

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) LOMBARDI	Membro designato dalla Banca d'Italia
(BO) CORRADI	Membro di designazione rappresentativa degli intermediari
(BO) PETRAZZINI	Membro di designazione rappresentativa dei clienti

Relatore BARBARA PETRAZZINI

Seduta del 28/02/2023

FATTO

Con ricorso depositato in data 11 ottobre 2022, il ricorrente espone:

- che per un periodo di un anno circa non riusciva ad accedere al proprio account della banca, collegato alla carta n. 5354*****0922;
- che presso la filiale dove aveva aperto il conto, gli riferivano che la suddetta problematica poteva dipendere dal fatto che il sistema avesse problemi con l'accesso tramite SPID, e lo sollecitavano a richiedere una nuova password tramite il sito;
- che a ogni tentativo di inserire la nuova password inviata dal sistema, appariva la dicitura "credenziali errate";
- che, dopo molti tentativi, riusciva a contattare il numero verde dedicato, che gli forniva la riattivazione del suddetto servizio spiegando che il problema era dato dall'istallazione dell'app su un altro dispositivo;
- che, alla riattivazione del servizio, si accorgeva di un pagamento mai effettuato, in data 22 novembre 2021 alle ore 13:52 presso [omissis] a Napoli, di 599,00 euro;

- che, essendo certo di non aver effettuato il pagamento, ipotizzava che la sua carta di debito fosse stata clonata;
- provvedeva quindi a disconoscere l'operazione e a presentare reclamo all'intermediario.

A fronte di negativo riscontro da parte dell'intermediario, si rivolge pertanto a quest'Arbitro chiedendo la restituzione della somma di 599,00 euro, corrispondente all'importo dell'operazione disconosciuta.

Costituendosi nel procedimento, l'intermediario resistente espone quanto segue:

- di inviare le controdeduzioni per conto dell'intermediario *****P, effettivo titolare del prodotto in questione;
- che il ricorrente è titolare di carta di debito n. 5354*****0922, associata a conto corrente n. 105****939, e ha richiesto il rimborso di un pagamento di 599,00 euro, effettuato il 22 novembre 2021;
- che le verifiche hanno accertato la legittima esecuzione e sostanziale regolarità della transazione;
- che, non avendo la controparte allegato documentazione circa la dinamica di frode intercorsa, l'istanza è ulteriormente meritevole di rigetto;
- che la transazione disconosciuta è stata disposta mediante l'ausilio del token, attraverso un digital wallet;
- che il truffatore è riuscito a ottenere dal ricorrente le chiavi di accesso necessarie per installare sul proprio cellulare l'app della banca, e all'interno di quest'ultima configurare G** Pay;
- che il cliente non ha dichiarato di aver ricevuto e/o risposto a comunicazioni potenzialmente truffaldine, volte a carpire le credenziali di accesso, ma che proprio l'assenza di un qualsiasi cenno ad una qualsivoglia operatività online intrapresa in concomitanza dell'illecito addebito, porta a ricondurre la frode di specie alla tipologia di phishing definita "classica" dal Collegio di Coordinamento;
- che, evidentemente, la parte ricorrente ha comunicato i propri dati personali nell'ambito di una navigazione Internet poco sicura, probabilmente dopo aver cliccato su un link truffaldino ricevuto tramite sms o e-mail;
- che la parte ricorrente avrebbe potuto evitare la truffa utilizzando la diligenza media, posto che la banca interloquisce con i propri clienti solo tramite canali ufficiali e mai richiedendo la comunicazione di dati relativi agli strumenti di pagamento forniti;
- che il cliente non ha né lamentato né denunciato il malfunzionamento della propria utenza telefonica, quindi non è verosimile che possa essere stato vittima di un episodio di SIM swap, circostanza che del resto non può essere dedotta presuntivamente.

DIRITTO

La questione concerne la valutazione del comportamento del ricorrente e dell'intermediario resistente in relazione all'esecuzione di un'operazione di pagamento *on line* non autorizzata, eseguita il 22 novembre 2021 alle ore 13:52, avente ad oggetto la somma richiesta in restituzione di 599,00 euro.

La materia è disciplinata dal d.lgs. 11/2010 (emanato in attuazione della Direttiva 2007/64/CE e successivamente modificato dal d. lgs. 218/2017 in attuazione della Direttiva 2015/2366/UE). Dalla richiamata normativa e, in particolare, dall'art. 10 del d. lgs. 11/2010, discende che, qualora l'utilizzatore neghi -come nella vicenda oggetto del ricorso- di aver autorizzato un'operazione di pagamento eseguita, gravi sull'intermediario l'onere di provare l'avvenuta autenticazione della medesima operazione, la sua corretta registrazione e contabilizzazione, nonché il mancato verificarsi di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti. Tale prova –precisa il comma 2 del citato articolo- non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utente medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi sul medesimo gravanti, essendo onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente.

Nel caso di mancato assolvimento dell'onere probatorio di cui si è detto, l'intermediario è obbligato a riaccreditarne l'importo sul conto del cliente, ai sensi dell'art. 11 del medesimo d.lgs. n. 11/2010.

L'onere di dimostrare la colpa grave o il comportamento fraudolento del titolare dello strumento di pagamento grava quindi sull'intermediario, ma, come più volte affermato dai Collegi territoriali e dal Collegio di Coordinamento, la relativa prova può essere fornita mediante «indizi chiari, precisi e concordanti idonei a comprovare che la ricorrente non abbia custodito la carta di pagamento con la dovuta diligenza» (cfr. la decisione ABF, Collegio di coordinamento, n. 897/2014), ovvero, fermo restando che «la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio», essere fornita dall'intermediario indicando «una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente» (così la decisione ABF, Collegio di Coordinamento, n. 22745/2019).

Osserva il Collegio che l'emittente ha l'obbligo di prevedere forme di autenticazione "forte" per l'autorizzazione di operazioni di pagamento a tutela della sicurezza delle operazioni stesse e del titolare del mezzo di pagamento.

La definizione di autenticazione forte si rinviene nell'art. 1, d.lgs. n. 11/2010, ove si prevede che per autenticazione forte del cliente si intende: «un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente) che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri (...)».

Occorre quindi verificare se nel caso in specie l'intermediario abbia fornito elementi a sostegno della legittimità dell'operazione contestata.

Dalla documentazione in atti, risulta che l'operazione di pagamento eseguita con la carta di debito è stata disposta mediante l'ausilio di Token, tramite l'applicazione mobile G***pay.

Sul punto occorre richiamare la decisione del Collegio di Coordinamento n. 21285/2021, che, con particolare riferimento all'autenticazione delle operazioni disposte tramite wallet, ha chiarito che l'intermediario deve fornire la prova di aver adottato l'autenticazione forte tanto nella fase di tokenizzazione della carta nel wallet quanto in quella relativa all'esecuzione delle operazioni. Invero, con la Q&A ID 2019_4910 l'EBA ha precisato che l'associazione di una carta di pagamento ad un wallet digitale rientra tra quelle azioni che possono comportare un rischio di frode nei pagamenti o altri abusi e, pertanto, richiede l'applicazione della SCA; ciò significa che i PSP devono impiegare una procedura di autenticazione forte per l'accesso al conto di pagamento e una seconda SCA quando l'utente aggiunge la carta di pagamento al digital wallet. È stato specificato, inoltre, che, laddove l'associazione della carta a un wallet digitale avvenga nell'ambito della stessa sessione e della medesima app trovano applicazione i principi dettati nella Q&A 2018_4141 che prevede la possibilità di riutilizzare uno degli elementi impiegati per accedere al conto di pagamento.

Nel caso di specie, la parte resistente afferma che il truffatore sarebbe riuscito ad ottenere le chiavi di accesso indispensabili per effettuare le operazioni di installazione e configurazione, del wallet G***pay, ma, sebbene dalla documentazione tecnica prodotta dall'intermediario sembri emergere che l'autenticazione delle operazioni è avvenuta mediante la carta digitalizzata sul wallet G***pay, ritiene il Collegio che, per nessuna delle due fasi dell'operazione, sia stata documentata l'autenticazione forte.

Ed infatti quanto alla fase di tokenizzazione della carta nel digital wallet non soltanto è lo stesso intermediario a dichiarare che uno dei due fattori di autenticazione è costituito dai dati statici della carta (che, secondo le guidelines EBA e i consolidati orientamenti ABF in materia, non costituiscono valido elemento di autenticazione forte: da ultimo Collegio di Bologna n. 8915/2022), ma non è stata prodotta evidenza in merito all'invio dell'OTP tramite sms al cellulare del ricorrente; quanto alla fase di autorizzazione del pagamento, l'intermediario non precisa quale sia l'ulteriore fattore di autenticazione (in aggiunta al fattore di possesso costituito dalle carte tokenizzate) utilizzato per autorizzare i pagamenti, né tale dato è ricavabile dalla documentazione tecnica in atti.

Ne consegue che la mancata allegazione della necessaria documentazione atta a dimostrare la corretta autenticazione registrazione e contabilizzazione dell'operazione contestata è imputabile all'intermediario che non ha dato prova della sua autorizzazione, rendendo irrilevante ogni ulteriore valutazione in merito alla sussistenza o meno della colpa grave in capo alla ricorrente.

La domanda del ricorrente, volta a chiedere il riaccredito dell'importo di 599,00 euro, merita pertanto accoglimento, senza applicazione della franchigia di legge che, secondo l'orientamento condiviso dai Collegi territoriali, non trova applicazione nel caso di mancata prova della corretta autenticazione delle operazioni disconosciute.

PER QUESTI MOTIVI

Il Collegio – in accoglimento del ricorso – dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 599,00 (cinquecentonovantanove/00).

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARCELLO MARINARI