COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) ABATE	Membro di designazione rappresentativa dei clienti

Relatore (MI) ABATE

Seduta del 13/02/2024

FATTO

Il ricorrente chiede la restituzione della somma di € 29.260,05, corrispondente all'importo di un'operazione di pagamento fraudolenta, oltre interessi legali a far tempo dall'operazione e spese legali.
Il ricorrente afferma quanto segue:
- in relazione ai fatti oggetto del presente ricorso è già intervenuta la decisione del Collegio di Milano n. 9749/22, emessa in accoglimento del ricorso n. 44045/22, presentato in proprio dal rappresentante legale dell'odierna parte ricorrente (sig. T***);
- egli ha infatti subito un attacco di SIM *swap fraud* che ha colpito, tra l'1 e il 2 dicembre 2020, la piattaforma di *business home banking* sulla quale erano appoggiati, oltre al conto corrente personale dell'amministratore (oggetto del ricorso sopra menzionato), anche i conti correnti dei diversi condomini da lui gestiti, tra cui quello dell'odierna parte ricorrente;
- questa piattaforma, tramite la quale è possibile gestire in un unico ambiente più conti correnti, è associata al numero di telefono dell'amministratore;

- in data 03/12/2020 l'amministratore si recava in filiale per associare un nuovo numero di telefono alla piattaforma, in quanto il numero precedente si era bloccato all'improvviso;
- a seguito di alcune verifiche con un consulente del gestore telefonico e sulla piattaforma di *home banking*, l'amministratore si accorgeva del compimento di alcune operazioni non autorizzate;
- l'amministratore presentava il primo ricorso all'ABF, in cui lamentava di essere stato vittima di una truffa che bloccava la sua utenza telefonica, trasferendola sulla scheda SIM di un frodatore, truffa denominata *SIM swap fraud*;
- detto ricorso (n. 44045/22) riguardava le somme prelevate illecitamente dal conto corrente personale dell'amministratore;
- già nell'immediatezza dei fatti, l'amministratore presentava a nome del condominio odierno ricorrente il modulo di disconoscimento di 3 operazioni addebitate sul conto del condominio stesso, per l'importo di € 14.390,00, €14.970,34 ed € 14.870,05;
- a seguito del disconoscimento, il bonifico di € 14.970,34 veniva definitivamente stornato dalla banca, mentre le somme relative agli altri due bonifici venivano accreditate "salvo buon fine", per poi essere successivamente riaddebitate;
- a seguito dell'accoglimento del ricorso n. 44045/22, avente ad oggetto le somme prelevate dal conto dell'amministratore, in data 03/07/2023, il condominio odierno ricorrente ha presentato un nuovo reclamo all'intermediario, relativamente all'operazione illecitamente disposta sul proprio conto nell'ambito del medesimo attacco informatico;
- a tale reclamo, l'intermediario rispondeva, oralmente, proponendo il rimborso del 50% delle somme stornate; la proposta non è stata accettata dall'odierno ricorrente;
- la perizia ingegneristica allegata ha dimostrato che l'accesso alla piattaforma di *home banking* non è conforme alla Direttiva PSD2 in quanto non esige un'autenticazione forte.

L'intermediario afferma quanto segue:

- il condominio ricorrente è titolare di un conto corrente abilitato alla piattaforma di *internet banking business*, gestita dall'amministratore (utente "Master");
- l'utenza Master era legata al numero di telefono ***047, intestato all'amministratore del condominio ricorrente;
- l'utente Master accedeva al portale tramite le credenziali di firma elettronica OTP virtuale;
- con questa utenza, sono stati disposti tre bonifici in data 01/12/2020 e 2/12/2020 a valere sul conto del condominio (di cui uno integralmente recuperato);
- la controversia attiene ai due bonifici sopra menzionati. Le altre operazioni menzionate dall'amministratore sono riferibili a condomini terzi, estranei al presente procedimento;
- è censurabile la condotta di parte ricorrente, che ha prodotto documentazione relativa a fascicoli di procedimenti diversi da quello di cui ci si occupa, senza che si possa esercitare il diritto al contradditorio;
- pur prendendo atto della decisione n. 9749/22 allegata da parte ricorrente, sottolinea che nessuna decisione arbitrale ha carattere vincolante e auspica un giudizio formulato esclusivamente sulla base della documentazione che attiene strettamente all'odierno ricorrente;
- l'accesso al portale è assoggettato all'utilizzo di OTP, congiuntamente alle credenziali di login (Codice Titolare e Codice PIN);
- con riferimento all'analisi prodotta da controparte, precisa che l'attivazione dell'app della banca su un telefono diverso da quello del cliente non si può realizzare senza la

cooperazione del cliente, che fornisce a chi effettua l'*enrollment* le credenziali statiche e dinamiche;
- sussiste la colpa grave del cliente, che ha violato gli obblighi contrattuali relativi alla corretta custodia delle credenziali e alla tempestività delle comunicazioni alla Banca;
- la truffa c.d. SIM *swap fraud* si articola in una prima fase di *phishing*, durante la quale il frodatore acquisisce le credenziali del soggetto truffato con la collaborazione di quest'ultimo e in una seconda fase in cui il truffatore ottiene dall'operatore telefonico la sostituzione della sim;
- la Banca è totalmente estranea ad entrambe le fasi sopra indicate;
- il ricorrente non si è tempestivamente attivato presso il gestore telefonico per ottenere chiarimenti e non ha prontamente comunicato alla Banca il blocco richiesto da terzi sconosciuti;
- il cliente avrebbe dovuto allertarsi per tempo in merito allo stato della sua linea telefonica, in quanto già dal 30/11/2020 aveva ricevuto un messaggio dal suo operatore che lo avvertiva di un imminente blocco;
- per ben 3 giorni, dal 30 novembre al 2 dicembre 2020, il ricorrente ha scelto consapevolmente di restare all'oscuro di tutte le comunicazioni che la Banca ha trasmesso sul suo numero certificato, a cui era connessa l'attività di tutti i Condomini;
- il cliente si limitava a chiedere un nuovo numero di telefono all'operatore, aspettando solo il 03/12/2020 per effettuare controlli e verifiche presso l'intermediario;
- l'amministratore aveva installato l'app di *home banking* anche su un altro dispositivo, dal quale avrebbe potuto controllare la movimentazione sui conti correnti;
- quanto precede evidenzia la colpa grave derivante dalle omissioni nei controlli, tanto più considerati i doveri in capo all'amministratore verso i condomini che rappresenta.

Nel replicare alle controdeduzioni, la parte ricorrente, richiamati i propri scritti, replica quanto segue:
- le difese dell'intermediario sono già state respinte con la decisione n. 9749/22 resa nei confronti dell'amministratore, nonché con la decisione n. 7062/2023, sempre riferita alla medesima vicenda;
- il presente ricorso ha per oggetto unicamente i due bonifici partiti dal conto corrente del ricorrente, mentre gli altri condomini, pure se soggetti alla medesima frode e all'epoca gestiti dal medesimo amministratore, si difenderanno autonomamente come riterranno opportuno;
- il caso di specie attiene comunque alla medesima vicenda sostanziale e agli stessi profili giuridici dedotti nei ricorsi già presentati e decisi da codesto Arbitro;
- si contesta la copia del contratto che regola il servizio di *business home banking* prodotta dall'intermediario, in quanto difforme da quella depositata dal ricorrente;
- si contesta l'attendibilità dei *log* informatici depositati dall'intermediario, in quanto costituiti da un file Excel e privi, in ogni caso, di informazioni utili relative a capire chi si sia autenticato sulla piattaforma, da quali dispositivo, con quali credenziali e con quali OTP;
- non è provato che l'amministratore sia stato vittima di una prima fase di *phishing* grazie alla quale ignoti avrebbero potuto carpire le credenziali necessarie per perpetrare le fasi successive della truffa;
- il solo possesso della password statica è sufficiente ad autenticarsi grazie al possesso di una nuova SIM;
- si richiama la perizia di parte, in base alla quale ci sarebbe una falla nel sistema informatico dell'intermediario che permetterebbe l'invio dell'OTP via SMS al nuovo *device* del frodatore, in possesso del medesimo numero di telefono;
- all'epoca dei fatti il sito internet dell'intermediario, nella sezione dedicata alla sicurezza on-line, non dava informazioni in merito alla *SIM swap fraud*;

- l'intermediario si sarebbe dovuto allertare del fatto che, in un arco temporale ristretto, venivano disposti bonifici per oltre 600.000 Euro dalla stessa piattaforma da parte di oltre venti condomini.

Insiste, quindi, per l'accoglimento del ricorso.

L'intermediario, riportandosi alle conclusioni in atti, controreplica quanto segue:

- è da censurare la linea difensiva adottata da controparte in quanto incentrata su operazioni e soggetti che non formano oggetto del presente procedimento;
- è da auspicare che il Collegio formuli un giudizio sulla presente vertenza, esclusivamente sulla base della documentazione che riguarda l'odierno ricorrente, senza tener conto delle decisioni n. 9749722 e n. 7062/23 rese dal medesimo Collegio territoriale;
- è già stato dimostrato che il sistema informatico della Banca non è stato violato;
- sono prive di pregio le contestazioni avversarie mosse al file *excel* delle tracciature informatiche prodotto in sede di controdeduzioni; ad ogni modo, è consolidato orientamento dell'Arbitro ritenere valida la produzione di log in formato *excel*;
- evidenzia che le credenziali non possono essere riportate in chiaro nelle tracciature in quanto debbono essere custodite con la massima riservatezza;
- con riferimento alla documentazione della stessa tipologia prodotta per casi analoghi, evidenzia che l'Arbitro Bancario e Finanziario ha ritenuto che l'intermediario abbia adeguatamente provato di aver utilizzato nell'esecuzione dell'operazione disconosciuta un sistema a doppio fattore con OTP dinamico inserito dal ricorrente (decisione Coll. Milano, n. 14542/2021);
- con le tracciature prodotte in allegato alle controdeduzioni, la Banca ha dimostrato di aver dato esecuzione alle disposizioni di bonifico così come ricevute con la validazione delle credenziali del rappresentante legale del ricorrente;
- il rilascio del certificato ISO/IEC 27001 rappresenta la garanzia che il sistema di gestione adottato offre massimi livelli di sicurezza nell'utilizzo dei servizi della banca online e dei sistemi di pagamento elettronici;
- la responsabilità di quanto occorso è riconducibile alla colpa grave del rappresentante legale della controparte;
- a monte della truffa del tipo di *swap sim* di cui controparte sostiene di essere stata vittima, ribadisce che a monte di tale tipo di truffa, sussiste sempre l'acquisizione delle credenziali del cliente attraverso tecniche di *phishing*;
- si ribadisce, in quanto non contestato in sede di repliche, la tardività del cliente nell'attivarsi dopo aver ricevuto il messaggio dell'operatore telefonico a seguito del blocco della sua linea;
- non risulta contestato il fatto che il rappresentante legale avrebbe potuto controllare tempestivamente i conti correnti attraverso l'applicazione presente su altro dispositivo mobile: rappresenta pertanto una grave e inescusabile negligenza da parte del rappresentante legale il fatto di aver atteso le ore 18:00 del 2 dicembre 2020 per accedere a tale app;
- richiama, infine, la sentenza di merito del Tribunale di Milano in cui l'analisi delle informazioni presenti sul sito web della Banca nella sezione dedicata alla sicurezza è stata dirimente per ravvisare la colpa grave del cliente.

L'intermediario insiste, quindi, per il rigetto del ricorso.

DIRITTO

La controversia, che ha ad oggetto due operazioni disconosciute disposte *on line* per un controvalore complessivo pari a € 29.260,05, è regolata dalla disciplina in materia di servizi di pagamento, in particolare dalle norme relative all'autenticazione di operazioni di pagamento disposte *on line*, nonché all'onere della prova di autenticazione ed esecuzione delle operazioni di pagamento in capo all'intermediario e alla responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento (articoli 10, 10-bis e 12 del D.lgs. 27 gennaio 2010, n. 11, e s.m.i. e Regolamento Delegato (UE) n. 389 del 27 novembre 2017).

Orbene, trattandosi di operazioni disconosciute dal ricorrente, l'intermediario è chiamato a fornire prova di adeguata autenticazione. Sulla prova di autenticazione, si richiamano altresì gli orientamenti condivisi dei Collegi in base ai quali la suddetta prova, in aderenza al dato normativo, rappresenta un antecedente logico rispetto alla prova della colpa grave dell'utente.

Secondo le posizioni condivise dai Collegi, nei casi di "*Sim swap fraud*" le richieste del cliente risultano - generalmente - meritevoli di accoglimento integrale, in quanto la sostituzione della SIM card deve essere equiparata alla mancanza di autenticazione dell'operazione di pagamento ai sensi e per gli effetti dell'art. 10 del D. Lgs. 11/2010. Sempre secondo l'orientamento dei Collegi, pur essendo la sostituzione della SIM riferibile ad un soggetto terzo (la compagnia telefonica), essa rientra nel rischio tipico dell'attività d'impresa dell'intermediario, il quale si avvale di una modalità di autenticazione (SMS OTP) che affida in parte a terzi la procedura di autenticazione.

Nel caso di specie, vengono fornite prove idonee a comprovare che la truffa presenti effettivamente i caratteri tipici c.d. "*SIM swap fraud*", attraverso la quale terzi soggetti trasferiscono l'utenza telefonica del titolare su una nuova SIM al fine di porre in essere un'operatività fraudolenta, ad esempio ricevendo le password dinamiche OTP inviate a tale numero.

L'intermediario resistente ha chiesto, in via subordinata, l'applicazione della franchigia di legge. Tuttavia, si rappresenta che, nel caso di utilizzi fraudolenti on-line (come nel caso di specie), la richiesta di applicazione della franchigia formulata dall'intermediario "non può essere accolta […] in quanto la stessa è prevista in ipotesi di 'utilizzo indebito dello strumento di pagamento conseguente al suo furto, smarrimento o appropriazione indebita' (art. 12, co. 3 d.lgs. n.11/2010)" (cfr. decisione del Collegio di Coordinamento n. 22745 del 10 ottobre 2019) (cfr. anche pronuncia 24366/19)

In base agli orientamenti condivisi dei Collegi e in linea con quanto già enunciato da questo Collegio con riguardo alla medesima vicenda già sollevata dall'amministratore con riguardo all'operatività sul proprio conto personale (decisione n. 9749 del 23 giugno 2022), il ricorso risulta meritevole di accoglimento senza che debba procedersi ad ulteriori indagini circa l'eventuale colpa ascrivibile al cliente.

La parte ricorrente ha chiesto la corresponsione degli interessi legali dall'operazione al saldo. Sul punto, come da orientamento consolidato, il Collegio ritiene che debbano essere riconosciuti i soli interessi legali dal reclamo al saldo. Non si riconosce invece il compenso per l'assistenza legale avuto anche presente che il ricorrente non allega evidenza di parcelle o compensi a favore del difensore.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 29.260,00, 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
FLAVIO LAPERTOSA