Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Decisione N. 4315 del 14 marzo 2022

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) MARINARI	Presidente
(BO) BERTI ARNOALDI VELI	Membro designato dalla Banca d'Italia
(BO) MAIMERI	Membro designato dalla Banca d'Italia
(BO) SOLDATI	Membro di designazione rappresentativa degli intermediari
(BO) PETRELLI	Membro di designazione rappresentativa dei clienti

Relatore FABRIZIO MAIMERI

Seduta del 08/02/2022

FATTO

Il ricorrente, titolare di una carta di pagamento, riferisce di aver ricevuto, in data 27.7.2021, un sms inserito nella "chat" ufficiale dell'intermediario, che, segnalando un accesso anomalo, lo invitava a cliccare un *link*, cosa che faceva, venendo reindirizzato su sito riconducibile alla parte convenuta, dove veniva avvisato che sarebbe stato contattato da un operatore. In effetti, alle 13.33 veniva effettivamente contattato da un falso addetto, che gli suggeriva di accedere al proprio conto tramite la *App* installata sul cellulare e di controllare se attraverso notifica *push* risultava segnalato un pagamento in uscita a favore di un sito straniero. Sussistendo una richiesta di autorizzazione, afferma di aver cliccato sull'opzione "non autorizza" e di aver ricevuto un sms dalla banca che l'informava del blocco dell'operatività sul conto. Telefonando al numero verde, apprendeva di essere stato vittima di una truffa: ammette di aver cliccato sul *link* contenuto nel messaggio civetta, di aver effettuato accesso alla *App* della banca e di aver fornito all'operatore il nuovo codice PIN generato dallo stesso truffatore, ma nega di aver fornito credenziali della carta o codici dispositivi, sottolineando che l'operatività sul conto risultava bloccata, dal momento che sullo stesso gravava una procedura di pignoramento. Nella denuncia agli Uffici di Polizia Giudiziaria specifica che il malfattore gli chiedeva di bloccare il pagamento effettuando un prelievo dalla carta del medesimo importo cliccando sulla notifica *push* ricevuta, cosa che ammette di aver fatto.

In sede di controdeduzioni, la banca rileva che è lo stesso ricorrente ad ammettere di aver cliccato sul *link* contenuto nell'sms "civetta", di aver seguito le istruzioni del falso operatore

entrando nella banca multicanale tramite *App* e di aver inserito i suoi dati personali; egli quindi autorizzava la transazione riceveva un messaggio truffaldino che lo informava del blocco dell'operazione poi disconosciuta. La banca attiva presidi di sicurezza di cui dà conto anche sul proprio sito, su cui fornisce pure raccomandazioni alla clientela per evitare situazioni di *phishing*. *smishing* e *vishing*, ma nessun presidio può valere quando è lo stesso cliente a fornire i codici richiesti senza prestare attenzione al contenuto dei messaggi ricevuti.
Alla luce delle rispettive argomentazioni, il ricorrente chiede al Collegio di "verificare la veridicità dei fatti e riavere la somma a me trattenuta"; l'intermediario di "rigettare integralmente la richiesta di rimborso avanzata poiché la responsabilità come dimostrato non è ascrivibile all'intermediario e, al contrario, appare provata la colpa grave del cliente".

DIRITTO

L'operazione disconosciuta consiste in un pagamento *on line* di importo pario a € 930,00 eseguito il 27.7.2021 alle ore 13.48 e agli atti è versata la documentazione che comprova lo svolgimento dei fatti come evidenziato nella parte in fatto.
A fronte del disconoscimento di operazioni di pagamento da parte dell'utente, incombe sull'intermediario l'onere di provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata ai sensi dell'art. 10, comma 1, d.lgs. n. 11/2010, che così dispone: "Qualora l'utilizzatore dei servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente seguita, è onere del prestatore di servizi di pagamento 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". Quanto alle modalità di autenticazione, l'art. 10-*bis* del medesimo d.lgs. prevede: "Conformemente all'art. 98 della direttiva (UE) 2015/2366 e alle relative norme tecniche di regolamentazione adottate dalla Commissione europea, i prestatori di servizi di pagamento applicano l'autenticazione forte al cliente quando l'utente: a) accede al suo conto di pagamento *online*; b) dispone un'operazione di pagamento elettronico: c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi". Ai sensi dell'art. 12, comma 2-*bis* del ripetuto d.lgs., qualora non sia stata adottata la c.d. autenticazione forte (SCA), il cliente risponde soltanto in caso di frode.
Per autenticazione forte s'intende (ai sensi dell'art. 1, lett. q-*bis* d.lgs. n. 11/2010) quella "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, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".
Occorre dunque verificare se, nel caso di specie, l'operazione contestata sia stata autenticata mediante la combinazione di almeno due dei tre elementi che caratterizzano la c.d. "autenticazione forte".
Dalle tracciature depositate in atti emerge l'attività di autenticazione e una nota tecnica prodotta dall'intermediario conclude per il rigetto dell'istanza di rimborso avanzata dal cliente motivando per il "fatto che si è avuto modo di verificare che la transazione contestata è stata effettuata attraverso l'utilizzo della tecnologia 3DS DINAMICO. Questa nuova tecnologia prevede l'utilizzo di password 'usa e getta', generate dagli stessi dispositivi normalmente utilizzati dal cliente per autorizzare operazioni dispositive su BVI (Baca via internet)" che "possono essere conosciute solamente dallo stesso".

Tuttavia, la descrizione – e la documentazione – fornita dalla banca fa emergere che l'autenticazione dell'operazione sia avvenuta mediante inserimento dei dati statici della carta e l'OTP generata tramite notifica *push*. Nelle controdeduzioni l'intermediario afferma che è stato inserito anche un codice PIN, ma questa affermazione non trova corrispondenza nelle tracciature trasmesse. I log infatti rilevano espressamente la mancanza di un Pin (*PINLess, PIN Present: NO*) ma solo la digitazione di una OTP tramite *push*; inoltre la banca afferma che il PIN fornito dal ricorrente ai truffatori era falso. In conclusione, dai log non documentata la presenza di un secondo fattore di autenticazione indipendente (vale a dire il PIN), sicché la SCA non risulta integrata.

Pare dunque che la metodologia autenticativa qui utilizzata non si discosti molto da quella frequentemente adottata dall'intermediario e sulla quale i Collegi hanno avuto modo già di esprimersi univocamente: "la resistente produce il log informatico da cui risulta che la transazione fraudolenta è stata perfezionata con l'utilizzo del protocollo 3D Secure, ovvero dire con il corretto inserimento dei dati della carta (comprensivi del cvv) e del codice OTP generato tramite token in dotazione alla cliente. Orbene, l'Opinion dell'EBA del 2019 ha escluso che i dati della carta di credito possano essere qualificati come uno degli elementi di conoscenza rilevanti ai fini della SCA. Questa conclusione trova conforto in una recente decisione di questo Collegio (Collegio di Roma, decisione n. 9905 del 13.04.2021) in cui è rilevato che i dati riportati sulla carta (numero, scadenza e cvv), non costituiscono un elemento di possesso e di conoscenza e che, pertanto, con riguardo alle operazioni successive al 14 settembre 2019, essi non integrano un idoneo fattore di autenticazione. In questo contesto fattuale l'indagine sulla eventuale colpa grave della parte istante risulta irrilevante e, pertanto, il ricorso può essere accolto": così Collegio di Roma, decisione n. 19529/2021; "Riepilogando, tutte le transazioni sembrano essere state autenticate tramite la spendita di un elemento di possesso, consistente in un codice OTP inviato sul cellulare dell'utente ora tramite sms, ora tramite notifica nell'applicazione. Dalle suddette evidenze non emerge, invece, l'utilizzo di un ulteriore, indipendente fattore di autenticazione" (Collegio di Bologna, decisione n. 21502/2021).

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 930,00 (novecentotrenta/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