

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) CORNO	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore (MI) GIORGIO CORNO

Seduta del 04/03/2025

FATTO

Il ricorrente è titolare di rapporto di conto corrente presso l'intermediario, al quale è appoggiata una carta di pagamento emessa da altro intermediario. In data 4 luglio 2023 il ricorrente riceveva un SMS sulla propria utenza mobile, il cui mittente risultava essere l'emittente della carta di pagamento, che lo avvisava di una movimentazione di denaro sospetta relativa ad un bonifico di € 4.970,00. Qualche minuto dopo la ricezione dell'SMS, il ricorrente riceveva una telefonata da un soggetto qualificatosi come del servizio sicurezza dell'intermediario, confermando l'operazione sospetta. Il ricorrente negava di averla autorizzata e l'interlocutore gli dava indicazioni su come bloccare l'operazione, che seguiva. L'interlocutore chiedeva altresì al ricorrente di digitare sulla tastiera del proprio cellulare il tasto “*21*” seguito da altri numeri. Con ulteriori SMS veniva avvisato dell'avvenuto blocco dell'*home banking*, della carta di pagamento e dell'app. Parallelamente il ricorrente contattava il direttore della propria filiale di riferimento, il quale gli confermava l'esecuzione dell'operazione e il cliente ribadiva la propria intenzione di bloccarla in quanto dal medesimo non eseguita. Richiamava infine il numero del presunto operatore del servizio di sicurezza, il quale gli diceva che la banca non era ancora stata informata dei passaggi effettuati per bloccare l'operazione non autorizzata. A quel punto il ricorrente si avvedeva di essere stato contattato da un truffatore e di non aver più accesso alla propria area riservata nonché che quanto digitato su indicazione del truffatore era

servito ad attivare una deviazione di chiamata. Infatti, il direttore della filiale aveva provato a ricontattare il cliente e alla sua utenza aveva presumibilmente risposto il truffatore, fingendosi il ricorrente e confermando la genuinità dell'operazione in quanto effettuata dalla moglie (mentre il ricorrente non è sposato). In data 5 luglio 2023 il ricorrente ha presentato denuncia alle Autorità. Il ricorrente ha presentato reclamo all'intermediario in data 25 settembre 2024 chiedendo il disconoscimento dell'operazione truffaldina, reclamo riscontrato negativamente dall'intermediario in data 3 ottobre 2024.

Con ricorso all'ABF in data 21 novembre 2024, il ricorrente chiede l'annullamento dell'operazione contestata e il rimborso della somma ingiustamente addebitata sul suo conto corrente per € 4.970,00. Il ricorrente afferma che il direttore della filiale non si sarebbe tempestivamente attivato a fronte della segnalazione del ricorrente in merito a quanto occorso; nonché che l'addebito sarebbe stato validato dalla banca che lo ricontattava sul cellulare, presumibilmente con chiamate deviate dai truffatori, per cui la chiamata veniva ricevuta da soggetto che confermava la bontà dell'operazione in quanto eseguita dalla moglie, malgrado egli non sia sposato.

Con le controdeduzioni, l'intermediario chiede il rigetto del ricorso. Produce documentazione che attesta che l'operazione è stata correttamente contabilizzata, registrata e autenticata tramite il corretto inserimento di un doppio fattore di autenticazione. Quanto alla dinamica della truffa l'intermediario rileva che nel ricorso non risulta essere stata fornita prova dell'SMS truffaldino, né della chiamata ricevuta. Peraltro, il ricorrente avrebbe dovuto contattare subito il supporto telefonico della banca, sempre attivo, o l'agenzia territoriale per verificare quanto stava accadendo. Inoltre dalla denuncia in atti si desume sia che è lo stesso ricorrente ad attivare il servizio di "deviazione chiamate", sia che gli operatori della filiale della banca hanno prontamente contattato il cliente per verificare le genuinità dell'operazione in questione. Afferma infine di essersi tempestivamente attivato per tentare il recupero delle somme oggetto della frode presso la banca beneficiaria, purtroppo con esito negativo.

Con repliche alle controdeduzioni, il ricorrente insiste per l'accoglimento della propria domanda. Ribadisce la scorrettezza della condotta della banca in quanto la filiale avrebbe rappresentato di non poter bloccare il bonifico, con evidente negligenza nella gestione della vicenda da parte della banca e una celerità nell'attivarsi per il disconoscimento da parte del cliente. Afferma di non aver mai comunicato le proprie credenziali e che i truffatori sarebbero entrati nella sua area *home banking*, conoscendone tutti i relativi dati in precedenza e quindi senza utilizzare la password di accesso.

L'intermediario nelle controrepliche richiama le precedenti difese e insiste per il rigetto del ricorso. Precisa che la ricostruzione dei fatti del cliente è contraddittoria a pretestuosa e si evince che lo stesso abbia collaborato con i truffatori al compimento della truffa, senza interpellare la banca.

DIRITTO

Oggetto del ricorso è la richiesta del rimborso di n. 1 operazione di bonifico per € 4.970,00 effettuata in data 4 luglio 2023 alle ore 12:19.

Il Collegio evidenzia che l'operazione di pagamento contestata rientra nell'ambito applicativo del D.lgs. 27 gennaio 2010, n. 11, come modificato dal D.lgs. 15 dicembre 2017, n. 218. Poiché il ricorrente, quale utente di servizi di pagamento, ha negato di aver autorizzato le operazioni di pagamento eseguite, è onere dell'intermediario, ai sensi dell'art. 10 del medesimo D.Lgs., quale prestatore di servizi di pagamento, provare che tali operazioni sono state autenticate, correttamente registrate e contabilizzate e che non

hanno subito le conseguenze del malfunzionamento delle procedure necessarie per la loro esecuzione o altri inconvenienti. Ai sensi dell'art. 10 bis del ricordato D.Lgs., i prestatori di servizi di pagamento sono tenuti ad applicare modalità di autenticazione forte del cliente (SCA *strong customer authentication*) quando l'utente: a) accede al suo conto di pagamento *on-line*; 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. Nel caso di avvio di un'operazione di pagamento elettronico a distanza, l'autenticazione forte del cliente applicata dai prestatori di servizi di pagamento comprende elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e ad un beneficiario specifico. L'autenticazione forte (SCA) è richiesta sia nella fase di accesso al conto / *enrollment* dell'app / registrazione della carta sul *wallet*, sia nella fase di esecuzione delle singole operazioni e si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza, inerenza, possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse. Alla luce del disconoscimento delle operazioni da parte del cliente, è altresì onere dell'intermediario di fornire prova della frode, del dolo o della colpa grave dell'utente.

Nel caso di specie, la prova della corretta autenticazione, corretta registrazione e contabilizzazione dell'operazione disconosciuta dal cliente deve avere ad oggetto l'accesso all'area web e l'esecuzione dell'operazione contestata.

Per entrambe le fasi, l'intermediario afferma che l'operazione è stata autorizzata tramite canale *web*, mediante notifica *push* sul *device* del ricorrente (elemento di possesso) e inserimento del PIN (elemento di conoscenza).

Dalla documentazione prodotta dall'intermediario, quanto all'accesso all'area web, si ricava quanto segue:

- l'accesso all'*home banking* è stato effettuato tramite Web ("canale: Web");
- lo *user id* coincide con quello del cliente;
- è stata inviata una notifica *push* autorizzata tramite inserimento del PIN ("tipo SCA: PushNotification con PIN"). L'inserimento del codice PIN si evidenzia dalla voce "inserimento_Codice_Pin: SI" (elemento di conoscenza);
- non è possibile rinvenire prova in merito al *device* (elemento di possesso) al quale sia stata inviata la notifica *push* - risulta una voce "Device print" contenente dati che tuttavia non sono spiegati e non sono quindi ricollegabili, in mancanza di altri elementi, al *device* del cliente.

Quanto all'esecuzione dell'operazione contestata, dalla documentazione in atti si desume che:

- è stata inviata una notifica *push* autorizzata tramite inserimento del PIN ("tipo SCA: PushNotification con PIN");
- è stato inserito il PIN (elemento di conoscenza). L'inserimento del codice PIN si evidenzia dalla voce "inserimento_Codice_Pin: SI" (elemento di conoscenza);
- non è possibile rinvenire prova in merito al *device* (elemento di possesso) al quale sia stata inviata la notifica *push* (elemento di possesso) - risulta una voce "Device print" contenente dati che tuttavia non sono spiegati e non sono quindi ricollegabili, in mancanza di altri elementi, al *device* del cliente.

In definitiva, in relazione ad entrambe le fasi, risulta l'inserimento di un PIN ("inserimento Codice PIN:SI") a seguito di ricezione di una notifica *push* ("tipo SCA: PushNotification con PIN"); manca, invece, evidenza del *device* a cui è stata inviata la predetta notifica *push* e quindi l'effettivo invio della *push* sul *device* del cliente.

Alla luce di quanto precede il Collegio non ritiene provata da parte dell'intermediario la corretta autenticazione, corretta registrazione e contabilizzazione delle operazioni di pagamento disconosciute dal cliente, con conseguente accoglimento integrale dalla richiesta di rimborso dell'operazione disconosciuta.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 4.970,00.

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
ANDREA TINA