

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) DENOZZA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) PERSANO	Membro di designazione rappresentativa dei clienti

Relatore NICOLA RIZZO

Seduta del 06/06/2024

FATTO

Il cliente, nel ricorso, afferma quanto segue:

- che, in data 26/04/2023, ignoti hanno potuto eseguire 5 ordini di pagamento a favore di terzi con la carta di debito emessa dall'intermediario e collegata al conto corrente del cliente per un importo complessivo di € 1.946,02;
- che, in precedenza alle operazioni non riconosciute, aveva ricevuto sulla sua utenza telefonica un SMS apparentemente riconducibile all'intermediario con il quale veniva informato del blocco della sua carta di pagamento e che di lì a breve sarebbe stato contattato da un operatore;
- di essere stato poi contattato da un sedicente operatore dell'intermediario il quale segnalava tentativi di pagamento non autorizzati, chiedendo di comunicare i codici che pervenivano via SMS al suo dispositivo;
- di aver appreso in data 26/04/2023 di 5 operazioni di pagamento eseguite con la sua carta collegata al suo conto corrente, senza che il cliente stesso avesse mai aperto alcun link né autorizzato alcun accesso al suo home banking;
- che l'intermediario non ha provato di aver adottato un sistema di autenticazione forte.

Il ricorrente domanda, pertanto, il risarcimento del danno per la somma complessiva di € 1.946,02.

Nelle controdeduzioni, l'intermediario, riportato il fatto, afferma quanto segue:

- che il cliente è stato vittima di “phishing” / “vishing”; con il ricorso, lamenta l'appropriazione indebita in data 26/04/2023 di fondi pari a € 1.946,02 mediante diverse transazioni a valere sul proprio saldo di moneta elettronica n. EM001***325;
- che le operazioni contestate sono state correttamente autenticate e contabilizzate nonché autorizzate personalmente dal cliente dal proprio dispositivo mobile in uso; ne deriva dunque che ci si trova di fronte ad una fattispecie alla quale, secondo l'orientamento generale dei collegi dell'Arbitro Bancario Finanziario, non si applica la disciplina delle operazioni di pagamento non autorizzate né, in particolare, i reciproci obblighi previsti dagli artt. 7 e ss. del d.lgs. 27 gennaio 2010, n. 11 (e successive modifiche);
- che, nel caso in esame, risulta infatti palese il consenso del cliente, il quale, come da lui stesso ammesso nella denuncia sporta alle autorità, ha provveduto ad accettare la notifica ricevuta sul proprio dispositivo mobile per autorizzare i pagamenti, sia pur indotto a ciò dal raggirio operato da terzi;
- che la ricostruzione dei fatti nel ricorso e nella denuncia è contraddittoria;
- che il riferimento telefonico di rete mobile indicato dal cliente nella denuncia non è in alcun modo riconducibile all'intermediario;
- che, in forza delle condizioni contrattuali sottoscritte dal cliente, l'intermediario enuncia espressamente di essere estranea ai rapporti e alle controversie relative ai beni e/o servizi acquistati;
- che le operazioni contestate sono state eseguite entro i limiti di spesa contrattualmente previsti;
- che non si rilevano indizi di anomalia poiché non sono presenti tentativi di cambio device o password, avendo il cliente eseguito l'accesso dal proprio dispositivo mobile in uso da tempo tramite le proprie credenziali;
- che il servizio SMS alert era attivo;
- che la banca ha inviato numerose mail al cliente specifiche sull'argomento; inoltre, al fine di raggiungere e sensibilizzare il maggior numero di clienti possibile, ha anche predisposto, sul tema di prevenzione frodi, determinati messaggi che, con cadenza regolare, invia ai clienti attraverso specifiche notifiche push che giungono sui dispositivi mobile dei clienti stessi.

L'intermediario convenuto domanda, quindi, il rigetto del ricorso in quanto infondato in fatto e in diritto.

DIRITTO

Oggetto della presente controversia sono alcune operazioni contestate, per un importo complessivo di € 1.946,02, poste in essere il 26/04/2023. Il ricorrente fornisce evidenza di n. 4 operazioni il cui importo complessivo è pari a € 1.946,02, ovvero la somma domandata con il ricorso. Alla data delle operazioni trovava applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018.

È in atti la denuncia del cliente presentata in data 11.06.2023.

In via preliminare, l'intermediario eccepisce che le operazioni contestate sono state autorizzate personalmente dal ricorrente dal proprio dispositivo mobile in uso. Dalle dichiarazioni rese dal cliente, si osserva che quest'ultimo nel ricorso e nell'allegato reclamo dichiara di aver comunicato al truffatore i codici OTP SMS che riceveva al suo

numero di cellulare. Nella denuncia, invece, afferma di aver “autorizzato le notifiche che arrivavano”.

Dai documenti agli atti di questo procedimento – e considerati anche i limiti istruttori dei giudizi di fronte a questo Collegio arbitrale – le operazioni possono considerarsi in parte autorizzata dal cliente. Secondo l’orientamento dei Collegi ABF, se il concorso causale dell’utente in fase dispositiva e/o autorizzativa è parziale, la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di “consenso”, dispone che quest’ultimo dev’essere prestato nella forma convenuta tra il pagatore stesso e il PSP.

Con riferimento all’accesso all’account del cliente, l’intermediario spiega che il giorno 26 aprile 2023 veniva registrato un accesso all’internet banking del cliente dallo stesso dispositivo in uso dal cliente mediante impiego del parametro biometrico. Dai LOG prodotti dal ricorrente emerge un login (Loginfast) alle ore 18:48 del 26/04/2023 dal device f382***01f6 in uso al cliente e associato al codice internet banking 03385769 (codice “IB CODE”); emerge, inoltre, l’univocità del device per gli accessi in precedenza effettuati. Quanto ai fattori di autenticazione utilizzati, l’intermediario spiega che l’accesso è stato effettuato mediante il dispositivo del cliente (elemento di possesso) e riconoscimento biometrico (elemento di inerenza).

Con riferimento alle operazioni contestate, l’intermediario allega, inoltre, evidenza dei LOG delle transazioni eseguite con la carta di pagamento di titolarità del cliente e relativa legenda dalla quale emerge che le operazioni in oggetto sono state autorizzate con protocollo 3DS2.0 tramite metodo di autenticazione “challenge” consistente nella richiesta di una Strong Customer Authentication con l’utilizzo di due fattori di sicurezza (notifica push e tap sulla medesima).

Dall’analisi delle evidenze agli atti si ricava quanto segue: risulta essere sussistente il primo fattore di autenticazione costituito dal dispositivo del cliente associato all’App della banca e sul quale è stata inviata la notifica push (elemento di possesso); quanto al secondo fattore di autenticazione utilizzato, l’intermediario si limita a dire che l’operazione è stata autorizzata tramite “strong customer authentication con l’utilizzo di due fattori di sicurezza”, ossia la notifica push su dispositivo mobile e “tap” sulla medesima, ovvero sia due elementi riconducibili alla stessa tipologia di fattore, il fattore di possesso. L’intermediario non specifica se alla notifica push abbia fatto seguito l’inserimento di un PIN (fattore di conoscenza) o l’utilizzo di una impronta digitale (fattore di inerenza).

Si deve rilevare, tuttavia, che il cliente, con riferimento alla fase autorizzativa delle operazioni contestate, ammette in denuncia di “aver autorizzato le notifiche che arrivavano”. La dichiarazione confessoria del cliente consente, pertanto, di ritenere raggiunta la prova dell’autenticazione forte delle operazioni contestate, ex art. 10 del D.lgs. n. 11 del 2010.

Il cliente riferisce nella denuncia di aver ricevuto in data 26/04/2023 un SMS apparentemente proveniente dall’intermediario con il quale veniva informato che la sua carta di pagamento era stata bloccata per motivi di sicurezza e che di lì a breve sarebbe stato contattato da un operatore.

Dalle evidenze dei messaggi, prodotte agli atti dal ricorrente, emerge: che, in data 24 aprile 19:15 e 26 aprile 18:34, risulta la ricezione di due SMS inseriti all’interno della chat ufficiale dell’intermediario aventi identico contenuto con i quali il cliente veniva informato del blocco della carta e che di lì a breve sarebbe stato contattato da un operatore; i predetti SMS non contengono alcun link e sono scritti in un italiano corretto; che risultano, in coda, degli SMS genuini contenenti i codici OTP relativi a solo due operazioni di pagamento (quella di € 779,00 e quella di € 693,00) che risultano essere “parlanti”, ovvero contenenti i dettagli dell’operazione che si andava ad autorizzare, l’importo e l’esercente e

4 SMS “fasulli” relativi all’avvenuto storno delle 4 operazioni di pagamento; che risultano altri due SMS “fasulli” con i quali il cliente veniva informato dell’apertura della pratica di storno delle operazioni fraudolente e della chiusura di detta pratica.

Da quanto precede emerge, pertanto, come la truffa in esame rientri nella fattispecie del c.d. spoofing. Al riguardo si ha presente che secondo l’orientamento condiviso dei Collegi ABF, deve ritenersi che allo stato, nonostante la maggiore diffusione di campagne informative sul tema, lo spoofing conservi ancora il carattere di insidiosità, in particolare con riferimento alle comunicazioni in apparenza provenienti dagli intermediari che inducono il cliente ad abbassare la sua soglia di attenzione. Ciò porta a qualificare come parzialmente scusabile la condotta colposa del cliente, attenuandone la rimproverabilità, con il conseguente riconoscimento di un parziale concorso di colpa tra le parti nella causazione dell’evento dannoso.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l’intermediario corrisponda alla parte ricorrente la somma di € 649,00.

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