Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) ACHILLE	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) PANZANI	Membro di designazione rappresentativa degli intermediari
(MI) BANI	Membro di designazione rappresentativa dei clienti

Relatore (MI) BANI

Seduta del 7/03/2023

FATTO

Con ricorso depositato in data 21 ottobre 2022 parte ricorrente afferma che:

- in data 21/09/2021 alle ore 19.55 l'amministratore della società riceveva un sms apparentemente proveniente dall'intermediario con cui veniva invitato ad aggiornare le utenze bancarie tramite link; sul cellulare su cui veniva ricevuto l'sms era installata la app della banca e trattavasi dell'utenza cui era associato l'home banking della società;
- nell'aprile 2021 il conto della società era stato bloccato per mancato aggiornamento delle credenziali: all'epoca era stato ricevuto un sms di tenore analogo a quello rivelatosi truffaldino;
- avere cliccato sul link e ricevuto una telefonata da un sedicente operatore della banca;
- si era accorto della truffa per avere ricevuto una notifica contenente un codice da inserire per autorizzare una operazione di ricarica che il cliente non stava in realtà eseguendo;
- aveva bloccato immediatamente il conto;
- aveva presentato reclamo, cui l'intermediario aveva risposto negativamente.

Sulla base di tali assunti, parte ricorrente formula la seguente domanda:

"Richiesta di rimborso della somma di € 1.459,00 fraudolentemente sottratta al cliente".

L'Intermediario afferma che:
- il cliente è stato vittima di phishing/smishing;
- nell'aprile 2021 non è stato bloccato l'accesso all'home banking della società cliente;
- le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto risulta che le operazioni sono avvenute con il corretto inserimento delle credenziali;
- sussiste la colpa grave del cliente che ha cliccato sul link truffaldino e seguito le istruzioni del finto operatore.

In forza di tutto ciò l'intermediario così conclude:
"Considerato dunque tutto quanto sopra esposto, la scrivente chiede all'Arbitro adito di rigettare interamente il ricorso perché infondato in fatto ed in diritto".

In sede di repliche, il cliente precisa che;
- non ha fornito le proprie credenziali bancarie e i codici, neppure quello per l'enrollment di un nuovo device;
- la app bancaria non consente di accedere al conto, che viene gestito unicamente dal sito di home banking;
- l'operazione fraudolenta è stata preceduta da altra non andata a buon fine, per la quale non sono state ricevute notifiche push che avrebbero invece consentito al cliente di bloccare tempestivamente il conto;
- l'intermediario non ha adempiuto al proprio onere probatorio.

In sede di controrepliche, l'intermediario precisa che:
- il cliente ha manipolato le affermazioni contenute nelle controdeduzioni: non corrisponde al vero che vi è stata una manipolazione del sistema;
- la registrazione di un nuovo dispositivo è avvenuta con la cooperazione del cliente che ha comunicato il codice OTP al truffatore;
- il blocco è avvenuto alle ore 20.07 del giorno della truffa;
- il tentativo di eseguire un'operazione da € 3.000,00 è avvenuto dopo l'enrollment della app e prima dell'operazione poi andata a buon fine;
- la app è stata nuovamente "enrollated" sul device del cliente, sovrascrivendo quella dei truffatori.

DIRITTO

L'operazione che il ricorrente disconosce e che per l'intermediario sarebbe stata invece correttamente contabilizzata registrata e autenticata, è riconducibile alla fattispecie di spoofing: un raggiro per cui si viene raggiunti sa un sms truffaldino, inserito in una chat riferibile all'intermediario, che invita ad accedere ad un link. Si viene poi contattati telefonicamente e seguendo le istruzioni si consente ai truffatori di sottrarre somme di denaro. Nonostante la diffusione di campagne informative, secondo gli orientamenti dei Collegi, questa fattispecie conserva ancora carattere di insidiosità. Nel caso di specie non solo non sembra potersi ritenere sussistente la colpa grave del cliente, che viene usualmente desunta attraverso indici di anomalia delle comunicazioni ricevute dallo stesso

(ad esempio dall'inequivoca non riconducibilità all'intermediario del link contenuto nel messaggio civetta nonché da evidenti errori grammaticali o di sintassi sempre contenuti nel messaggio civetta), ma non risulta provata a monte l'esistenza dell'autenticazione forte richiesta dalle norme applicabili al caso di specie. Con riferimento alla strong customer authentication (cd. SCA) le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA.
In merito ai fattori di autenticazione, nel caso di specie risulta documentato l'utilizzo del codice OTP trasmesso via sms al numero di cellulare dell'amministratore della società come anche riportato in denuncia: la trasmissione dell'sms ha avuto esito positivo, come da spunta verde indicata nel log e come anche risultante nello stesso screenshot prodotto dal cliente, ma in merito al secondo fattore, dai log prodotti non è possibile verificare quale fattore sia stato richiesto ai truffatori e pertanto non viene data dall'intermediario la prova della SCA

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.450,00.

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