Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TENELLA SILLANI	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) BENINCASA	Membro di designazione rappresentativa degli intermediari
(MI) BARGELLI	Membro di designazione rappresentativa dei clienti

Relatore TENELLA SILLANI CHIARA

Seduta del 04/06/2020

FATTO

Il ricorrente, premesso di essere titolare della carta prepagata nr. *********3684 emessa dall'intermediario convenuto e di aver attivato in data 28/05/2019 un sistema di sicurezza a due fattori, associando alla carta il proprio numero di cellulare, riferisce quanto segue. In data 29/05/2019 ha ricevuto la telefonata di un sedicente operatore dell'intermediario con la quale veniva informato che l'operazione del giorno precedente non era andata a buon fine e che per sistemare il problema era necessario comunicare il codice appena inviato sul suo telefono; avendo effettivamente ricevuto un codice dalla stessa utenza dalla quale aveva ricevuto altri codici dell'intermediario, ha ritenuto legittima la richiesta e ha comunicato il codice; il giorno seguente riscontrava un addebito per un pagamento da lui non effettuato, ma disposto alla stessa ora in cui aveva ricevuto la telefonata; sporgeva quindi denuncia alle forze dell'ordine e inoltrato reclamo all'intermediario in data 04/06/2019, ma la richiesta di rimborso veniva rifiutata il 07/06/2019; inoltrava quindi nuovo reclamo il 28/09/2019, rimasto senza risposta. Rilevato che il sistema di sicurezza dell'intermediario non è sicuro, in quanto ha consentito ad ignoti di sapere quando egli aveva aderito al nuovo protocollo di autenticazione; che la *password* ricevuta in occasione della telefonata truffaldina è stata generata senza che comunicasse a terzi le credenziali necessarie, probabilmente carpite durante la procedura di attivazione del giorno precedente; che la responsabilità della truffa ricade sull'intermediario che non ha garantito

opportuni livelli di sicurezza, chiede il rimborso della somma fraudolentemente sottratta, pari a € 1.400,00

L'intermediario, nelle controdeduzioni, afferma che il ricorrente è stato vittima di *phishing* "*perpetrato tramite un SMS, al quale il giorno successivo seguiva una telefonata, con la quale gli venivano carpiti i dati segreti necessari per effettuare l'operazione*" contestata. Rileva, in particolare, che gli SMS ricevuti dal cliente presentavano diversi elementi che ne rivelavano la non autenticità; che la stessa telefonata poteva essere considerata come non autentica stante il numero sconosciuto allo stesso non riferibile e la richiesta di un codice segreto non in linea con le regole aziendali. Precisa, inoltre, che le evidenze informatiche dimostrano che l'operazione è stata autorizzata regolarmente al primo tentativo senza essere preceduta da richieste negate; che è stata disposta mediante sistema di autenticazione a due fattori: che la password OTP è stata regolarmente inviata all'utenza del cliente. Ribadito di aver adottato tutti gli strumenti possibili per rendere sicure le operazioni di pagamento, chiede il rigetto del ricorso.

Il cliente, in sede di repliche, precisa di non aver mai richiesto di essere contattato telefonicamente dall'intermediario; di non aver mai aperto i *link* dei messaggi truffaldini ricevuti e di aver aderito al sistema di sicurezza offerto dall'intermediario di propria iniziativa e attraverso il sito ufficiale; di essere stato indotto in errore dal fatto che gli sms truffaldini sembravano provenire dalla stessa utenza da cui venivano quelli autentici, dalla circostanza che il sedicente operatore fosse a conoscenza dell'adesione dallo stesso effettuata il giorno prima, dalla genericità del messaggio con cui veniva comunicato il codice OTP per l'operazione contestata, posto che dal testo non si poteva capire che quel codice fosse necessario ad autorizzare un pagamento (ed infatti i messaggi dell'intermediario successivi saranno modificati). Ribadito che la responsabilità della sottrazione delle proprie credenziali è da attribuire al non sufficiente livello di protezione delle operazioni *online* garantito dall'intermediario, riconferma la richiesta formulata nel ricorso.

DIRITTO

Il Collegio, rilevato che all'operazione contestata, effettuata nel maggio 2019, si applica il D.lgs. n. 11/2010, come modificato dal D.lgs. n. 218/2017, di attuazione della Direttiva 2015/2366/EU (PSD II), richiama l'art. 8 del suddetto decreto, secondo il quale il prestatore dei servizi di pagamento che emette uno strumento di pagamento ha, tra gli altri, "*l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo dello strumento di pagamento non siano accessibili a soggetti diversi dall'utilizzatore legittimato ad usare lo strumento medesimo, fatti salvi gli obblighi posti in capo a quest'ultimo dall'art. 7*"; l'art. 10, comma 1, a tenore del quale, in caso di disconoscimento di un'operazione da parte dell'utente, è onere del prestatore di tali servizi "*provare che, nell'ambito delle proprie competenze, l'operazione di pagamento 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 […*]"; l'art. 10 *bis*, comma 1, secondo cui "*i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente: a) accede al suo conto di pagamento on-line; b) dispone un'operazione di pagamento elettronico; c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi*"; gli artt. 11, comma 1, e 12, comma 4, i quali, rispettivamente, dispongono che quando l'operazione di pagamento non sia stata autorizzata, il prestatore di servizi di pagamento deve rimborsarla immediatamente fatto salva l'ipotesi in cui l'utente "*abbia agito in modo fraudolento o non*

abbia adempiuto ad uno o più obblighi di cui all'articolo 7, con dolo o colpa grave", nel qual caso, questi "*sopporta tutte le perdite derivanti da operazioni di pagamento non autorizzate e non si applica il limite di 50 euro di cui al comma 3*".

Sulla base della normativa sopra riportata è l'intermediario a dover provare l'insussistenza di malfunzionamenti dei dispositivi di pagamento, nonché l'autenticazione, la corretta registrazione e contabilizzazione della operazione disconosciuta, prova comunque di per sé non sufficiente a dimostrare il dolo o la colpa grave dell'utente. Il Collegio di Coordinamento, nella decisione n. 22745/19, ha infatti affermato il seguente principio di diritto: *"la previsione di cui all'art. 10, comma 2, del d.lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l''autenticazione' e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente*".

Con riguardo alla fattispecie in esame si rileva che parte resistente ha prodotto evidenze dell'operazione disconosciuta, idonea a comprovare che è stata posta in essere mediante i codici identificativi statici e i dispositivi di sicurezza dinamici affidati alla cliente, per mezzo dei quali si è resa possibile la transazione e la contestuale autenticazione ad opera dell'utente. In particolare, dai dettagli informatici versati in atti, risulta che il canale attraverso cui è stata posta in essere l'operazione è a due fattori e che l'OTP è stato inviato tramite *sms* al numero di telefono del cliente.

Quanto al livello di diligenza del cliente, si evidenzia che è lo stesso a riferire di aver aggiornato il sistema di sicurezza, come proposto dall'intermediario, e di aver comunicato, il giorno seguente, la *password* ricevuta via *sms* al sedicente operatore telefonico perché non aveva motivo di dubitare dell'autenticità della telefonata, in quanto tale soggetto era a conoscenza dell'abilitazione al servizio di sicurezza disposto il giorno prima. In proposito, si osserva che quello descritto è uno degli schemi tipici e ricorrenti di frodi informatiche, consistenti nell'indurre il titolare di una carta di pagamento, a seconda dei casi tramite telefono, e-mail, sms (*sms* nella specie chiaramente fraudolenti, stante la loro formulazione), a comunicare e/o a inserire su dispositivi o piattaforme informatiche le proprie credenziali personalizzate, solitamente adducendo falsamente l'esistenza di tentativi di accesso abusivo o più genericamente l'opportunità di verificare o implementare caratteristiche di sicurezza, come avvenuto nella specie. Trattandosi di fenomeni ormai noti, la cui pericolosità è ben evidenziata dagli stessi intermediari, l'impiego di una media diligenza da parte dei clienti sarebbe sufficiente a scongiurare il pericolo e ad impedire le truffe. Alla luce di quanto sopra esposto, si ritiene, in definitiva, che l'operazione fraudolenta sia stata resa possibile da un comportamento gravemente colpevole del ricorrente, caduto vittima di un fenomeno di *phishing*. Da ciò consegue che la richiesta di rimborso debba essere respinta.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA