COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) PERON

Seduta del 22/02/2024

FATTO

Parte ricorrente rappresenta al Collegio di aver ricevuto in data 09/08/2023 un SMS apparentemente proveniente da N** con il quale veniva informata di una spesa di € 710,20 invitandola a seguire un link nel caso in cui avesse disconosciuto la predetta operazione di pagamento. Dopo aver aperto il link si apriva una pagina analoga a quella dell'intermediario che l'invitava a chiamare un operatore. Chiamava quindi la sua filiale ma, essendo le 17:35, nessuno rispondeva. Di lì a poco riceveva una telefonata da parte di un sedicente operatore C**dell'intermediario il quale la informava di aver bloccato il pagamento di € 710,20 non autorizzato. Parte ricorrente chiedeva all'operatore di dimostrargli di essere effettivamente un operatore della banca; di fronte a tale richiesta, l'operatore le comunicava che di lì a breve avrebbe ricevuto un SMS e una chiamata di conferma, rassicurata nel corso della telefonata parte ricorrente comunicava la password del suo c/c. Riceveva quindi un'altra chiamata da parte di un altro operatore il quale confermava la veridicità del nominativo del precedente operatore nonché un ulteriore SMS che confermava quanto detto dall'operatore. In effetti, in data 10/08/2022, riceveva un altro SMS apparentemente riconducibile all'intermediario con il quale veniva informata che era stata bloccata un'operazione di bonifico di € 2.200,00 e, poco dopo, veniva nuovamente

contattata da parte del primo operatore C**. Questa volta tuttavia insospettitasi della telefonata, non forniva alcuna informazione e si recava in filiale dove scopriva che in data 10/08/2023 era stato effettuato un bonifico transfrontaliero on-line di € 2.200,00. Presentava quindi denuncia alle Autorità e due reclami, ma senza successo.
Chiede quindi il rimborso di € 2.200,00 per responsabilità dell'intermediario che non avrebbe garantito sufficiente sicurezza informatica.
L'intermediario, controdeduce osservando che parte ricorrente, titolare di un c/c acceso presso una sua filiale dove sono attivi i servizi di banca telematica, al momento dell'attivazione del servizio di home banking, ha fornito i suoi contatti associati alla sua utenza, dalla stessa mai modificati ed ha ricevuto il codice utente e la password solo a lei noti. Dalle verifiche svolte è emerso che l'operazione disconosciuta è stata correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali e preceduta dalla disinstallazione dell'APP sul dispositivo della cliente e dalla installazione dell'APP sul dispositivo dei frodatori (APP che può essere installata su un unico dispositivo). Precisa che non essendo stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici, deve presumersi la colpa grave della parte ricorrente, la quale ha tenuto un comportamento attivo e collaborativo per l'esecuzione della truffa. Nel caso in specie, infatti ha *(i)* cliccato su un link contenuto in un SMS apparentemente riconducibile ad altro intermediario; *(ii)* dichiarato di aver comunicato la password del suo c/c; *(iii)* intrattenuto più telefonate con un presunto operatore bancario di altro intermediario e seguito pedissequamente le istruzioni impartite; *(iv)* colpevolmente ignorato la mail inoltrata all'indirizzo di posta elettronica contestualmente all'autorizzazione dell'operazione contestata. Inoltre, dalle evidenze documentali risulta che parte ricorrente ha disinstallato l'APP dal suo dispositivo come (presumibilmente) richiesto dal frodatore e dato quindi la possibilità al suo interlocutore di procedere con l'installazione dell'APP su altro dispositivo. Ritiene verosimile che parte ricorrente abbia inserito le proprie credenziali personali nella pagina apparentemente riconducibile a quella dell'intermediario e comunicato i codici OTP ricevuti sui propri contatti certificati dall'intermediario necessari per installare l'APP sul dispositivo del frodatore. Peraltro dalle evidenze fornite dalla parte ricorrente, risulta che una delle chiamate ricevute risulta provenire da un numero "sconosciuto" e le altre da un numero proveniente apparentemente riconducibile ad un diverso intermediario. Sottolinea che con la decisione n. 9628/2023 il Collegio di Milano, in un caso analogo, ha dichiarato provata la SCA, seppur in accoglimento parziale del ricorso presentato dalla cliente ritenendo giustificata l'attribuzione di una responsabilità a carico delle parti nella misura del 50%. Anche la Corte di Cassazione, con ordinanza n. 7214 del 13 marzo 2023, ha chiarito che l'intermediario non è tenuto al risarcimento in presenza di una condotta gravemente negligente del cliente. Infine dichiara di aver attivato apposite campagne informative anti-frode, volte a sensibilizzare la clientela rispetto alle forme di truffa più diffuse.
Alla luce di quanto sopra esposto, l'intermediario chiede il rigetto della domanda, avendo egli provato la correttezza del suo operato. In via subordinata, laddove dovesse ravvisarsi una qualche responsabilità in capo all'intermediario, chiede che il Collegio tenga conto del comportamento colpevole e imprudente tenuto dalla parte ricorrente, rilevante ai fini di un concorso di colpa ai sensi dell'art. 1227 c.c. ed anche alla luce della recente decisione del Collegio di Milano n. 9628/2023.

Parte ricorrente replica affermando:

- che l'SMS ricevuto in data 09/08/2023 era riconducibile ad un terzo intermediario, ovvero a N** contenente un link sul quale cliccava;

- che una volta cliccato sul link, veniva ricondotta ad una pagina analoga a quella dell'intermediario convenuto;
- che le successive telefonate ricevute in 17:42 e in data 18:22 come anche l'SMS dell1 8:25 sembravano provenire da un numero apparentemente riconducibile a quello dell'intermediario convenuto;
- che, stante la apparente riconducibilità delle predette chiamate alla banca, la cliente comunicava la propria password in una sola circostanza (chiamata delle 17:42);
- di non aver fornito alcun PIN e di non aver disinstallato l'APP dal suo cellulare;
- che le campagne informative antifrode poste in essere dall'intermediario sono caratterizzate da comunicazioni generiche, non idonee ad assolvere allo specifico onere informativo in capo all'intermediario il quale avrebbe invece dovuto fornire un foglio informativo con il quale con poche parole chiare e semplici avrebbe dovuto spiegare al cliente che non avrei mai dovuto fornire alcun codice a nessun operatore della banca.

Per i motivi sopra esposti, insiste per l'accoglimento del ricorso.

L'intermediario, riportandosi alle conclusioni in atti, insiste nelle medesime argomentazioni difensive già svolte in sede di controdeduzioni, chiedendo l'accoglimento delle conclusioni già rassegnate e affermando inoltre quanto segue:

- parte ricorrente è rimasta vittima della classica frode c.d. "*smishing*" misto a "*vishing"*;
- appare strano che un SMS apparentemente proveniente da altro intermediario contenga un link che rimanda ad una pagina identica al sito web dell'intermediario convenuto;
- l'SMS civetta è un SMS isolato e non uno in cronologia con altri SMS dell'intermediario N**;
- che è verosimile ritenere che una volta entrata nella pagina "specchio" dell'intermediario convenuto, parte ricorrente abbia inserito le proprie credenziali di accesso personali all'internet banking;
- che dalle evidenze documentali risulta la disinstallazione dell'APP dal dispositivo della parte ricorrente;
- che dal registro chiamate prodotto in atti dalla parte ricorrente, si evince che tutte le chiamate risultano provenire dall'altro intermediario N** eccetto una che risulta essere anonima;
- nell'ambito dei propri presidi di sicurezza, la banca ha più volte sensibilizzato la parte ricorrente, prima rispetto alla data in cui sono state poste in essere le operazioni contestate, sui temi della sicurezza e riservatezza dei dati, trasmettendo alla parte ricorrente un messaggio denominato "Attenzione alle truffe";
- che già al momento della sottoscrizione del contratto di accensione dei servizi di home banking, l'intermediario comunicava alla parte ricorrente di non comunicare le proprie credenziali personali a terzi.

DIRITTO

La fattispecie in oggetto concerne la richiesta di rimborso di parte ricorrente del complessivo importo di € 2.200,00 sottratto con un'operazione fraudolenta (bonifico estero) in data 10.08.2023 alle ore 10:05.
L'operazione in esame è disciplinata dal D.Lgs. 27.1.2010 n. 11 di recepimento della Direttiva sui servizi di pagamento (Direttiva 2007/64/CE del 13 novembre 2007) e del

relativo Provvedimento attuativo della Banca d'Italia del 5.7.2011. Come è noto, i principi fissati da tale impianto normativo, in materia di *strong customer authentication* (SCA), fissano due passaggi ineludibili che attengono al piano degli oneri probatori: *a)* è l'intermediario a dover provare (oltre all'insussistenza di malfunzionamenti) l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni disconosciute, avendo presente che l'autenticazione forte (SCA) è richiesta sia nella fase di accesso al conto / enrollment dell'applicazione / registrazione della carta sul *wallet*, sia nella fase di esecuzione delle singole operazioni; inoltre la SCa si realizza con il ricoso ad almeno due dei seguenti tre fatttori: conoscenza, inerenza, possesso. Tali elementi devono essere reciprocamente indipentendi e appartenere a categorie diverse; *b)* 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. In quest'ambito dunque, costante giurisprudenza arbitrale, ritiene che l'eventuale negligenza del cliente possa solo venire in rilievo solo allorquando l'intermediario abbia fornito la prova piena della scrupolosa osservanza del sistema di SCA e della predisposizione di congegni di *alert*.

Ciò posto, si impone dunque in prima battuta la verifica sul sistema di autenticazione predisposto dall'intermediario e sul rispetto dei requisiti di cui alla predetta disciplina, avendo egli l'onere di provare *(a)* che «*l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti*»; *(b)* che il sistema di autenticazione e l'autorizzazione delle operazioni di pagamento contestate sono conformi alla SCA, che 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.

L'intermediario afferma che l'operazione è stata correttamente contabilizzata, registrata e autenticata, e produce documentazione informatica a supporto, dalla quale l'intermediario ricostruisce come segue l'operatività fraudolenta:

- registrazione di un nuovo dispositivo sull'app, con attivazione del servizio "*smart OTP*", previa disinstallazione della app presente sul dispositivo del cliente;
- accesso all'app dal nuovo dispositivo;
- esecuzione del bonifico disconosciuto.

Il Collegio procede dunque a verificare la corretta applicazione della SCA con riferimenti a ciascuno dei passaggi sopra indicati.

Con riferimento alla registrazione di un nuovo dispositivo, con attivazione del servizio "*smart OTP*", l'intermediario rileva che alle ore 18:29 del 09/08/2023 è stata attivata una nuova licenza "*smartotp*", presumibilmente dal terzo truffatore (sul proprio dispositivo), il quale, per attivare la nuova licenza, ha dovuto necessariamente inserire correttamente "Utenza + Password + OTP ricevuto via email + OTP ricevuto via SMS sul cellulare certificato dalla cliente in fase di contrattualizzazione". Precisa che l'app può essere installata su un unico dispositivo mobile per volta, sicché l'attivazione dell'app/licenza smart OTP sul nuovo dispositivo è stata preceduta dalla disinstallazione della app sul device della cliente. L'intermediario inoltre dichiara che il processo di *enrollment* prevede sempre inserimento di UTENZA + PASSWORD + OTP ricevuto via e-mail + OTP ricevuto via SMS.

Il Collegio tuttavia rileva che dalle evidenze in atti manca la prova dell'inserimento di Utenza + Password, nonostante l'intermediario affermi l'*enrollment* avviene sempre con l'inserimento di detti fattori. Mentre in relazione all'invio dei codici OTP all'attivazione della licenza sul nuovo dispositivo i log dell'intermediario riportano la dicitura ESITO = OK, il Collegio osserva quanto segue: *a)* quanto al primo codice OTP inoltrato via mail, nei log è indicato l'inoltro di quest'ultimo all'indirizzo e-mail della parte ricorrente; quanto al secondo codice OTP inoltrato via SMS è indicato parimenti l'inoltro del predetto codice al numero di cellulare che coincide con quello indicato in denuncia. In entrambi i codici OTP, tuttavia, non è possibile verificare il contenuto del testo dell'SMS contenente l'OTP; *b)* in relazione all'attivazione della licenza sul nuovo dispositivo i log riportano la dicitura ESITO = OK, che, secondo la legenda, indica la corretta attivazione della licenza "*con inserimento dei codici di verifica OTP*".

Con riferimento all'accesso al conto, l'intermediario specifica che, ai fini del login, l'applicazione richiede l'inserimento di Utenza + Password + PIN; e che la dicitura ESITO = 000 conferma l'inserimento di tutti i parametri di sicurezza previsti.
Il Collegio tuttavia rileva che dalle evidenze in atti manca la prova dell'inserimento di Utenza + Password + PIN che secondo l'intermediario l'applicazione richiede ad ogni accesso e vi è unicamente l'indicazione che l'esito degli eventi di login è uguale a "000" (che secondo quanto indicato nella legenda, indica il corretto inserimento dei parametri di sicurezza).

Con riferimento all'esecuzione del bonifico disconosciuto, l'intermediario specifica che per l'autorizzazione dell'operazione di pagamento riepilogata tramite notifica *push* è stato necessario inserire il codice utente e la password personale e il PIN dispositivo.
Il Collegio tuttavia rileva che dalle evidenze in atti manca la prova dell'inserimento del PIN ai fini dell'autorizzazione del bonifico e vi è unicamente l'indicazione che l'esito del bonifico è uguale a "000" (che secondo quanto indicato nella legenda, indica il corretto inserimento dei parametri di sicurezza).

Sulla base di quanto emerso il Collegio ritiene che l'intermediario non abbia fornito piena prova della corretta autenticazione dell'operazione disconosciuta dalla parte ricorrente, in relazione alla registrazione di un nuovo *device*, all'accesso al servizio home banking e all'esecuzione dell'operazione disconosciuta, dato che per tutte le fasi richiamate, manca la prova dell'inserimento delle credenziali di accesso (login e password), né del codice OTP e del PIN dispositivo di volta in volta inviati, il cui inserimento sarebbe confermato, secondo la legenda esplicativa prodotta dall'intermediario, unicamente dai codici "000" (cfr. in proposito Collegio di Milano decisione n. 11139/2023: «*Nella legenda fornita dall'intermediario il processo di enrollment prevede l'inserimento di UTENZA + PASSWORD + OTP ricevuto via MAIL + OTP ricevuto via SMS. La documentazione prodotta mostra che per il primo passaggio è richiesto l'inserimento di utenza + password; per il secondo l'inserimento del codice OTP ricevuto via mail; per il terzo l'inserimento del codice OTP ricevuto via SMS. Sono provati l'invio di una mail all'indirizzo di posta elettronica del cliente asseritamente contenente il primo OTP di attivazione (come si desume dall'oggetto della mail), nonché l'invio di un SMS il cui oggetto riporta "LOG invio OTP per attivazione smartphone" e, per il nuovo dispositivo, l'invio di un SMS contenente il secondo OTP di attivazione. Non sono tuttavia allegati né il testo della mail, né il contenuto dell'SMS al numero del cliente. In sintesi, manca la prova dell'inserimento di Utenza, Password e i due OTP (quello ricevuto via mail nonché quello ricevuto via SMS)*»).

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 € 2.200,00 fraudolentemente sottratta tramite l'operazione di bonifico esaminata.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.200,00.
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