COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) BALDINELLI

Seduta del 10/06/2025

FATTO

Il cliente afferma quanto segue:

- di essere titolare della carta n. 1141;
- alle ore 17:11 del 25/02/2025 riceveva un SMS che sembrava provenire dall'intermediario, in quanto inserito nella medesima chat di messaggistica da cui provenivano i messaggi genuini della banca;
- con l'SMS gli veniva comunicata una limitazione della propria utenza;
- poco dopo riceveva una chiamata da un sedicente operatore dell'intermediario, il quale gli comunicava la necessità di comunicargli i codici ricevuti via SMS al fine sbloccare il suo conto corrente;
- a questo punto il cliente comunicava tali codici al truffatore, inconsapevole che avrebbero autorizzato delle transazioni;
- una volta terminata la chiamata si rendeva conto dell'esecuzione dell'operazione, e subito dopo il truffatore eseguiva autonomamente il pagamento di € 31,67;
- una volta resosi conto della truffa, il cliente contattava l'intermediario per tentare di bloccare le operazioni;
- non sussiste colpa grave in capo al ricorrente, in quanto è stato vittima di una truffa sofisticata in cui l'utente medio, nonostante la diligenza ordinaria, può essere facilmente tratto in inganno;

- presentava denuncia presso le Autorità in data 26/02/2025 e reclamo all'intermediario in data 25/02/2025, che veniva riscontrato negativamente.

Nel formulare le richieste all'Arbitro, contesta fermamente la decisione della banca sulla base della mancata colpa grave:

- ai sensi dell'art. 10 del D.Lgs. 11/20, la banca è tenuta a dimostrare che l'utente ha agito con dolo o colpa grave per escludere l'obbligo del rimborso;
- l'inganno subito è un esempio evidente di frode sofisticata (*smishing*), in cui l'utente medio, nonostante la diligenza ordinaria, può essere facilmente tratto in inganno.

Nelle controdeduzioni, l'intermediario, riportato il fatto, afferma quanto segue:

- il cliente è stato vittima di *vishing* misto a "*SMS spoofing*", in quanto è stato prima adescato per sms e poi contattato per telefono da un sedicente operatore della banca;
- l'operazione di € 31,67, disconosciuta dal cliente, verrà rimborsata al cliente;
- le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali;
- sussiste la colpa grave del cliente in quanto lo stesso ha collaborato con il truffatore, condividendo i propri codici OTP, e permettendo il verificarsi della truffa;
- non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.

In conclusione, l'intermediario chiede che il ricorso venga rigettato.

Il cliente, richiamati i propri scritti, replica che:

- il movimento di € 31,67 è già stato rimborsato dall'intermediario;
- precisa di essere stato indotto sotto pressione psicologica a fornire i codici OTP, convinto di bloccare transazioni anomale in corso dalla Svizzera;
- rinnova la propria richiesta di rimborso dell'operazione fraudolenta di € 700,00.

L'intermediario, riportandosi alle conclusioni in atti, insiste nel rigetto del ricorso e contesta l'affermazione del ricorrente secondo cui la telefonata sia pervenuta da un numero riferibile alla banca, in quanto il cliente non ha fornito alcuna prova della riconducibilità della stessa alla banca.

DIRITTO

Con riferimento alla domanda del ricorrente, si osserva che il cliente, in sede di ricorso, contesta n. 2 operazioni di pagamento. In sede di repliche, tuttavia, specifica che oggetto del presente ricorso è il rimborso della sola operazione di € 700,00, in quanto l'operazione di € 31,67 è stata già oggetto di rimborso da parte della banca.

Alla data delle operazioni, trovava applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018.

Con riferimento alla *strong customer authentication* (cd. SCA) le fonti normative 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).

L'intermediario fornisce una ricostruzione delle fasi che hanno costituito la frode:

- alle ore 17:21 accesso all'app da dispositivo diverso da quello abitualmente utilizzato dal ricorrente;
- alle ore 17:22 modifica della password
- alle ore 17:25 registrazione della carta di debito del ricorrente con un *wallet*;
- alle ore 17:39 esecuzione operazione di € 700,00;
- alle ore 17:44 esecuzione operazione di € 31,67.

Con riferimento alla fase di accesso all'app, l'intermediario fa riferimento ad un'unica operazione di *login* (alle ore 17.21) che ha preceduto l'operazione contestata e che, a suo avviso, è stata autenticata tramite doppio fattore. L'accesso in app è stato autenticato mediante inserimento di username, password e del codice OTP inviato via SMS al numero di telefono riconducibile al cliente.

Si rammenta che lo stesso cliente dichiara di aver comunicato i codici OTP necessari a compiere le operazioni al truffatore. Tutti i successivi accessi in app sono invece stati eseguiti tramite il solo inserimento dello username e della password (*medio de autenticaciòn=02*), compreso l'accesso delle ore 17:37, l'ultimo prima dell'esecuzione dell'operazione contestata.

Alla luce di quanto sopra esposto, solo l'accesso all'app delle ore 17:21 risulta autorizzato mediante inserimento di username e password (elemento di conoscenza), e l'inserimento del codice OTP (elemento di possesso), mentre tutti gli accessi successivi risultano autorizzati esclusivamente mediante username e password (elemento di conoscenza).

Si pone quindi la questione di stabilire se, una volta avuto accesso al conto mediante ricorso a un unico fattore (in applicazione di apposita 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 con la Q&A 2020_5516, richiamando, tra l'altro, la precedente Q&A 2018_4141, nella quale è stato specificato 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.

Nella Q&A 2020_5516 in esame, l'EBA ha ritenuto 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 stabilite nella Q&A 2018_4141.

Sul punto, questo Collegio ritiene che – posto che la disposizione di cui all'art. 10 limita l'esenzione dalla SCA ai soli accessi di tipo meramente informativo – i principi sopra espressi non possono trovare applicazione laddove, in concreto, l'accesso sia di tipo

dispositivo, in quanto prodromico all'esecuzione delle operazioni di pagamento. Si vedano Collegio di Milano, decisioni 10636/24, 8155/24 e 7574/2024; Collegio di Bologna, decisioni 11652/24 e 9591/24; Collegio di Bari, decisione 6380/2024.

Nel caso in esame, è da ritenersi dunque non provata la SCA, essendo stata documentata con riguardo soltanto al login delle ore 17.21 e non già all'accesso all'area riservata del cliente delle ore 17.37 che ha preceduto l'operazione contestata.

L'operazione di € 700,00 è stata autenticata attraverso inserimento del codice OTP ricevuto tramite SMS sul numero di cellulare del cliente (elemento di possesso) e inserimento del CVV dinamico. Con riferimento alla valenza da attribuire al CVV dinamico ai fini della prova della SCA, l'intermediario qualifica detto CVV dinamico come elemento di conoscenza. Tuttavia, alla luce delle indicazioni fornite dall'EBA nell'Opinion del 21 giugno 2019, il CVV dinamico è qualificabile come elemento di possesso (in questo senso, Collegio di Bari, decisione n. 9345/2023; Collegio di Roma, decisioni n. 2840/2023 e n. 10679/2023; da ultimo, Collegio di Milano, decisione n. 8153/2024).

Come noto, un doppio fattore di possesso non risulta conforme alla SCA in quanto, in base all'Opinion dell'EBA, l'autenticazione forte presuppone il ricorso a due fattori di autenticazione appartenenti a categorie diverse. Si segnala che, con riferimento a ricorsi nei confronti del medesimo intermediario qui convenuto caratterizzati da analoghe modalità di autenticazione (tramite CVV dinamico), il Collegio di Milano ha ritenuto non provata l'autenticazione a doppio fattore (Collegio di Milano, decisione n. 3554/2024; Collegio di Milano, decisione n. 8153/2024).

Si rammenta che, in difetto di piena prova sull'autenticazione delle transazioni disconosciute, secondo l'orientamento dei Collegi il ricorso deve essere accolto integralmente, posto che la mancanza anche parziale 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, in aderenza al dato normativo, 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 € 700,00.
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