Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) COTTERLI	Membro designato dalla Banca d'Italia
(TO) FERRANTE	Membro designato dalla Banca d'Italia
(TO) BUONINCONTI	Membro di designazione rappresentativa degli intermediari
(TO) DE FRANCESCO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - SIMONETTA COTTERLI

Seduta del 30/07/2019

FATTO

Il ricorrente afferma nel ricorso di aver scoperto che il giorno 28 dicembre 2017 era stata disattivata la SIM del suo telefono cellulare da un centro del proprio operatore telefonico, poi riattivata da un soggetto che si era sostituito alla sua persona, il quale, dopo essersi impossessato del numero di telefono, effettuava pagamenti *online* con la carta di credito emessa dall'intermediario convenuto. Precisa inoltre che i movimenti fraudolenti sono avvenuti per un totale di € 1.270,47 e di aver bloccato la carta solamente al ricevimento dell'estratto conto, quando si avvedeva delle operazioni di pagamento effettuate lo stesso giorno in cui gli era stata disattivata la sim.
Disconosciute le operazioni ma avendo l'intermediario negato il loro rimborso, sostenendo che le stesse fossero avvenute senza anomalie, si rivolge all'ABF, specificando che le operazioni superavano il limite massimo consentito di utilizzo della carta, e chiede il rimborso della somma di € 1.270, 47.
L'intermediario nelle controdeduzioni afferma che dalla ricostruzione dei fatti emerge che, il 28 dicembre 2017, il ricorrente ha sporto denuncia/querela presso la Questura per truffa telefonica e sostituzione di persona, dopo essersi accorto, intorno alle ore 17:00, che il proprio cellulare era stato disattivato ed aveva pertanto smesso di funzionare, sia per le chiamate in entrata sia per le chiamate in uscita. Specifica che il ricorrente scopriva, tramite il proprio operatore telefonico, che qualcuno si era recato in un centro specializzato e aveva disattivato la sim collegata al suo telefono chiedendone un'altra in sostituzione, e che egli, trovandosi senza la linea telefonica, attivava una nuova sim. In merito alle operazioni non autorizzate, ipotizza che i malfattori dovessero avere a disposizione le

credenziali della carta di credito, perché senza queste non avrebbero potuto portare a termine le transazioni fraudolente, effettuate in modalità "*e-commerce sicuro*", per un importo complessivo € 1.270,47. Dichiara inoltre che la carta di credito è stata bloccata soltanto l'8 gennaio 2019, alle ore 13:54, ossia ben undici giorni dopo la denuncia del furto di identità e il blocco dell'utenza telefonica. Nega pertanto ogni responsabilità, ipotizzando il non corretto comportamento dell'operatore telefonico, che non avendo effettuando il dovuto controllo sui documenti dei soggetti che richiedevano il cambio della sim associata al numero del ricorrente, i codici OTP di autorizzazione delle operazioni venivano regolarmente inviati al numero di cellulare che il ricorrente aveva fornito, già nella disponibilità materiale dei malviventi che hanno così potuto agire indisturbati.
Quanto ai propri obblighi, precisa che dalla verifica dei *log* delle operazioni *online* effettuate nel giorno di esecuzioni delle operazioni non riconosciute, si ha la conferma che tutti i parametri di sicurezza richiesti dai propri sistemi siano stati rispettati. In particolare, ogni operazione di questo tipo è composta da momenti diversi rappresentati da tre *log*: il primo conferma che i dati inseriti sono corretti, il secondo richiede l'inserimento del codice OTP (*One Time Password*), mentre il terzo dà conferma che è stato inserito il codice OTP corretto e che la transazione si è conclusa positivamente.
Conclude evidenziando che il ricorrente, pur avendo sporto regolare denuncia per il reato di sostituzione di persona e furto della sim, non ha in alcun modo pensato di comunicare all'intermediario il cambio del numero di cellulare, né vi ha provveduto personalmente sul Portale Clienti; di conseguenza, ritiene possa configurarsi in capo al ricorrente una colpa grave in quanto lo stesso, vittima di truffa perpetrata tramite sostituzione di persona e attivazione di una nuova utenza telefonica a suo nome, non ha agito tempestivamente provvedendo sul portale *internet* – dove pure era abituato a navigare per sua stessa ammissione – oppure avvertendo gli operatori del Servizio Clienti di distaccare la propria carta di credito dal numero di telefono in precedenza fornito e ormai bloccato a seguito della truffa.
L'intermediario chiede il rigetto del ricorso.

DIRITTO

La controversia verte sulla questione relativa alle responsabilità in caso di utilizzo fraudolento di uno strumento di pagamento.
Il Collegio precisa che le operazioni contestate sono disciplinate dal d.lgs. 27 gennaio 2010, n. 11, di attuazione della direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno (c.d. PSD) e del provvedimento di attuazione della Banca d'Italia del 5 luglio 2011. Devono in particolare essere richiamati gli artt. 7, 10 e 12 del citato decreto.
In base all'art. 7 del d. lgs. 11/2010, l'utilizzatore dello strumento di pagamento è tenuto ad utilizzarlo nel rispetto delle condizioni contrattuali che ne disciplinano l'emissione e l'uso (lett. a). Inoltre, ai sensi del secondo comma della norma, "*l'utilizzatore, non appena riceve uno strumento di pagamento, adotta le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo*".
Ciò posto, l'art. 12 del d. lgs. n. 11/2010 regola il regime della responsabilità a fronte dell'utilizzo non autorizzato di strumenti e servizi di pagamento. La disposizione, con un evidente *favor* nei confronti dell'utilizzatore, opera uno spostamento della responsabilità in capo al prestatore dei servizi di pagamento in caso di utilizzo fraudolento, estendendola a tutte le ipotesi di violazione degli obblighi di custodia e sicurezza non caratterizzate da frode, dolo o colpa grave. L'utilizzatore infatti può sopportare le conseguenze delle operazioni fraudolente nel limite massimo della franchigia di € 150,00, salvo il caso in cui abbia agito in frode, con dolo o con colpa grave, sole ipotesi a fronte delle quali sarà

gravato di una responsabilità illimitata (art. 12, comma 3). Ne consegue che, nel caso in esame, al fine di escludere la responsabilità illimitata del ricorrente, è necessario escludere che il comportamento dello stesso possa configurarsi quale colpa grave.
Infine, ai sensi dell'art. 10 del d. lgs. n. 11/2010, l'onere della prova che l'utilizzatore abbia agito con dolo o colpa grave incombe sull'intermediario, il quale, in base al primo comma della norma, nel caso di un'operazione di pagamento disconosciuta è tenuto a "*provare che 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*". Inoltre in base al secondo comma della medesima norma "*quando l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7*".
Tanto premesso, in merito ai fatti accaduti, dalla documentazione agli atti appare pacifico, stanti sia la denuncia effettuata dal ricorrente ai Carabinieri l'8 gennaio 2018, cioè non appena avvedutosi delle operazioni fraudolente, sia la ricostruzione dei fatti operata da entrambe le parti, che il ricorrente sia stato vittima di una truffa telefonica, recentemente diffusa e denominata "*sim swap*", attraverso la quale i malviventi, utilizzando documenti falsi, ottengono il duplicato della sim del soggetto titolare dello strumento di pagamento, le cui credenziale vengono preliminarmente carpite tramite tecniche di *hacking* ovvero di ingegneria sociale, riuscendo in tal modo ad entrare in possesso di tutti i codici necessari per eseguire operazioni *on line*.
Tali circostanze non consentono di ritenere provata la colpa grave del ricorrente, come necessario, ai sensi del citato art. 12 del d. lgs. n. 11/2010, perché questi possa essere chiamato a sopportare le perdite derivanti da operazioni di pagamento non riconosciute, ed il ricorsa merita pertanto di essere accolto.
In sintonia con l'orientamento espresso sul punto dalla Corte di Cassazione, l'uniforme giurisprudenza dell'ABF qualifica la colpa grave come "*un comportamento consapevole dell'agente che, senza volontà di arrecare danno agli altri, operi con straordinaria e inescusabile imprudenza o negligenza, omettendo di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti*" (cfr. per una simile prospettiva, in tema di gravità della colpa, Cass. civ., 19 novembre 2001, n. 14456; ABF, Collegio di Milano, decisioni n. 40/2012 e n. 2310/2011; ABF, Collegio di Roma, decisioni n. 2157/2011 e n. 712/2010). Si tratta, evidentemente, non di una semplice distrazione o negligenza, bensì di "*un comportamento abnorme e, in quanto tale, non scusabile*", la cui valutazione deve essere compiuta con riguardo alle specificità di ogni singolo caso, con riferimento sia agli obblighi di custodia sia dello strumento sia di tutti i codici necessari per l'esecuzione delle operazioni. Nel caso in esame l'architettura complessa della truffa e la sua relativamente recente diffusione, diversamente dai casi di comune *phishing*, non consentono di valutare come non scusabile il comportamento del ricorrente, il quale non ha collegato quanto successo in relazione alla sua scheda telefonica ad una ipotesi di truffa nel sistema dei pagamenti. Non risulta pertanto provato, pur a fronte di un sistema di sicurezza a due fattori e l'evidenza dell'autenticazione, corretta registrazione e contabilizzazione, né che il ricorrente abbia consentito l'accesso ai dati del proprio strumento di pagamento, che gli sono verosimilmente stati carpiti con tecniche di *hacking* non facilmente riconoscibili, se non riconoscibili affatto, né tantomeno che abbia comunicato incautamente a terzi l'OTP

necessario per l'esecuzione delle operazioni, carpiti attraverso un furto di identità telefonica (Cfr. Collegio di Torino, decisione n. 25065/2018).
Pertanto, poiché l'intermediario resistente non prova né il dolo né la colpa grave della parte ricorrente, ma solo che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata, in applicazione dell'art. 11, comma 3, d. lgs. n. 11 del 2010, il ricorrente non può sopportare perdite, derivanti dalle operazioni disconosciute, come risultanti dall'estratto conto da questi versato agli atti e sulle quali non vi è controversia, e cioè 8 operazioni di *e-commerce* per un importo complessivo di € 1.270,47*,* per un importo superiore ad € 150.

P.Q.M.

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.120,47.
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
EMANUELE CESARE LUCCHINI GUASTALLA