COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) BARENGHI	Membro designato dalla Banca d'Italia
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) PUDDU	Membro di designazione rappresentativa dei clienti

Relatore GIUSEPPE SPENNACCHIO

Seduta del 23/10/2024

FATTO

Il ricorrente chiede la restituzione della somma di €. 2.999,00=, corrispondente all'importo di un'operazione di pagamento fraudolenta. Afferma di aver ricevuto, in data 24 gennaio 2024, una telefonata.
Il chiamante, presentatosi come operatore dell'ufficio antifrode della banca, gli riferiva di una frode in atto e lo invitava a seguire le proprie istruzioni. Eseguiva quanto richiesto e comunicava al sedicente operatore il codice ricevuto tramite sms.
Immediatamente riceveva un secondo sms relativo all'esecuzione di un pagamento di €. 2.999,00=. Era rassicurato dal sedicente operatore, il quale gli riferiva che detto importo sarebbe stato successivamente oggetto di storno.
Subito dopo l'operatore lo invitava ad effettuare un'altra operazione. Riceveva, quindi, un sms con un codice per confermare un finanziamento.
Così si rendeva conto di essere stato vittima di un raggiro e non comunicava il codice ricevuto. Presentava denuncia alle autorità e comunicava l'avvenuta frode alla banca.
Dalla denuncia non risulta ravvisabile in capo al ricorrente alcun tipo di condotta dolosa o gravemente negligente. Infatti, in tema di responsabilità della banca in caso di operazioni effettuate a mezzo di strumenti elettronici, è del tutto ragionevole ricondurre tale responsabilità nell'area del rischio professionale del prestatore dei servizi di pagamento.

Il fatto che la telefonata provenisse dal numero dell'intermediario, così come i messaggi di storno, ha reso la frode non evitabile nonostante l'adozione di tutte le precauzioni possibili. Conclude per l'ottenimento del rimborso della somma di €. 2.999,00=.

L'intermediario nelle controdeduzioni, riportato il fatto, afferma quanto segue:

- in data 24 gennaio 2024 il ricorrente subiva una frode avente ad oggetto l'esecuzione di un pagamento con la carta di debito associata al proprio conto corrente, per un importo di €. 2.999,00=.
- l'operazione disconosciuta è stata correttamente contabilizzata, registrata ed autenticata in quanto posta in essere con il corretto inserimento delle credenziali statiche e dinamiche in possesso del ricorrente con autorizzazione forte a due fattori, senza aver subito la conseguenza di alcun malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti;
- l'accesso è avvenuto tramite inserimento delle credenziali statiche in quanto vi erano le condizioni per l'esenzione SCA previste dall'art. 10 del regolamento delegato 2018/389;
- la *password* può essere modificata secondo una procedura a doppio fattore di autenticazione;
- le operazioni sono avvenute previo inserimento delle credenziali statiche della carta, CVV dinamico e OTP inviato via sms;
- il ricorrente ha comunicato a terzi lo *username* per accedere alla propria area riservata di *internet banking*, le due cifre del PIN della carta richieste dal sistema e la OTP necessaria a confermare l'operazione di modifica *password*;
- i malfattori, una volta modificata la *password*, aumentavano il limite massimo giornaliero di spesa ad €. 3.000,00=, mediante inserimento del codice OTP inviato al ricorrente, generavano il CVV dinamico con inserimento di un secondo OTP ed eseguivano l'operazione, inserendo i dati statici della carta, il CVV dinamico ed un ulteriore OTP;
- sussiste la colpa grave del cliente, a fronte della collaborazione fornita ai malfattori, gravemente colposa seppur non volontaria;
- l'intermediario ha diffuso apposite campagne informative volte a sensibilizzare la clientela rispetto alle forme più diffuse di frode.

Nel replicare alle controdeduzioni, la parte ricorrente precisa:

- che sussistono profili di grave inadempimento da parte dell'intermediario in relazione alla debolezza dei presidi di sicurezza informatica, anche considerata la facilità con cui un soggetto può simulare una comunicazione ufficiale della banca;
- che conferma di quanto precede trova evidenza negli sms ricevuti e nel registro chiamate prodotti.

DIRITTO

La controversia è regolata dalla disciplina in materia di utilizzi fraudolenti di servizi di pagamento di cui al d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore del d.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 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; in particolare dalle norme relative all'autenticazione di operazioni di pagamento disposte *on line*, nonché all'onere della prova dell'autenticazione ed esecuzione delle operazioni di pagamento in capo all'intermediario ed alla responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento (artt. 10, 10-*bis* e 12 del d.lgs. n. 11/2010 e regolamento delegato (UE) n. 389 del 27 novembre 2017). L'operazione contestata consiste in un pagamento *on line*, eseguito con carta, per l'importo di €. 2.999,00=, in data 24 gennaio

2024; essa risulta dalla lista movimenti della carta allegata in atti e dal dettaglio dell'operazione stessa prodotto dall'intermediario.
Il ricorrente ha riferito nel ricorso di aver ricevuto anche un OTP sms per sottoscrivere un finanziamento: operazione che, tuttavia, non è stata conclusa. Nella denuncia, ha dichiarato che veniva contattato da un soggetto che si spacciava per un operatore dell'intermediario e lo avvisava di un tentativo di accesso al suo conto, riferendogli la necessità di procedere ad alcune operazioni, comunicandogli un codice che gli avrebbe inviato tramite sms.
Si tratta di una delle più attuali strategie e tecniche con le quali soggetti malintenzionati possono tentare accessi fraudolenti a server esposti al web, quali ad esempio *account* di *home banking*.
Sulla base della normativa sopra indicata, in primo luogo è l'intermediario a dover provare, oltre all'insussistenza di malfunzionamenti, la corretta autenticazione, registrazione e contabilizzazione delle operazioni disconosciute, prova che comunque di per sé non è sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore (cfr. art. 10, comma 2, del d.lgs. n. 11/2010, secondo cui "*l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento* (…) *non è di per sé necessariamente sufficiente a dimostrare 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*"). Al riguardo, i Collegi ABF hanno, in più occasioni, precisato che la disciplina in esame istituisce un regime di speciale protezione e di altrettanto speciale *favor* probatorio a favore degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema.
Ne consegue che, qualora l'utente neghi di aver autorizzato un'operazione di pagamento già effettuata, l'onere di provare la genuinità della transazione ricade essenzialmente sul prestatore del servizio; e nel contempo quest'ultimo è obbligato a rifondere con sostanziale immediatezza il cliente in caso di operazione disconosciuta, tranne ove vi sia un motivato sospetto di frode e salva la possibilità per il prestatore di servizi di pagamento di dimostrare, anche in un momento successivo, che l'operazione di pagamento era stata autorizzata.
Preliminarmente, si osserva che la parte ricorrente ha eccepito l'inidoneità della documentazione prodotta dall'intermediario sulla prova della SCA, in quanto di formazione interna al medesimo. L'intermediario ha eccepito che questa documentazione è considerata idonea dall'orientamento uniforme dei Collegi.
A tal riguardo si segnala che, per consolidato orientamento dei Collegi, le dichiarazioni e le allegazioni degli intermediari sono considerate in linea generale genuine, tenuto conto del dovere in capo a questi ultimi di cooperazione al funzionamento della procedura.
Ciò premesso, si osserva che l'intermediario ha dichiarato come le operazioni dispositive possano essere eseguite dall'area riservata al cliente, a cui si accede tramite l'inserimento delle credenziali statiche dell'utente e dell'OTP sms inviato al numero di telefono validato. Ha precisato che tale accesso, eseguito con l'autenticazione forte a due fattori, si verifica nelle ipotesi di primo accesso del cliente all'area riservata e nei casi in cui siano trascorsi più di 180 giorni dall'ultimo accesso eseguito con SCA.
In ogni caso, è possibile usufruire di accessi informativi per i quali non è richiesta l'autenticazione forte, ma che sono limitati alle informazioni relative al saldo del conto ed alle operazioni di pagamento eseguite negli ultimi 90 giorni attraverso uno o più conti di pagamento.

La banca ha poi rappresentato che, nel caso di specie, i truffatori hanno eseguito un'operazione di cambio della *password*, perfezionabile con le seguenti modalità: inserimento del nome utente; inserimento di due cifre del PIN della carta di debito, scelte in maniera randomica dal sistema; autorizzazione al cambio della *password* tramite l'immissione del codice OTP sms giunto al cellulare del ricorrente. L'intermediario ha, quindi, dichiarato che, successivamente al *reset* della *password*, i terzi accedevano all'area personale del cliente mediante le nuove credenziali impostate e, prima di predisporre l'operazione di pagamento, modificavano il massimale giornaliero della carta di debito direttamente dall'area riservata tramite l'inserimento di un codice OTP sms inviato al cellulare certificato.
Infine, sulla base del sistema adottato dall'intermediario ai fini della SCA, per eseguire le operazioni di pagamento, si rendono necessari: la generazione di un codice CVV dinamico mediante inserimento di *username* e *password* e di un codice OTP ricevuto sullo *smartphone*, nonché l'inserimento di un'ulteriore OTP inviata sull'utenza mobile certificata per confermare l'operazione di pagamento. L'intermediario ha riferito che effettivamente, a seguito delle suddette attività propedeutiche, l'operazione di pagamento contestata è stata autenticata dai malfattori mediante: la generazione del CVV dinamico, tramite inserimento del codice OTP sms all'interno dell'area riservata; l'inserimento manuale delle credenziali statiche della carta di debito, consultabili dall'area riservata, e del CVV dinamico generato dall'*app*; la conferma dell'operazione di pagamento di €. 2.999,00= mediante il codice OTP sms inviato al cellulare certificato.
A fronte di quanto rappresentato in merito, il Collegio ritiene che non sia sufficiente ai fini della prova della SCA il contenuto delle evidenze documentali fornite dal PSP relativamente all'esecuzione del pagamento di *e-commerce*. Si rileva innanzitutto che, quanto all'inserimento dei dati statici della carta (inserimento delle credenziali statiche, PAN e data di scadenza, della carta nel POS virtuale), gli stessi non costituiscono né un valido elemento di possesso né un valido elemento di conoscenza, secondo quanto precisato nella *Opinion* EBA del 21 giugno 2019.
Se, dunque, uno degli elementi di autenticazione, costituito dall'OTP sms inviato al cellulare certificato, costituisce senza dubbio un elemento di possesso, anche il CVV dinamico della carta generato in *app* pare debba essere qualificato come ulteriore elemento di possesso, alla luce delle indicazioni fornite dall'EBA nell'*Opinion* del 21 giugno 2019. Sembrerebbe, dunque, essere stato utilizzato un doppio fattore di possesso laddove, invece, in base alla citata *Opinion* dell'EBA, la SCA presuppone il ricorso a due fattori di autenticazione, appartenenti a categorie diverse.
Come tale, la procedura non risulta idonea ad integrare una SCA. Il Collegio non deve, dunque, passare ad esaminare la condotta della parte ricorrente, al fine di accertarne l'eventuale colpa grave, con riguardo all'operazione di bonifico.

P.Q.M.

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.999,00.
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