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) BARGELLI

Seduta del 30/05/2023

FATTO

La cliente afferma di avere ricevuto, in data 19/03/2022, un sms proveniente dall'intermediario che comunicava l'attivazione di un Mobile Token; una successiva telefonata da parte di sedicente personale dell'intermediario, che lo informava della necessità di attivare ulteriore livello di sicurezza, nel corso della quale ella comunicava il suo numero cliente, ma non il PIN e il codice riservato presente nel corpo del messaggio, rifiutandosi di attivare il mobile token. Allo scopo di verificare se tale attivazione era avvenuta, afferma di avere effettuato lo stesso 19/03/2022 un bonifico dal proprio home banking con digitazione del solo PIN , che andava a buon fine, con ciò rassicurandosi del fatto che il mobile token non era stato attivato;. Dichiara poi di avere provato a usare la propria carta di credito in data 30/03/2022 e di essersi accorto che la stessa era stata bloccata; di avere nel contempo ricevuto due SMS dall'intermediario, che le confermavano il blocco del conto corrente, del bancomat e della carta; invitata a chiamare al numero verde dell'intermediario (***060) dell'assistenza clienti, dove veniva informata di anomalie sul conto, si recava in banca dove scopriva che era stato disposto un bonifico estero fraudolento per € 24.00,00; presentata denuncia presso le Autorità in data 31/03/2022, la filiale lo contattava per segnalare la presenza di una ricarica di €150,00 verso numero sconosciuto, cosicché si rendeva necessaria una seconda denuncia presso le Autorità in data 04/03/2022. Inoltrato reclamo all'intermediario, che

rispondeva negativamente, domanda la restituzione di euro 24150,00, oltre alle spese di avvio della procedura ABF.

L'intermediario, premesso che la cliente è titolare del conto corrente n. ***85, al quale è collegato il servizio "Rapporti a distanza tra Banca e Cliente", c.d. home banking, che prevede l'accesso alle funzioni di inquiry e dispositive mediante un sistema di autenticazione "forte" e che ella aveva attivato il servizio SMS Alert collegato al suo telefono cellulare n.***282, eccepisce la mancata ricostruzione dei fatti che possono avere portato al compimento della frode; eccepisce poi l'inammissibilità del ricorso in quanto l'operazione è stata resa possibile dalla conoscenza in capo al presunto frodatore delle credenziali di sicurezza dell'home banking del ricorrente che solo lei può avere comunicato oppure attraverso il suo diretto coinvolgimento da parte del terzo non autorizzato. Eccepisce altresì che le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto avvenute con il corretto inserimento delle credenziali; che sussiste la colpa grave della cliente in quanto (i) la cliente, dopo aver ricevuto l'sms riguardante l'attivazione di un Mobile Token da lei non richiesta, non ha contattato immediatamente il personale della propria agenzia o il Servizio clienti al numero verde; se lo avesse fatto, nel termine di 8 giorni, si sarebbe resa conto di essere rimasta vittima di un raggiro ed avrebbe evitato le operazioni fraudolente; (ii) l'operazione è stata resa possibile esclusivamente dalla conoscenza in capo al frodatore delle credenziali di sicurezza dell'home banking della ricorrente, che solo lei può avere comunicato oppure attraverso il diretto coinvolgimento da parte del terzo non autorizzato. Nega la presenza di malfunzionamenti o intrusioni nei propri sistemi informatici.

Conclude per il rigetto del ricorso.

La cliente replica che le tracciature informatiche prodotte in occasione delle operazioni disconosciute e dell'attivazione del token indicano che (i) le operazioni contestate sono state poste in essere da IP mai utilizzati in precedenza dal cliente, dei quali uno è situato a Londra e l'altro a Parma, aree estranee al luogo di residenza della cliente; (ii) il device utilizzato ("Samsung 8") è diverso da quello in uso all'intestataria del conto; ulteriore anomalia sarebbe rappresentata dalla distanza di 18 secondi dal termine delle operazioni compiute sul Galaxy S8 del truffatore localizzato a Londra, laddove invece la cliente ha effettuato subito dopo un accesso con il device consueto localizzato altrove. Rileva che l'uso contemporaneo di due IP collocati a grandissima distanza rende evidente l'anomalia della situazione che avrebbe potuto porre in allarme la banca. Nega di avere comunicato, nel corso della chiamata, il PIN o il codice OTP inviato via SMS.

L'intermediario controreplica che l'utilizzo di un device diverso da quello abitualmente utilizzato dal cliente o il diverso IP non costituiscono indice di anomalia per la Banca che, nell'operatività online, identifica il cliente attraverso la combinazione delle credenziali di sicurezza e dei codici OTP generati dal Mobile Token attivato mediante utilizzo delle medesime credenziali; ciò in quanto vi è la possibilità di attivare contemporaneamente n.2 Mobile Token su due diversi dispositivi e la sostituzione del proprio apparecchio cellulare non richiede la comunicazione alla Banca. Nega che sia sofisticata il tipo di frode di cui non si conoscono nel dettaglio le modalità con le quali è stata perpetrata. Insiste, dunque, nel rigetto del ricorso.

DIRITTO

Il presente ricorso ha a oggetto 2 operazioni contestate, dell'importo complessivo di € 24.150,00; la prima è stata eseguita in data 27/03/2022, per € 24.000,00, alle ore 22:56; la seconda in data 29/03/2022, per € 150,00.
È in atti la prima denuncia della cliente presentata il 31/03/2022 alle ore 17:58 in merito all'operazione fraudolenta di valore pari a € 24.000,00; risulta altresì la denuncia integrativa presentata il 04/04/2022 in merito alla ricarica telefonica fraudolenta di valore pari a € 150,00.
Il Collegio, richiamati gli artt. 10, 12, 12 bis e 12ter del D.lgs. 27 gennaio 2010, n. 11, ricorda che è l'intermediario a dover provare l'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e la contabilizzazione delle operazioni: prova che comunque di per sé non è sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore. D'altra parte, il Collegio giudicante non potrebbe desumere la sussistenza della frode, del dolo o della colpa grave dell'utente soltanto dalla prova della "regolarità formale" dell'operazione: cosicché 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 particolare, la valutazione della condotta dell'utilizzatore dello strumento di pagamento, ai fini dell'eventuale giudizio di colpa grave, deve fondarsi sulla considerazione del complesso di circostanze che caratterizzano il caso concreto.
Il Collegio, nel verificare il sistema predisposto dall'intermediario alla luce dei criteri previsti per l'autenticazione forte, richiama altresì l'art. 12 del d.lgs. 27.1.2010, n. 11, "Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento", che recita: "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 Collegio ricorda altresì che, in base all'art. 1, lett. q-bis, l'"autenticazione forte del cliente" è definita come "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione". Tale autenticazione forte è richiesta, ai sensi dell'art. 10-bis, comma 1, lett. b) del d.lgs. 27.1.2010, n. 11, quando l'utente dispone un'operazione di pagamento elettronico.
Tenuto conto, poi, del Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (in particolare, quello del 21 giugno 2019), il Collegio ribadisce che l'autenticazione forte (SCA) è richiesta sia nella fase di (i) accesso al conto/enrollment dell'app/ registrazione della carta sul wallet, sia nella fase di (ii) esecuzione delle singole operazioni. La SCA 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 le operazioni sono state correttamente contabilizzate, registrate e autenticate e illustra le modalità d'accesso ed autenticazione.
È opportuno premettere che l'intermediario non allega i log relativi alla seconda operazione di ricarica telefonica in data 29/03/2022, di valore pari a € 150,00, ma solo quelli relativi all'operazione di bonifico eseguita in data 27/03/2022 alle ore 22:56 di valore pari a €24.00,00.

Rispetto a tale operazione, pertanto, il Collegio conclude agevolmente per l'assenza della prova dell'autenticazione e dichiara accoglibile la richiesta del cliente di rimborso della somma di 150 euro.
Quanto alle modalità di esecuzione della prima operazione contestata di € 24.000, l'Intermediario afferma la presenza di un sistema di autenticazione "forte", che include, per l'accesso, l'inserimento delle credenziali di accesso (numero cliente + PIN) + codice OTP (One Time Password) e, per la disposizione delle singole operazioni, il PIN + codice OTP (One Time Password). Il codice OTP è generato da Mobile Token integrato nella APP che il cliente ha attivato sul proprio device. Il testo della notifica che appare sul device e sul quale l'utente deve fare "tap" per autorizzare indica in chiaro quale operazione si autorizza.
L'intermediario specifica inoltre che l'attivazione del mobile token su un nuovo dispositivo è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente con due diversi canali: la prima parte del codice OTP viene inviata via email e la seconda parte via SMS al cellulare collegato indipendentemente dalla attivazione del servizio SMS Alert.
L'intermediario fornisce evidenza dell'sms contenente il codice OTP necessario per l'attivazione del Mobile Token, corrispondente a quello indicato dalla cliente nella denuncia.
Risulta inoltre l'inserimento del PIN, ovvero del fattore conoscenza.
L'intermediario, tuttavia, nulla dice né produce sul precedente LOGIN necessario per l'attivazione del Mobile Token, cosicché, pur risultando che l'accesso sia stato effettuato con il PIN (fattore conoscenza), manca il secondo elemento che consenta di ritenere integrata la SCA.
I Collegi condividono l'importazione che, in mancanza della prova anche solo di un passaggio del procedimento che conduce all'autenticazione delle operazioni, l'onere probatorio posto a carico dell'intermediario non possa dirsi assolto.
A nulla rileva, ai fini della responsabilità dell'intermediario, che quest'ultimo sia stato invece in grado di dimostrare l'autenticazione forte con riguardo alle transazioni contestate dalla cliente, poiché, come si è precisato, la prova della SCA deve essere fornita con riferimento a tutte le fasi del procedimento che porta al pagamento.
Non rileva neppure l'eventuale prova della colpa grave del cliente nel rispondere ai messaggi e alle telefonate truffaldine, in quanto la prova dell'autenticazione forte ha carattere prioritario rispetto a quella avente a oggetto l'elemento soggettivo (cfr., per un caso analogo, Collegio di Milano decisione n. 1461/23 del 16/02/2023).
La domanda di rimborso, pertanto, merita di essere accolta.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 24.150,00.
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