

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) CESARE

Seduta del 10/02/2026

FATTO

Il cliente afferma di aver ricevuto in data 22 settembre 2020 messaggi apparentemente provenienti dalla banca che segnalavano un tentativo di bonifico. Il giorno successivo è giunta una telefonata da un numero mobile, nel corso della quale l'interlocutore riferiva che le operazioni in questione erano relative a prove che stava effettuando la banca. In quei giorni il cliente si trovava in Svizzera e non ha autorizzato i pagamenti indicati nei messaggi, né ha utilizzato i codici riportati. La moglie del cliente si è recata in banca il 24 settembre 2020 per chiedere chiarimenti e ha appreso che il 22 e il 23

settembre erano stati effettuati tre prelievi cardless per un totale di € 5.000,00. Il cliente afferma di non aver mai ricevuto alcuna comunicazione relativa all'autorizzazione di tali operazioni e contesta di aver comunicato informazioni relative a codici e password. Il cliente osserva che la banca è obbligata a dimostrare la corretta autenticazione delle operazioni, obbligo che risulta particolarmente rafforzato in caso di operazioni sospette.

Per tali ragioni il cliente chiede il rimborso delle somme addebitate, degli interessi legali e delle spese legali sostenute.

Nelle controdeduzioni l'intermediario afferma che in data 22 e 23 settembre 2020 sono stati effettuati 2 prelievi cardless di € 2.000,00 e € 1.000,00 il primo giorno e un prelievo di € 2.000,00 il secondo giorno. Per accedere ai servizi online della banca è richiesto l'inserimento simultaneo di password statiche e dinamiche, ossia il codice Titolare, il codice PIN e il codice OTS. L'intermediario ha ottenuto la certificazione ISO che attesta la qualità dei servizi di sicurezza offerti e invia comunicazioni alla clientela riguardanti la conservazione delle credenziali. Le operazioni sono state correttamente contabilizzate, registrate e autenticate. Il cliente si connette prevalentemente usando uno smartphone con sistema operativo iOS, mentre l'operativa disconosciuta è stata effettuata usando uno smartphone del tipo Android. In data 19 settembre 2020 alle ore 15:49 si è verificata un'attività di enrollment del nuovo dispositivo resa possibile in quanto il truffatore era a conoscenza delle credenziali del cliente. Sussiste la colpa grave del cliente in quanto ha violato gli obblighi di custodia delle credenziali posti a suo carico. Il cliente è stato vittima di smishing e vishing che esulano dalla responsabilità della banca. L'intermediario osserva che le operazioni disconosciute non sono state eseguite con carta di pagamento né in Stati diversi. L'intermediario chiede il rigetto del ricorso e l'applicazione della franchigia di € 50,00.

DIRITTO

La controversia riguarda il disconoscimento di tre operazioni di prelievo cardless eseguite in data 22 e 23 settembre 2020 per un importo complessivo di € 5.000,00 a seguito di truffa ai danni del cliente. All'operatività contestata si applica il decreto legislativo 27 gennaio 2010, n. 11 come modificato dal decreto legislativo n. 218/17 di attuazione della direttiva 2015/2366/UE (PSD2).

L'articolo 10 del decreto legislativo n. 11/2010 prevede che il prestatore di servizi di pagamento deve provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata senza anomalie. Successivamente deve dimostrare che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti dall'articolo 7 del decreto.

Nel caso di specie l'intermediario ha fornito prova dell'autenticazione delle operazioni. In data 19 settembre 2020 alle ore 15:49 è stato effettuato l'enrollment di un nuovo dispositivo mediante inserimento delle credenziali statiche e del codice dinamico OTS inviato via SMS al numero certificato del cliente. Il cliente ha ricevuto notifica SMS dell'attivazione con invito espresso a contattare la filiale. Le tre operazioni successive del 22 e 23 settembre 2020 risultano autorizzate mediante inserimento del PIN e del codice OTS, in conformità all'autenticazione forte richiesta dalla normativa PSD2.

Una volta provata l'autenticazione l'intermediario deve fornire la prova della colpa grave del cliente. Il cliente riferisce di aver ricevuto SMS e una telefonata sospetti, ma non ha prodotto evidenza dell'SMS civetta né del registro chiamate. Secondo l'orientamento consolidato dei Collegi la mancata allegazione del messaggio civetta determina il rigetto del ricorso in quanto non consente di verificare se il mittente risulti riconducibile all'intermediario. Inoltre il cliente ha ignorato la notifica SMS dell'attivazione del nuovo dispositivo, ha autorizzato tre operazioni mediante inserimento dei codici OTS senza alcuna verifica e non ha bloccato tempestivamente le credenziali nonostante fosse a conoscenza dell'attività anomala. Gli elementi così ricostruiti integrano la colpa grave di cui all'articolo 10, comma 2, del decreto legislativo n. 11/2010.

Alla luce delle considerazioni che precedono il ricorso non può essere accolto.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE