

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) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) BARGELLI	Membro di designazione rappresentativa dei clienti

Relatore (MI) BARGELLI

Seduta del 19/12/2023

FATTO

La cliente afferma di aver ricevuto alcuni messaggi provenienti dall'intermediario che l'avvisavano di bonifici effettuati dal suo conto a soggetti sconosciuti per un importo di € 39.990,00 nella notte tra il 15 e il 16 marzo 2023. Dichiara di aver contattato la filiale via email, tramite la figlia, per comunicare l'evento fraudolento, alle ore 01:48. Presentata denuncia presso le Autorità in data 16/03/2023 e presentato reclamo con lettera del 17/03/2023, riceveva risposta negativa dall'intermediario, che sosteneva che l'attivazione di un secondo dispositivo token fosse stata autorizzata dal dispositivo abituale della cliente e che la stessa avesse tardato nella segnalazione alla filiale. Riscontrato, tramite i suoi procuratori, il diniego della banca, la cliente escludeva l'attivazione di un altro token e contestava la mancata predisposizione di adeguate misure di sicurezza da parte della banca, nonostante l'individuazione dell'attività fraudolenta e dei beneficiari dei bonifici. Domanda di effettuare lo storno dei bonifici effettuati in data 15/16 marzo 2023 e di restituirle la somma di euro 39.900,00 euro, oltre agli interessi legali e alle spese della procedura.

L'intermediario afferma che non è stata riscontrata alcuna anomalia né manomissione o intrusione nei sistemi informatici della banca e che le operazioni sono state correttamente



contabilizzate, registrate e autenticate in quanto avvenute con il corretto inserimento delle credenziali. Sostiene la colpa grave della cliente che ha volontariamente ceduto i propri codici di accesso all'area riservata dell'home banking al truffatore, ha consentito al truffatore l'attivazione di un nuovo token e ha ignorato il messaggio il relativo messaggio alert; sottolinea che la cliente ha avuto più di 24 ore dall'inserimento del primo bonifico fraudolento per rendersi conto del tentativo di frode in atto. Precisa di avere informato la cliente dell'avvenuto inserimento di un bonifico di €10.000,00 nonché dei bonifici successivamente eseguiti ad orari distanziati tra loro in data 14/03/2023, alle ore 12:12, ma tali sms venivano ignorati dalla cliente. Nega il carattere insidioso dello spoofing, non essendo la cliente stata adescata tramite SMS o chiamate apparentemente proveniente dalla banca. Ravvede la colpa grave della cliente nel contegno successivo da lei ha adottato, avendo ella ignorato una serie di segnali di allarme che, qualora presi in considerazione, avrebbero potuto evitare la truffa o quantomeno ridurne l'entità. Precisa di essersi immediatamente attivata nella richiesta di storno delle operazioni contestate, rimaste senza esito, fatte eccezione per un bonifico di € 13.540,00 riaccreditato sul conto della cliente, per quanto da lei non considerato, richiedendosi la restituzione dell'intero importo dei bonifici fraudolenti. La richiesta della cliente comporterebbe pertanto non solo una rimessione in pristino della situazione, ma un indebito arricchimento ai danni dell'istituto bancario.

Conclude per il rigetto del ricorso.

La cliente, richiamati i propri scritti, replica che la diligenza posta in capo alla banca corrisponde alla diligenza dell'accorto banchiere che implica, quindi, l'obbligo di adottare un modello organizzativo adeguato alla tipologia di operazioni poste in essere; che spetta alla banca l'onere di provare di aver posto in essere tutte le procedure necessarie onde evitare il compimento di operazioni fraudolente; che la prova documentale volta a provare l'autenticazione e la regolarità delle operazioni non può soddisfare di per sé l'onere probatorio, essendo necessario che la banca provveda specificamente ad indicare le modalità esecutiva da cui trarre, in via presuntiva, la colpa grave dell'utente; che nel caso di specie la documentazione prodotta dalla banca non è idonea a fornire prova dell'adozione di un sistema di autenticazione forte; che la banca non ha fornito alcun elemento di prova sulla colpevolezza della cliente; che la colpa grave non può essere desunta dall'aver ignorato gli sms, dal momento che la stessa pensava che i vari SMS fossero trappole finalizzate a carpire i dati di accesso, assumendo, pertanto, un comportamento ragionevolmente esigibile dal soggetto "utilizzatore"; che la cliente si è attivata subito con la segnalazione ma ciò non ha comunque influito sul richiamo dei bonifici effettuati, dal momento che solo il bonifico più risalente nel tempo è stato stornato. Conferma, infine, di aver ricevuto lo storno del bonifico di €13.540,00.

L'intermediario non ha prodotto controrepliche.

DIRITTO

Il presente ricorso ha a oggetto la contestazione di 7 operazioni, dell'importo complessivo di € 39.990,00, eseguite: il 15/03/2023, alle h. 11:22 (€ 13.540,00); il 15/03/2023, alle h. 14:39 (€ 5.000,00); il 15/03/2023, alle h. 14:55 (€ 6.000,00); il 15/03/2023, alle h. 16:09 (€



450,00); il 16/03/2023, alle h. 00:04 (€ 9.000,00); il 16/03/2023, alle h. 00:46 (€ 4.000,00); il 16/03/2023, alle h. 00:48 (€ 2.000,00).

A fronte di una richiesta complessiva di € 39.990,00, l'intermediario rileva che è stato riaccreditato alla cliente il primo bonifico dell'importo di € 13.540,00. Detta circostanza è altresì confermata dalla cliente nelle repliche, cosicché l'importo richiesto va rideterminato nella minor somma di € 26.450,00.

Nonostante emerga, dall'estratto conto allegato, anche l'addebito di una commissione pari ad € 2,75 per ogni bonifico istantaneo effettuato, la cliente non ne chiede il rimborso.

È in atti la denuncia presentata il 16/03/2023, nella quale la cliente rappresenta di avere ricevuto nella notte a cavallo tra mercoledì 15 e giovedì 16 marzo 2023 dei messaggi da parte dell'intermediario che l'avvisavano di alcuni bonifici effettuati fraudolentemente a suo nome e sul suo conto per un totale di €39.990,00. Tuttavia, non specifica ulteriori circostanze idonee a ricostruire le modalità della truffa.

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. Afferma, in particolare, che l'esecuzione delle operazioni contestate è stata preceduta da un accesso



effettuato il 14/03/2023 mediante SCA, autorizzato dalla cliente stessa; che l'attivazione di un nuovo token software è avvenuto mediante "OTP plus" attraverso token della cliente. Specifica, inoltre, come vengono generati i citati OTP.

Con riferimento all'accesso, l'intermediario afferma che, in data 14 marzo 2023, alle 10:10, il truffatore avrebbe effettuato "un accesso [...] mediante SCA, inserendo nome utente e password del cliente e codice OTP generato dal token e, a sostegno di questa ricostruzione, produce le evidenze e relativa legenda esplicativa, precisando che "per ciascuna attività viene evidenziato il tipo di autenticazione utilizzato". L'accesso è avvenuto da indirizzo IP diverso da quello associato al token dell'utente. Le evidenze mostrano che è stato generato un OTP (elemento di possesso) dal token in uso alla cliente nel periodo antecedente alla truffa mediante "pressione manuale dei pulsanti sul token Id***tel"; quest'ultimo appare a sua volta legato ad un elemento di inerenza - la biometria - di cui l'intermediario afferma di recare evidenza, senza, tuttavia, indicare un orario o una data che permetta di collegare tale specifico elemento all'accesso delle 10:10; inoltre, la colonna "stato autorizzazione" non risulta valorizzata.

La documentazione prodotta dall'intermediario offre evidenza dell'inserimento dei codici OTP generati tramite token software, mentre non fornisce piena prova del fattore di inerenza. Tale carenza è riscontrata anche con riferimento all'attivazione del nuovo token software e all'esecuzione delle singole operazioni contestate.

Secondo l'orientamento di questo Collegio, è necessario il raggiungimento della piena prova di ciascuno dei fattori chiamati a comporre l'autenticazione forte, essendo richiesta la specifica verifica dei singoli passaggi che in concreto hanno condotto all'autorizzazione dell'operazione.

In mancanza anche parziale dell'evidenza della SCA con riferimento all'enrollment dell'app, i Collegi sono unanimi nel ritenere che il ricorso debba essere accolto integralmente.

La (piena) prova della SCA, inoltre, è ritenuta prodromica rispetto a ogni altro elemento rilevante ai fini dell'accertamento della responsabilità dell'intermediario e, in particolare, assume valore assorbente rispetto alla valutazione di eventuali profili di colpa grave dell'utente.

Per queste ragioni, la cliente ha diritto al rimborso delle operazioni contestate (v.m per un caso analogo, Coll. Milano, decisione n. 10032 del 17/10/2023), limitatamente alla somma di € 26.450,00.

La cliente chiede altresì gli interessi legali dalle operazioni fraudolente. Il Collegio tiene conto, sul punto, di quanto statuito dall'art. 11 D.lgs. 11/2010 (testo in vigore dal 13.1.2018): "il prestatore di servizi di pagamento riporta il conto nello stato in cui si sarebbe trovato se l'operazione di pagamento non avesse avuto luogo, assicurando che la data valuta dell'accredito non sia successiva a quella dell'addebito dell'importo".

Infine, la domanda include le "spese della procedura" senz'altro specificare. Poiché, tuttavia, non sono allegati evidenze di parcelle o compensi a favore del difensore, nulla a titolo di spese legali può esserle dovuto.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 26.450,00 con buona valuta.

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



Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

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