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 25.06.2024 avesse ricevuto una telefonata riconducibile all'intermediario con la quale il sedicente operatore bancario lo allertava circa alcuni movimenti sospetti effettuati con la carta di debito collegata al suo conto corrente.
Riferiva di aver chiesto il blocco della carta e che l'interlocutore, dopo aver elencato i sui dati personali e bancari, gli avesse chiesto il CVV; soggiungeva che, dopo aver comunicato tale numero e dopo pochi istanti, avesse ricevuto la notifica di una operazione di pagamento dell'importo di € 2.980,00 effettuata con la sua carta di debito.
Faceva altresì presente di aver "spento" immediatamente la carta di debito dall'app della banca e di aver contattato il servizio clienti, il quale lo informava che fosse stato truffato.
Precisava di aver sporto denuncia alle autorità competenti e di aver presentato reclamo all'intermediario che lo riscontrava negativamente.
Chiedeva, pertanto, il rimborso dell'importo di € 2.980,00.
Costituitosi ritualmente, l'intermediario rilevava che l'operazione disconosciuta dal ricorrente fosse stata autorizzata mediante l'utilizzo delle credenziali statiche e dinamiche in possesso del ricorrente con autenticazione forte a due fattori, registrata e contabilizzata senza aver subito le conseguenze di alcun malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti.

Sottolineava che tutti gli accessi all'area riservata del 25.06.2024 fossero stati effettuati dal ricorrente, ad eccezione di quello relativo alla giornata della presunta truffa, registrato alle ore 19:27:28, in occasione del quale il motore antifrode della banca aveva bloccato l'area personale del cliente. Riteneva, pertanto, che il cliente fosse stato vittima di *vishing*.
Soggiungeva che egli non avesse fornito alcuna prova in merito alla telefonata e neppure sulla riconducibilità del numero all'intermediario, tenuto conto che – quando la banca contatta telefonicamente un proprio cliente – invia un avviso con notifica in app e mai un sms.
Considerava, quindi, sussistente la colpa grave del ricorrente che aveva dato seguito alla telefonata contraffatta e aveva fornito codici bancari al truffatore.
Faceva presente che la banca mette a disposizione dei propri clienti numerosi contenuti sia sul web che tramite e-mail per prevenire le frodi perpetrate mediante il c.d. *vishing*.
Chiedeva, pertanto, il rigetto del ricorso.
Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale precisava che il numero da cui proveniva la telefonata fosse lo stesso che appare nell'area riservata dell'app della banca e che quest'ultima avesse inviato le comunicazioni informative solo dopo la segnalazione della presunta frode, il che indica una mancanza di proattività nel monitoraggio delle operazioni sospette.
Considerava non sussistente la propria colpa grave in quanto non erano presenti indici di anomalia (errori grammaticali, numero di telefono del chiamante estero o sconosciuto, lacune informative, etc.).
Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale ribadiva che le comunicazioni fossero precedenti alla frode subita dal cliente e che esistesse in commercio una banale tecnica che permette ai truffatori di effettuare telefonate e inviare SMS facendo visualizzare al destinatario un nome e numero prescelto in luogo del vero numero del mittente.
Riteneva, quindi, che ciò non potesse essere in alcun modo imputabile alla banca (che non può evitare e/o bloccare tale tipologia di telefonate/SMS, ma mette in guardia i propri clienti da tali tecniche e spiega come proteggersi dalle stesse) e che invece fosse evidente che terzi ignoti avessero adoperato la tecnica soprarichiamata per compiere la truffa; soggiungeva che il cliente stesso avesse eseguito le operazioni nella propria area personale, senza malfunzionamenti o compromissione dei sistemi di sicurezza né tantomeno alcun apporto causale di operatori della banca.
Sottolineava che, con l'impiego di normale diligenza, il cliente avrebbe potuto accorgersi dell'anomala telefonata, nonché delle strane richieste del sedicente operatore.

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 25.6.2024 alle ore 19:53 per un ammontare di 2.980,00 €.

Tanto premesso, parte resistente dichiara che il cliente abbia fatto più volte accesso alla propria area riservata, in differenti orari tra le 19:17 e le 19:43, con autenticazione mediante riconoscimento biometrico.

In particolare, dall'esame dei log in atti risulta, subito prima della modifica dei limiti operativi della carta ("modify card limits") alle ore 10:29:27, un accesso ("Login GT") alle ore 19:28:20.

Riferisce, inoltre, che prima dell'esecuzione dell'operazione contestata si fosse registrata una modifica dei limiti operativi della carta di pagamento alle ore 19:29:27 mediante l'inserimento di una apposita OTP ricevuta tramite SMS sul numero di cellulare univocamente associato al conto.

Anche in tal caso, dalla lettura dei log, unitamente alla legenda, è possibile evincere che vi sia stato l'inserimento dell'OTP (riga 74, colonna "Tipo Trans = Modificar limites de una tarjeta" e colonna "Tipo de firma" recante il codice "05") ed il riconoscimento biometrico disponibile sul *device* utilizzato per l'accesso (colonna F "Medio de autentificación: 106").

Alla luce delle tracciature informatiche prodotte e delle dichiarazioni delle parti risulta invece che l'accesso all'area riservata prodromico alla modifica dei massimali risulta effettuato solo tramite il riconoscimento biometrico.

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 la modifica dei limiti operativi e dispositivi dello strumento di pagamento; pertanto, questa 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; giova rilevare, inoltre, che l'intermediario non abbia neppure fornito alcuna prova circa l'operazione asseritamente avvenuta nel termine dei 180 giorni precedenti.
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.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 2.980,00.
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