

## COLLEGIO DI MILANO

composto dai signori:

(MI) LAPERTOSA	Presidente
(MI) TINA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) DALMARTELLO	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) DALMARTELLO

Seduta del 16/07/2024

### FATTO

Parte ricorrente afferma che:

- in data 29/2/2024 riceveva una telefonata da parte del contatto ufficiale del "Servizio relazioni con la Clientela" dell'intermediario;
- gli veniva comunicata la necessità di aggiornare l'app Token del cellulare e veniva invitato a scaricare l'applicazione dell'intermediario;
- a questo punto non dubitando circa l'affidabilità dell'interlocutore, procedeva con l'installazione dell'app;
- non ha fornito al sedicente incaricato alcun codice OTP o password;
- l'operatore concludeva la telefonata anticipando un successivo contatto nel pomeriggio per la verifica circa la corretta installazione dell'app;
- in data 1/3/24 si recava presso la filiale ed apprendeva dell'esecuzione dal suo conto di un bonifico di € 34.900,00 a favore di soggetto a lui sconosciuto.

Pertanto, il ricorrente chiede la restituzione degli importi relativi all'operazione sconosciuta, per un importo di € 34.900,00.

Nelle controdeduzioni, l'intermediario eccepisce che non è versato in atti l'SMS contenente il link usato per l'installazione della app token apparentemente riferibile all'intermediario. La colpa grave del ricorrente sarebbe desumibile da tale mancanza e dalla corretta autenticazione dell'operazione sconosciuta, mediante autenticazione forte (SCA).



Arbitro Bancario Finanziario  
Risoluzione Stragiudiziale Controversie

Alle repliche, il ricorrente ha allegato immagini delle schermate del proprio telefono ove confrontare l'app truffaldina con quella ufficiale dell'intermediario. Esse, ad avviso del ricorrente, coincidono perfettamente.

Nelle controrepliche, l'intermediario insiste sul difetto di prova del messaggio civetta, dal quale desumere la colpa grave del ricorrente.

## DIRITTO

L'operazione contestata è 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”*, incumbendo 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).

Tale autenticazione non deve essere richiesta (art. 10bis d.lgs. n. 11/2010, che riporta quanto previsto dall'art. 98 della direttiva PSD2) solo in occasione dell'operazione di pagamento, ma anche in relazione all'accesso del cliente al conto di pagamento elettronico e quando l'utente *“effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi”*. Pertanto, la richiesta di SCA deve caratterizzare anche la fase che precede l'operazione di pagamento, là dove *“tramite un canale a distanza”* siano state effettuate operazioni che possono incidere sul rischio di frode, come, ad esempio, l'*enrollment* di un nuovo device, la tokenizzazione di una carta di pagamento (v. Coll. Coordinamento, dec. n. 21285/2021), ovvero la



registrazione del dato biometrico necessario per autorizzare successive operazioni di pagamento.

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 un'operazione di bonifico online effettuata da ignoti in data 29/2/2024, che risulta correttamente contabilizzata e registrata dall'intermediario per complessivi € 34.900,00.

Nelle controdeduzioni, l'intermediario afferma che l'operazione è stata correttamente autenticata mediante SCA, ma non ha dato evidenza – della quale pure è onerato ai sensi del citato art. 10 - dell'operatività concreta di tale sistema in relazione all'operazione oggetto di contestazione. Non vi è agli atti prova del corretto inserimento di alcune delle credenziali necessarie per consentire ai terzi malfattori il *login* al *mobile banking* e l'esecuzione dell'operazione.

Più precisamente, l'intermediario afferma che sarebbero stati inseriti, per effettuare il login all'area personale, le credenziali di sicurezza (username e PIN) e il Codice OTP generato dalla *app* installata sul *device* univocamente associato dal ricorrente. Tuttavia, non vi è evidenza univoca dell'effettivo inserimento delle credenziali del ricorrente e in particolare del PIN. Risulta infatti un login alle ore 13:39 del 29/2/2024 ma vi è la sola dicitura "accesso con *Id Utente e Pin con verifica a due fattori con OTP da Mobile token*" e l'indicazione del codice OTP, ma il campo "*Esito Operazione*" non è popolato in alcun modo. Parimenti assente, è la dimostrazione dell'inserimento del PIN con riferimento alla documentazione versata in atti relativa all'operazione di bonifico, benché in questo caso la colonna "*Esito Operazione*" sia popolata ("*eseguita*"), senza dare conto dell'inserimento del secondo elemento di autenticazione (cfr. per fatti analoghi Coll. Milano, dec. n. 4760/2024). In ogni caso, trattandosi di operazione eseguita in una sessione già aperta, rispetto alla quale non vi è riscontro dell'inserimento completo della SCA, essa non potrebbe comunque considerarsi correttamente autenticata.

In assenza di evidenze documentali riguardanti la concreta operatività del sistema di autenticazione forte, non si può che concludere, in conformità a precedenti di questo Collegio (v. ad es. Coll. Milano, dec. n. 14699/2021), che l'intermediario resistente debba corrispondere ex art. 12, comma 2-*bis*, d.lgs. 11/2010 l'intero importo dell'operazione contestata. 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 € 34.900,00.**

**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  
FLAVIO LAPERTOSA