

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCA DELL ANNA MISURALE

Seduta del 07/01/2025

FATTO

Con ricorso del 3 settembre 2024 il cliente espone quanto segue:

- in data 31/01/24 veniva contattato dal numero verde ***60, contatto ufficiale della banca, e un operatore in possesso dei suoi dati personali e bancari, lo induceva ad aggiornare l'app dell'intermediario;
- era già successo in precedenza, circa 15 giorni prima della frode, che l'intermediario sollecitasse al cliente l'aggiornamento di alcuni dati con l'invio di un messaggio sull'app;
- non dubitando dell'affidabilità dell'interlocutore, poste la provenienza della telefonata e la dettagliata conoscenza dei suoi dati personali, procedeva con le operazioni indicate dal sedicente operatore;
- gli veniva chiesto di aggiornare l'applicazione cliccando su un link ricevuto tramite messaggio whatsapp. Il messaggio riportava il logo dell'intermediario e un numero del servizio assistenza clienti ***40;
- gli veniva chiesto di attendere l'arrivo di un codice tramite messaggio SMS e di inserirlo nella barra che si sarebbe aperta al termine della procedura. Il messaggio ricevuto era inserito all'interno della chat con l'intermediario e ne riportava la sigla;

- precisa che durante la telefonata con il truffatore non ha comunicato alcun codice di sicurezza;
- terminata la procedura veniva invitato ad accedere all'app ma, poco dopo l'accesso, cadeva la linea telefonica. Non ricevendo più alcuna telefonata dal presunto operatore cercava di accedere nuovamente all'app, ma notava che questa non era più presente sul proprio smartphone e che i messaggi ricevuti su whatsapp erano stati cancellati;
- provvedeva, quindi, a contattare il medesimo numero del servizio clienti e veniva a conoscenza della disposizione di un bonifico istantaneo ad un beneficiario sconosciuto pari ad € 14.980,00;
- nei giorni successivi subiva un nuovo tentativo di truffa del tutto uguale;
- presentava un primo reclamo all'intermediario in data 08/02/2024, al quale ne seguiva un altro in data 05/03/2024. In entrambi i casi l'intermediario ha negato il rimborso della somma fraudolentemente sottratta;
- è ravvisabile una responsabilità dell'intermediario per diverse ragioni. In primo luogo, il canale utilizzato per attuare il raggio è quello ufficiale della banca. In secondo luogo, la quantità e la qualità dei dati in possesso del truffatore, evidenzia una grave falla nel sistema di gestione dei dati dell'intermediario. Infine, l'operazione eseguita risulta del tutto anomala in relazione al consueto utilizzo del conto: il cliente non ha mai usato in precedenza il bonifico istantaneo, del quale lamenta anche l'illegittima attivazione;
- ciò palesa una totale assenza di qualsivoglia controllo da parte della banca che ha, di fatto, permesso un'operatività agevolmente riconoscibile come sospetta;
- risulta evidente la mancanza di colpa grave, ma anche lieve, in capo al cliente.

Chiede, pertanto, il rimborso di € 14.980,00.

L'intermediario, riportato il fatto, afferma quanto segue:

- il ricorrente è intestatario del conto corrente n.***32, al quale è collegato il servizio di home banking;
- il servizio di home banking risulta collegato alla utenza cellulare del cliente, n. ***60 lo stesso dichiarato nella denuncia, al quale l'intermediario, il 31 gennaio 2024, ha inviato gli sms e le notifiche push riferite alla operatività disconosciuta (all.4);
- il n. ***40 dal quale è stato inviato il messaggio whatsapp contenente il link, anche se riporta il logo dell'intermediario, non è presente tra i contatti memorizzati dal ricorrente, a differenza del contatto ufficiale che è invece presente sul device del cliente;
- il cliente avrebbe dovuto ricevere tutti i messaggi in coda alla chat con l'intermediario, già attiva sul suo cellulare, e nella quale risulta presente il codice OTP necessario per attivare un nuovo Mobile Token;
- a fronte dell'sms "parlante" ricevuto, il cliente, sapendo di non aver richiesto lui una nuova attivazione dell'app avrebbe dovuto insospettirsi ed interrompere la telefonata, ma soprattutto non avrebbe dovuto rivelarlo e neppure inserirlo in un eventuale link o pagina web, come da raccomandazione contenuta nella stessa comunicazione;
- eseguito l'accesso al link, editando un codice riferitogli dal suo interlocutore è plausibile ritenere che il cliente abbia consentito al terzo di assumere il controllo del suo device e carpire così le credenziali di sicurezza, digitate successivamente per accedere all'app ufficiale della Banca ed anche il codice OTP ricevuto via sms che deve aver comunicato al telefono o inserito sul web;
- in merito al canale di provenienza di SMS e telefonate: non si deve riporre troppa fiducia nel "caller ID" che appare su telefono fisso o mobile, in quanto è risaputo

che esso non garantisce che la chiamata sia effettivamente partita dall'utenza indicata sul display in quanto è possibile, con pochi passaggi, modificare il mittente di un numero telefonico da parte di terzi;

- le operazioni, sia di attivazione del Mobile Token, sia di login che di bonifico, risultano correttamente autenticate, registrate ed eseguite mediante un sistema di autenticazione "forte", senza che sia emerso alcun malfunzionamento o compromissione dei sistemi della Banca;
- nonostante il disconoscimento dell'operazione non ha potuto bloccarla, trattandosi di bonifico istantaneo. Ha avviato l'azione di recall verso la banca del beneficiario, che ha avuto esito negativo;
- precisa che i dati personali che il ricorrente eccepisce siano stati forniti dalla Banca possono essere stati acquisiti da una qualsiasi altra fonte;
- il comportamento tenuto dal ricorrente integra la sua colpa grave per non aver adempiuto con la dovuta diligenza ai propri obblighi di custodia e protezione delle credenziali di sicurezza personalizzate del suo strumento di pagamento, rendendo inefficaci le misure di sicurezza e prevenzione adottate dall'intermediario.

Conclude chiedendo il rigetto del ricorso.

Il cliente, confermando integralmente le premesse, i fatti e le considerazioni esposte nel ricorso, replica quanto segue:

- l'intermediario non ha dimostrato la legittimità dell'attivazione del servizio di bonifico istantaneo;
- in particolare, non ha dimostrato: la specifica sottoscrizione da parte del ricorrente di un'apposita clausola contrattuale che prevedesse la possibilità di modifica unilaterale delle condizioni contrattuali; la specifica indicazione di un giustificato motivo per l'introduzione di detta modifica; l'effettiva ricezione (nemmeno l'invio) da parte del cliente della proposta di modifica unilaterale introduttiva la funzionalità di bonifico istantaneo;
- il cliente non era a conoscenza del pericolo insito nel servizio di bonifico istantaneo e dell'attivazione sul suo conto corrente. Ne è riprova il fatto che detto servizio mai è stato utilizzato dal cliente;
- l'operazione disconosciuta risulta eseguita con una modalità (bonifico istantaneo) non validamente concordata tra le parti e, quindi, priva di alcun effetto, con la conseguenza che sussiste il diritto del ricorrente al rimborso integrale dell'importo corrispondente alle medesime operazioni;
- non ha comunicato i dati di accesso e nemmeno gli OTP ricevuti, ma ha inserito detti dati sull'app della quale, poi, gli è stato dai malviventi tecnicamente sottratto il controllo.

Insiste per l'accoglimento integrale del ricorso.

L'intermediario, riportandosi alle conclusioni in atti, controreplica che:

- il servizio "bonifico istantaneo" è un nuovo servizio legittimamente offerto alla clientela, regolarmente comunicato tramite PMU, già allegate alle controdeduzioni, inclusa l'evidenza della relativa postalizzazione;
- la PMU 2022 prevede la facoltà per il cliente di ridurre, fino ad azzerare, il limite massimo (€ 15.000) previsto per i bonifici istantanei in uscita e della quale il ricorrente non si è avvalso.

Insiste per il rigetto integrale del ricorso.

DIRITTO

La questione sottoposta all'esame del Collegio ha ad oggetto il disconoscimento di una operazione di bonifico effettuata in data 31.01.2024 alle ore 13:41 per € 14.980,00. È in atti la denuncia del cliente presentata lo stesso giorno e integrata in data 13.02.2024.

Preliminarmente si rileva che il cliente contesta la funzionalità del "bonifico istantaneo" assumendone l'illegittima attivazione. In particolare, sostiene che tale modalità non gli fosse stata resa nota dall'intermediario, il quale non avrebbe dimostrato:

- la specifica sottoscrizione da parte del cliente di un'apposita clausola contrattuale che prevedesse la possibilità di modifica unilaterale delle condizioni contrattuali;
- la specifica indicazione di un giustificato motivo per l'introduzione di detta modifica;
- l'effettiva ricezione (nemmeno l'invio) da parte del cliente della proposta di modifica unilaterale introduttiva la funzionalità di bonifico istantaneo.

Ebbene, la contestazione non coglie nel segno perché l'art. 126 *sexies* TUB richiede esclusivamente l'invio da parte dell'intermediario di una PMU chiara e completa. Al riguardo, l'intermediario afferma di aver regolarmente comunicato al cliente, tramite proposta di modifica unilaterale del contratto, l'attivazione del servizio, producendo evidenza della PMU del 2019 e del 2022, oltre che l'evidenza della relativa postalizzazione. La proposta del 2019 è denominata "Proposta di modifica del contratto per introduzione del nuovo servizio di bonifico istantaneo" e reca comunicazione del nuovo servizio; la proposta del 2022, denominata, "Proposta di modifica unilaterale del contratto" comunica al cliente che il bonifico istantaneo non è revocabile e che è possibile limitarne il funzionamento avendo il cliente anche facoltà di "di azzerare, se lo ritiene, il servizio di bonifico istantaneo".

In merito alla introduzione della funzionalità di bonifico istantaneo si è pronunciato il Collegio di Coordinamento, affermando il principio secondo cui: *"La proposta al consumatore di introduzione della modalità di pagamento tramite bonifico istantaneo, ai sensi dell'art.126-sexies, comma 4-bis, del T.U.B., può essere validamente formulata se corredata da una informazione completa e corretta delle relative caratteristiche. Tale non è quella che si limiti a evidenziare il costo del bonifico istantaneo, a conferma implicita della nuova opportunità offerta al destinatario, senza indicazione della caratteristica della irrevocabilità della operazione, determinativa dell'aumento del rischio in capo all'ordinante"*.

La comunicazione del 2022 sembra rispettare le prescrizioni di cui all'art. 126 *sexies* TUB per come interpretate dal Collegio di Coordinamento e, pertanto, non è rimproverabile all'intermediario alcuna condotta scorretta al riguardo.

Si deve quindi procedere ad esaminare la prova di autenticazione delle operazioni ai sensi del D.lgs. 11/2010.

In particolare, le fonti normative applicabili alla fattispecie sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del D. Lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019). Nello specifico è richiesta l'autenticazione forte (SCA) quando il cliente 1. accede al suo conto di pagamento online; 2. dispone un'operazione di pagamento elettronico; 3. effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.

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.

Al riguardo, giova precisare che l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e

graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione 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; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.

Ciò premesso, per quanto attiene al primo profilo sopra individuato, l'intermediario resistente non ha prodotto piena prova della SCA.

In particolare, per quanto attiene alla fase di accesso all'area riservata per l'attivazione del mobile token dai log prodotti dall'intermediario risulta che non è presente specifica evidenza dell'inserimento del PIN, il cui utilizzo si ricava dalla descrizione "attività utente".

La colonna "esito operazione" non è valorizzata e non risulta la generazione in app dell'OTP c.d. silente. L'evidenza del PIN manca inoltre per quanto attiene all'attivazione del mobile token e, del pari, per quanto infine attiene all'operazione di bonifico (sia nella fase prodromica del login che in quella di disposizione del bonifico).

In linea con la giurisprudenza di questo Arbitro che, in casi analoghi a quello di cui in contestazione (cfr. Collegio Milano, decisione n. 4760/24) non ha ritenuto provata la SCA, deve reputarsi non assolto l'onere probatorio gravante sull'intermediario.

Ebbene, secondo il consolidato orientamento dei Collegi, in difetto di piena prova sull'autenticazione delle transazioni disconosciute il ricorso deve essere accolto integralmente, posto che la mancanza della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente. La prova di autenticazione rappresenta infatti, come sopra evidenziato, un *prius* logico rispetto alla prova della colpa grave dell'utente.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 14.980,00.

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
ANDREA TINA