COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) DENOZZA	Membro designato dalla Banca d'Italia
(MI) CETRA	Membro designato dalla Banca d'Italia
(MI) CORNO	Membro di designazione rappresentativa degli intermediari
(MI) GRIPPO	Membro di designazione rappresentativa dei clienti

Relatore (MI) CORNO

Seduta del 08/02/2024

FATTO

Il ricorrente è titolare di rapporto di conto corrente presso l'intermediario nonché della carta di debito n. ***069, della carta di debito n. ***851, della carta di credito prepagata n. ***238, emessa da altro istituto diverso dall'intermediario resistente, e della carta di credito n. ***349. In data 24 marzo 2023 alle ore 15:30 il cliente riceveva SMS apparentemente proveniente dall'istituto emittente di una delle sue carte di pagamento – diverso dall'intermediario resistente – il quale informava il ricorrente che era in corso un'operazione anomala, invitandolo ad eseguire una verifica cliccando sul link ivi contenuto ("*Gentile cliente, a seguito di un pagamento anomalo con le carte a lei intestate.La invitiamo ad eseguire la verifica al portale: http://bitly.ws/C448*"). Il ricorrente cliccava sul link, aprendo una pagina apparentemente riconducibile all'emittente della carta dal quale sembrava provenire l'SMS e gli veniva chiesto di inserire le proprie credenziali, cosa che il medesimo faceva. Veniva infine contattato telefonicamente alle ore 16:36 da una utenza mobile e l'interlocutore informava il ricorrente che erano in corso movimenti anomali, invitandolo a recarsi presso il più vicino ATM, cosa che non faceva essendo impossibilitato. L'interlocutore allora gli chiedeva verbalmente di fornire dei codici (credenziali personali PIN e user ID) che il medesimo forniva, per poi chiudere la telefonata informando che avrebbe ricevuto gli importi oggetto delle operazioni sul suo conto entro ventiquattro ore. Dopo circa mezz'ora dai fatti, il ricorrente veniva contattato dall'intermediario resistente il quale informava di taluni movimenti e chiedeva se fossero

stati dal medesimo autorizzati, chiedeva altresì all'operatore il blocco delle operazioni, delle carte di pagamento e del suo conto corrente. Verificava infine che ignoti avevano effettuato alcune operazioni per l'importo complessivo di euro 2.292,08 e, in data 30 marzo 2023, ha presentato denuncia alle Autorità per quanto occorso. Il ricorrente ha altresì provveduto al disconoscimento delle operazioni truffaldine in data 20 maggio 2023.
Con ricorso all'ABF in data 25 luglio 2023 il cliente ha chiesto il rimborso di euro 2.292,08 oggetto delle operazioni non autorizzate e disconosciute, affermando di essere rimasto vittima di una truffa.
L'intermediario resiste con controdeduzioni del 10 ottobre 2023 chiedendo il rigetto del ricorso. In primo luogo, afferma la propria carenza di legittimazione passiva quanto alle operazioni effettuate con carta di credito prepagata n. ***238, in quanto emessa e gestita da altro intermediario. Produce prova della corretta autenticazione, registrazione e contabilizzazione delle operazioni disconosciute, con utilizzo di due fattori e quindi in conformità alla SCA, e dell'assenza di rilevi di alcuna anomalia in tali operazioni. L'intermediario afferma altresì che il ricorrente sarebbe stato tempestivamente informato circa l'effettuazione delle operazioni con invio di appositi SMS *alert*. Rileva infine che il ricorrente non ha prodotto alcunché al fine di provare l'asserita truffa subita e, in particolare, l'SMS civetta asseritamente ricevuto, con ciò ritenendo sussistente la colpa grave del ricorrente. Ad ogni modo l'intermediario precisa che il ricorrente stesso ammette di aver seguito pedissequamente le indicazioni del truffatore, comunicando le proprie credenziali personali.
Con repliche del 2 novembre 2023 il ricorrente produce l'SMS civetta ricevuto sulla sua utenza mobile e afferma la lacunosità dei sistemi di sicurezza dell'intermediario. Contesta l'eccezione di carenza di legittimazione passiva per quanto attiene alla carta prepagata n. ***238.
Con le controrepliche del 24 novembre 2023 l'intermediario ribadisce l'autenticazione forte con riguardo alle operazioni contestate, avvenuta grazie al contributo del ricorrente che ha comunicato a terzi le proprie credenziali personali. Quanto all'SMS civetta prodotto, l'intermediario rileva che il link contenuto nell'SMS non aveva alcun rimando all'intermediario o all'emittente della carta prepagata, con evidente natura non genuina del medesimo. Evidenzia altresì che il ricorrente non avrebbe prodotto evidenza del numero dal quale proveniva la telefonata truffaldina. Insiste infine sulla propria carenza di legittimazione passiva quanto alla carta prepagata.

DIRITTO

Oggetto del ricorso è la richiesta del rimborso di n. 6 operazioni di pagamento per complessivi euro 2.291,00 e rispettivamente:

- operazione con la carta di credito prepagata n. ***238, emessa da altro istituto diverso dall'intermediario convenuto, in data 24 marzo 2023 per euro 400,00;
- bonifico istantaneo in data 24 marzo 2023 per euro 90,00 alle ore 16:23;
- operazione con la carta di debito n. ***069, appoggiata al conto con l'intermediario, in data 24 marzo 2023 per euro 425,00 alle ore 16:39 ed euro 350,00 alle ore 16:41;
- operazione con la carta di debito n. ***851, appoggiata al conto con l'intermediario, in data 24 marzo 2023 per euro 660,00 alle ore 16:29 ed euro 366,00 alle ore 16:35;

Preliminarmente, con riguardo all'operazione effettuata con la carta di credito prepagata n. ***238, il Collegio, come da proprio orientamento consolidato, deve dichiarare il difetto di legittimazione passiva dell'intermediario resistente, in quanto mero collocatore della carta di pagamento e prestatore di servizi in convenzione con l'emittente dello strumento di pagamento. Dalla documentazione in atti emerge che l'intermediario resistente riceve la richiesta di emissione della carta, la istruisce e la trasmette all'emittente, il quale è proprietario esclusivo della carta ed è destinatario di eventuali reclami e/o ricorso all'ABF (art 45 del contratto in atti). La richiesta di rimborso dell'operazione effettuata con tale carta, pertanto, non potrà essere esaminata da questo collegio non sussistendo la legittimazione passiva dell'intermediario resistente.

Quanto all'operazione di bonifico istantaneo ed alle operazioni effettuate con la carta di debito n. ***069, in base alle evidenze in atti, esse sono state eseguite con accesso alla APP dell'intermediario dal *device* del ricorrente (elemento di possesso) e con inserimento del fattore biometrico del ricorrente già registrato (elemento di inerenza). Da ciò ne discende che le operazioni sono state effettuate materialmente dal ricorrente medesimo e non dal truffatore, seppure in quanto indotto in errore dal medesimo. Alla fattispecie non può, pertanto, trovare applicazione il D.lgs. n. 11/2010 che disciplina le operazioni non autorizzate e, cioè, ai sensi dell'art. 5, quelle effettuate in assenza del consenso del pagatore. Secondo l'orientamento consolidato dei Collegi, peraltro, non può essere configurata "come non autorizzata l'operazione compiuta personalmente dalla parte ricorrente, sia pure sulla base del vizio di volontà sopra descritto." (così Collegio di Milano n. decisione 4567/2022). Il Collegio di Milano ha di recente affermato che, quando l'operazione è compiuta direttamente dal cliente, sia pure su induzione di un terzo truffatore, la banca è esonerata dalla prova dell'autenticazione. Peraltro, come da giurisprudenza di questo Collegio, considerando il rilievo degli obblighi di protezione che discendono dalle norme di diritto comune, (si veda Collegio di Milano, decisione n. 8435/2023), la banca, tuttavia, può rispondere in tutto o in parte del danno subito dal cliente quando questi sia stato indotto all'operazione sulla base di uno *spoofing* sofisticato oppure in assenza di *alert* nell'ipotesi di una pluralità di operazioni significativamente distanziate temporalmente o anche in presenza di operazioni particolarmente anomale.

Nel caso di specie non si ravvisa alcun indice di *spoofing* particolarmente sofisticato considerato che il link contenuto nell'SMS truffaldino non aveva alcuna attinenza con l'intermediario convenuto né con altro istituto emittente di carte di pagamento e la telefonata ricevuta dal ricorrente – in base a quanto dal medesimo dichiarato in sede di denuncia – proveniva da un numero mobile non riconducibile all'intermediario. Pertanto, la richiesta di rimborso deve essere rigettata.

Quanto alle altre operazioni oggetto del presente ricorso, effettuate con la carta di debito n. ***851, occorre precisare che le medesime rientrano 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 a un beneficiario specifico. L'autenticazione forte (SCA) è richiesta sia nella fase di *(i)* accesso al conto / *enrollment* dell'app / registrazione della carta sul *wallet*, sia nella fase di *(ii)* 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 dell'autenticazione forte deve avere ad oggetto tutte le fasi relative all'effettuazione delle operazioni contestate ovvero *(i)* l'accesso all'area riservata e l'attivazione della password statica *(ii)* l'effettuazione delle operazioni.
L'intermediario afferma che l'accesso all'area riservata sarebbe avvenuto tramite web con inserimento del codice utente e del primo codice segreto (elemento di conoscenza) e del codice generato da notifica *push* autorizzativa (elemento di possesso). Dalle evidenze prodotte in atti dall'intermediario risulterebbe nella colonna "descrizione operazione" l'inserimento del codice utente; quanto invece all'inserimento del primo codice segreto, si legge, in corrispondenza della stringa "descrizione operazione" la dicitura "login di secondo livello" e in corrispondenza della stringa "descrizione dati operativi", si riscontra l'inserimento del "codice corretto" (elemento di conoscenza). Non si ha tuttavia evidenza dell'inoltro del codice generato da notifica *push* autorizzativa (elemento di possesso).
Il Collegio, pertanto, non ritiene provato l'utilizzo del secondo fattore di autenticazione dell'elemento di possesso non essendo stato prodotta agli atti la relativa evidenza. Tanto basta a ritenere non provata l'autenticazione forte con riguardo alle operazioni effettuate con la carta di pagamento n. ***851 con conseguente riconoscimento del diritto al rimborso di tali operazioni in favore del ricorrente per complessivi euro 1.026,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.026,00.
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
FLAVIO LAPERTOSA