COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) BARTOLOMUCCI

Seduta del 06/03/2025

FATTO

Il ricorrente, insoddisfatto dell'interlocuzione intercorsa nella fase del reclamo, adiva questo Arbitro deducendo di aver ricevuto, in data 19/11/2023, una chiamata da un numero corrispondente al numero verde dell'intermediario, che segnalava alcuni movimenti sospetti sul proprio conto.
Faceva presente che nel corso della telefonata, avesse ricevuto sms che apparentemente dovevano servire per bloccare alcune operazioni illecite; convinto della genuinità della chiamata, e nella concitazione del momento, seguiva "scrupolosamente" le istruzioni dell'operatore.
Precisava che il giorno stesso, insospettito, avesse scoperto la truffa e contattato l'intermediario per bloccare le operazioni truffaldine, le quali tuttavia venivano addebitate per € 13.000,00.
Chiedeva, pertanto, il rimborso dell'importo di € 13.000,00 oltre al risarcimento del danno, quantificato in € 1.000,00, per violazione dell'art. 82 GDPR, "individuato nel necessitato esborso delle spese legali".
Costituitosi ritualmente, l'intermediario rilevava che le operazioni contestate fossero state correttamente autorizzate con autenticazione a due fattori; sottolineava pure che il giorno della truffa fossero stati effettuati due accessi mediante *username* e *password*.

Sosteneva di avvalersi dell'art.10 del Reg. delegato (UE) 2018/389, che autorizza i prestatori di servizi di pagamento a non applicare l'autenticazione forte del cliente qualora non siano trascorsi 180 giorni dall'ultima volta che il cliente ha avuto accesso al conto mediante autenticazione forte.
Specificava che, nel caso di specie, il precedente accesso all'area personale con autenticazione forte fosse stato eseguito il 7/10/2023 mediante inserimento di codice OTP ricevuta tramite SMS sul numero di cellulare univocamente associato al rapporto; in seguito a questo, precisava che fosse stato attivato il riconoscimento biometrico con inserimento di OTP e, quindi, effettuato un nuovo accesso con riconoscimento biometrico per la disposizione di un bonifico di € 7.000,00, autenticato con riconoscimento biometrico e conferma con *token*.
Soggiungeva che fosse stata eseguita pure una modifica ai massimali della carta, nonché due generazioni di CVV dinamico, tramite accesso con riconoscimento biometrico e utilizzo della conferma con il *token* attivato precedentemente; successivamente, rilevava che fosse stato effettuato un pagamento di € 3.000,00, autenticato con l'inserimento del CVV dinamico generato (fattore di inerenza incluso nel procedimento di generazione), nonché la conferma con *token* (fattore di possesso).
Da ultimo, precisava che fosse seguito un ulteriore accesso con riconoscimento biometrico e, nella medesima sessione, fossero stati eseguiti tre bonifici istantanei di € 1.000,00 ciascuno, anch'essi autenticati mediante conferma con *token*.
Riteneva che sussistesse la colpa grave del cliente, caduto vittima di *vishing*.
Chiedeva, pertanto, il rigetto del ricorso.
Alle controdeduzioni dell'intermediario replicava il ricorrente, il quale affermava di non disporre di un dispositivo con riconoscimento dell'impronta digitale.
Osservava che l'operatività descritta dall'intermediario fosse stata posta in essere dai truffatori e che, a prescindere dagli indicatori di frode di cui al D.M. n. 112/2007, le operazioni fossero state evidentemente anomale rispetto alla normale operatività, e l'intermediario avrebbe pertanto dovuto avvedersene.
Le repliche del ricorrente venivano riscontrate dall'intermediario, il quale rimarcava che il numero di cellulare associato al conto del cliente fosse corrispondente a quello da quest'ultimo fornito. Inoltre, ribadiva che la truffa subita dal cliente non potesse ritenersi particolarmente sofisticata e che non potesse neppure essere richiesto alla banca di bloccare qualsiasi tipo di operazione "non solitamente" eseguita.

DIRITTO

La domanda proposta dal ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di alcune operazioni, successivamente disconosciute.
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 le operazioni contestate consistono in quattro bonifici ed un pagamento mediante carta, eseguiti il 19 novembre 2024, tre le ore 10.34 e 10.46, per un ammontare complessivo di € 13.000,00.
Dai log informatici versati in atti emerge che le operazioni fraudolente siano state effettuate nell'ambito di due diverse sessioni, pur registrate entro un breve lasso temporale.
L'intermediario, tuttavia, precisa che gli accessi della ricorrente siano avvenuti senza la necessità dell'inserimento di un secondo fattore di autenticazione, ai sensi dell'art. 10 del Regolamento Delegato (UE) 2018/389, "poiché solo pochi minuti prima era stato eseguito l'accesso con doppio fattore mediante modifica della password".
La norma appena richiamata, come modificata dal Regolamento Delegato (UE) 2022/2360, consente invero 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, a prescindere da quanto dedotto dall'intermediario (il quale riferisce che il precedente accesso con autenticazione forte sarebbe stato eseguito il 07/10/2023, senza peraltro allegare i log di tale accesso, ma limitandosi a fornire prova dell'invio del relativo OTP SMS) il Collegio rileva – come già ha avuto occasione di chiarire in altri precedenti – che gli accessi all'area riservata nel giorno della truffa non siano stati di carattere meramente informativo, bensì di tipo operativo, essendo stati effettuati per finalizzare le operazioni fraudolente; pertanto, essi non possono ritenersi rientranti 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.
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, costituendo, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell'utente (cfr. Coll. coord., dec. n. 22745/2019).
Deve, pertanto essere riconosciuto il diritto del ricorrente ad ottenere il rimborso del controvalore delle operazioni contestate.
Non può trovare accoglimento, invece, la domanda risarcitoria in considerazione del fatto che essa (pur formulata in relazione ad una presunta violazione dell'art. 82 GDPR non meglio argomentata) appare comunque finalizzata ad ottenere la rifusione delle spese di assistenza difensiva, peraltro non provate e non richieste nel preventivo reclamo.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 13.000,00.
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