COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) BARTOLOMUCCI	Membro designato dalla Banca d'Italia
(MI) BALDINELLI	Membro designato dalla Banca d'Italia
(MI) PERON	Membro di designazione rappresentativa degli intermediari
(MI) CESARE	Membro di designazione rappresentativa dei clienti

Relatore PIERFRANCESCO BARTOLOMUCCI

Seduta del 17/12/2024

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo che in data 15.03.2024, alle ore 13:30 circa, avesse ricevuto un messaggio da un intermediario terzo che gli comunicava l'attivazione di un'app e gli forniva un numero di telefono da contattare per disconoscere l'operazione; chiamava il numero indicato e una voce preregistrata chiedeva l'inserimento del codice cliente e del codice d'accesso, inseriti i quali la chiamata veniva trasferita ad un operatore che gli comunicava la necessità di effettuare un aggiornamento dell'applicazione della banca.
Faceva presente di aver acconsentito alla richiesta e di aver seguito le istruzioni telefoniche impartite dall'interlocutore; a quel punto, il telefono cellulare entrava in modalità aggiornamento, con lo sfondo del logo della banca e una icona di aggiornamento. Risultava peraltro inutilizzabile in rete per circa tre ore, durante le quali il sedicente operatore rimaneva in linea con lui, lamentando l'insorgenza di numerosi problemi tecnici; alle ore 16,00, circa, il sedicente operatore comunicava che l'aggiornamento fosse terminato, ma che l'*home banking* della banca terza non sarebbe stato fruibile per le successive 24 ore.
Precisava che, in relazione a tale operazioni, non avesse comunicato alcuna informazione riservata relativa ai codici di accesso al conto corrente dell'odierno resistente; soggiungeva che, immediatamente dopo la telefonata, avesse constatato la ricezione di

una e-mail da parte dell'intermediario che lo informava che fosse stato richiesto un bonifico dell'importo di € 5.900,00 (a favore di un soggetto a lui ignoto), la cui esecuzione veniva confermata in seguito ad una telefonata al numero verde.
Avvedutosi della truffa, chiedeva l'annullamento dell'operazione; tuttavia, alle ore 17:36, riceveva una comunicazione da parte dell'intermediario che lo informava che le sue credenziali di accesso all'app e all'area clienti fossero state temporaneamente bloccate.
Sporgeva quindi denuncia alle autorità competenti e in data 19.03.2024 aggiungeva alla denuncia la richiesta di decreto di sequestro delle somme presenti sul conto corrente del beneficiario; precisava che, in seguito al reclamo, l'intermediario avesse provveduto a riaccreditare il minor importo di € 1.923,00.
Chiedeva, pertanto, il rimborso dell'importo residuo di € 3.977,00, oltre al risarcimento del danno forfetariamente quantificato in € 600,00.
Costituitosi ritualmente, l'intermediario rilevava che l'operazione di bonifico contestata fosse stata correttamente contabilizzata, registrata e autenticata senza aver subito le conseguenze di alcun tipo di malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.
Precisava pure che essa fosse stata eseguita (così come tutti gli accessi) in data 15.03.2024 tramite il dispositivo ordinariamente utilizzato dal ricorrente; pertanto la banca, dai propri sistemi informativi, non avrebbe potuto ravvisare alcuna attività potenzialmente anomala. Osservava pure che le contestazioni circa l'intempestività con cui avrebbe proceduto al blocco dell'operazione risultassero del tutto infondate, avendo il ricorrente chiamato la banca solo dopo aver visualizzato la mail di comunicazione di un bonifico di importo elevato.
Sottolineava, quindi che – non appena ricevuta la comunicazione di quanto accaduto – avesse provveduto al blocco cautelativo dell'operatività del conto corrente beneficiario del pagamento, riuscendo a vincolare il minor importo di € 1.923,00, poi restituito al cliente, come anche dal medesimo riconosciuto.
Riteneva che sussistesse la colpa grave del ricorrente per aver permesso a terzi di accedere liberamente al proprio *smartphone* installando un'applicazione su indicazione del truffatore, che peraltro si annunciava come operatore di una banca terza.
Si opponeva, da ultimo, alla richiesta di risarcimento danni, in quanto l'importo richiesto era stato calcolato forfettariamente.
Chiedeva, pertanto, il rigetto del ricorso.

Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale ribadiva che, pur essendo pacifico che la disposizione contestata fosse stata effettuata dal suo *smartphone* contro la sua volontà, egli non avesse comunicato le credenziali statiche (*username* e *password*) per effettuare il bonifico.
Sottolineava che non fosse sufficiente per configurare la responsabilità del cliente la circostanza che il cellulare fosse finito nella disponibilità dei truffatori e che questi fossero riusciti a utilizzare l'app della banca per disporre un bonifico; soggiungeva pure che l'accesso all'area riservata non potesse essere avvenuto tramite riconoscimento biometrico e che i malfattori fossero stati in grado di ovviare alla procedura di riconoscimento del volto con espedienti tecnologici ed informatici, resi possibili da un'applicazione bancaria i cui sistemi di sicurezza si erano rivelati fallaci e non idonei ad impedire l'utilizzo fraudolento.
Riteneva, quindi, sussistente la responsabilità della banca per aver effettuato l'operazione di bonifico nonostante avesse rilevato la potenziale truffa e nonostante egli avesse richiesto il blocco dell'operazione dopo circa un'ora dalla ricezione della mail della banca;

faceva altresì presente che il conto corrente del beneficiario del bonifico fosse anch'esso acceso presso l'intermediario che quindi avrebbe potuto operare con grande libertà.
Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale ribadiva che l'operazione di bonifico fosse stata correttamente autorizzata mediante doppio fattore di autenticazione (riconoscimento biometrico quale elemento di conoscenza; conferma con *token* quale elemento di possesso) dallo *smartphone* ordinariamente utilizzato dal ricorrente e univocamente associato alla sua area riservata mediante attivazione della conferma con *token*; riteneva, pertanto, la tesi avversa – secondo cui l'attivazione del riconoscimento biometrico e della conferma con *token* non sarebbe stata possibile nel caso in esame – fosse una mera petizione di principio, priva di qualsivoglia riscontro.
Respingeva pure l'accusa di inerzia della banca, tenuto conto che proprio il suo tempestivo intervento avesse consentito il recupero di € 1.923,00 che altrimenti sarebbero stati trasferiti al di fuori del rapporto; precisava, da ultimo, che la comunicazione e-mail inviata al ricorrente in occasione del bonifico non fosse stata inviata poiché la banca avesse sospettato che l'operazione potesse essere fraudolenta, ma perché essa viene inviata a tutti i clienti qualora eseguano un'operazione di bonifico di importo maggiore di € 1.000,00, in aggiunta alla *push notification* di esecuzione dell'operazione.
Si opponeva alla richiesta di risarcimento del danno, in quanto sfornita di qualsivoglia supporto e calcolata in maniera arbitraria.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di un'operazione, successivamente disconosciuta.
La materia, come noto, è regolata dal d. lgs. n. 11/2010 come modificato dal d. lgs. n. 218/2017 con cui è stata recepita la direttiva 2015/2366/Ue (c.d. PSD2- *Payment Services Directive 2*).
Tale disciplina, al fine di rafforzare i presidi di sicurezza e di incentivare il corretto utilizzo di strumenti di pagamento diversi dal contante, introduce una serie di obblighi in capo tanto ai fruitori quanto ai prestatori di servizi di pagamento: ai primi è imposto di usare detti strumenti in modo diligente, in conformità alle prescrizioni contrattuali, adottando misure idonee ad assicurare la segretezza dei codici personalizzati necessari per usufruire dei servizi e onerando gli stessi di informare tempestivamente i prestatori in caso di operazioni fraudolente; ai secondi, invece, è imposto di predisporre sistemi di sicurezza che impediscano l'accesso da parte di terzi ai dispositivi personali degli utilizzatori (c.d. *strong customer authentication* SCA), nonché ad impedire l'uso degli strumenti di pagamento successivamente alla comunicazione ricevuta da questi ultimi nei casi di operazioni disconosciute.
Al fine di bilanciare le diverse posizioni, ed in ragione del rischio d'impresa riconosciuto in capo al prestatore dei servizi di pagamento, la normativa *de qua* prevede una diversa distribuzione degli oneri probatori in conseguenza del disconoscimento di un'operazione, con l'obiettivo di attribuire la responsabilità degli utilizzi fraudolenti all'impresa, nel caso in cui essi non siano stati cagionati da frode, dolo o colpa grave del cliente. Tale criterio di imputazione della responsabilità, tuttavia, presuppone sul piano fattuale che gli utilizzi non autorizzati siano stati effettuati in conseguenza del furto o dello smarrimento degli strumenti di pagamento, ovvero dell'illecito utilizzo dei codici dispositivi degli strumenti di pagamento da parte di terzi frodatori.
Risulta documentalmente che l'operazione contestata consiste in un bonifico eseguito il 15.3.2024 alle ore 15:48 per un ammontare di € 5.900,00.

Mette conto rilevare che risulta pacifico e incontestato tra le parti il fatto che l'intermediario abbia provveduto a rimborsare al cliente la somma di € 1.923,00, ancora disponibile sul conto corrente del beneficiario del bonifico contestato, tanto che il ricorrente stesso allega evidenza del riaccredito.

Ciò premesso, parte resistente dichiara che l'accesso all'area riservata, prodromico alla esecuzione del bonifico, sia stato effettuato il 15.03.2024 tramite riconoscimento biometrico attivato dal ricorrente in data 04.03.2023; precisa pure che tale accesso non ha richiesto l'inserimento di un OTP quale secondo fattore di autenticazione in quanto l'ultimo accesso all'area riservata mediante autenticazione forte era stato registrato meno di 180 giorni prima.

Dalle tracciature informatiche versate in atti emerge che siano stati effettuati, nella data indicata, tre login eseguiti in orari antecedenti all'operazione contestata (in particolare, alle ore 14:42; alle ore 15:08 e alle ore 15:30); pur non specificando quale sia effettivamente il *login* prodromico alla operazione fraudolenta, considerato che l'operazione è stata effettuata alle ore 15:48, il *login* che appare più compatibile è quello delle ore 15:30.

Le ulteriori allegazioni e le risultanze provenienti dalla legenda rivelano altresì che l'accesso da parte dei malfattori all'area riservata del cliente sia stato effettuato utilizzando un solo fattore di autenticazione, *id est* il riconoscimento biometrico ("Medio de autentificacion", codice 106; tant'è vero che il campo "Tipo de firma", relativo al secondo fattore di autenticazione, non risulta popolato).

Tale circostanza, peraltro, è pacificamente ammessa dallo stesso intermediario nelle controdeduzioni, mentre il cliente nega di aver utilizzato la biometria per autorizzare l'operazione, dato che il suo *smartphone* risultava bloccato durante la telefonata con il truffatore.

A tale specifico riguardo, l'intermediario richiama l'art. 10 del Regolamento delegato (UE) 2018/389, come modificato dal Regolamento Delegato (UE) 2022/2360, il quale consente che l'accesso c.d. informativo al conto possa avvenire senza applicare la SCA, a condizione che non siano decorsi più di 180 giorni dall'ultima applicazione della SCA.

Rispetto alla richiamata disposizione normativa, si pone la questione di stabilire se, una volta avuto accesso al conto mediante ricorso a un unico fattore (in applicazione della citata esenzione dalla SCA), sia o meno possibile riutilizzare detto fattore e combinarlo con un secondo elemento di autenticazione per autorizzare un'operazione di pagamento.

Sul tema si è pronunciata l'EBA (cfr. Q&A 2018_4141) la quale ha chiarito che il Regolamento delegato consente di riutilizzare uno dei fattori di autenticazione inseriti per l'accesso al conto per disporre un'operazione di pagamento online nell'ambito della medesima sessione, purché l'associazione di entrambi fattori produca il *dynamic linking* richiesto dall'art. 5 del Regolamento stesso; l'Autorità ha pure precisato (cfr. Q&A 2020_5516) che tale principio trova applicazione anche allorché l'accesso al conto non sia presidiato da SCA, in quanto riconducibile a una delle ipotesi per le quali è prevista l'esenzione ai sensi dell'art. 10 del Regolamento delegato. In tali casi, è possibile per gli intermediari riutilizzare l'(unico) elemento utilizzato per l'accesso al conto ai sensi dell'esenzione di cui all'art. 10, quando è eseguita un'operazione di pagamento elettronico nell'ambito della stessa sessione, a condizione che siano soddisfatte le condizioni appena descritte.

Nel caso di specie, il Collegio rileva – come già ha avuto occasione di chiarire in altri precedenti – che l'accesso al conto non sia stato di carattere meramente informativo, bensì di tipo operativo, essendo stato effettuato per finalizzare l'operazione di bonifico; pertanto, questo non può ritenersi rientrante nell'ambito di applicazione del richiamato art. 10, con la conseguenza che non può considerarsi applicabile la prevista esenzione dalla SCA (cfr. Coll. Milano, dec. n. 10636/2024; n. 8155/2024; n. 7574/2024).

In considerazione del fatto che le stesse indicazioni dell'EBA precisano che – laddove il cliente disconosca le operazioni eseguite in applicazione di una esenzione dalla SCA normativamente prevista – resta comunque ferma la responsabilità dell'intermediario che ha deciso di non adottare l'autenticazione forte, fatte salve le ipotesi di frode dell'utilizzatore, il ricorso deve essere accolto.
La mancanza anche parziale della prova del rispetto dei presidi di sicurezza in tutte le fasi dell'operazione di pagamento, e quindi sin da quella di accesso al sistema, è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente; essa rappresenta infatti, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente.
Deve, pertanto essere riconosciuto il diritto della ricorrente ad ottenere il rimborso del controvalore dell'operazione contestata, al netto dell'importo che ha già formato oggetto di ripetizione da parte dell'intermediario.
Deve invece essere respinta la domanda di risarcimento del danno, in assenza di qualsivoglia elemento di prova in ordine al pregiudizio asseritamente subito.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 3.977,00.
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