COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore (MI) RIZZO

Seduta del 06/12/2022

FATTO

Il cliente, nel ricorso, afferma: di aver subito una truffa (*phishing*) tramite un noto sito di vendite online tra privati; che stava vendendo alcuni articoli quando gli è arrivato un messaggio che, almeno apparentemente, proveniva dal sito; che, nel messaggio, gli si chiedeva di registrare il conto per l'accredito del prezzo della vendita. Seguiva le indicazioni e gli si apriva una schermata del suo home banking nella quale inseriva: dati di accesso e dati della carta; che, in seguito, ignoti effettuavano un pagamento online tramite la carta; che si accorgeva tempestivamente dell'operazione non autorizzata e provvedeva a bloccare carta e conto e presentare denuncia alle autorità; che effettuava, presso la filiale di riferimento, il disconoscimento dell'operazione. Inizialmente, l'intermediario provvedeva a riaccreditare l'importo dell'operazione contestata (€ 743,03), ma, dopo aver fornito riscontro negativo alla richiesta di disconoscimento, riaddebitava l'importo.
Il ricorrente domanda la restituzione della somma di euro 743,03.

L'intermediario, riportato il fatto, afferma: che le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto risulta che le operazioni sono avvenute con il corretto inserimento delle credenziali; che ha ottenuto la certificazione ISO/IEC 27001 che rappresenta la garanzia che il sistema di gestione adottato è in grado di offrire massimi livelli di sicurezza nell'utilizzo dei servizi della banca online e dei sistemi di pagamento elettronici; che ha attivato una campagna informativa per i clienti in cui vengono fornite specifiche indicazioni per difendersi dai tentativi di truffa. Inoltre, il cliente viene esplicitamente invitato a prestare attenzione al contenuto dei messaggi ricevuti, nei quali l'intermediario precisa sempre a quale azione è collegata la comunicazione che il cliente riceve; che sussiste la colpa grave del cliente in quanto: (i) ha cliccato su un link inviato da un presunto acquirente su un sito di vendite online tra privati; (ii) ha fornito ai truffatori il numero della propria carta di debito e le credenziali di accesso all'APP (ID e password), inserendole nel sito che si apriva cliccando sul link; (iii) il sito sul quale è avvenuto l'"accalappiamento" pubblica delle indicazioni di sicurezza volte ad impedire truffe del tipo di quelle subite dal cliente; (iv) non si è insospettita nonostante la ricezione di un SMS relativo all'invio di un OTS ed alla notifica *push* dell'avvenuto *enrollement* del *device* dei malfattori.

L'intermediario domanda, quindi, il rigetto del ricorso. In via subordinata, chiede di definire la ripartizione fra le parti del danno in misura proporzionale alle rispettive responsabilità, sulla base dell'art. 1227 c.c., con l'applicazione della franchigia di euro 50,00.

DIRITTO

Oggetto della presente controversia è una operazione contestata per un importo di € 743,03, effettuata il 25/06/2022 alle ore 21:05. 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 il 28/06/2022.

L'Intermediario afferma che le operazioni sono state correttamente contabilizzate, registrate e autenticate. L'intermediario ricostruisce i singoli passaggi esecutivi nella esecuzione dell'operazione fraudolenta, fornendo quindi una schematizzazione della frode, nei seguenti termini. Per accedere ai servizi online è richiesto l'inserimento simultaneo di password statiche e dinamiche, cioè il codice Titolare (password statica), il

codice PIN (password statica) e il codice O***y (OTP, ossia la password dinamica). Una volta collegati al servizio online, per autorizzare le operazioni dispositive è necessario il codice dinamico OTP. Dalle evidenze prodotte emerge che l'*enrollment* del *device* del truffatore sia avvenuto con inserimento delle credenziali, il successivo invio di OTS per attivare il nuovo telefono sul numero di cellulare del cliente, il suo inserimento ed il successivo reinserimento delle credenziali. Risulta, inoltre, che l'operazione contestata sembra essere stata autenticata tramite inserimento del PIN (elemento di conoscenza) nell'app installata sul *device* riconducibile ai truffatori (a seguito del relativo *enrollment*) che ha generato un OTP silente (elemento di possesso).

Il cliente ha dichiarato che la frode è stata perfezionata attraverso un portale di vendite online. Verosimilmente ha ricevuto dal sedicente venditore, nella chat intrattenuta in relazione allo scambio, link malevoli che lo hanno portato ai siti attraverso i quali gli sono state carpite le credenziali.

Del resto, il cliente nella denuncia riconosce di aver cliccato sui link ricevuti e di aver provveduto a inserire tutti i dati della carta e le credenziali di accesso che gli venivano richieste. Osserva il Collegio come, da tutto quanto precede, risulti pienamente raggiunta la prova della colpa grave del cliente.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA