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 27 novembre 2023, parte ricorrente riferiva che in data 10.8.2023 riceveva un sms con il quale veniva invitato a cliccare su un link per certificare l'indirizzo e-mail utilizzato per le operazioni bancarie; che successivamente veniva contattato da una utenza fissa riconducibile all'intermediario e che, nel corso della telefonata, un presunto operatore lo assisteva nella compilazione di un form online con l'inserimento delle credenziali di accesso ai servizi di home banking; il giorno dopo, contattato dalla propria banca, apprendeva dell'avvenuta esecuzione di alcuni bonifici che disconosceva; due di questi, per l'importo complessivo di € 5.000,00, non venivano annullati dalla banca. Presentato senza esito il reclamo nei confronti dell'intermediario convenuto, attivava, quindi, il presente procedimento per richiedere il rimborso delle somme sottratte, pari ad euro 5.000,00.

L'intermediario, nelle controdeduzioni, precisava che il cliente era titolare del conto corrente n. ***100, sul quale erano attivi i servizi di Banca Telematica *Web; che nel sistema anagrafico della banca erano censiti/certificati i contatti (numero di cellulare e indirizzo mail) comunicati dal cliente al momento dell'attivazione dei servizi di banca telematica e che tali contatti, associati all'utenza di internet banking del cliente non sono

mai stati modificati nelle giornate contingenti la data della truffa; riferiva che, al momento dell'attivazione dei servizi di internet banking, la banca fornisce al cliente le credenziali di accesso (Codice utente ed una password inviata tramite email all'indirizzo fornito dal correntista), dati questi personali e necessari per effettuare correttamente: i) l'attivazione dell'App *Mobile (scaricabile dagli store ufficiali Apple e/o Android); ii) il login all'internet banking (sia tramite App *Mobile, sia tramite il sito internet della Banca); i contatti certificati erano gli unici canali utilizzati per l'invio delle comunicazioni al cliente; rilevava che, per installare una nuova App *Mobile ed attivare così una nuova licenza SmartOTP era necessario inserire correttamente Codice utente+Password+OTP ricevuto per email+OTP ricevuto per sms; che in fase di installazione ed attivazione della nuova App l'applicazione richiedeva al cliente di inserire un PIN numerico di 5 cifre, scelto il quel momento, utile poi per effettuare le svariate operazioni bancarie, fra cui i bonifici; oltre a ciò veniva richiesto di scegliere se effettuare i successivi accessi all'APP e le future operazioni bancarie tramite fattore biometrico o PIN; per accedere all'internet banking tramite App era necessario inserire sulla App il codice utente, la password e il Pin e una volta collegati le operazioni dispositive venivano autorizzate con l'inserimento del PIN sulla notifica push sull'App; evidenziava come il frodatore avesse potuto beneficiare delle operazioni contestate solo grazie alla piena collaborazione del cliente; che i log in atti indicano: i) l'avvenuto invio da parte della banca ai recapiti certificati e ricezione da parte del cliente, dell'email contenente il primo codice di attivazione e dello SMS contenente il secondo codice OTP necessario per l'attivazione di una nuova APP; ii) il corretto inserimento dei codici autorizzativi comunicati al cliente con specifico testo; iii) l'avvenuto invio delle comunicazioni di notifica relative all'esecuzione delle operazioni; che già dalla lettura della denuncia e del successivo reclamo emergessero evidenti elementi di anomalia nella condotta negligente ed imprudente tenuta dal cliente il 10.8.2023; lo stesso cliente aveva, infatti, dichiarato di aver cliccato sui link contenuti nei messaggi civetta a lui inviati, fornendo tutti i propri dati bancari di accesso all'internet banking e di aver disinstallato l'APP dal proprio smartphone; riteneva che il cliente, seguendo la procedura illustrata dal proprio interlocutore, avesse pure consentito l'attivazione della APP su un nuovo telefono cellulare; precisava che l'APP *Mobile può essere installata solo un unico dispositivo mobile per volta, pertanto, nel caso in cui il cliente richiedesse (quale il caso di specie) l'attivazione di una nuova APP *Mobile/licenza smartOTP, doveva i) prima procedere alla disinstallazione dal proprio dispositivo mobile della predetta APP (proprio come avvenuto nel caso di specie), e solo successivamente, ii) poi procedere con una nuova installazione/installazione della medesima; tenuto conto di quanto affermato in sede di denuncia, riteneva verosimile che il cliente avesse comunicato al presunto operatore: i) i propri dati personali di accesso all'internet banking; ii) i codici OTP per l'attivazione di una nuova licenza smartOTP/App *Mobile sul altro dispositivo; il cliente aveva così consentito ai frodatori di eludere i sistemi di sicurezza della banca e conseguentemente di operare autonomamente dal suo conto corrente; le dichiarazioni rese dal cliente e le evidenze documentali, erano tali da delineare la colpa grave in capo al cliente stesso; in fase di attivazione della nuova licenza smartOTP sul nuovo cellulare il frodatore aveva potuto impostare autonomamente un nuovo PIN dispositivo; dai log era rilevabile che per autorizzare le operazioni di bonifico, riepilogate tramite notifica push, era stato necessario inserire il PIN dispositivo; al cliente erano state inoltrate all'indirizzo mail certificato le notifiche relative all'esecuzione dei bonifici; lamentava che il cliente non avesse prodotto copia del messaggio, né l'evidenza delle telefonate ricevute, in ogni caso il cliente faceva riferimento a un messaggio recante come mittente un intermediario terzo e indicava un numero di telefono non riconducibile a quello della Filiale di radicamento del conto bensì a quello di altra Filiale della banca; la banca aveva autonomamente provveduto a bloccare i

bonifici effettuati in data 11.8.2023, mentre per quelli relativi alla giornata del 10.8.2023 la richiesta di recall ha avuto esito negativo; sosteneva che nessuna responsabilità potesse essere attribuita alla banca avendo la stessa, adottato un sistema di autenticazione forte e provato la corretta autenticazione, registrazione ed esecuzione delle operazioni contestate, in assenza di malfunzionamenti. 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, in sede di repliche, allegava la schermata dei messaggi e della telefonata ricevuta; richiamava alcune decisioni con le quali i Collegi ABF hanno annoverato il c.d. "sms spoofing" tra le truffe potenzialmente "sofisticate" e che in tali casi non era generalmente ravvisabile la colpa grave del cliente, a meno che non si rinvengano indici di inattendibilità o anomalia del messaggio come sancito dal Collegio di Coordinamento (decisione n. 22745/20) e che in tal caso potrà essere ravvisato un concorso di colpa tra le parti. Il ricorrente insisteva quindi nella domanda espressa nel ricorso. L'intermediario, con le controrepliche, ribadiva di aver dimostrato: l'insussistenza di qualsivoglia responsabilità in capo alla banca e la colpa grave del cliente; sottolineava che dalle evidenze depositate dal cliente solo in sede di repliche, era possibile evincere che: la truffa aveva avuto origine da un messaggio apparentemente riconducibile ad altro intermediario il quale, in quanto ente gestore delle carte di pagamento, non aveva alcun titolo per chiedere l'accesso all'internet banking; che il testo del messaggio era del tutto sgrammaticato; che il link ivi riportato non risultava in alcun modo riconducibile alla banca; che dal registro chiamate ricevute dal cliente non si leggeva da nessuna parte il nome della banca quale soggetto chiamante; che nel caso di specie non risulta essersi verificato alcuno spoofing.

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 affermato che le operazioni siano state correttamente contabilizzate, registrate e autenticate e, a tal fine, ricostruisce i singoli passaggi che hanno condotto alle operazioni fraudolente, per giungere a sostenere che i bonifici contestati siano stati realizzati solo grazie alla collaborazione attiva del cliente che con il proprio imprudente comportamento. Questi, infatti, si sarebbe collegato sul link contenuto in un messaggio ricevuto sul cellulare e apparentemente riconducibile ad un intermediario terzo gestore delle carte di pagamento, ove inseriva le informazioni richieste (nome, cognome, mail, contatto telefonico); avrebbe dato seguito ad un secondo messaggio ricevuto nel corso della telefonata intrattenuta con un presunto operatore inserendo (per sua stessa ammissione) nel link ivi contenuto i propri dati personali di accesso all'internet banking (codice utente e password); avrebbe disinstallato l'App *Mobile della banca dal proprio smartphone per poi autorizzare l'installazione della stessa su altro dispositivo mobile, fornendo ai frodatori i due codici OTP autorizzativi necessari per il buon fine dell'operazione di attivazione della licenza smartOTP/App *Mobile [OTP inviati i) all'indirizzo email del cliente; ii) per sms al numero di cellulare certificato]; ha così consentito ai frodatori di poter disporre/autorizzare in completa autonomia le operazioni oggetto di contestazione. Nello specifico, l'intermediario ricostruisce la vicenda rilevando che in data 10/08/2023, alle ore 04:15:36 PM è stata attivata, sull'utenza Internet banking del cliente, una nuova APP*Mobile/licenza smartOTP sul dispositivo dei truffatori: "Realme RMX3623"; per l'attivazione della nuova licenza sul cellulare in mano ai frodatori sono stati necessariamente inseriti correttamente: Utenza+Password+OTP ricevuto dal cliente sul proprio indirizzo email +OTP ricevuto dal cliente per sms sul numero di cellulare certificato; in sede di attivazione della App il terzo frodatore ha potuto impostare autonomamente un nuovo PIN dispositivo da utilizzare per tutte le operazioni tramite internet banking; alle ore 16:19:05 i sistemi della Banca hanno registrato un accesso all'Internet Banking del Cliente tramite mobile, ossia tramite APP *Mobile, dal nuovo dispositivo (Android) su cui era stata installata la "nuova" App/licenza smartOTP; alle ore 16:26:24 è stato autorizzato il bonifico SEPA di € 2.350,00; alle ore 16:26:54 è stato autorizzato il bonifico SEPA di € 2.650,00.
Per l'autorizzazione le due operazioni di pagamento, riepilogate tramite notifica push, è stato necessario inserire il PIN dispositivo; alle ore 16:26 sono state inviate all'indirizzo mail certificato del cliente le mail contenenti le notifiche relative all'esecuzione dei bonifici.
L'intermediario precisa che la App può essere installata solo un unico dispositivo mobile per volta. Pertanto, nel caso in cui il cliente richiede (quale il caso di specie) l'attivazione di una nuova APP *Mobile/licenza smartOTP, deve i) prima procedere alla disinstallazione dal proprio dispositivo mobile della predetta APP (proprio come avvenuto nel caso di

specie), e solo successivamente, ii) potrà, una volta realizzata l'installazione, procedere con una nuova installazione della medesima.
Il Collegio, tuttavia, con riferimento alla fase di enrollment della APP sul nuovo dispositivo, rileva che, dalla documentazione in atti, non è riscontrabile con certezza l'utilizzo della password (elemento di conoscenza), parimenti non parrebbe riscontrarsi l'avvento inserimento dei due codici OTP autorizzativi che integrerebbero l'elemento del possesso. L'intermediario sostiene che la corretta attivazione della App sul nuovo device sia rilevabile dall'Esito OK riportato nella Relazione tecnica e da quanto indicato anche nel doc. 4 (cfr. supra Esito OK= "attivazione licenza riuscita con l'inserimento di codici di verifica OTP"). Il Collegio, invece, ritiene che non è possibile riscontrare la ricezione del secondo codice autorizzativo inviato per SMS al numero di telefono del cliente, né il testo del messaggio stesso; inoltre, nel campo "Codice evento": Attivazione Licenza SmartOTP nella colonna "descrizione" si legge: "Indica che è avvenuta la disattivazione della App".
Questo Collegio, in casi analoghi, ha reputato che non è 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, pertanto, sulla base di quanto emerso, conclude 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. 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.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 5.000,00.
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