

COLLEGIO DI MILANO

composto dai signori:

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

Relatore (MI) AFFERNI

Seduta del 21/04/2026

FATTO

Il ricorrente, persona di età avanzata (85 anni), espone che in data 24/04/2025 riceveva una chiamata sul proprio telefono cellulare da un numero sconosciuto. L'interlocutore, proponendo un'offerta finanziaria, chiedeva al ricorrente un recapito telefonico per l'invio di informazioni. A seguito del consenso, il ricorrente riceveva un SMS contenente un *link*. Dopo aver cliccato su tale *link*, il suo telefono cellulare cessava di funzionare per circa 30 minuti. In serata, si accorgeva di aver ricevuto tre *e-mail* dall'intermediario che lo informavano dell'avvenuta esecuzione di tre bonifici istantanei, rispettivamente di € 2.800,00 (ore 20:57), € 3.400,00 (ore 21:07) e € 940,00 (ore 21:23). A quel punto, contattava immediatamente il servizio clienti della banca per disconoscere le operazioni e bloccare il conto. In data 27/04/2025 sporgeva denuncia-querela alle Autorità competenti, presentando poi formale reclamo all'intermediario in data 20/05/2025, cui seguiva il diniego di responsabilità da parte di quest'ultimo. Il ricorrente chiede quindi la condanna dell'intermediario convenuto alla restituzione della somma complessiva di € 7.140,00.

L'intermediario ha presentato le proprie controdeduzioni, chiedendo il rigetto del ricorso. Sostiene di aver fornito alla clientela un'adeguata informativa sui rischi di frode e che le operazioni contestate sono state regolarmente autenticate mediante l'inserimento delle credenziali personali del cliente (PIN e codice OTP). Afferma, inoltre, l'assenza di malfunzionamenti o intrusioni nei propri sistemi informatici. L'intermediario addebita l'accaduto alla colpa grave del ricorrente, il quale avrebbe acconsentito

all'invio di un *link* da un numero non riconducibile alla banca e vi avrebbe successivamente cliccato, nonostante l'evidente natura fraudolenta della comunicazione. A riprova della corretta autenticazione, produce i log informatici relativi agli accessi e alle disposizioni di pagamento. L'intermediario chiede quindi il rigetto del ricorso.

Nelle repliche, il ricorrente ha ribadito l'assenza di una propria colpa grave, contestando all'intermediario di non aver vigilato sulla sua operatività, palesemente anomala rispetto alle sue abitudini. Insiste quindi per l'accoglimento del ricorso.

Nelle controrepliche, l'intermediario ha insistito sulle proprie difese, eccependo la novità della contestazione relativa alla mancata verifica dell'operatività abituale del cliente. Insiste quindi per il rigetto del ricorso.

DIRITTO

Il Collegio ritiene che il ricorso non possa trovare accoglimento.

La disciplina di riferimento in materia di responsabilità per le operazioni di pagamento non autorizzate è contenuta nel D.Lgs. 27 gennaio 2010, n. 11 e successive modifiche. L'art. 10 di tale decreto legislativo stabilisce che, a fronte del disconoscimento di un'operazione da parte dell'utilizzatore, grava sul prestatore di servizi di pagamento (PSP) l'onere di provare che l'operazione sia stata autenticata, correttamente registrata e contabilizzata e che non abbia subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione. Una volta fornita tale prova, la responsabilità dell'utilizzatore per le perdite derivanti da operazioni non autorizzate può essere affermata solo qualora il PSP dimostri che l'utente ha agito con dolo o colpa grave (art. 10, comma 2).

Nel caso di specie, l'intermediario ha fornito prova adeguata della corretta autenticazione delle operazioni contestate. Dalle evidenze tecniche prodotte, risulta che gli accessi all'applicativo di *home banking* e le successive disposizioni dei tre bonifici istantanei sono stati autorizzati mediante una procedura di autenticazione forte (SCA), che ha previsto l'utilizzo combinato di due fattori: il codice PIN personale del cliente (elemento di "conoscenza") e un codice monouso (OTP) generato tramite l'applicazione installata sul dispositivo del ricorrente (elemento di "possesso"). Tale dispositivo risulta essere quello abitualmente utilizzato dal cliente per accedere ai servizi bancari. L'intermediario ha quindi assolto all'onere probatorio posto a suo carico dal primo comma dell'art. 10 del D.Lgs. n. 11/2010.

Occorre, pertanto, valutare se la condotta del ricorrente integri la fattispecie della colpa grave, idonea a escludere la responsabilità dell'intermediario ai sensi dell'art. 12 del medesimo decreto. Dalla ricostruzione dei fatti, emerge che il ricorrente, pur essendo un soggetto in età avanzata, ha tenuto un comportamento connotato da un'evidente e inescusabile negligenza. Egli ha infatti (i) risposto a una chiamata proveniente da un numero di telefono sconosciuto e non riconducibile all'intermediario; (ii) acconsentito a ricevere un SMS con un *link* sul proprio numero di cellulare per una non meglio precisata "offerta finanziaria"; e (iii) cliccato su tale *link*, contenuto in un SMS che, come risulta dalla documentazione in atti, non proveniva da una *chat* ufficiale dell'intermediario, ma da un contatto privato, e conteneva un URL palesemente non riconducibile al dominio della banca.

Tale sequenza di azioni configura una grave violazione dei più elementari doveri di prudenza e diligenza che gravano su chiunque utilizzi strumenti di pagamento elettronici. Il fenomeno del *phishing*

e dello *smishing* è ormai ampiamente noto e gli istituti di credito, così come i media, mettono costantemente in guardia gli utenti dal cliccare su *link* sospetti e dal fornire dati personali a seguito di contatti non richiesti. La condotta del ricorrente, che ha attivamente collaborato con i truffatori, ha di fatto neutralizzato i presidi di sicurezza predisposti dalla banca, consentendo ai malintenzionati, con ogni probabilità, di installare un *software* malevolo (*malware*) e di assumere il controllo da remoto del suo dispositivo, utilizzandolo per autorizzare le operazioni fraudolente.

La giurisprudenza, anche di questo Arbitro, è costante nel ritenere che la comunicazione di credenziali o l'accesso a *link* palesemente fraudolenti integri la colpa grave dell'utente, escludendo la responsabilità dell'intermediario. Nel caso in esame, la concatenazione degli eventi, innescata da una chiamata non sollecitata e culminata nel *click* su un *link* sospetto, rappresenta proprio quella "negligenza inescusabile" che interrompe il nesso di causalità tra l'erogazione del servizio da parte della banca e il danno subito dal cliente. Il danno, infatti, è riconducibile in via esclusiva alla condotta gravemente colposa del danneggiato stesso.

Né può essere accolta la doglianza del ricorrente circa la presunta anomalia delle operazioni, che l'intermediario avrebbe dovuto rilevare e bloccare. Sebbene gravi sull'intermediario un generale obbligo di protezione del cliente, che si estrinseca anche nell'adozione di sistemi di monitoraggio delle transazioni, non si può pretendere che tale obbligo si spinga fino a bloccare ogni operatività che si discosti dalle abitudini del cliente, soprattutto quando le operazioni sono state autorizzate con le procedure di sicurezza previste e dal dispositivo certificato del cliente stesso.

Per le ragioni sopra esposte, la domanda del ricorrente deve essere respinta, in quanto il danno lamentato è conseguenza diretta ed esclusiva della sua colpa grave.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE