

COLLEGIO DI MILANO

composto dai signori:

- (MI) [REDACTED] Presidente
- (MI) [REDACTED] Membro designato dalla Banca d'Italia
- (MI) [REDACTED] Membro designato dalla Banca d'Italia
- (MI) [REDACTED] Membro di designazione rappresentativa degli intermediari
- (MI) [REDACTED] Membro di designazione rappresentativa dei clienti

Relatore [REDACTED]

Seduta del 17/09/2024

Esame del ricorso n. [REDACTED]

proposto da [REDACTED]

nei confronti di [REDACTED]

COLLEGIO DI MILANO

composto dai signori:

(MI) [REDACTED]	Presidente
(MI) [REDACTED]	Membro designato dalla Banca d'Italia
(MI) [REDACTED]	Membro designato dalla Banca d'Italia
(MI) [REDACTED]	Membro di designazione rappresentativa degli intermediari
(MI) [REDACTED]	Membro di designazione rappresentativa dei clienti

Relatore [REDACTED]

Seduta del 17/09/2024

FATTO

Parte ricorrente, titolare di una carta di credito emessa dall'intermediario resistente, afferma che, in data 05/04/2024, si accorgeva che l'applicazione della banca non era più attiva e procedeva con una nuova installazione della medesima app. In quell'occasione, si accorgeva di due operazioni di pagamento da lui mai autorizzate per complessivi € 970,00. Pertanto, il ricorrente chiede la restituzione degli importi relativi alle operazioni disconosciute.

Nelle controdeduzioni, l'intermediario, oltre a eccepire l'inammissibilità del ricorso per difetto del preventivo reclamo, rileva nel merito che non trova applicazione la disciplina speciale invocata *ex adverso* (d.lgs. n. 11/2010), in quanto le operazioni risultano effettuate dallo stesso ricorrente, poiché risultano correttamente autenticate con sistema dinamico a doppio fattore. Per contro, sussisterebbe la colpa grave del ricorrente, che ha ceduto a terzi ignoti le credenziali necessarie per effettuare le operazioni disconosciute.

L'intermediario chiede, pertanto, il rigetto del ricorso.

Nelle repliche, il ricorrente chiarisce di aver inviato il modulo di disconoscimento all'intermediario, che pacificamente costituisce il reclamo prodromico all'introduzione del ricorso avanti all'arbitro. Il ricorrente evidenzia, poi, che l'intermediario non ha fornito la prova della registrazione e contabilizzazione delle operazioni e nega la sussistenza della propria colpa grave.

Nelle controrepliche, l'intermediario rimarca che il giorno delle operazioni ha inviato al ricorrente una notifica sms contenente la notizia della contabilizzazione delle operazioni.

L'intermediario sottolinea, per un verso, la sussistenza della SCA e, per l'altro, la colpa grave del ricorrente, da presumersi in ragione delle evidenze informatiche circa gli accessi all'area riservata per l'effettuazione delle operazioni.

DIRITTO

Occorre, preliminarmente, disattendere l'eccezione preliminare dell'intermediario che lamenta l'assenza del preventivo reclamo. È orientamento consolidato di questo Arbitro che, specie in materia di utilizzi fraudolenti di strumenti di pagamento, il modulo di disconoscimento delle operazioni sia equiparabile al reclamo, quale *"atto con cui il cliente chiaramente identificabile contesta in forma scritta all'intermediario un suo comportamento anche omissivo"* (cfr. la Sezione I, paragrafo 3 "Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari").

Passando al merito del ricorso, è opportuno premettere che, a dispetto di quanto eccepito dall'intermediario (il quale pure ammette che il *device* del cliente risulta essere stato dissociato), le operazioni contestate sono disciplinata dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno. Devono in particolare essere richiamati gli artt. 7, 10, 10-bis e 12 del citato decreto: disposizioni che, con l'obiettivo dichiarato di tutelare l'utente, allocano in via tendenziale sull'intermediario il rischio di utilizzazione fraudolenta degli strumenti di pagamento. In particolare, l'art. 10 grava il PSP dell'onere di 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"*, precisando, al secondo comma, che *"l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7"*, incombendo sull'intermediario anche *"la prova della frode, del dolo o della colpa grave dell'utente"*. L'art. 12, comma 2-bis, d.lgs. n. 11/2010 esclude che la perdita derivante da un'operazione fraudolenta possa essere sopportata, anche solo in parte, dall'utilizzatore quando, eccettuato il caso della frode commessa da quest'ultimo, il prestatore del servizio non abbia richiesto l'autenticazione forte (*"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 beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente"*), se dovuta ai sensi dell'art. 10-bis. L'autenticazione forte consiste in *"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"* (art. 1, comma 1, lett. q-bis, d.lgs. n. 11/2010).

In assenza della dimostrazione della corretta autenticazione forte (artt. 10, 10-bis e 12, comma 2-bis, d.lgs. n. 11/2010) e salva la dimostrazione dell'agire fraudolento del pagatore (nel caso di specie assente), il rischio di operazioni di pagamento disconosciute da quest'ultimo deve essere integralmente sopportato dal prestatore del servizio di pagamento.



Venendo ai fatti oggetto del ricorso, il ricorrente disconosce e contesta due operazioni di pagamento elettronico effettuate da ignoti in data 05/04/2024, che risultano correttamente contabilizzate e registrate dall'intermediario per complessivi € 970,00.

Nelle controrepliche, l'intermediario descrive in modo accurato il funzionamento del proprio sistema di autenticazione forte, operante per i pagamenti online tramite app, in particolare affermando che ciascuna utenza può essere associata a due dispositivi diversi.

Tuttavia, l'intermediario non ha dato evidenza – della quale pure è onerato ai sensi del citato art. 10 - dell'operatività concreta di tale sistema in relazione alle operazioni oggetto di contestazione e in particolare con riferimento all'*enrollment* di un nuovo dispositivo quale strumento di autenticazione delle operazioni di pagamento elettroniche.

E espressamente previsto (art. 10 *bis* d.lgs. n. 11/2010) che l'autenticazione mediante SCA sia richiesta, non solo per autorizzare le operazioni di pagamento, ma anche per “*effettuare qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi*”: è pertanto pacifico che l'*enrollment* di un nuovo dispositivo debba (quantomeno) essere autenticato, mediante sistemi di autenticazione forte. Più precisamente, l'intermediario chiarisce che alle ore 17:43 del 5/4/2024, a seguito di accesso all'app, effettuato mediante username e password, veniva richiesta l'associazione di un nuovo dispositivo. Non risulta che tale operazione sia stata autenticata mediante altri fattori. Né l'intermediario ha fornito evidenza dell'inserimento del fattore di conoscenza (password) necessario per l'autenticazione di tale delicata fase.

In assenza di elementi probatori riguardanti la concreta operatività del sistema di autenticazione forte, con riguardo alla fase di *enrollment* del dispositivo dal quale sono state autorizzate le operazioni fraudolente, non si può che concludere, in conformità a precedenti di questo Collegio (v. ad es. Coll. Milano, dec. n. 14699/2021), che l'intermediario debba corrispondere ex art. 12, comma 2-*bis*, d.lgs. 11/2010 l'intero importo delle operazioni contestate, comprensivo delle commissioni addebitate per ciascun pagamento. La legge non consente, inoltre, alcun sindacato circa l'eventuale concorso di colpa del pagatore con riferimento alla perdita subita: non è pertanto consentita alcuna valutazione circa eventuali profili di colpa di quest'ultimo che dovessero emergere dalle allegazioni delle parti, comprovate dalla documentazione agli atti.

PER QUESTI MOTIVI

Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 970,00.

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