COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) DENOZZA

Seduta del 14/07/2020

FATTO

Parte ricorrente espone che

- in data 4/09/2019, si recava presso il proprio sportello bancario e veniva a conoscenza di due bonifici effettuati a soggetti sconosciuti in data 2/09/19 e 3/09/19 dell'importo rispettivamente di euro 45.000 e di euro 14.500;

- due giorni prima, precisamente in data 2/09/2019, precisa che alle ore 14.00 circa il proprio telefono risultava "bloccato" e non ne consentiva l'utilizzo; circostanza che sarebbe stata confermata dall'assistenza del proprio rivenditore cellulare xxx; nei mesi precedenti afferma di aver ricevuto un sms tramite il quale le veniva comunicato dalla Banca la non operatività del proprio token fisico e la necessità di utilizzo dell'apposita procedura di generazione dei codici; a tale richiesta non veniva dato seguito;

- in data 6/09 trasmetteva integrazione di querela chiedendo il blocco dei conti correnti verso i quali risultavano effettuati i bonifici fraudolenti;

- trascorsi alcuni mesi senza che la Banca procedesse allo storno delle operazioni, pur avendo identificato i soggetti, provvedeva ad inviare formale comunicazione di messa in mora all'Istituto Bancario il quale negava ogni responsabilità;

- nega di aver ceduto a terzi i propri codici ma afferma di essere stata vittima di una falla nel sistema di sicurezza della Banca e di essersi attivata immediatamente affinché le somme potessero essere annullate e stornate da parte dell'intermediario anche in ragione dell'entità delle stesse;

Chiede il complessivo rimborso di € 70.000 (importo comprensivo delle spese legali e del risarcimento danno);

L'intermediario afferma:

- che il cliente chiede il rimborso di euro 70.000 a fronte di n. 2 operazioni fraudolente (euro 59.500 inerenti i due bonifici, euro 10.500 per risarcimento danni e spese legali); tale richiesta risultava già oggetto di reclamo riscontrato negativamente in data 6/03/20;

- che risulta essere titolare del conto xxx3, al quale è collegato il servizio home banking ed attivo il servizio SMS alert; il sistema previsto per accedere alle operazioni dispositive (bonifici) risulta essere c.d. "forte" e prevede l'inserimento dell'identificativo del cliente, del codice PIN e di una terza credenziale OTP generata dall'APP (Mobile Token);

- che, in merito all'attivazione del Mobile Token, è stata resa possibile dall'APP tramite digitazione delle credenziali di sicurezza e del codice OTP trasmesso tramite SMS; la ricorrente, contrariamente a quanto affermato nelle proprie difese, avrebbe richiesto in data 30/06/19 tale attivazione;

- che, in sede di denuncia, la cliente dichiara che avrebbe ricevuto un "sms strano" non fornendo tuttavia nessun ulteriore dettaglio al riguardo e non attivandosi nel contattare immediatamente la Banca; si conferma di non aver trasmesso alcun messaggio che non fosse attinente alle operazioni di pagamento;

- che, ha posto in essere tutte le misure di sicurezza e prevenzione idonee per tutelare il cliente; le operazioni risultano correttamente autenticate, registrate ed eseguite mediante un sistema di autenticazione "forte", in assenza di anomalie; l'episodio è imputabile pertanto a colpa grave del ricorrente per non aver rispetto gli obblighi di custodia e protezione delle proprie credenziali di sicurezza;

- che, con riferimento alle ulteriori richieste restitutorie, nessuna assistenza di terzi professionisti è necessaria e inoltre non risulta prova del danno patito in aggiunta al disconoscimento delle operazioni.

Chiede che il ricorso sia rigettato.

Parte ricorrente in risposta alle affermazioni contenute nelle controdeduzioni:

- afferma che, dall'analisi dei log prodotti dalla Banca, emergerebbe chiaramente l'utilizzo di un device differente rispetto a quello in uso;

- ribadisce che il proprio telefono non risultava funzionante; terzi soggetti avrebbero effettuato fraudolentemente le operazioni, circostanza avvalorata dal fatto che, nei giorni in cui risultano compiute, la ricorrente non stesse utilizzando il proprio telefono;

- dall'analisi dei messaggi trasmessi, dichiara che si evidenzia l'istallazione dell'APP della banca e di ulteriori servizi per operare online, operazioni che avrebbero comportato la riconfigurazione dell'utenza e l'emissione di nuove credenziali di accesso da parte dei malfattori; specifica ulteriormente di non aver mai utilizzato servizi online;

- afferma di aver ricevuto maggiori informazioni inerenti le coordinate IBAN dei soggetti beneficiari, solo 2 giorni dopo (informazioni riferite in sede di integrazione alla denuncia) e pertanto la Banca non avrebbe avuto un comportamento corretto;

- ribadisce di non aver comunicato a nessuno i propri codici di accesso, insiste sulla responsabilità dell'istituto bancario per la vicenda confermando le richieste contenute in sede di ricorso;

L'intermediario in risposta alle dichiarazioni contenute nelle repliche, specifica ulteriormente:

- che spetta al cliente provare che "*durante i 15 giorni*" non stesse utilizzando il proprio telefono cellulare; la Banca ha adempiuto all'onere della prova in merito all'invio degli SMS al numero di cellulare della ricorrente;

- che la Banca non è tenuta a conoscere il modello di device utilizzato, il quale può essere modificato liberamente dal cliente;

- che l'utilizzo dell'APP della Banca è previsto nel contratto ("Rapporti a distanza tra Banca e Cliente"); il cliente può scegliere se accedere al proprio home banking tramite internet o tramite mobile senza che la Banca sia tenuta a verificarne la modalità; operare da APP non comporta alcuna sostituzione delle credenziali di sicurezza, id/utente e pin restano invariati;

- che la ricorrente già in data 30.06.19, aveva richiesto l'attivazione del Mobile Token;

- che la banca ha dimostrato tramite i relativi Log la corretta autenticazione delle operazioni attraverso un sistema forte "a due fattori"; pertanto si può desumere che il frodatore conoscesse le credenziali di sicurezza, denotando una incauta custodia del cliente dei propri strumenti personali;

- che non ha potuto bloccare i bonifici in uscita in quanto risultavano già eseguiti;

- che ha posto in essere tutte le misure di sicurezza e prevenzione idonee a tutelare il cliente, la frode è stata resa possibile esclusivamente dalla conoscenza, in capo ai frodatori, delle credenziali di accesso all'home banking, senza le quali non sarebbero stati in grado di accedere alla App, scaricare il Mobile Token e disporre le operazioni;

- che l'asserita prova testimoniale (allegata alle repliche) non è ammissibile in quanto presumerebbe l'apertura di un contraddittorio non previsto in questa sede;
- conferma la richiesta di rigetto del ricorso.

DIRITTO

Le operazioni contestate (n. 2 bonifici) risultano effettuate in data 2/09/19 e 3/09/2019. Circostanza confermata dalla ricorrente in sede di denuncia. A detta data era vigente il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II).
Da tale disciplina (in particolare, art.10; art 12d. lgs cit.) si desume da una parte, che è onere dell'intermediario provare che l'operazione di pagamento disconosciuta è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o altri inconvenienti, e dall'altra, che il cliente non sopporta perdite se il prestatore di servizi di pagamento non esige un'autenticazione forte. Anche l' autenticazione forte ai sensi dell'art. 72,2 della Direttiva citata, *"non è di per sé necessariamente sufficiente a dimostrare che l'operazione di pagamento sia stata autorizzata dal pagatore né che questi abbia agito in modo fraudolento o non abbia adempiuto, dolosamente o con negligenza grave, a uno o più degli obblighi di cui all'articolo 69. Il prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornisce gli elementi di prova che dimostrano la frode o la negligenza grave da parte dell'utente di servizi di pagamento".*
Nella specie, la convenuta non sembra avere assolto ai suddetti oneri probatori su di lei gravanti, non avendo fornito elementi atti a dimostrare l'esistenza di un comportamento doloso o gravemente colposo del ricorrente.
Va considerato inoltre che la presente vicenda attiene in particolare all'utilizzazione abusiva effettuata da ignoti di un sistema di home banking fondato sull'utilizzazione di apposita APP e relativo Mobile Token, sistema di cui la ricorrente sostiene di non avere mai chiesto l'attivazione e di non avere mai fatto uso (in sede di denuncia parte ricorrente dichiara di non avere mai operato come home banking tramite telefonino e di non avere mai neppure avuto l'applicazione necessaria).
In questo contesto sembra anzitutto opportuno rilevare che l' esercizio del c.d. home banking tramite APP e relativo Mobile Token rappresenta una modalità caratterizzata da peculiari rischi (alcuni dei quali sono addirittura estranei al rapporto intermediario – cliente, in quanto coinvolgono l'operatore di telefonia mobile e sfuggono, in questo senso, al controllo dell'intermediario).
E', ovviamente, del tutto naturale che ciascun cliente possa consapevolmente scegliere, con tutte le conseguenze del caso, di passare all'utilizzazione di questa modalità, in seguito ad una sua personale valutazione in cui stima che le comodità sopravanzano i rischi. Altrettanto ovvio è, però, che ciò non può escludere la necessità di riservare adeguata tutela al cliente che decida di non utilizzare questo sistema. Quest'ultima categoria di clienti, quelli che ritengono l'home banking via APP e Mobile Token troppo rischioso, o comunque non conveniente per loro, non possono vedere il proprio rischio comunque aumentato dal fatto che il servizio in questione venga offerto in maniera generalizzata a tutti i clienti, e sia perciò suscettibile di essere oggetto di falsa attivazione da parte di un terzo male intenzionato.
Questa considerazione implica che la concreta volontà di attivazione del servizio da parte del singolo utente dovrebbe essere accertata dall'intermediario in maniera che non possa

lasciare adito al minimo dubbio circa l'esistenza e l'effettiva provenienza di tale volontà. Tale accertamento , del resto, non si presenta non come ricorrente, ma come destinato ad essere compiuto *una tantum*, e non presenta perciò le necessità di velocità e speditezza che possono presentare gli accertamenti ricorrenti relativi al compimento di singole operazioni..

Ciò premesso, va rilevato, da una parte, che non esiste agli atti chiara e sicura prova che parte ricorrente avesse effettivamente chiesto l'attivazione del sistema di home banking mediante APP e Mobile Token sin dal giugno precedente i giorni (02 e 03 settembre) in cui sono state effettuate le operazioni contestate (al giugno risultano bonifici effettuati genericamente via internet) , e dall'altra che dette operazioni contestate sono state precedute da alcune altre operazioni di cui non è chiaro il senso e che avrebbero dovuto apparire come alquanto sospette (in particolare risultano in data 02 settembre una serie di log - in e ben due attivazioni del Mobile Token alle 16, 01 e alle 16,20 con differenti nickname, rispettivamente Micia 2 e Micetta).

La domanda relativa al risarcimento del danno, di cui non è provata entità e consequenzialità, non può essere accolta neppure sotto il profilo del rimborso delle spese di difesa, stante la natura del giudizio avanti all' ABF che non prevede la necessità di difesa tecnica.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 59.500,00.

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