

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) DELL'ANNA MISURALE	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) AFFERNI	Membro di designazione rappresentativa dei clienti

Relatore (MI) AFFERNI

Seduta del 24/03/2026

FATTO

Il ricorrente espone di essere stato vittima di una complessa frode informatica. In particolare, dichiara di essere stato contattato da un'utenza telefonica apparentemente riconducibile all'intermediario, da un sedicente operatore che lo allertava di un accesso anomalo al suo conto da Bari. In seguito, l'app bancaria veniva bloccata. Nei giorni successivi, sempre contattato da presunti operatori della banca, veniva indotto a collaborare per la "riconfigurazione" dell'applicazione. Successivamente, riceveva notifiche relative a bonifici, alcuni bloccati e altri eseguiti, e veniva rassicurato dai truffatori circa

l'imminente storno delle somme. Si avvedeva inoltre dell'apertura a suo nome di un prestito di € 15.000,00, il cui importo veniva parimenti sottratto tramite bonifici. Solo dopo aver subito addebiti per un totale di € 23.599,00 (composti da due bonifici di € 19.900,00 e € 2.999,00, più una frazione di € 700,00 di un terzo bonifico non coperta dal prestito fraudolento), e dopo aver notato ulteriori tentativi di bonifico e un aumento dei massimali, provvedeva a sporgere denuncia e a richiedere il blocco degli strumenti di pagamento. Il ricorrente precisa quindi di non aver mai comunicato a terzi le proprie credenziali, di essere caduto vittima di una truffa particolarmente insidiosa (c.d. ID caller spoofing), che ha aggirato i sistemi di autenticazione a due fattori (SCA). Sostiene che l'intermediario non avrebbe adottato misure di sicurezza adeguate, consentendo l'associazione dell'app a un nuovo dispositivo sconosciuto e l'esecuzione di plurimi bonifici istantanei anomali per importo e frequenza, senza attivare efficaci sistemi di allerta o blocco. Contesta, pertanto, la sussistenza di una propria colpa grave. Il ricorrente chiede quindi la condanna dell'intermediario convenuto alla restituzione della somma complessiva di € 23.599,00, oltre interessi.

L'intermediario si è costituito in giudizio chiedendo il rigetto del ricorso. Sostiene che le operazioni sono state regolarmente autenticate mediante sistema SCA, reso possibile dalla collaborazione attiva del cliente, il quale avrebbe comunicato ai truffatori i codici OTP necessari per associare l'app a un nuovo dispositivo (diverso da quello del ricorrente) e per autorizzare le operazioni. Afferma che la frode è stata agevolata dalla condotta gravemente negligente del cliente, che ha seguito le istruzioni dei falsi operatori, anche quando una delle chiamate proveniva da un'utenza mobile non riconducibile alla banca. Evidenzia di aver messo a disposizione della clientela documentazione informativa per prevenire tali fenomeni e che, data la natura istantanea dei bonifici, non era possibile bloccarli una volta eseguiti.

Nelle repliche, il ricorrente ha ribadito l'assenza di prove sulla sua presunta colpa grave, sottolineando l'anomalia del blocco iniziale dell'app e l'impossibilità di verificare l'autenticità delle chiamate. Ha negato di aver mai comunicato il PIN e ha lamentato la mancata ricezione di informative specifiche sulle frodi. Ha inoltre evidenziato come l'inerzia dei sistemi di sicurezza della banca, a fronte di un'operatività palesemente anomala protrattasi per più giorni, costituisca un'autonoma fonte di responsabilità per l'intermediario.

L'intermediario, in controreplica, ha insistito sulla colpa del cliente, il quale non avrebbe utilizzato gli strumenti di verifica messi a disposizione dalla banca per accertare l'identità dell'interlocutore.

DIRITTO

Il ricorso non può trovare accoglimento.

La materia del contendere è disciplinata dal D.Lgs. 27 gennaio 2010, n. 11 e successive modifiche (in attuazione della Direttiva UE 2015/2366, c.d. PSD2), che regola i diritti e gli obblighi delle parti nei servizi di pagamento. L'art. 10 del citato decreto pone a carico del prestatore di servizi di pagamento (PSP) l'onere di provare che l'operazione di pagamento contestata sia stata autenticata, correttamente

registrata e contabilizzata e che non abbia subito le conseguenze di un malfunzionamento tecnico. Il medesimo articolo, al comma 2, stabilisce che l'utilizzo di uno strumento di pagamento registrato dal PSP non è di per sé sufficiente a dimostrare che l'operazione sia stata autorizzata dal pagatore, né che questi abbia agito in modo fraudolento o con dolo o colpa grave. Spetta, infatti, all'intermediario fornire la prova di tali circostanze.

Nel caso di specie, l'intermediario ha fornito i log informatici relativi sia alla fase di associazione dell'app a un nuovo dispositivo (c.d. enrollment), avvenuta in data 01/04/2025 su un device Samsung, sia alle successive operazioni di aumento dei massimali e di esecuzione dei bonifici disconosciuti. Da tale documentazione emerge che le procedure sono state perfezionate mediante un sistema di autenticazione forte del cliente (SCA), che ha previsto l'utilizzo combinato di un fattore di conoscenza (PIN/SmartCode) e di un fattore di possesso (codice OTP inviato all'utenza telefonica del ricorrente e/o validazione tramite l'app installata sul dispositivo del truffatore). L'intermediario ha quindi assolto all'onere probatorio su di esso gravante ai sensi dell'art. 10, comma 1, del D.Lgs. n. 11/2010.

Accertata la regolarità formale delle operazioni, occorre valutare se il danno sia conseguenza di una condotta gravemente colposa del ricorrente, ai sensi dell'art. 12, comma 4, del D.Lgs. n. 11/2010, che in tal caso porrebbe a suo esclusivo carico tutte le perdite derivanti.

Il Collegio ritiene che, sulla base degli atti, emergano plurimi e concordanti elementi che configurano la colpa grave del ricorrente.

In primo luogo, la stessa dinamica della frode, così come descritta dal ricorrente, presuppone necessariamente una sua cooperazione attiva con i truffatori. L'associazione dell'app bancaria a un nuovo dispositivo, estraneo al ricorrente, non sarebbe stata possibile senza che quest'ultimo comunicasse al falso operatore i codici OTP ricevuti sul proprio cellulare. Il ricorrente ammette di aver "collaborato" con il presunto operatore per "riconfigurare l'applicazione". Tale condotta costituisce una palese violazione dell'obbligo fondamentale, sancito dall'art. 7 del D.Lgs. n. 11/2010, di adottare tutte le ragionevoli misure idonee a proteggere le proprie credenziali di sicurezza personalizzate e di non comunicarle a terzi, per nessuna ragione. Sebbene la tecnica dell'ID caller spoofing, che fa apparire sul display il numero di telefono ufficiale della banca, sia indubbiamente insidiosa e atta a ingenerare un legittimo affidamento, essa non può giustificare la comunicazione a terzi di codici segreti e "usa e getta", la cui funzione è proprio quella di certificare in modo univoco la volontà del titolare.

In secondo luogo, il ricorrente ha dimostrato una significativa negligenza nel non rilevare evidenti segnali di allarme che avrebbero dovuto indurlo a interrompere ogni contatto e a rivolgersi immediatamente alla banca tramite i canali ufficiali. Dagli atti emergono infatti diverse incongruenze nelle comunicazioni ricevute:

- gli SMS, pur inserendosi in una chat apparentemente riconducibile alla banca, presentavano anomalie stilistiche (alternanza tra forma di cortesia e seconda persona singolare) e di formattazione (andata a capo anomala dopo il simbolo dell'euro);

- alcuni messaggi contenevano istruzioni palesemente sospette, come quella di "attendere 24 ore prima di prendere visione del conto corrente", un'indicazione chiaramente finalizzata a ritardare la scoperta della frode;
- la stessa sequenza di messaggi relativi al prestito appariva contraddittoria, comunicando prima la "revoca" e subito dopo la "disponibilità" della somma sul conto.

Un utente minimamente diligente avrebbe dovuto percepire tali anomalie come campanelli d'allarme e dubitare dell'autenticità dei suoi interlocutori.

In terzo luogo, e in modo dirimente, il ricorrente ha violato l'obbligo di cui all'art. 7, comma 1, lett. b), del D.Lgs. n. 11/2010, che impone di comunicare "senza indugio" al prestatore lo smarrimento, il furto, l'appropriazione indebita o l'uso non autorizzato dello strumento di pagamento. La frode si è protratta per diversi giorni. Già in data 01/04/2025, l'intermediario ha inviato al ricorrente una notifica via e-mail relativa all'avvenuta attivazione dell' app su un nuovo dispositivo. Successivamente, sono state inviate notifiche per l'aumento dei massimali e per l'esecuzione di ogni singolo bonifico. A fronte di questa mole di avvisi, relativi a un'operatività del tutto anomala e da lui non posta in essere, il ricorrente è rimasto inerte per giorni, fidandosi delle rassicurazioni telefoniche dei truffatori, invece di contattare autonomamente e "senza indugio" la propria banca per verificare la situazione e chiedere il blocco cautelativo del conto e degli strumenti. La denuncia e la richiesta di blocco sono intervenute solo il 05/04/2025, quando ormai il danno si era quasi interamente prodotto.

La combinazione di questi elementi – la comunicazione attiva di codici segreti, l'aver ignorato palesi segnali di anomalia e, soprattutto, il grave ritardo nella segnalazione alla banca a fronte di plurime notifiche di operazioni sospette – integra un comportamento di grave negligenza che si discosta in modo macroscopico da quello prudente ed accorto che si richiede al titolare di uno strumento di pagamento. Tale condotta ha interrotto il nesso di causalità tra l'attività del PSP e il danno, rendendo il ricorrente l'artefice principale della propria perdita.

Né può essere accolta la doglianza relativa alla presunta inadeguatezza dei sistemi di monitoraggio dell'intermediario. Non sussistono infatti nel caso di specie anomalie talmente macroscopiche che avrebbero dovuto indurre l'intermediario a bloccare l'operatività del ricorrente.

Per le ragioni sopra esposte, la domanda del ricorrente deve essere respinta.

PER QUESTIMOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE