Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) DENOZZA	Membro designato dalla Banca d'Italia
(MI) ACHILLE	Membro designato dalla Banca d'Italia
(MI) FERRETTI	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) AFFERNI

Seduta del 11/06/2019

FATTO

Il ricorrente ha esposto di essere rimasto vittima di una frode informatica. In particolare, ha affermato che in data 31/10/2018, alle ore 19.08 e 19.09, riceveva due SMS da parte dell'intermediario tramite i quali veniva informato della richiesta di autorizzazione di due pagamenti (di euro 1.000 ciascuno) a favore della società X; disconosceva, tramite il Servizio Clienti, le due operazioni e contestualmente bloccava la carta; il giorno successivo, veniva a conoscenza di altri prelievi per euro 100,99 complessivi.
Più precisamente, ha esposto che, a seguito della ricezione di un SMS dal presunto intermediario, dopo un tentativo di chiamata al numero indicato negli SMS, veniva ricontattato da un "operatore" che segnalava al ricorrente la richiesta di autorizzazione per un importo di euro 2.000 inerente la carta di credito xxxx3767; tale soggetto informava il cliente di aver già bloccato il pagamento sospetto e consigliava di attivare il servizio Google Pay (attivato dal ricorrente alle ore 19.00 tramite codice ricevuto sul suo cellulare).
Il ricorrente quindi sostiene di essere stato vittima di truffa in quanto non gli era stato possibile distinguere tra l'SMS ufficiale dell'intermediario e quello inviato invece dal soggetto che *"si era spacciato per un operatore di Nexi"* dando corso pertanto ad una serie di digitazioni sul suo smartphone tramite le quali è stato possibile per i truffatori eseguire le operazioni poi disconosciute e di essere stato quindi vittima di "SMS PHISHING".
In conclusione, parte ricorrente chiede il rimborso di € 2.100,99.
L'intermediario, nelle controdeduzioni, afferma:

- che, in data 31/10/2018, il cliente riceveva 2 SMS apparentemente provenienti dall'intermediario e seguendo le indicazioni fornite da un falso operatore forniva i dati della sua carta e il codice OTP ricevuto via SMS dall'intermediario (necessario per attivare il servizio Google Pay che consente di effettuare transazioni *contactless* tramite *smartphone*). Alcuni minuti dopo venivano effettuate 3 operazioni *contactless*;
- che il ricorrente contattava il servizio clienti e alle 18,49 bloccava la carta.
- che la richiesta di rimborso non può essere accolta poiché attraverso il cosiddetto "vishing" il cliente ha divulgato informazioni riservate con colpa grave e negligenza; l'SMS ricevuto non proveniva da un numero ufficiale ma da un numero in chiaro di un telefono cellulare e conteneva esclusivamente la denominazione xxx utilizzata in maniera illecita. Il ricorrente avrebbe pertanto dimostrato una mancanza di cautela.

In considerazione di quanto sopra esposto, l'intermediario ha chiesto il rigetto del ricorso.
Nelle repliche parte ricorrente, in risposta alle controdeduzioni, precisa che tra gli SMS ufficiali e quelli fraudolenti risultano forti somiglianze ed analogie e pertanto non era possibile accorgersi della provenienza illecita. Inoltre, specifica che nel documento informativo sulla sicurezza, l'intermediario non fa riferimento ai fenomeni di "vishing" o di "smishing" e pertanto gli stessi non possano ritenersi risaputi e diffusi in quanto la clientela non risulta esserne informata preventivamente.
Il cliente conferma pertanto la domanda di rimborso contenuta nel ricorso.

DIRITTO

Molti dei tentativi di truffa posti in essere con modalità telematiche in materia di servizi di pagamento si svolgono secondo uno schema tipico e ampiamente noto, consistente nell'indurre il titolare dello strumento, a seconda dei casi tramite telefono, e-mail, sms o altri strumenti di comunicazione, 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 (c.d. *phishing* che, se tradizionalmente prende le forme di una e-mail civetta, può tuttavia presentarsi anche mediante l'invio di sms – c.d. SMShing – o l'effettuazione di chiamate vocali – c.d. *vishing*).
La diffusione del fenomeno è tale che i Collegi ABF ormai ritengono da tempo, da un lato, che l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa. Parte ricorrente specifica che nel documento informativo sulla sicurezza, l'intermediario non fa riferimento ai fenomeni di "vishing" o di "smishing" e pertanto gli stessi non possano ritenersi risaputi e diffusi in quanto la clientela non risulta esserne informata preventivamente. Sul punto, si osserva che questa argomentazione è priva di pregio, in quanto l'impiego di media diligenza avrebbe impedito il comportamento incauto del ricorrente, essendo anche il fenomeno di SMS phishing/SMShing ormai molto noto e diffuso.
La vicenda che ci occupa riguarda, come detto, un fenomeno di SMShing (come dichiarato dallo stesso ricorrente nella denuncia ai Carabinieri della stazione di Bressanone). Al fine di risolvere odierna controversia è dunque necessario analizzare il comportamento dell'intermediario e quello del ricorrente. Quanto al primo profilo risulta dai documenti prodotti che i pagamenti disconosciuti sono transazioni *contactless* eseguite tramite *smartphone*; che l'intermediario ha dato prova della contabilizzazione e registrazione delle operazioni disconosciute dal cliente e della loro legittima esecuzione e regolarità; che le transazioni sono state effettuate mediante un sistema dinamico di autenticazione, ossia mediante l'inserimento di un codice OTP inviato al cliente via SMS. In relazione al

ricorrente, invece, occorre sottolineare che il suo comportamento risulta essere inadempiente rispetto agli obblighi previsti dalla disciplina generale (artt. 1175, 1176, 1218, 1227, 1375, 1710 cod. civ.) nonché da quella speciale (d.lgs. n. 11/2010). In particolare, il ricorrente ha violato gli obblighi di diligenza e riservatezza in quanto, seppure incautamente, ha dato seguito alle richieste dell'apparente intermediario.
Quanto precede consente di ritenere, ad avviso di questo Collegio, che il resistente ha fornito la prova che l'operazione di cui trattasi è stata autenticata, correttamente registrata e contabilizzata e che, in relazione alla stessa, non si sono verificati malfunzionamenti del sistema ovvero altre anomalie, come richiesto dal citato art. 10 del D.Lgs. 11/2010. Tale prova impone a questo Collegio di considerare l'operazione di pagamento di cui si discute come autorizzata dalla ricorrente e, pertanto, a lei opponibile, benché dalla medesima disconosciuta. Sul punto si veda, tra le tante, Collegio di Milano – Decisione n. 7131 del 22 giugno 2017.
Lo svolgimento della vicenda e la valutazione delle rispettive condotte inoltre inducono ad escludere la configurabilità di un concorso di colpa tra le parti. Ne consegue che le conseguenze derivanti dall'operazione fraudolenta gravano esclusivamente a carico del ricorrente, che ha agito con colpa grave.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
FLAVIO LAPERTOSA