Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) PEDERZOLI	Membro designato dalla Banca d'Italia
(MI) BENINCASA	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) PEDERZOLI

Seduta del 09/12/2021

Esame del ricorso n. 1246844/2021 del 02/09/2021

proposto da [redacted]

nei confronti di [redacted].

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) PEDERZOLI	Membro designato dalla Banca d'Italia
(MI) BENINCASA	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) PEDERZOLI

Seduta del 09/12/2021

FATTO

Il ricorrente ritualmente espone di essere stato vittima di frode informatica sussumibile nella c.d *swim swap fraud* con riguardo allo specificato numero telefonico collegato al conto corrente *on line*, dichiaratamente ad uso personale (vedasi testualmente in ricorso e come risultante dal contratto di *internet banking* prodotto dal resistente) intrattenuto presso l'intermediario resistente.
Espone di essersi accorto di perdita di segnale dell'utenza telefonica verso le 19.30 del 16 luglio 2021, di avere contattato quindi il gestore telefonico da cui ha appreso che ignoti avevano attivato una nuova sim avente la stessa utenza, di avere provveduto quindi subito al blocco della utenza telefonica (così in denuncia ai C.C del 17 luglio 2021 ore 9.50)
Lamenta che peraltro nella notte si erano verificati ben 80 tentativi dispositivi dei quali 10 andati a buon fine per un importo di € 1.110, 00 complessivo (e comprensivo di commissioni) che disconosce, addebiti che scoperti il mattino successivo lo hanno determinato all'immediato blocco del conto tramite chiamata al numero verde.
Chiede il rimborso dell'intera somma, ritenendo insufficiente l'offerta del resistente (con email del 27 agosto 2021) di rifondergli il solo 50%.
Parte resistente espone che le operazioni eseguite con successo erano consentite dalla App "...enrollata nel telefono cellulare del presunto truffatore" ma che pur tuttavia l'installazione ed attivazione dell'App su un nuovo *device* non era potuta avvenire se non con l'inserimento dei codici personali del Cliente e che quindi il passaggio di credenziali aveva potuto operare o perché il titolare le aveva comunicate ovvero non le aveva

custodite diligentemente. Rileva in ispecie che l'indirizzo email riconducibile genuinamente al Cliente non è stato affatto compromesso dai presunti malfattori e che ai fini dell'enrollment dell'app del diverso device era stato necessario anche l'inserimento *in primis* del codice inviato proprio via email. Conclude quindi che "un maggiore presidio della casella di posta elettronica "avrebbe potuto evitare le operazioni fraudolenti con tempestivo blocco.
Ancora rileva che il blocco dell'utenza bancaria è stata disposta con chiamata al numero verde solo il 17 luglio 2021 dopo circa ventiquattro ore allorchè le operazioni erano già state eseguite ed addebitate.
Deduce di avere sempre sensibilizzato la clientela sul tema prevenzione frodi con la raccomandazione in particolare di non comunicare mai a nessuno le credenziali di accesso.
Eccepisce infine che dalla ricostruzione avversaria non risultano in modo chiaro né le modalità né le circostanze della supposta frode, e che della clonazione della Sim non vi sono elementi atti a comprovarla né sono prodotte evidenze relativa alla sostituzione della Sim
Chiede quindi il rigetto del ricorso.
Nella propria replica il ricorrente chiede che non vengano distratte dal conto ulteriori € 2.000,00 che l'intermediario nelle controdeduzioni ha prospettato come possibile futuro addebito, in quanto oggetto di un bonifico Sepa a terzi autorizzato su piattaforma/circuito diverso e annullato solo per errore operativo.
Nella controreplica il resistente deduce la novità e inammissibilità della domanda nuova, la mancanza di interesse attuale per un ipotetico danno non ancora verificatosi, la propria carenza di legittimazione passiva attesa la gestione del contratto da soggetto terzo.

DIRITTO

Osserva il Collegio che la stessa resistente nella già citata email del 27 agosto 2021 (dalla stessa prodotta) di riscontro al reclamo ,a seguito delle verifiche effettuate ed agli opportuni approfondimenti, ipotizza che la truffa perpetrata sia del tipo denominato "Sim Swap" che definisce avanzata tipologia di frode informatica articolata in vari passaggi : una volta individuata la vittima si procede all'acquisizione dei suoi dati e delle credenziali di *home banking* tramite tecniche di "hacking" ovvero di ingegneria sociale e successivamente , utilizzando documenti falsificati *ad hoc* , si sostituisce la Sim card della vittima e, attraverso lo stesso numero telefonico , si dispongono le operazioni fraudolenti tramite applicazione telefonica necessaria per operare sul conto corrente on line . Prosegue la resistente: "Le *analisi poste in essere sulle dinamiche con cui le operazioni fraudolente sono state effettuate non hanno evidenziato anomalie nei sistemi di sicurezza, infatti i codici autorizzativi sono stati inviati correttamente all'utenza telefonica. Nulla poteva far supporre che la sim card presente nel suo cellulare fosse stata duplicata da malfattori e utilizzata su altro dispositivo mobile non in suo possesso. È ipotizzabile che i truffatori abbiano in qualche maniera carpito alcuni suoi dati (dati anagrafici, email, utenza telefonica, utenza home banking ecc) ed abbiano quindi potuto procedere all'installazione dell'applicazione per poter effettuare le operazioni fraudolente.*"
La resistente stessa dà quindi per "*accertato lo SWAP della Sim telefonica*".
La tesi allora sostenuta in questo procedimento dalla resistente che addebita al Cliente una non sufficiente ricostruzione della fattispecie si appalesa defatigatoria.
Il ricorrente ha dedotto di non avere mai dato alcuno dei suoi dati a terzi e non è dato offrire dell'assunto prova, in quanto prova meramente negativa.

Il ricorrente ha allegato, anche in denuncia ai C.C, di avere appreso dall'operatore telefonico proprio l'avvenuta attivazione di altra Sim da parte di ignoti e di aver bloccato quella sera stessa l'utenza telefonica, e lo stesso Istituto riconosce che proprio quella sera stessa è avvenuto il nuovo *enrollement* dell'App.
L'intermediario conferma che le operazioni disconosciute sono seguite all' *enrollment* dell'APP e che l'*enrollment* dell'App è avvenuto attorno alle 20:21 del 16 luglio 2021, con inserimento di codice ID, password e OTP inviato via sms al cellulare certificato.
Fino a quella data l'utente aveva invece utilizzato il Token "enrollato" in data 04/11/2020 sul suo *device.*

Dopo il nuovo *enrollment* l'utente truffaldino ha creato un PIN dispositivo e ha certificato l'APP con l'inserimento di un codice inviato alla e-mail del cliente.
All'*enrollment* appena eseguito sono seguiti subito in successione numerosi e consecutivi (circa 80) accessi all'APP e operazioni tentate di cui appunto 10 comunque utilmente portate a termine e addebitate in conto, senza alcun previo blocco del sistema nel contesto indiziario.
Il ricorrente afferma di avere bloccato la propria utenza appena appreso dal gestore della duplicazione della SIM. La prospettazione trova ulteriore conferma nella tracciatura sms fornita dalla banca, da cui si ricava che, dopo quello delle 20:55 del 16 luglio, nessun altro messaggio è stato recapitato al destinatario per tutta la durata dell'attacco dei frodatori.
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.
È 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.
È 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 (la stessa banca, come sopra visto, le elenca come oggetto di appropriazione : dati anagrafici, email, utenza telefonica , utenza home banking ecc) 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 resistente 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.
Quanto poi alla residua domanda proposta in sede di replica dal ricorrente, di cui riferito nella parte in fatto, si rileva che è orientamento costante in punto dell'ABF che una domanda è inammissibile quando è stata presentata per la prima volta, ed esclusivamente, in sede di repliche, come nel caso in esame. Nella fattispecie meritano seguito anche le eccezioni difensive della ricorrente di mancanza di interesse attuale per conseguire il rimborso in relazione ad ipotetico danno non ancora verificatosi e meramente possibilistico.
Quanto alla domanda del ricorrente di rimborso spese di difesa, si ritiene che la stessa non sia documentata né nell'*an* né nel *quantum* e quindi non meriti seguito.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.110,00.
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