Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) BATTELLI	Membro designato dalla Banca d'Italia
(TO) COTTERLI	Membro designato dalla Banca d'Italia
(TO) DALMOTTO	Membro di designazione rappresentativa degli intermediari
(TO) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - SIMONETTA COTTERLI

Seduta del 07/01/2021

FATTO

Il ricorrente come di seguito espone i fatti accaduti. In data 22/07/20, alle ore 16.14, veniva contattato sul cellulare dal numero +398002xxxx6, corrispondente al numero verde dell'intermediario. Risultando poco chiara la comunicazione, veniva ricontattato alle 16.17 e interloquiva con un sedicente operatore dell'intermediario, che lo informava dell'utilizzo indebito della propria carta di credito, asseritamente clonata, e della necessità di procedere allo storno di nuovi pagamenti effettuati dai malviventi. Precisamente si trattava di bloccare "ulteriori 5 prelievi di 490 € cadauno". Durante la conversazione riceveva sul cellulare gli SMS contenenti le OTP per la conferma dei pagamenti, che l'operatore chiedeva di conoscere "per far sì che il pagamento venisse autorizzato e stornato" al termine dei movimenti. Comunicava così i codici richiesti e, dopo il quinto, la conversazione si interrompeva. Provava a chiamare "lo stesso numero alle ore 16.33" e riceveva la risposta automatica del *call center* dell'intermediario. Alle 16.35, compreso di essere rimasto vittima di una frode, disponeva il blocco della carta. Dichiara in merito alla frode che la sottrazione delle somme ha visto "l'involontaria complicità" dell'Istituto Bancario, da cui sarebbero stati trafugati diversi dati personali riferibili alla persona ed alle condizioni contabili bancarie e le cui linee telefoniche, inoltre, sarebbero state violate.
Proposto reclamo e disconosciute le operazioni 28/07/2020, il ricorrente chiede il riaccredito di € 2.450,00, corrispondenti alle somme indebitamente sottratte.
L'intermediario in sede di controdeduzioni conferma che le operazioni disconosciute sono 5 e sono state eseguite il 22/7/2020, per un totale di € 2.450,00. In merito a quanto

accaduto, dichiara che il cliente è stato vittima di frode, in cui è incorso dopo aver rivelato incautamente i codici dispositivi al malfattore, che millantava fossero necessari per disporre lo storno dei pagamenti. Precisa che gli sms ricevuti contenevano non solo il codice autorizzativo, ma anche l'ammontare ed il beneficiario dei pagamenti e che non constano violazioni dei sistemi da cui terzi possano avere attinto ai dati personali del ricorrente. Sottolinea inoltre come le campagne informative e la documentazione periodica inviata dall'intermediario contengono avvisi circa la necessità di non rivelare a terzi OTP, PIN, password e dati personali.
L'intermediario resistente chiede il rigetto del ricorso.
In sede di repliche il ricorrente argomenta che nell'informativa sulle "operazioni di pagamento" dell'ottobre 2018 e del febbraio 2019 constano avvisi contraddittori giacché, da un lato, si induce il cliente a credere di poter usare la propria carta in tranquillità, mentre dall'altro si specifica che il servizio clienti potrebbe entrare in contatto con l'utilizzatore, al fine di verificare la correttezza delle operazioni effettuate. Argomenta inoltre che i codici OTP non sembrano rientrare nella nozione di dato personale di cui si il cliente non dovrebbe dare comunicazione a terzi e che la comunicazione prodotta con le controdeduzioni, che avrebbe dovuto mettere in condizione il ricorrente di evitare la truffa in cui è incorso, è successiva all'evento dannoso. Sottolinea inoltre di aver ricevuto non una, ma due telefonate in un breve lasso di tempo da un soggetto che si qualificava operatore della banca, tramite un numero coincidente con quello usato anche attualmente dall'intermediario. Tali circostanze attesterebbero una potenziale intrusione dei truffatori nella linea dell'istituto di credito, ovvero la presenza di personale infedele all'interno della banca. Argomenta ancora che negli sms ricevuti non viene riportata la dicitura "3D secure code", indicazione mai ricevuta nemmeno prima e che nelle controdeduzioni si afferma che il sistema di controllo della banca ha registrato una "fraudolenta richiesta di transazioni", per inizializzare la quale erano necessari dati (nome, cognome, numero carta, CVV2, scadenza) mai forniti né al soggetto che si qualificava come operatore della banca, né a terzi. Conclude che il cliente non è tenuto a conoscere gli articoli di giornale o le informative di polizia allegate dalla controparte e che la sua colpa, laddove ritenuta sussistente, non risulta caratterizzata da profili di gravità.

DIRITTO

La controversia verte sulla questione relativa alle responsabilità in caso di esecuzione fraudolenta di operazioni di pagamento effettuate *on line*.
Il Collegio precisa che le operazioni contestate sono disciplinate dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del d.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta. Devono in particolare essere richiamati gli artt. 10 e 12 del citato decreto.
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. Ne consegue che, nel caso in esame, al fine di escludere la responsabilità della ricorrente è necessario escludere che il comportamento della stessa possa configurarsi quale colpa grave. Sul punto deve essere richiamato l'art. 7, comma 3 del d. lgs. n.

11/2010, in base al quale l'utente "adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate".
Ai sensi del comma 2 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, ai sensi del 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", ciò che non è in ogni caso di per se atto a presumere la colpa grave dell'utilizzatore (Cfr. Collegio di Coordinamento, decisione n. 22745/2020).
Tanto premesso, in merito ai fatti accaduti, in base alla documentazione prodotta, le 5 operazioni disconosciute, del valore di € 490,00 ciascuna, risultano eseguite il 22/7/2020, rispettivamente alle ore 06:23 AM PST; 06:25 AM PST; 06:26 AM PST; 06:29 AM PST; 06:30 AM PST La stessa parte ricorrente riferisce che l'operatività fraudolenta ha avuto origine, e si è successivamente perpetrata, da una telefonata proveniente da un numero nominativamente intestato all'intermediario resistente, nel corso della quale, tratto in inganno, ha fornito i codici ricevuti tramite SMS credendo di annullare le operazioni poi fraudolentemente eseguite.
Il sistema di autenticazione delle operazioni di pagamento adottato dall'intermediario ricorre ad una tecnologia multifattoriale, con una *password* dinamica erogata al cliente con SMS. In base alla documentazione prodotta dalla resistente, e come dalla stessa precisato, il cliente ha ricevuto 5 SMS contenente le OTP necessarie per completare le operazioni.
Ne consegue che il Collegio non può che concludere che le operazioni contestate siano scaturite da un fenomeno di *vishing* realizzato ai danni del cliente, utilizzando il metodo dello *spoofing* (applicato al numero verde dell'intermediario). La diffusione del fenomeno è tale che i Collegi ABF ormai ritengono da tempo che l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e ad impedire la truffa.
Tuttavia, nonostante l'incauta rivelazione delle OTP da parte della ricorrente, il Collegio rileva in primo luogo come, per quanto parte resistente dichiari che il sistema di autenticazione per l'effettuazione delle operazioni di pagamento *on-line* sia a due fattori, di cui uno consiste in una OTP inviata tramite SMS sul *device* del cliente, non vi è evidenza di quale sia l'ulteriore fattore utilizzato, che potrebbe in ipotesi consistere nei dati presenti sulla carta, come prospettato dal ricorrente in sede di repliche. Sul punto, si osserva che con l'introduzione della nuova Direttiva Europea sui servizi di pagamento PSD2, all'EBA è stato attribuito l'incarico di specificare i requisiti delle procedure di autenticazione forte del cliente e le relative esenzioni d'uso. A tal proposito l'EBA si è espressa pubblicando propri RTS (*Regulatory Technical Standards*), i quali sono stati redatti ai sensi dell'Articolo 98 della Direttiva PSD2 e la Commissione Europea ha adottato il Regolamento Delegato (UE) n. 389 del 27 novembre 2017, entrato in vigore a far data dal 14/09/2019. Nel documento "*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*", del 21/06/2019, l'EBA specifica, precisando quanto contenuto negli RTS, che le credenziali della carta non possono costituire né un elemento di conoscenza né un elemento di possesso. Ne consegue che, nel caso in esame, l'intermediario non prova l'esistenza di un sistema di autenticazione forte per l'esecuzione delle operazioni.
Per quanto la Banca d'Italia abbia concesso una proroga al 31/12/2020 agli intermediari per il completamento degli adeguamenti tecnici richiesti per l'adozione dei sistemi di autenticazione forte della clientela nei pagamenti *online* con carta di pagamento (31/12/2020), tuttavia nel caso di operazioni per le quali non sia provata l'esistenza per

l'esecuzione di un sistema di autenticazione forte, come nel caso in esame, non può ritenersi provata la colpa grave dell'utilizzatore (cfr. n. 14954 del 10/07/2018 del Collegio di Torino). A maggior ragione, per quanto qui interessa, in presenza della circostanza che le telefonate in cui sono stati rivelati i codici necessari al compimento delle operazioni risultano effettuate da un numero telefonico che coincide con il numero verde dell'intermediario, ciò che fa ritenere che questi abbia subito un'intrusione e falsificazione dei propri sistemi di comunicazione, circostanza che ha concorso sensibilmente alla realizzazione della truffa subita dal ricorrente.
Il Collegio ritiene pertanto che il ricorso meriti di essere accolto, non potendo ritenersi provata da parte della resistente l'esistenza di un sistema di autenticazione forte per l'esecuzione delle operazioni contestate e la colpa grave del ricorrente.

P.Q.M.

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.450,00.
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
EMANUELE CESARE LUCCHINI GUASTALLA