COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) ACHILLE	Membro designato dalla Banca d'Italia
(MI) DENOZZA	Membro designato dalla Banca d'Italia
(MI) CAPIZZI	Membro di designazione rappresentativa degli intermediari
(MI) BARGELLI	Membro di designazione rappresentativa dei clienti

Relatore (MI) ACHILLE

Seduta del 30/05/2023

FATTO

Con ricorso presentato in data 16 febbraio 2023, preceduto dal reclamo, la parte ricorrente chiede il rimborso di € 9.800,00 relativo a due transazioni effettuate il 20 gennaio 2023 con lo strumento di pagamento di cui è titolare e dalla stessa disconosciute. A tal fine deduce, anche secondo quanto risulta dalla denuncia depositata agli atti della procedura, che: i) in data 19 gennaio 2022, alle ore 15:22, riceveva sul proprio cellulare un SMS proveniente da un terzo intermediario con il quale veniva informato di una limitazione apposta sulla propria carta di credito per “mancata autorizzazione servizi web”; ii) dopo aver cliccato sul link contenuto nel messaggio, gli venivano richiesti alcuni dati tra i quali il numero di telefono e i propri dati anagrafici; iii) poco dopo riceveva una chiamata da un’utenza fissa corrispondente a quella della banca nel corso della quale un presunto operatore lo invitava ad accedere alla propria APP per aggiornare le autorizzazioni dei servizi web; iv) nella schermata di accesso gli veniva richiesto un codice alfanumerico che gli era stato inviato con e-mail della banca; v) seguendo le istruzioni impartite al telefono inseriva, tramite il proprio cellulare e senza comunicarli a voce, il codice ricevuto per e-mail e un ulteriore codice numerico inviato sul proprio cellulare e proveniente dal numero da cui provenivano i codici di attivazione S***OTP; vi) la procedura non andava a buon fine e il presunto operatore lo informava che lo avrebbe richiamato il giorno seguente per risolvere il problema; vii) da quel momento in poi l’applicazione rimaneva bloccata; viii) il

giorno seguente, ricontattato dallo stesso presunto operatore della banca, seguiva la stessa procedura che questa volta andava a buon fine, tuttavia l'applicazione non riprendeva a funzionare; ix) il presunto operatore gli consigliava di disinstallare l'APP e di effettuarne nuovamente l'installazione il lunedì successivo; x) dopo aver tentato invano di installare l'APP decideva di attendere il lunedì come indicato dal presunto operatore; xi) il 21 gennaio 2023 la moglie, utilizzando la propria applicazione, si avvedeva che erano stati eseguiti dal conto corrente cointestato due bonifici fraudolenti per complessivi € 9.800,00; xii) tentava quindi di contattare l'assistenza clienti della banca senza ricevere alcuna risposta in quanto dalle ore 14:00 di sabato e per tutta la domenica risultava attivo il servizio di casella vocale che permetteva di lasciare solo un messaggio; xiii) in data 22 gennaio 2023 presentava denuncia e solo in tale occasione, tramite le autorità competenti, riusciva a contattare la banca ricevendo una e-mail di conferma dell'avvenuto blocco del proprio account; xiv) il 23 gennaio 2023 chiedeva alla banca di effettuare il recall dei due bonifici ordinari ma l'operazione, anche se prontamente eseguita, non andava a buon fine a causa del ritardo con il quale aveva avanzato richiesta; xv) in data 26 gennaio 2023 inoltrava reclamo alla banca chiedendo infruttuosamente la restituzione della somma sottratta.

Con le proprie controdeduzioni, l'intermediario resistente chiede in via principale il rigetto del ricorso e in via subordinata l'applicazione dell'art. 1227 c.c. Deduce a tal fine che: i) il cliente non fornisce una chiara e coerente ricostruzione dei fatti verificatisi il 20 gennaio 2023; ii) l'asserita frode è iniziata già il 19 gennaio 2023, circostanza questa taciuta dal cliente sia in sede di reclamo sia in sede di ricorso ma rilevabile dalle dichiarazioni rese dallo stesso in sede di denuncia; iii) il cliente ha intrattenuto contatti con il frodatore già giovedì 19 gennaio 2023 come rilevabile dalla documentazione dallo stesso allegata in sede di denuncia (registro chiamate in entrata, registro messaggi ricevuti contenenti il link truffaldino cliccato dal cliente); iv) dalla ricostruzione effettuata attraverso l'analisi dei log è emerso che in data 19 gennaio 2023, alle ore 19:15, è stato effettuato un login, presumibilmente dal cliente, all'internet banking tramite APP e inserendo codice utente, password personale e PIN personale impostato dal cliente; v) successivamente, sempre in data 19 gennaio 2023, è stata tentata l'installazione dell'APP sul dispositivo dei truffatori poi non andata a buon fine; vi) in data 20 gennaio 2023, dopo che il cliente veniva ricontattato da un presunto operatore alle ore 14:34:10 è stata attivata, presumibilmente dal frodatore, una nuova licenza S***OTP sul proprio dispositivo mobile, inserendo correttamente Utenza+Password+OTP ricevuto dal cliente sull'indirizzo e-mail + OTP ricevuto dal cliente per SMS sul numero di cellulare certificato; vii) alle 14:34:23 e alle ore 17:46:35 del 20 gennaio 2023 è stato realizzato l'accesso all'internet banking del cliente tramite APP *Mobile, presumibilmente da parte del frodatore con utilizzo delle credenziali comunicate dal cliente; viii) alle ore 17:49:03 e alle 17:49:50 del 20 gennaio 2023 sono stati autorizzati rispettivamente il bonifico di € 6.200,00 e di € 3.600,00 con l'inserimento del codice utente, password e PIN personale del cliente; ix) è dunque incontrovertibile che il cliente abbia espressamente comunicato al frodatore, come dallo stesso affermato, i codici ricevuti sui propri contatti certificati permettendo così la corretta installazione dell'applicazione; x) lo stesso cliente ammette in sede di denuncia di aver inserito nel link contenuto nel messaggio truffaldino i propri dati (presumibilmente anche le proprie credenziali) e di aver interloquito con il terzo frodatore consentendogli dapprima di accedere all'internet banking e poi di installare l'APP e disporre le operazioni; xi) contestualmente all'autorizzazione dei bonifici disconosciuti, sono state inviate le due e-mail di notifica delle operazioni; xii) la frode non si sarebbe mai perfezionata senza l'attiva collaborazione del cliente; xiii) le contestazioni sollevate dal cliente (per lo più in sede di reclamo) sono finalizzate a "celare" la colpa grave in cui lo stesso è incorso; xiv) il cliente

ha tenuto una condotta del tutto negligente ed imprudente non prestando la dovuta attenzione agli elementi di evidente anomalia del messaggio truffaldino ricevuto (provenienza da un terzo intermediario emittente solo la carta di pagamento e contenente l'utilizzo improprio della terminologia "conto") e al contenuto delle e-mail ricevute; xv) la truffa subita dal cliente non risulta essere particolarmente sofisticata; xvi) è stata provata la corretta autenticazione, registrazione ed esecuzione dei bonifici in assenza di malfunzionamenti; xvii) ha più volte sensibilizzato la propria clientela sui temi della sicurezza e riservatezza dei dati introducendo apposite e specifiche informative, chiarendo come riconoscere tale tipologie di truffe e il comportamento da tenere; xviii) nonostante il cliente abbia preso visione delle comunicazioni, già due mesi prima dell'accaduto, ha posto in essere tutti quei passaggi e comportamenti "vietati"; xix) l'utenza del cliente è stata bloccata già in data 22 gennaio 2023; xx) in data 23 gennaio 2023, nel corso della prima giornata lavorativa disponibile, ha provveduto ad effettuare le richieste di recall dei bonifici in contestazione con esito negativo; xxi) il servizio di emergenza/call center, disponibile tramite numero verde, nel fine settimana opera con un c.d. servizio di casella e-mail con segreteria telefonica tramite la quale il cliente può registrare un messaggio vocale (secondo le indicazioni fornite dalla voce registrata) indicando l'intervento richiesto sull'account e con successiva esecuzione delle operazioni richieste di cui viene inviata conferma all'indirizzo e-mail del cliente.

Con le repliche alle controdeduzioni, la parte ricorrente eccepisce che: i) non ha taciuto alcuna circostanza in sede di ricorso avendo fatto richiamo integrale, per la compiuta descrizione dei fatti, alla denuncia; ii) la truffa, anche se iniziata il 19 gennaio 2023, si è perfezionata il 20 gennaio 2023; iii) ha da tempo utilizzato il riconoscimento biometrico facciale con uso del proprio telefono cellulare sia per l'accesso alla APP, sia per l'autorizzazione delle operazioni, di conseguenza non ha comunicato al terzo truffatore le credenziali (username, password, PIN) per l'accesso al conto; iv) l'intermediario omette di considerare che le telefonate, ricevute a seguito del messaggio, provenivano tutte dall'utenza fissa riconducibile ad una filiale dello stesso; v) la documentazione prodotta dall'intermediario non prova l'effettiva ricezione delle e-mail di avvenuta esecuzione dei bonifici; vi) nell'orario di esecuzione dei bonifici non aveva possibilità di accesso all'applicazione poiché la stessa era stata bloccata; vii) il terzo frodatore violando il sistema informatico della banca e dell'APP ha autorizzato i pagamenti contestati; viii) per tutto quanto illustrato, il proprio comportamento non si può ritenere "grave" e certamente nell'accaduto concorrerebbe con colpa l'intermediario per l'acclarata inadeguatezza dei propri sistemi informatici; ix) il messaggio truffaldino non conteneva errori grammaticali o anomalie grafiche tali da far nascere il sospetto del cd. phishing/smishing; x) l'intermediario emittente le carte di pagamento da cui proveniva il messaggio truffaldino non può considerarsi terzo estraneo alla vicenda posto che tutte le operazioni addebitate sulla carta sono poi scalate, a date prestabilite, dal conto corrente intrattenuto con la banca; xi) la banca, nonostante l'ascolto dei messaggi attinenti la richiesta di blocco dei bonifici ordinari contestati, ha atteso il lunedì mattina, dopo l'apertura della filiale, per avviare il tentativo di recall non andato a buon fine; xii) i bonifici emessi in data 20 gennaio 2023 dovevano essere accreditati sul conto del beneficiario solo alle ore 00:01 del lunedì 23 gennaio 2023; xiii) se ai messaggi vocali lasciati alla casella del servizio clienti fosse seguita la doverosa procedura di blocco il conto corrente non avrebbe subito l'addebito delle contestate operazioni; xiv) l'intermediario ha articolato una difesa dettagliata e precisa solo in sede di controdeduzioni, limitandosi invece a fornire una sintetica contestazione in sede di riscontro al reclamo.

Con le controrepliche, l'intermediario resistente eccepisce che: i) il frodatore ha potuto beneficiare delle operazioni contestate solo grazie alla piena e protratta collaborazione del

cliente come dimostrato dalla documentazione dallo stesso allegata; ii) l'attivazione della APP è avvenuta correttamente su un dispositivo Android e le operazioni sono state eseguite dal medesimo indirizzo IP attivato dai frodatori; iii) il cliente ha quindi comunicato al frodatore le proprie credenziali di accesso all'internet banking e anche le OTP di installazione dell'APP; iv) non hanno valore le considerazioni fatte dal cliente sul riconoscimento facciale in quanto il riconoscimento biometrico può essere utilizzato solo dopo l'installazione della APP quale elemento sostitutivo del PIN; v) il sistema di autenticazione forte adottato, conforme alla normativa, è costruito in modo tale da impedire l'utilizzo dell'internet banking a soggetti non autorizzati, ma può essere bypassato solo attraverso la divulgazione a terzi sconosciuti di tutti i codici di accesso/autorizzativi; vi) è stato provato l'avvenuto invio all'indirizzo e-mail del cliente, mai modificato, delle notifiche relative all'esecuzione delle operazioni; vii) anche la frode nota come caller ID spoofing non costituisce un indicatore di anomalia o violazione dei sistemi informatici della banca bensì indice del piano criminoso posto in essere dal frodatore; viii) il messaggio esca al quale il cliente ha abboccato presentava errori grammaticali e di sintassi (privo di una corretta punteggiatura, del carattere maiuscolo e delle giuste preposizioni e/o articoli); ix) in un caso simile, la giurisprudenza di legittimità più recente ha negato il risarcimento del danno subito dal cliente.

DIRITTO

Il ricorso, avente ad oggetto la richiesta di rimborso di € 9.800,00 pari all'importo di due transazioni effettuate il 20 gennaio 2023 con lo strumento di pagamento di cui è titolare la parte ricorrente e dalla stessa disconosciute, deve essere deciso facendo applicazione delle disposizioni del d. lgs. n. 11 del 27 gennaio 2010, come modificate in seguito al recepimento della seconda Direttiva sui servizi di pagamento (Direttiva 2015/2366/UE del 25 novembre 2015), applicabile ratione temporis a decorrere dal 13 gennaio 2018.

In base a tali disposizioni, come applicate da questo Arbitro (da ultimo, ABF-Coll. Coord. n. 22745 del 10 ottobre 2019, al § 8), due sono i passaggi ineludibili in materia. In primo luogo, è l'intermediario a dover provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e la contabilizzazione delle operazioni, dovendo in particolare fornire evidenza di aver applicato un c.d. "Sistema di autenticazione forte" (strong customer authentication o SCA), posto che ai sensi del comma 2-bis dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente". In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento (art. 12, co. 2-ter e s., d.lgs. n. 11/2010).

In tale contesto e con riguardo al caso di specie è possibile rilevare, quanto al primo dei suddetti passaggi ed in base alle evidenze fornite agli atti della procedura, che l'intermediario resistente non ha assolto i propri oneri probatori avendo omesso di provare la corretta contabilizzazione, registrazione e autenticazione applicando un c.d. "Sistema di autenticazione forte" (strong customer authentication o SCA), dovendosi al riguardo ricordare che un tale sistema è richiesto dall'art. 10-bis, co. 1, d.lgs. n. 11 del 27 gennaio 2010 "quanto 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".

In particolare, per quanto l'intermediario resistente abbia dettagliatamente illustrato il processo di autenticazione che ha condotto alle operazioni disconosciute, anche supportando le evidenze da una leggenda esplicativa, occorre rilevare che: con riguardo all'accesso all'APP effettuato il 19 gennaio 2023 alle ore 15:08:42 (non alle 19:15 come dedotto dall'intermediario) e alle 17:46:35 del 20 gennaio 2023 non vi è evidenza dell'inserimento dell'utenza, della password e del PIN; con riguardo all'enrollement dell'APP effettuata alle 14:34:10 del 20 gennaio 2023 si ha una evidenza parziale dell'invio dell'OTP (via e-mail e non via SMS) e non si ha evidenza dell'inserimento della password; con riferimento alle operazioni di bonifico disconosciute non si ha evidenza dell'inserimento dei fattori di autenticazione.

Si deve quindi ritenere che le operazioni di pagamento disconosciute sono state disposte senza adottare gli standard di sicurezza corrispondenti alla disciplina oggi applicabile come sopra individuata.

Ciò è di per sé sufficiente, secondo il consolidato orientamento di questo Arbitro cui si è già fatto riferimento (cui, tra le tante, si può aggiungere ABF-Coll. Milano n. 10983 del 28 aprile 2021), a condurre all'accoglimento della pretesa dell'utilizzatore dello strumento di pagamento che chiede il rimborso dell'operazione disconosciuta, dovendosi quindi disporre che l'intermediario resistente corrisponda alla parte ricorrente la somma di € 9.800,00.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 9.800,00.
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