Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) MODICA

Seduta del 18/03/2025

FATTO

Il cliente afferma di aver ricevuto una chiamata che lo avvertiva di alcune operazioni sospette sul suo conto corrente e lo invitava a bloccare il proprio conto. Nel corso della telefonata il cliente riferiva all'interlocutore i codici ricevuti nel frattempo via sms. Simultaneamente riceveva la notifica di un avvenuto pagamento di € 1.850,00. Resosi conto di essere stato vittima di una frode sporgeva denuncia e presentava reclamo all'intermediario in data 27/11/2024, riscontrato negativamente.
Disconosce l'operazione e chiede il rimborso di € 1.850,00.
L'intermediario afferma che il cliente è stato vittima di vishing in quanto ha dato seguito alle richieste di un terzo ignoto condividendo le credenziali segrete necessarie per permettere l'operatività dello strumento di pagamento; che le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali; che non sono stati riscontrati malfunzionamenti o intrusioni nei propri sistemi informatici.
Chiede il rigetto del ricorso.

DIRITTO

L'operazione contestata, un pagamento con carta effettuato alle ore 18:28 del 22 novembre 2024 per € 1.850,00, ricade sotto il raggio d'azione del D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).
Ai sensi dell'art. 10, comma 1, del d.lgs. n. 11/2010, "Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento 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". L'assolvimento di tale onere è necessario ma non sufficiente, dovendo il prestatore ulteriormente provare, ai fini dell'esonero da responsabilità (art. 10, comma 2, D.Lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 D.Lgs. 11/2010: come chiarito dal Collegio di Coordinamento, "la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente" (decisione n. 22745/2019).
Il Collegio, richiamati gli artt. 97 e 98 della PDS2, l'articolo 10 bis del D. Lgs. 11/2010, le 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 (in particolare il parere dell'EBA del 21 giugno 2019), richiama altresì l'art. 12 del d.lgs. 27.1.2010, n. 11, "Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento": "Salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Il Collegio, ancora, ricorda che, in base all'art. 1, lett. qbis, l'"autenticazione forte del cliente" è definita come "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione". L'autenticazione forte è richiesta quando il cliente accede al suo conto di pagamento online; dispone un'operazione di pagamento elettronico; effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.
Nel caso di specie, con riferimento all'accesso all'area riservata, l'intermediario dà evidenza di avere fatto ricorso al riconoscimento biometrico quale elemento di inerenza e invoca, quanto al secondo fattore, l'esenzione prevista dall'art. 10 del Regolamento delegato (UE) 2018/389 che consente l'accesso c.d. informativo al conto senza applicare la SCA, a condizione che non siano decorsi più di 180 giorni dall'ultima applicazione della SCA. In particolare, l'art. 10 del Regolamento delegato (UE) 2018/389, come modificato dal Regolamento Delegato (UE) 2022/2360, prevede che "I prestatori di servizi di pagamento sono autorizzati a non applicare l'autenticazione forte del cliente, fatto salvo il

rispetto dei requisiti di cui all'articolo 2, se l'utente dei servizi di pagamento accede direttamente al suo conto di pagamento online, a condizione che l'accesso sia limitato a uno dei seguenti elementi online senza che siano divulgati dati sensibili relativi ai pagamenti: a) il saldo di uno o più conti di pagamento designati; b) le operazioni di pagamento eseguite negli ultimi 90 giorni attraverso uno o più conti di pagamento designati. 2. In deroga al paragrafo 1, i prestatori di servizi di pagamento non sono esenti dall'applicazione dell'autenticazione forte del cliente se una delle seguenti condizioni è soddisfatta: a) l'utente del servizio di pagamento accede online alle informazioni di cui al paragrafo 1 per la prima volta; b) sono trascorsi più di 180 giorni dall'ultima volta che l'utente del servizio di pagamento ha avuto accesso online alle informazioni di cui al paragrafo 1 ed è stata applicata l'autenticazione forte del cliente".

Questo Collegio, nel solco dei suoi molti precedenti in materia, ritiene che la previsione di cui al citato art. 10 non sia suscettibile di applicazione fuori dall'ipotesi di accessi meramente informativi. In assenza di autenticazione a doppio fattore, l'accesso al conto di natura non meramente informativa, perché seguito dalla disposizione di una operazione di pagamento, non risulta conforme ai requisiti normativamente previsti (decisione n. 10636/24; decisione 8155/24; decisione n. 7574/2024).

Tale circostanza risulta assorbente rispetto alla verifica delle modalità di autenticazione dell'operazione contestata. La mancanza di autenticazione a doppio fattore nella procedura di accesso all'APP non consente infatti di ritenere provata la regolare autenticazione delle operazioni contestate (Collegio di Bologna, n. 12274/2022; Collegio di Bari, n. 9425/2022 e 2568/2023).

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.850,00.

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