Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) TINA

Seduta del 22/12/2022

FATTO

Nel ricorso presentato all'Arbitro, il ricorrente riferisce quanto segue:

- è cointestatario del rapporto di conto corrente n. 431[***]529 e unico titolare del rapporto di conto corrente n. ***571 attivi presso l'intermediario resistente;
- il 29/03/2022, alle ore 14:08, riceveva, in coda ai messaggi genuini, un sms riconducibile all'intermediario con il quale veniva invitato a cliccare su un link per riattivare la sua carta/conto limitata/o per "*mancata verifica della sicurezza web*" e al quale non dava seguito;
- alle ore 16:28 dello stesso giorno riceveva un secondo messaggio, sempre in coda ai precedenti, con il quale gli veniva anticipato l'arrivo di una telefonata da parte di un operatore della banca "*in merito alla nuova sicurezza web*";
- alle ore 16:29 riceveva, dal numero verde dell'intermediario, la preannunciata telefonata nel corso della quale, un presunto operatore della banca, nell'informarlo della necessità di aggiornare "*il profilo clienti dell'applicazione*", lo induceva ad installare sul proprio cellulare una nuova applicazione da scaricare tramite l'utilizzo di un nuovo messaggio inviato sempre nella stessa chat telefonica dell'intermediario;

- tratto in inganno dall'apparente legittima provenienza della telefonata e dei messaggi (tutti scritti in corretto italiano e pervenuti in coda a quelli genuini della banca, oltre che apparentemente collegati ai contenuti di un messaggio genuino inoltrato dalla banca del 15/03/2022) e ottenute dal finto operatore rassicurazioni circa l'idoneità di quanto consigliato, provvedeva a scaricare la nuova applicazione denominata "*Banca Sicura*" del tutto simile, nella grafica, a quella dell'intermediario resistente;
- sempre su indicazione del presunto operatore e al fine di confermare la propria identità, senza comunicare alcun codice effettuava l'accesso alla propria App e, dopo averla chiusa, provvedeva a disinstallarla;
- il presunto operatore, nell'informare il ricorrente di aver riscontrato dei problemi nell'installazione della nuova applicazione, gli fissava un ulteriore appuntamento telefonico per il giorno successivo;
- nei giorni 30/03/2022 e 31/03/2022, il ricorrente riceveva altre telefonate dallo stesso numero nel corso delle quali si ripeteva "*la medesima operazione*" nel tentativo di installare la nuova applicazione con uso di ulteriori sms sempre pervenuti nella chat dell'intermediario resistente;
- nel corso della telefonata del 31/03/2022 il sedicente operatore, a causa del mancato funzionamento della app, effettuava su sua richiesta un pagamento di F24 per Euro 173,81, senza la preventiva comunicazione di alcun codice;
- in data 01/04/2022, il ricorrente si recava presso gli uffici dell'intermediario resistente e in tale occasione apprendeva di essere caduto vittima di frode e che nelle date del 30 e 31 marzo 2022 erano stati eseguiti due bonifici non autorizzati dell'importo di Euro 24.997,00 ed Euro 29.910,00;
- verso le ore 14:17 dell'1/04/2022, quindi entro le 24 ore dall'esecuzione dell'ultimo bonifico, il ricorrente provvedeva a disconoscere le due operazioni, chiedendo anche espressamente il blocco dei propri conti correnti e, nello stesso giorno presentava denuncia alle autorità;
- il lunedì successivo (04/04/2022) l'intermediario lo informava che i codici di accesso alla home banking sarebbero stati disattivati;
- in data 11/04/2022 apprendeva però dell'avvenuta illegittima esecuzione di ulteriori tre operazioni di ricarica carta per l'importo complessivo di Euro 150,00 (Euro 50,00 ciascuna) effettuate in data 01/04/2022 e addebitate sul conto il 06/04/2022;
- l'effettivo blocco dei codici di accesso al servizio di Home banking veniva apposto dall'intermediario solo in data 11/04/2022;
- in data 3/05/2022 avanzava infruttuosamente reclamo al fine di ottenere la restituzione delle somme sottratte;

Il ricorrente ha, inoltre, contestato: la mancata ricezione dei messaggi di *alert* riferiti ai bonifici in contestazione; il tardivo blocco dell'operatività da parte dell'intermediario; l'elevato importo dei bonifici rispetto all'ordinaria operatività; l'inadeguatezza del sistema di autenticazione predisposto dall'intermediario. fondato sull'utilizzo di un codice pin fisso su "tastiera sicura" invece che sull'uso dell'OTP dinamico normativamente previsto.

Il ricorrente ha, quindi, chiesto il rimborso dell'importo complessivo di Euro 54.907,00, corrispondente alle due operazioni non autorizzate, oltre a Euro 150,00 per le tre operazioni di ricarica.

Con le proprie controdeduzioni, l'intermediario resistente ha precisato quanto segue:

- ha fornito riscontro al reclamo in data 21/05/2022;

- ha riconosciuto al cliente, con successiva nota del 17/08/2022, il rimborso della somma di Euro 150,00 relativa alle tre operazioni di ricarica telefonica effettuate nelle more che i blocchi apposti sul conto fossero resi operativi;
- il cliente, unitamente alla cointestataria intervenuta nel ricorso, è intestatario di conto corrente collegato al servizio di home banking, con attivato il servizio di sms Alert;
- il sevizio di home banking prevede l'accesso alle funzioni informative e dispositive mediante sistema di autenticazione forte in linea con la normativa PSD2, come riconosciuto dall'orientamento dei Collegi ABF;
- per effettuare il login da APP è necessario inserire le credenziali di sicurezza (numero cliente +PIN) più il codice OTP;
- per disporre le operazioni una volta inserite le stesse devono essere confermate con l'inserimento del PIN e il codice OTP;
- l'OTP è valido solo per l'operazione richiesta e viene generato in modo silente dal Mobile token integrato nell'APP che il cliente ha attivato sul proprio device; il testo della notifica appare sul device ed indica in chiaro l'operazione che si sta autorizzando, su di essa il cliente deve fare "tap" per autorizzare;
- l'attivazione del mobile Token avviene con autenticazione forte attraverso la digitazione delle credenziali di sicurezza (numero cliente +PIN) e del codice OTP inviato per SMS;
- in data 29/03/2022 alle ore 16:42 al cellulare del cliente è stato inviato sms contenente l'OTP necessario all'attivazione del Mobile Token;
- a fronte di tale messaggio il cliente avrebbe dovuto interrompere la chiamata e rivolgersi al servizio clienti della banca e soprattutto non avrebbe dovuto comunicare a nessuno il codice OTP ricevuto con l'sms;
- al fine di prevenire le frodi la banca da tempo pubblica, nella pagina di accesso al portale sull'App e sugli schermi degli ATM, raccomandazioni per l'utilizzo dei canali telematici e con i quali si avverte la clientela anche del fatto che nessun dipendente chiederà mai le credenziali di sicurezza;
- le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto risulta che le operazioni sono avvenute con il corretto inserimento delle credenziali, in assenza di anomalia;
- dalla ricostruzione fornita dal cliente si evince come lo stesso assecondando una persona sconosciuta abbia incautamente cliccato sul link contenuto nel primo sms ricevuto (senza alcun riferimento alla banca) e poi su un secondo link di altro messaggio, consentendo così l'installazione di App non ufficiale in sostituzione della precedente e consegnando di fatto il proprio strumento di pagamento al frodatore;
- il cliente avrebbe dovuto invece insospettirsi e interpellare la banca anche per aver notato il blocco dell'attività di messaggistica sul proprio cellulare;
- quanto poi al canale di provenienza degli sms truffa riconducibile all'intermediario è risaputo che con pochi passaggi è possibile modificare il mittente di un numero telefonico da parte di terzi;
- è evidente che il cliente ha abboccato ad un sms di phishing e a una telefonata di uno sconosciuto, installando addirittura una nuova app estranea alla Banca, incorrendo così in colpa grave come anche confermato dalle decisioni ABF;
- la diffusione del fenomeno è tale che i Collegi ABF ormai ritengono da tempo che l'impiego di una media diligenza sia sufficiente a impedire la truffa;

- a fronte dell'operatività disconosciuta sono stati inviati e consegnati al cliente le notifiche push e gli sms alert delle operazioni;
- il cliente avrebbe dovuto notare il tenore palesemente diverso del messaggio civetta rispetto agli sms genuini di cui anche nel ricorso il cliente riporta a titolo di esempio e privo di qualsiasi link;
- venuto a conoscenza delle operazioni fraudolente, ha attivato senza successo l'azione di recall nei confronti dell'intermediario del beneficiario;
- l'importo delle operazioni non può essere considerato elemento anomalo rispetto l'ordinaria operatività del cliente in quanto nessuna modifica del plafond è stato effettuato dal cliente e la banca non può limitare l'utilizzo del cliente.

DIRITTO

La questione rimessa all'esame del Collegio riguarda l'esecuzione di due operazioni di pagamento (due bonifici) effettuate on-line, tramite il servizio home banking dell'intermediario resistente, per un importo complessivo di Euro 54.907,00. Il ricorrente riferisce, in sintesi, di essere rimasto vittima di un episodio di spoofing avvenuto in data 29-31 marzo 2022. Le operazioni contestate dal ricorrente, avvenute il 30 e il 31 marzo 2022, sono, quindi, assoggettate alle disposizioni del D.lgs. n. 11/2010 nella versione oggi vigente.
Ciò premesso, giova precisare che, per l'ipotesi di disconoscimento di operazioni da parte del cliente, l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.
Nel caso di specie, sotto il primo profilo, l'Intermediario resistente ha fornito piena prova circa l'adozione di un adeguato sistema di sicurezza a due fattori e la corretta autenticazione delle operazioni disconosciute dal ricorrente, secondo i criteri e i parametri richiesti dalla SCA.
Per quanto attiene, invece, alla condotta tenuta dal ricorrente, in relazione alla fattispecie di sms spoofing, truffa particolarmente insidiosa consistente nell'invio di sms dall'utenza dell'intermediario, i Collegi sono unanimi nel ritenere che non sia generalmente ravvisabile la colpa grave del cliente, a meno che non si rinvengano degli indici di inattendibilità (quali, ad esempio, errori grammaticali o sintattici) o anomalia del messaggio (quali, ad esempio, l'invito a selezionare un link in nessun modo riferibile all'intermediario); in tale caso, potrà essere ravvisato un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa, similmente a quanto avviene negli episodi di phishing e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario.
Con riguardo al caso di sms spoofing in oggetto, si rileva che:

- il cliente versa in atti screenshot dell'SMS civetta e dei successivi SMS, i quali risultano memorizzati dal cellulare con la medesima denominazione presente nei messaggi genuini dell'intermediario;
- il messaggio c.d. civetta, seguito nella medesima chat da messaggi 'genuini' dell'intermediario resistente, presenta un link non immediatamente riconducibile al dominio di quest'ultimo.

Con riferimento al lamentato *ID caller spoofing/*vishing, il ricorrente produce evidenza della chiamata ricevuta, con l'indicazione di un numero telefonico riferibile all'intermediario resistente.

Per quanto riguarda, infine, la mancata ricezione di messaggi di sms alert relativi alle operazioni disconosciute, che, nel caso di specie, avrebbero effettivamente consentito con tutta probabilità al ricorrente di impedire l'esecuzione del secondo bonifico (effettuato a distanza di circa 24 ore dal primo), l'intermediario resistente produce evidenza dei messaggi inviati al ricorrente, all'utenza cellulare dallo stesso indicata in ricorso, così superando la contestazione del ricorrente.

Alla luce del quadro complessivo ora delineato, il Collegio, valutata la gravità delle rispettive colpe in relazione ai fatti illustrati e documentati, ritiene, dunque, di doverle ripartire nella misura del 50% per ciascuna delle parti. L'intermediario dovrà quindi rimborsare al ricorrente l'importo di Euro 27.454,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 27.454,00.

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