

**COLLEGIO DI MILANO**

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TENELLA SILLANI	Membro designato dalla Banca d'Italia
(MI) MINNECI	Membro designato dalla Banca d'Italia
(MI) FERRETTI	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - MINNECI UGO

Seduta del 05/10/2021

**FATTO**

Parte ricorrente riferisce:

- di essere titolare del conto corrente n.\*\*\*957 acceso presso l'intermediario;
- che in data 13.03.2021, alle ore 12:40, riceveva sul cellulare un SMS proveniente apparentemente dai canali ufficiali dell'intermediario, che la invitava ad accedere ad un sito per evitare il blocco delle proprie utenze bancarie;
- che, ingannata dal mittente del messaggio, cliccava sul link ivi contenuto;
- che, subito dopo, veniva contattata da un sedicente operatore dell'intermediario che la aiutava nella procedura di aggiornamento;
- che, in buona fede, seguiva le indicazioni del truffatore e disinstallava la App dal device;
- che, in seguito, scopriva che ignoti avevano compiuto operazioni non autorizzate con conseguente addebito sul conto corrente per € 1.490,00 tramite la carta n.\*\*\*340 ed € 1.490,00 tramite della carta n.\*\*\*439;
- di aver provveduto prontamente a bloccare le carte;
- di non aver fornito alcun codice o password al sedicente operatore telefonico, bensì di essersi limitata esclusivamente a disinstallare la App R\*\*\*;
- che la frode è stata perpetrata tramite sofisticati metodi di intrusione grazie alla perfetta inserzione nell'ambiente informatico originale;
- che, difatti, gli sms alert ricevuti ed il messaggio civetta risultano inviati tramite il medesimo canale;



- che vi è un unico beneficiario per tutte le operazioni fraudolente;
- che vi è una falla nel sistema informatico della banca e che pertanto è di quest'ultima la responsabilità della riuscita della truffa.

Ciò posto, chiede la retrocessione delle somme fraudolentemente sottratte.

In sede di controdeduzioni, l'intermediario convenuto sottolinea che:

- la ricorrente chiede il rimborso di una serie di operazioni effettuate tramite carta di credito e carta di debito alla stessa intestate a seguito di episodio di smishing e successivo vishing;
- prima del blocco delle carte, venivano effettuate operazioni fraudolente per un ammontare totale di euro 2.900;
- in particolare, con la carta di credito veniva effettuata un'operazione di euro 1.490,00 e con la carta di debito venivano effettuate 5 operazioni, rispettivamente di euro 490,00, euro 240,00, euro 240,00, 100,00 e 340,00;
- presso la Banca sarebbero in essere sistemi di autenticazione forte (SCA) e la modalità di utilizzo risponderrebbe ai requisiti PSD2;
- le operazioni contestate sarebbero state eseguite in assenza di anomalie con la corretta ed immediata digitazione delle credenziali delle carte originali;
- che a fronte delle operazioni contestate, la ricorrente avrebbe ricevuto i relativi sms alert;
- la ricorrente sarebbe stata vittima di un episodio di smishing/vishing originato in particolare da un sms ricevuto dalla cliente, apparentemente proveniente dalla sua banca (sms spoofing), nel quale era contenuto l'invito ad utilizzare un link appositamente generato dai terzi malfattori;
- la palese inattendibilità del messaggio avrebbe dovuto indurre parte ricorrente a non dar seguito alle istruzioni comunicate dal falso avviso;
- che da tempo tramite i propri canali ufficiali (sito internet, e-mail, sms, push notification su App ed estratto conto) ha fornito alla propria clientela le indicazioni per riconoscere i tentativi di phishing/vishing;
- la cliente avrebbe fornito le credenziali richieste da presunto operatore, vanificando così la predisposizione di qualsivoglia meccanismo di sicurezza.

Insiste pertanto per il rigetto del ricorso.

## DIRITTO

Nell'affrontare la presente controversia, occorre preliminarmente sottolineare l'assoggettabilità della stessa alla disciplina di cui al decr. lgs. n. 11/2010 nella versione oggi vigente; risultano infatti contestate cinque operazioni di pagamento per un ammontare complessivo di Euro 2.900,00, eseguite il 13 marzo 2021.

Sempre *in limine*, deve segnalarsi che parte ricorrente riferisce di essere rimasta vittima di un episodio di spoofing misto a vishing. A tale riguardo, preme fin da subito notare che agli atti non vi è evidenza del messaggio truffaldino ricevuto dalla cliente e tanto meno della riconducibilità della successiva telefonata a una utenza riconducibile a un numero ufficiale dell'intermediario convenuto. D'altro canto, anche per il tipo di operazione che la stessa parte ricorrente riferisce di avere compiuto attraverso il sedicente operatore dell'intermediario convenuto (disattivazione di un App), è del tutto ragionevole presumere che siano stati comunicati codici Otp.

Tutto ciò premesso, mette conto di precisare che, per l'ipotesi di disconoscimento di operazioni da parte del cliente, il suddetto decreto fissa – all'art. 10 – un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e



Arbitro Bancario Finanziario  
Risoluzione Stragiudiziale Controversie

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.

Ora, con riguardo al caso di specie, può considerarsi acquisita la prova richiesta dal comma 1 dell'art. 10, avendo l'intermediario offerto idonea documentazione informatica in ordine alla corretta registrazione, autenticazione e contabilizzazione delle operazioni contestate.

D'altro canto, di fronte alla mancata allegazione di evidenze tali da far presumere una oggettiva confondibilità in ordine alla provenienza tanto del messaggio sms quanto della successiva chiamata telefonica, il fatto (ammesso dalla stessa cliente) di aver dato seguito ad entrambi induce a ravvisare nella condotta tenuta dalla ricorrente l'elemento della colpa grave.

Il ricorso non può pertanto trovare accoglimento.

### **PER QUESTI MOTIVI**

**Il Collegio non accoglie il ricorso.**

IL PRESIDENTE

Firmato digitalmente da  
FLAVIO LAPERTOSA