COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) ACHILLE	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) CORNO	Membro di designazione rappresentativa degli intermediari
(MI) COLOMBO	Membro di designazione rappresentativa dei clienti

Relatore (MI) COLOMBO

Seduta del 09/11/2023

FATTO

Il Condominio istante, in persona del proprio amministratore, espone preliminarmente che i fatti oggetto di doglianza sono stati già enunciati nell'ambito di un precedente ricorso, presentato personalmente da esso amministratore, ricorso definito con decisione n. 9749/22 di questo Collegio, di totale accoglimento della domanda ivi spiegata.
Viene infatti allegato e documentato, anche nell'ambito del presente ricorso, che la persona fisica in questione, la quale svolge l'attività di amministratore di condomìni, ha subito una truffa del tipo *SIM swap fraud*, che aveva 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 e deciso in senso a lui favorevole), anche i conti correnti dei diversi condomìni da lui gestiti, tra cui quello odierno ricorrente.
In data 3 dicembre 2020, infatti, 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, sia a valere sul proprio conto personale, sia a valere sui conti dei condomìni amministrati.

Per quanto concerne il Condominio odierno ricorrente, si era trattato di una disposizione non autorizzata e dunque disconosciuta, dell'importo € 14.390,05.
Detto importo veniva in un primo tempo riaccreditato sul conto del Condominio, salvo buon fine, ma successivamente sarebbe stato riaddebitato.
Presentato inutilmente reclamo all'intermediario, a seguito dell'accoglimento del ricorso relativo al conto personale dell'amministratore, il Condominio ricorrente – nel richiamare le motivazioni contenute nella menzionata decisione Coll. Milano, n. 9749/22 – conclude affinché venga disposta la restituzione, a carico dell'intermediario convenuto, dell'importo di € 14.390,05, oltre interessi dal dovuto al saldo e spese rifuse.
Nelle proprie controdeduzioni l'intermediario conferma la titolarità, in capo al Condominio ricorrente, di un conto corrente abilitato alla piattaforma di *internet banking business*, gestita dall'amministratore (utente "Master"); tale utenza era collegata ad un numero di telefono intestato all'amministratore.
Proseguendo, la parte resistente allega che la c.d. utenza Master avrebbe effettuato un accesso al portale, tramite le credenziali di firma elettronica OTP virtuale, e che in data 1° dicembre 2020 è stato disposto il bonifico sopra menzionato, a valere sul conto del Condominio.
Sostiene l'intermediario che l'attivazione della *App* della banca su un telefono cellulare diverso da quello del cliente non potrebbe realizzarsi senza la cooperazione del medesimo, mediante la fornitura delle credenziali statiche e dinamiche a chi effettua l'*enrollment*.
Nel caso specifico l'operazione sarebbe stata correttamente contabilizzata, registrata e autenticata, in quanto posta in essere con il corretto inserimento delle credenziali.
Sussisterebbe, dunque, la colpa grave del cliente, che avrebbe violato gli obblighi contrattuali relativi alla corretta custodia delle credenziali necessarie all'accesso ai servizi di *home banking* e all'autorizzazione delle operazioni.
Dedotto inoltre che non sarebbero stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici, l'intermediario contesta le conclusioni della perizia informatica presentata dal cliente ed argomenta che la truffa c.d. SIM *swap fraud* si articolerebbe in una prima fase di *phishing*, durante la quale il frodatore acquisirebbe le credenziali del soggetto truffato con la collaborazione di quest'ultimo; solo nella fase successiva il truffatore otterrebbe una nuova SIM dall'operatore telefonico, soggetto peraltro estraneo rispetto all'intermediario.
La parte resistente, inoltre, contesta al cliente la tardività con la quale avrebbe reagito al messaggio ricevuto dal proprio operatore telefonico in data 30 novembre 2020, ciò che configurerebbe un ulteriore elemento da cui desumerne la colpa grave.
Conclude, dunque, per il non accoglimento del ricorso e, in subordine, per l'applicazione del concorso di colpa e della franchigia di legge.
In sede di replica, il Condominio ricorrente evidenzia anzitutto che le difese dell'intermediario risultano identiche a quelle già reputate infondate dal Collegio nell'ambito del ricorso relativo al conto personale dell'amministratore, nonché nell'ambito di altri ricorsi, presentati da altri Condomìni gestiti dallo stesso amministratore, relativamente alla stessa vicenda, a loro volta definiti con decisioni di accoglimento.
Contestata inoltre la valenza probatoria delle produzioni effettuate dall'intermediario con le controdeduzioni, il ricorrente deduce come non sia 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 sarebbe infatti sufficiente ad autenticarsi, grazie al possesso di una nuova SIM.

A riguardo, viene infatti richiamata la perizia di parte in atti, 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.
Inoltre, l'intermediario si sarebbe dovuto allertare del fatto che, in un arco temporale estremamente ristretto, venivano disposti bonifici per oltre € 600.000,00, dalla stessa piattaforma, da parte di oltre venti condomìni. Insiste, dunque, per l'accoglimento del ricorso.
Nelle controrepliche, la parte resistente ribadisce la valenza probatoria dei documenti prodotti con le controdeduzioni, ed insiste a sua volta per il rigetto del ricorso.

DIRITTO

Non è in contestazione tra le parti, e comunque è provato, che i fatti oggetto del presente ricorso siano stati già valutati nell'ambito della decisione n. 9749/22 di questo Collegio (nonché, successivamente, nell'ambito delle ulteriori decisioni n. 7062/23, n. 8550/23 e n. 9389/23, relative ai ricorsi di altri Condomini coinvolti nella stessa vicenda).
Deve dunque ribadirsi quanto in quelle sedi già statuito, e cioè che il cliente ha provato di essere stato vittima di una *SIM Swap Fraud*, perpetrata tra il 30 novembre 2020 ed il 2 dicembre 2020 (lasso temporale entro cui è stata effettuata la disposizione qui contestata).
La parte ricorrente ha infatti prodotto documentazione, proveniente dal gestore telefonico, che attesta le modalità in cui la truffa si è articolata. In particolare, il gestore telefonico ha dichiarato che l'utenza era stata bloccata, in seguito ad una segnalazione di smarrimento pervenuta al Servizio Assistenza Clienti il 30 novembre 2020, alle ore 14.11, da persona che si era presentata come l'intestatario, fornendone i dati anagrafici. Il cambio della SIM avveniva lo stesso giorno, alle ore 14.22, presso un punto vendita del gestore telefonico, dietro presentazione della denuncia di smarrimento della suddetta SIM e della carta d'identità.
Il cliente – nel presente ricorso, come in quelli già decisi dal Collegio in relazione alla posizione personale dell'amministratore ed a quella di altri Condomini da lui gestiti – ha dedotto di non avere mai fornito alcuno dei propri dati a terzi, né sarebbe peraltro dato offrire evidenza di tale assunto, in quanto prova meramente negativa. Il cliente ha poi allegato, anche nella denuncia ai C.C., che effettivamente il proprio numero si era improvvisamente bloccato e che quindi il messaggio ricevuto dalla Compagnia di avvenuto blocco non gli era parso erroneo o insidioso, pur non avendo egli previamente segnalato il guasto e richiesto il blocco. In buona fede si è quindi premurato di provvedersi di altra SIM, salvo poi accorgersi dei bonifici contestati. Il tutto, peraltro, avveniva in un contesto temporale ravvicinato di soli due giorni.
Ciò posto, deve dunque ribadirsi l'orientamento consolidato tra i Collegi, a mente del quale, qualora il cliente documenti di avere subito una truffa del genere di quella in discorso, non ne sia ravvisabile la colpa grave, posto che detta truffa risulta particolarmente sofisticata (cfr. anche Coll. Milano, n. 6758/21; Coll. Bari, n. 13285/21).
Come già statuito nella pronunzia n. 9749/22 di questo Collegio, relativa ai medesimi fatti, ma con riferimento alle disposizioni effettuate sul conto personale dell'amministratore, "*la valutazione congiunta e coerente di tutti i suesposti elementi e presunzioni consente di ritenere quindi che il ricorrente abbia positivamente assolto l'onere della prova a suo carico ex art 2967 c.c. dei fatti costitutivi la sua domanda vieppiù alla luce dell'orientamento limitativo delle pronunce della Suprema Corte (n. 10638/2016, 9721/2020). Secondo normativa (D.Lgs. n. 11 del 2010) e orientamento ormai dominante e condiviso, ove l'utente neghi di aver autorizzato un'operazione di pagamento, l'onere di provare la genuinità della transazione ricade essenzialmente sul prestatore del servizio e*

nel contempo obbliga quest'ultimo a rifondere il correntista, tranne ove vi sia un motivato sospetto di colpa grave o frode del cliente. E' l'intermediario che risponde dei danni conseguenti al fatto di non aver impedito a terzi di introdursi illecitamente nel sistema telematico del cliente mediante la captazione dei suoi codici di accesso e le conseguenti illegittime disposizioni di bonifico, se non prova la colpa o la frode dell'interessato. E' onere non dei correntisti, ma della Banca, dimostrare la riconducibilità dell'operazione al cliente e non al terzo così riconducendosi nell'area del rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente, la possibilità di una utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo. A tal riguardo si osserva allora e però che è ormai generalmente riconosciuto che le tecniche di acquisizione dei codici identificativi personali sono sempre più sofisticate e tali da rendere possibile l'acquisizione di tali dati da parte di terzi, a prescindere da qualsiasi forma di negligenza del titolare, potendo essere carpiti da archivi di banche come pure da reti telematiche sulle quali transitano flussi di informazione, così superandosi la eccezione che non è ricostruito come le credenziali di accesso e personali (oggetto di appropriazione: dati anagrafici, email, utenza telefonica, utenza home banking etc.) possano essere conosciute da persone diverse dal titolare. L'apprezzamento di quanto esposto, in un contesto di frode tecnicamente sofisticata, consente quindi di confutare la tesi a carico del ricorrente che non avrebbe sufficientemente presidiato le proprie credenziali, al fine di delineare profili di colpa grave a suo carico (art 10 secondo comma D.lgs 11/2010). In definitiva il condiviso orientamento dei Collegi comporta che nei casi di sim swap fraud il ricorso di rimborso venga accolto integralmente poiché in tale fattispecie la sostituzione della sim card va equiparata alla mancanza di autenticazione dell'operazione di pagamento ai sensi e per gli effetti dell'art. 10 del D.lgs. 11/2010".

La natura decisiva delle suesposte motivazioni – che qui si ribadiscono – consente dunque al Collegio di accogliere il ricorso, sulla scorta della c.d. ragione più liquida, senza entrare nel merito della valutazione degli elementi di prova forniti dall'intermediario, a proposito dell'utilizzazione o meno, nel caso specifico, di un sistema *compliant* con la normativa in materia di *Strong Customer Authentication* (c.d. S.C.A.).

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 14.390,00, oltre interessi 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
ROSSANA LO GRASSO