COLLEGIO DI BARI

composto dai signori:

(BA) DE CAROLIS	Presidente
(BA) CAMILLERI	Membro designato dalla Banca d'Italia
(BA) PAGNONI	Membro designato dalla Banca d'Italia
(BA) STEFANELLI	Membro di designazione rappresentativa degli intermediari
(BA) PANZARINO	Membro di designazione rappresentativa dei clienti

Relatore CONSIGLIA SILVIA PANZARINO

Seduta del 31/05/2018

FATTO

Il ricorrente, intestatario di una carta prepagata rilasciata dalla resistente, riferisce di aver ricevuto, in data 18/10/2017, una telefonata apparentemente proveniente da un operatore dell'intermediario, il quale gli proponeva di eseguire la procedura di modifica del numero di cellulare associato alla carta, necessaria per l'utilizzo online in modalità securizzata del suo dispositivo di pagamento.
Confidando nella veridicità della chiamata per il fatto di aver chiesto, quattro mesi prima, delucidazioni sull'argomento al servizio di assistenza dell'intermediario, seguiva le indicazioni impartite dall'interlocutore telefonico; in particolare, si collegava all'App della resistente ove immetteva il proprio codice ID e "un codice di 4 cifre" ricevuto tramite sms, "senza mai fornir[e] verbalmente" alcuna credenziale all'operatore.
"Lo stesso giorno, dopo circa un'ora", riscontrava un diverso numero di cellulare associato alla carta, a lui sconosciuto, e si avvedeva di cinque operazioni di pagamento del valore di € 3.880,62 non autorizzate.
Il giorno successivo presentava denuncia presso le competenti Autorità, integrata il 21/10/2017, e formale reclamo per il disconoscimento delle operazioni.
L'intermediario rileva anzitutto che la questione sottoposta all'ABF è da inquadrare in quella particolare tipologia di frode nota come *phishing*. Perviene a tale conclusione esaminando la denuncia del 19/10/2017, in cui il ricorrente afferma - contrariamente a quanto dichiarato nel ricorso - di aver comunicato all'operatore i dati relativi alla carta di cui era titolare.

Evidenzia, inoltre, come nel ricorso il cliente esponga di essersi avveduto del cambio del numero di cellulare e dell'ammanco appena un'ora dopo la chiamata fraudolenta; in relazione a tanto, l'intermediario rileva la tardività del blocco, avvenuto alle 09:32 del 19/10/2017. Sottolinea, al riguardo, che una reazione più tempestiva avrebbe potuto sventare la frode, compiutasi tra le ore 16:10 del 18/10/2017 e le ore 08:44 del 19/10/2017.
Sostiene, in ogni caso, che l'operazione è stata possibile esclusivamente a causa della cooperazione del ricorrente. Lo stesso infatti, utente da tempo dei servizi mobili e online dell'intermediario (e, quindi, in possesso della "diligenza necessaria" per comprenderne i meccanismi di funzionamento), ha consentito al frodatore di installare e rendere dispositiva l'App sul suo cellulare e, successivamente, di sincronizzarla con l'applicazione presente sul device del cliente. Quest'ultimo avrebbe, poi, modificato anche le impostazioni del proprio apparato "(ossia il primo su cui è stata installata l'App), «settando» il secondo come il device di preferenza", sì da consentire al frodatore di disporre del conto e della carta della vittima.
Sostiene, in ogni caso, che la richiesta dell'operatore avrebbe dovuto indurre il cliente a sospettare della veridicità della comunicazione, posto che le modalità di rilascio e di modifica del numero associato alla carta avvengono attraverso "canali blindati", tra i quali non rientrano i contatti telefonici con il personale. Peraltro, con riferimento alla richiesta al servizio di assistenza dell'intermediario avvenuta quattro mesi prima della truffa, la resistente evidenzia come i suoi operatori, al contrario del frodatore, non siano riusciti a contattare il cliente per fornire le corrette indicazioni da seguire; produce, al riguardo, evidenza dei tentativi di contatto falliti con il cliente.
Conclude affermando che la solerte collaborazione telefonica con il supposto operatore – il quale, peraltro, ha scelto di attuare la frode tramite operazioni 3d secure, implicanti "un elevato grado di sicurezza" - "ha consentito [allo stesso] di adottare un comportamento del tutto analogo a quello dell'utente in buona fede, impedendo pertanto l'insorgere di segnalazioni nel giorno della frode".
Alla luce delle precedenti considerazioni, esclude ogni responsabilità nella produzione dell'evento dannoso e, a supporto della sua prospettazione, richiama la decisione del Collegio Coord. n. 3498/12.
Il ricorrente chiede al Collegio di voler riconoscere il proprio diritto al rimborso della somma di € 3.880,62.
La resistente chiede il rigetto nel merito del ricorso.

DIRITTO

Le operazioni contestate sono state poste in essere sotto il vigore del 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.
In base a quanto emerge dalla denuncia e/o dalle ulteriori evidenze in atti, è pacifico che il ricorrente sia stato vittima di un'articolata truffa via telefono.
In particolare, con riferimento alle modalità, è verosimile - dalla ricostruzione dei fatti - che il cliente, dalla sua app, abbia consentito di installare tale app con le credenziali del proprio conto anche su un nuovo *device*, in possesso del frodatore, consentendo così a quest'ultimo di effettuare le operazioni contestate.
Al riguardo, da un lato si rileva che l'intermediario non produce alcuna evidenza circa le caratteristiche e il funzionamento del sistema di sicurezza associato all'app; in particolare, non fornisce alcuna spiegazione in ordine alle modalità di accesso a quest'ultima. Si limita

ad affermare che è previsto un presidio OTP (codice di sicurezza inviato tramite sms) per autorizzare un nuovo *device* a operare.
Dall'altro, il cliente espressamente, in sede di denuncia, (diversamente da quanto dichiarato nel ricorso) afferma di aver fornito l'OTP e il codice ID all'operatore, mettendolo, in tal modo, nelle condizioni di poter disporre le operazioni contestate.
Inoltre, la carta di credito è stata bloccata il 19.10.2017 alle ore 9:32, come risulta dal modulo di disconoscimento allegato al ricorso. Tuttavia, sussistono alcune contraddizioni tra quanto dichiarato dal ricorrente nel ricorso e il contenuto della denuncia rispetto alla evidenza dell'ammanco e cioè:

- Il ricorrente contesta n. 5 transazioni *on line*, eseguite con la carta prepagata a lui intestata, che ammontano complessivamente ad € 3.880,62;
- l'intermediario ha prodotto evidenza della tracciatura informatica delle operazioni per dimostrare che, in relazione alle stesse, non si è verificata alcuna anomalia. Risulta negato un solo tentativo di pagamento del 18/10/2017 per superamento del limite giornaliero; l'operazione *de qua* è stata comunque effettuata il giorno successivo;
- tutte le operazioni fraudolente sono state eseguite tramite *3d secure* .

Non è provato, invece, l'invio di codici OTP in relazione ai pagamenti contestati, secondo quanto richiesto dall'art. 10 del Dlgs n. 11/2010. Tali codici - come affermato dallo stesso intermediario - sarebbero stati, comunque, inviati al numero fraudolentemente associato alla carta e non a quello del ricorrente.
Tanto considerato e stante le campagne di informazione e di prevenzione antitruffa avviate dagli intermediari, non può non considerarsi caratterizzata da colpa grave la condotta del ricorrente.
Al di là di tutto ciò, comunque, pure merita riconoscere come nella causazione del pregiudizio subito dal ricorrente risulti aver concorso una qualche vulnerabilità dei presidi complessivamente apprestati dall'intermediario dedotto in lite. Fermo restando, difatti, come la truffa di cui il ricorrente è indubbiamente stato vittima mai si sarebbe potuta consumare se egli, dopo aver dato seguito all'invito ad avviare la procedura di autorizzazione sollecitatagli da un interlocutore mai conosciuto precedentemente, non gli avesse poi riferito la credenziale informatica ricevuta Sms; vero è pure che la possibilità, per un tale interlocutore del ricorrente, di carpire il codice segreto Otp per via telefonica (e in questo senso allora ben può parlarsi di *phishing*) non si sarebbe mai verificata se quello, a monte, non fosse potuto accedere in alcun modo al sistema. Appare cioè verosimile come l'ignoto interlocutore, oltre ad essere certamente venuto a conoscenza dell'utenza telefonica del ricorrente, essendo altresì a conoscenza della sua titolarità di conto on line con l'intermediario, sia stato poi in grado di interagire - in qualche modo ed almeno fino ad un certo livello - all'interno dell'ambiente informatico al quale avrebbe dovuto poter accedere solamente il ricorrente. Fu l'ignoto interlocutore, difatti che, almeno da quanto emerge in atti, riuscì ad attivare la procedura di autorizzazione che comportò poi l'invio al ricorrente della richiesta (tramite una apposita "finestra") di abilitazione di una nuova utenza telefonica.
In ogni caso, non può affermarsi che l'intermediario convenuto abbia nella fattispecie fornito la prova che l'operazione contestata sia stata autenticata e non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti connessi al servizio di disposizione di ordine di pagamento prestato, come prescritto dall'art. 10 del d. lgs. n.11/2010.
In definitiva, dalle circostanze emerse in atti risulta che se, da un lato, senza la gravemente colpevole cooperazione del ricorrente mai si sarebbe potuta perpetrare la truffa da lui subìta (cfr. Collegio di Bari dec. n. 14195/17); d'altro lato, la medesima truffa neppure avrebbe potuto, a monte, organizzarsi se l'intermediario avesse predisposto dei

presidi di sicurezza idonei ad impedire qualsiasi accesso non autorizzato al sistema di home banking utilizzato dal ricorrente (cfr. Collegio di Roma dec. n. 10125/18).
Sono considerazioni, queste, che inducono dunque a ravvisare, nel caso di specie, un concorso di colpa dell'intermediario, in ragione della limitata efficacia dei sistemi di sicurezza da esso predisposti, che ne determinano una responsabilità risarcitoria nella misura di € 1.940,00.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente l'importo di € 1.940,00.
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 al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
BRUNO DE CAROLIS