziali ai truffatori;
- che il ricorrente tuttavia fornisce una ricostruzione vaga e generica dei fatti, così tenendo un comportamento che è stato censurato da diversi Collegi ABF;
- che è tuttavia certo che il ricorrente abbia comunicato le credenziali di sicurezza dell'*home banking* che hanno consentito ai presunti frodatori, grazie alla comunicazione dell'OTP pervenuto sul cellulare del ricorrente nei giorni precedenti le operazioni, di scaricare il *mobile token*;
- che il cliente è quindi incorso in colpa grave, violando gli obblighi di diligente custodia delle credenziali sullo stesso incombenti in base alla disciplina legale;
- che, dalle verifiche effettuate, non è emerso alcun malfunzionamento o compromissione dei sistemi, le operazioni risultano correttamente autenticate, registrate e contabilizzate (così come previsto dall'art. 10 del D.Lgs. n. 11/2010), come dimostrato nelle evidenze *log*;
- che, in particolare, sia l'accesso che le operazioni dispositive controverse sono state correttamente autorizzate con un sistema di autenticazione a due fattori (PIN + OTP generato da *mobile token*);
- che, a seguito della fraudolenta temporanea sostituzione della SIM del cellulare del ricorrente, la sua utenza telefonica non era attiva e quindi gli SMS inviati dalla Banca non gli sono stati consegnati;
- che, a seguito alla segnalazione effettuata dal ricorrente, la Banca si è tempestivamente attivata per tentare il rientro dei fondi, ma purtroppo il recupero dell'importo non è stato possibile anche a causa del ritardo della segnalazione;
- che veniva infatti a conoscenza del disconoscimento delle operazioni a distanza di otto giorni dalla data del primo bonifico disconosciuto, sebbene il ricorrente avesse a disposizione l'*home banking* per un controllo delle sue movimentazione del c/c, e non era quindi più in grado di bloccare le operazioni controverse, alcune delle quali disposte tramite bonifico istantaneo, immediatamente esecutivo a favore del beneficiario;
- che, da quanto esposto si evince che la Banca, nello svolgimento della propria attività professionale, ha posto in essere tutte le misure di sicurezza e prevenzione idonee al fine di tutelare il cliente;
- che la asserita frode è stata resa possibile esclusivamente dalla conoscenza, in capo ai presunti frodatori, delle credenziali di accesso all'*home banking*,

sicuramente fornite dallo stesso ricorrente, senza le quali non sarebbero stati in grado di accedere alla *App,* scaricare il *mobile token* e solo successivamente disporre le operazioni;
- che la richiesta di risarcimento di presunti danni è stata formulata in maniera assai generica e non è stata prodotta adeguata prova dell'entità degli stessi;

Chiede quindi il rigetto del ricorso.

Nel replicare alle controdeduzioni, la parte ricorrente, a propria volta:
- ha eccepito, in via preliminare, la tardività delle controdeduzioni, che risultano depositate ben oltre il termine perentorio di 30 giorni previsto dalla vigente disciplina e chiesto pertanto al Collegio, come previsto dalle Disposizioni ABF, di non tenerne conto e dare conseguentemente atto della mancata prova dell'autenticazione, registrazione e contabilizzazione delle operazioni contestate;
- ha poi eccepito che, in ogni caso, l'intermediario non avrebbe provato la corretta autenticazione, registrazione e contabilizzazione delle quattro operazioni contestate in quanto si è limitato a produrre un file Excel dallo stesso predisposto - e in quanto tale inidoneo a costituire fonte di prova - del tutto incomprensibile e incompleto;
- ha, in particolare, rilevato che nei *log* prodotti dall'intermediario mancano l'indicazione dell'indirizzo IP dal quale sono stati eseguiti gli accesi al sistema di *home banking*, dello specifico codice IMEI del *device* utilizzato per gli accessi medesimi nonché del *browser* utilizzato e della cella telefonica del dispositivo mobile, utili a determinare la coerenza tanto dei dispositivi *hardware* e *software* normalmente usati, quanto della posizione geografica rispetto a quella usuale del correntista (informazioni invece fornite da altre banche);
- ha rilevato la mancata produzione, da parte dell'intermediario, della documentazione allo stesso richiesta *ex* art. 119 TUB in sede di ricorso;
- ha affermato che l'intermediario non ha in alcun modo provato la colpa grave del ricorrente, onere di cui è invece chiaramente gravato in base alla cristallina giurisprudenza dei Collegi ABF (compreso quello di Torino);
- ha ribadito di aver sempre diligentemente custodito le proprie credenziali di accesso all'*home banking;*
- a ulteriore dimostrazione di aver subito, quale vittima incolpevole, una truffa particolarmente sofisticata, ha allegato gli atti di indagine della Procura sul caso controverso nei quali lo stesso figura come persone offesa e dai quali emerge che il beneficiario delle operazioni disconosciute era persona nota alle forze dell'ordine;
- ha evidenziato che la stessa banca ha confermato, nel caso di specie, che vi è stata una *sim swap fraud*, per la quale l'orientamento dell'ABF è chiarissimo nel ritenere che – proprio per le sue specifiche modalità esecutive – una corretta esecuzione dell'operazione non possa nemmeno ritenersi astrattamente ipotizzabile;
- ha evidenziato l'irrilevanza del presunto SMS riportato nella documentazione prodotta da controparte, che non potrebbe costituire prova alcuna, «essendo un'evidente stampa su carta intestata della banca, non riconducibile al gestore telefonico e dunque inidoneo a dimostrare tanto l'invio quanto l'effettiva ricezione dell'SMS medesimo» e che comunque appare inidoneo a informare su una possibile frode in corso e appare ambiguo ed irrilevante se inviato a chi, come il ricorrente, aveva già il *token mobile* attivo;
- ha poi rilevato che l'utilità di tutti gli SMS successivamente inviati veniva vanificata dalla *sim swap fraud*;

- ha quindi concluso che nessuna colpa (tantomeno grave) possa essergli addebitata quale vittima di una frode particolarmente complessa ed insidiosa, inevitabile e fuori dalla sua personale possibilità di intervento;
- ha poi rilevato una grave carenza organizzativa in capo alla banca, la cui struttura informatica non sarebbe idonea alla gestione sicura dei rapporti di *home banking*. Nel mese di giugno del 2020, infatti, il sistema di consegna, installazione e gestione del Token mobile dell'intermediario prevedeva unicamente, in seguito al primo accesso con le credenziali statiche (*UserID* e PIN), l'invio di un semplice SMS con i codici di attivazione: una procedura non sicura e non rispondente ai requisiti di autenticazione a doppio fattore dinamico;
- ha quindi riferito che soltanto nei mesi successivi alla vicenda controversa l'intermediario cambiava la procedura in questione;
- ha evidenziato che l'*e-mail* informativa prodotta da controparte – del quale tuttavia non è provato l'invio – si riferisce unicamente ai rischi di *phishing*, ma non contiene alcuna menzione ai casi di *sim swap fraud* (il quale tuttavia, come si è ormai appreso, era noto alle banche già da anni);
- ha infine ribadito che nel caso di specie il sistema antifrode della banca non ha rilevato «le chiare anomalie insite nell'esecuzione di quattro bonifici di importo così rilevante ad un unico beneficiario, subito dopo un intervento sul *mobile token* e con l'utilizzo di un device telefonico diverso da quello usuale».

Ciò posto, il Collegio osserva quanto segue.

DIRITTO

Le operazioni contestate sono disciplinate 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 (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 specificamente, le operazioni disconosciute sono n. 4 bonifici (di cui 3 istantanei) disposti da *App* tutti a favore di A.L., soggetto che il ricorrente dichiara essergli ignoto, e in particolare: bonifico istantaneo dell'importo di € 7.930,00 effettuato l'8 giugno 2020; bonifico ordinario dell'importo di € 7.640,00 effettuato il 9 giugno 2020; bonifico istantaneo dell'importo di € 7.250,00 effettuato il 12 giugno 2020; bonifico istantaneo dell'importo di € 7.450,00 effettuato il 12 giugno 2020.

Il ricorrente ha allegato di essere stato vittima di *sim swap fraud*.

Lo stesso ha infatti dichiarato che, a partire dall'8 giugno 2020, subiva l'indebita sostituzione della SIM associata alla propria utenza telefonica nr. xxx384, a sua volta collegata al servizio di *internet banking*. In particolare, nella denuncia e nella relativa integrazione presentate all'autorità, parte ricorrente ha riferito di aver appreso dal proprio operatore telefonico che la sua SIM era stata disattivata e poi riattivata in diverse occasioni (l'8, il 9 e poi il 12 giugno 2020) tramite procedura perfezionatasi telefonicamente.

In effetti, dalla documentazione in atti si ricava che il ricorrente è stato vittima di una frode perpetrata mediante il meccanismo conosciuto come *sim swap fraud o* «truffa di scambio di SIM», attraverso il quale i malviventi, con il raggiro o con la complicità di un operatore di telefonia, ottengono il duplicato della SIM del soggetto titolare dello strumento di pagamento, le cui credenziali erano state preliminarmente carpite tramite tecniche di

hacking ovvero di ingegneria sociale, riuscendo in tal modo ad entrare in possesso di tutti i codici necessari per eseguire operazioni *on line*.
Tale truffa si è ripetuta in più occasioni, a distanza ravvicinata di tempo, senza che il ricorrente, usando l'ordinario diligenza, potesse accorgersi della sottrazione di denaro dal proprio conto, in quanto le OTP dispositive venivano inviate al duplicato della SIM nei periodi in cui il telefonino del ricorrente subiva temporanei malfunzionamenti, che questi, senza sua colpa, non riusciva a ricollegare immediatamente alla truffa in atto.
Secondo gli orientamenti da ultimo condivisi dai Collegi territoriali, nelle fattispecie di *sim swap fraud,* l'operazione non può ritenersi «regolarmente autenticata», in quanto conseguenza della sostituzione della SIM dell'utenza telefonica associata al servizio di *home banking* (cfr., in questo senso, Collegio di Torino, decisione n. 21366 del 11 settembre 2019).
La domanda di restituzione di quanto illegittimamente sottratto, oltre agli interessi dal reclamo al saldo, deve essere pertanto accolta.
Non può essere invece accolta la domanda di pagamento delle spese legali, trattandosi di spese non necessarie, non essendo obbligatoria l'assistenza di un difensore.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 30.270,00, 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