## COLLEGIO DI MILANO

composto dai signori:

| | |
|---|---|
| (MI) LAPERTOSA | Presidente |
| (MI) TINA | Membro designato dalla Banca d'Italia |
| (MI) CETRA | Membro designato dalla Banca d'Italia |
| (MI) SANTARELLI | Membro di designazione rappresentativa degli intermediari |
| (MI) PERSANO | Membro di designazione rappresentativa dei clienti |

Relatore (MI) CETRA

Seduta del 04/04/2024

## FATTO

Con ricorso del 16 novembre 2023, parte ricorrente riferiva di essere titolare del conto corrente n. ***700 presso l'intermediario e di fruire del servizio home banking con l'app D*** scaricata sul proprio cellulare e una seconda app N** della carta di credito ***496 collegata al conto corrente; esponeva che in data 10.8.2023 tentava di entrare nella propria app N** collegata alla carta di credito, non riuscendovi; alle ore 13.47 veniva contattato telefonicamente da un asserito operatore dell'intermediario dal numero *****671, corrispondente al contatto di una filiale dello stesso, a suo dire per fornire assistenza con la carta di credito anzidetta; tale operatore lo informava della necessità di aggiornare l'app installata sul proprio cellulare; il cliente accedeva alla propria app e inseriva manualmente il PIN ed effettuava il riconoscimento biometrico; nel corso della chiamata, comunicava al frodatore l'indirizzo di posta elettronica; in una successiva chiamata delle 14.36 il sedicente operatore comunicava la buona riuscita delle operazioni di aggiornamento e che l'app avrebbe ripreso a funzionare in data 14.8.2023; nel suddetto giorno veniva contatta dal direttore di una filiale dell'intermediario che gli comunicava che dal suo conto corrente erano stati disposti n. 3 bonifici (di € 2.600,00, € 2.400,00 e € 1.300,00); non avendo autorizzato tale operazioni, disconosceva le stesse e sporgeva denuncia alle autorità competenti; sempre in data 14.8.2023 l'intermediario comunicava il blocco del terzo bonifico e ne preannunciava il riaccredito. Poco dopo, veniva comunicato il blocco

dell'utenza collegata all'app D***; seguiva un'interlocuzione dalle parti, nella quale veniva comunicato al cliente il rigetto della richiesta di rimborso dei primi due bonifici; a settembre 2023 il cliente rilevava di aver ricevuto una mail da parte dell'intermediario nella quale comunicava l'attivazione di un nuovo dispositivo il giorno 10.8.2023. Tale mail era archiviata nella posta indesiderata. Presentato senza esito il reclamo nei confronti dell'intermediario convenuto, attivava, quindi, il presente procedimento per richiedere il rimborso delle somme sottratte, pari ad € 5.000,00 oltre le commissioni per € 7,00.

L'intermediario, nelle controdeduzioni, precisava che presso il suo sistema anagrafico erano censiti, registrati e certificati i contatti che il cliente aveva comunicato in sede di attivazione/contrattualizzazione dei servizi telematici, associati all'utenza internet banking n. ***692. Tale utenza non era stata mutata nelle giornate contingenti la data in cui si era perpetrata la truffa; le operazioni erano state correttamente contabilizzate, registrate e autenticate in quanto risulta che le stesse fossero avvenute con il corretto inserimento delle credenziali; che sussisteva la colpa grave del cliente, in quanto lo stesso avrebbe comunicato le credenziali necessarie alla configurazione dell'APP su un nuovo dispositivo, permettendogli il controllo della sua internet banking. Inoltre, il ricorrente avrebbe effettuato l'accesso all'app D***, convinto ad effettuare un asserito aggiornamento necessario da parte del frodatore, malgrado avesse riscontrato problemi con l'utilizzo dell'app N** riferibile ad un altro intermediario e connessa all'utilizzo della carta di credito; che il numero dal quale il cliente aveva ricevuto la chiamata non poteva essere ricondotto all'intermediario in quanto il nome dello stesso non compariva nel display del cellulare del ricorrente. In ogni caso, la riconducibilità del numero a parte resistente era stata effettuata in data 30.8.2023 e quindi successivamente all'occorso; non erano stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici. Chiedeva, per tutto quanto precede, il rigetto del ricorso ovvero, in subordine, di considerare il comportamento del ricorrente ai fini del riconoscimento del concorso di colpa.

Il ricorrente replicava che l'intermediario non avesse provato la corretta autenticazione delle operazioni di bonifico; che dall'analisi delle controdeduzioni, risultava che le suddette operazioni erano state effettuate dai frodatori in completa autonomia; che risulta provato che durante l'occorso il cliente non avesse fornito alcun codice e che durante le asserite operazioni di aggiornamento non avesse visualizzato alcuna schermata dalla quale si desumesse una disposizione di pagamento; che la comunicazione dell'indirizzo mail non potesse costituire motivo di una sua colpa grave. Il cliente insisteva quindi nella domanda espressa nel ricorso. L'intermediario, con le controrepliche, eccepiva che le telefonate ricevute dal cliente in data 10 agosto 2023 dal numero ***691 non erano allo stesso riconducibili; contestava l'affermazione avversaria secondo cui i n. 2 codici OTP sarebbero stati inviati dall'intermediario al numero di telefono del device dei truffatori in quanto è documentalmente provato che tali OTP sono state inviati esclusivamente ai contatti del cliente; ribadiva che il cliente avesse tenuto una condotta non corretta e diligente, non custodendo le proprie credenziali, ma comunicandole al truffatore.

## DIRITTO

Il Collegio è chiamato a pronunciarsi su una controversia attinente alla richiesta di rimborso di somme indebitamente sottratte alla parte ricorrente attraverso due operazioni di bonifico avvenute il 10 agosto 2023: esse, pertanto, in quanto operazioni disconosciute,

rientrano nell'ambito di applicazione della disciplina del d. lgs. 27.1.2010, n. 11 di recepimento della Direttiva 2007/64/CE sui servizi di pagamento, come modificata dal d. lgs. 15 dicembre 2017, n. 218, di recepimento della Direttiva 2015/2366/UE.

Il Collegio ricorda che, per la normativa appena richiamata, la corretta esecuzione di un'operazione di pagamento è subordinata al consenso del pagatore (art. 5 d. lgs. 11/2010), prestato nella forma e secondo la procedura contrattualmente prevista. Qualora l'utente neghi di aver autorizzato l'operazione o sostenga che questa non sia stata correttamente eseguita, lo stesso può ottenerne il rimborso dell'importo (art. 11 d. lgs. 11/2010), a meno che il prestatore dei servizi di pagamento non riesca a provare che l'operazione contestata sia stata autenticata, correttamente registrata e contabilizzata e che non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti (art. 10, comma 1, d. lgs. 11/2010). Il prestatore dei servizi, peraltro, assolto con successo questo primo onere, necessario ma di per sé insufficiente a dimostrare che l'operazione sia stata autorizzata dal titolare, deve ancora provare, al fine dell'esonero da responsabilità (art. 10, comma 2, d. lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento, fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 d. lgs. 11/2010, trattandosi primariamente di obblighi di custodia del dispositivo e delle chiavi di accesso al servizio. La valutazione della condotta dell'utilizzatore, ai fini dell'eventuale giudizio di colpa grave, deve fondarsi sulla considerazione del complesso di circostanze che caratterizzano il caso concreto.

Il Collegio ricorda, inoltre, che la suddetta autenticazione si deve realizzare in forma di autenticazione forte (c.d. strong customer authentication in acronimo SCA), secondo quanto stabilito dagli artt. 97 e 98 della PDS2, dall'art 10-bis del d. lgs. 10/2011 e nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dallo stesso EBA. E questo sia nella fase di accesso al conto/*enrollment* dell'*app*/registrazione della carta sul *wallet*, sia nella fase di esecuzione delle singole operazioni: l'autenticazione, in tutti questi casi, richiede almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso; gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Il Collegio, passando allo specifico caso oggetto di decisione, rileva che l'intermediario ha sostenuto che le operazioni siano state correttamente contabilizzate, registrate e autenticate e ricostruisce l'operatività fraudolenta nelle seguenti fasi: registrazione di un nuovo dispositivo sull'app, con attivazione del servizio "*licenza smart OTP*"; accesso all'app dal nuovo dispositivo; esecuzione delle operazioni disconosciute.

Il Collegio ravvisa, tuttavia, che il file prodotto dall'intermediario è in parte illeggibile e, pertanto, non è possibile confermare la ricostruzione da esso offerta della dinamica della truffa. Inoltre, sempre con riferimento *all'enrollment* l'intermediario, allega alle controrepliche evidenza relativa alle fasi del processo di attivazione di un nuovo dispositivo ma senza fornire evidenza dell'inserimento di Utenza + Password dopo l'attivazione dell'app sul nuovo dispositivo; l'analisi dei log relativi all'inserimento del nuovo PIN non permette di riscontrare l'ora dell'operazione; anche in relazione l'inserimento del secondo codice OTP, l'intermediario allega evidenze carenti dal momento che, pur indicando l'invio di un presunto messaggio contenente l'OTP al cellulare del cliente alle

ore 13:59:02 del 10.08.2023, non è possibile evincere il contenuto dell'sms che dovrebbe contenere tale codice.

Questo Collegio, non diversamente da come si è già orientato in casi analoghi, ritiene che non sia provata la SCA perché dalla documentazione prodotta, pur rilevandosi l'utilizzo del dispositivo oggetto di *enrollment* (elemento di possesso), non è possibile ricavare l'inserimento della password o del PIN (elemento di conoscenza).
Il Collegio, sulla base di quanto emerso, ritiene che l'intermediario non ha fornito piena prova della corretta autenticazione dell'operazione disconosciuta dalla parte ricorrente, in relazione alla registrazione di un nuovo device. E una volta constatato il mancato raggiungimento della prioritaria prova della SCA, è irrilevante indagare ulteriormente se la condotta della parte ricorrente sia stata improntata a diligenza, o se la dinamica della frode sia stata circostanziata a sufficienza. Per questa ragione, il Collegio ritiene di dover accogliere la domanda di rimborso della somma di € 5.000,00 fraudolentemente sottratta tramite le operazioni di bonifico esaminate, oltre rimborso delle relative commissioni per un totale di € 7,00.

**PER QUESTI MOTIVI**

**Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 5.007,00.**

**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