

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) FORMAGGIA	Membro di designazione rappresentativa degli intermediari
(MI) SCARANO	Membro di designazione rappresentativa dei clienti

Relatore (MI) SCARANO

Seduta del 17/03/2026

FATTO

Con ricorso presentato in data 18.11.2025, il consumatore espone di aver ricevuto, intorno alle ore 16:00 del giorno 11.11.2025, un messaggio di testo sulla propria utenza telefonica che sembrava provenire dall'intermediario, in quanto il nome di quest'ultimo era menzionato all'inizio del testo, e che faceva riferimento a un presunto trasferimento di € 980,00 in fase di approvazione, invitando a

contattare un numero telefonico in caso di disconoscimento dell'operazione. Il ricorrente riferisce di aver immediatamente chiamato il numero indicato nel messaggio, dal quale rispondeva un uomo che sosteneva di essere un operatore dell'intermediario e che, per bloccare la transazione, era necessario modificare le proprie credenziali di accesso e tramite una e-mail provvedeva a fornirgli direttamente la nuova password da inserire. Si avvedeva quindi di essere stato vittima di una truffa allorché, una volta inserite le nuove credenziali, i frodatori riuscivano ad accedere al suo account e a eseguire dapprima un giroconto di € 2.100,00 da un libretto di risparmio cointestato verso una carta prepagata personale, e poi da quest'ultima un pagamento di € 230,00 verso un indirizzo di commercio elettronico con sede a Madrid. Dichiara di aver bloccato la carta immediatamente dopo aver riscontrato l'ammancio e di aver presentato denuncia presso le Autorità in data 13.11.2025 e reclamo all'intermediario in data 14.11.2025, riscontrato negativamente. Il ricorrente conclude domandando il rimborso dell'operazione contestata.

Con le controdeduzioni, l'intermediario afferma che il ricorso sarebbe inammissibile in quanto l'operazione risulta correttamente autorizzata con procedura di autenticazione forte (SCA), mediante utilizzo delle credenziali personali e inserimento del codice identificativo ricevuto in applicazione, senza anomalie tecniche né modifiche dell'utenza securizzata associata al rapporto. Sostiene che il cliente sarebbe stato vittima di *phishing* classico, nel quale il malcapitato, comunicando i propri codici, avrebbe consentito al frodatore di predisporre le operazioni dispositive, partecipando in tal modo, seppur inconsapevolmente, alla truffa in suo danno. Afferma che le operazioni sono state correttamente contabilizzate, registrate e autenticate con il corretto inserimento delle credenziali e che sussiste la colpa grave del cliente in quanto questi, ricevuto un contatto fraudolento da un numero non riconducibile all'intermediario, ha seguito le istruzioni del frodatore condividendo codici e credenziali in violazione degli obblighi di custodia e delle regole di ordinaria diligenza. Dichiara infine di non aver riscontrato malfunzionamenti o intrusioni nei propri sistemi informatici.

DIRITTO

L'operazione oggetto di contestazione rientra nell'ambito di applicazione del 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 e alla disciplina in materia di *strong customer authentication* (SCA).

Ai sensi dell'art. 10 del D.lgs. 11/2010, è onere dell'intermediario provare che le operazioni contestate siano state correttamente autenticate, registrate e contabilizzate e che non vi siano stati malfunzionamenti dei sistemi; solo successivamente spetta all'intermediario provare dolo o colpa grave in capo all'utilizzatore (Collegio di Coordinamento, decisione n. 22745/2019).

Con riferimento alla SCA, le fonti normative sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10 bis del D. Lgs. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019). Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1) accede al suo conto di pagamento online; 2) dispone un'operazione di pagamento elettronico; 3) effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza;

inerenza; possesso. Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.

Nel caso in esame, l'operazione disconosciuta riguarda un pagamento per l'importo di € 230,00, eseguito in data 11.11.2025 alle ore 16:03 mediante carta prepagata.

Per completezza si evidenzia che parte ricorrente riferisce che durante la truffa veniva effettuato un giroconto di € 2.100,00 da un suo libretto di risparmio cointestato, verso la carta prepagata, allo scopo di creare su quest'ultima la provvista per l'operazione di cui qui il ricorrente chiede il rimborso.

Dai Log informatici forniti dall'intermediario, è possibile notare traccia di entrambi i movimenti, di cui solo il secondo ha però arrecato un effettivo danno patrimoniale ed è per questo l'unico contestato in questa sede, per il quale soltanto si procede alla analisi della SCA.

Infatti, il Collegio di Coordinamento, con la decisione 23.07.2024, n. 8671, si è pronunciato specificamente sulla questione dell'applicabilità dell'art. 10-bis del d.lgs. n. 11/2010 alle cosiddette operazioni di costituzione della provvista, enunciando il seguente principio di diritto: *“I pagamenti da e verso lo stesso utente titolare di diversi conti accesi presso lo stesso intermediario possono essere sottratti all'obbligo della SCA anche nell'ipotesi in cui essi abbiano costituito la provvista necessaria per la realizzazione di successive operazioni fraudolente”*. Il Collegio di Coordinamento ha tuttavia precisato che, ferma l'esenzione dall'obbligo della SCA, resta configurabile una responsabilità dell'intermediario ai sensi dell'art. 11 del D. Lgs. n. 11/2010 qualora le operazioni di acquisizione della provvista, pur realizzate senza la SCA, costituiscano incontrovertibilmente fonte diretta e immediata di perdite patrimoniali, ovvero — al di fuori dell'ambito applicativo del citato decreto — sulla base del principio generale di cui all'art. 1218 c.c., qualora sia dimostrata la negligenza dell'intermediario nell'adempimento di obblighi contrattuali, come ad esempio in caso di omessa adozione di misure di sicurezza e di monitoraggio adeguate, circostanze che non ricorrono nel caso in esame.

Per tali ragioni, l'analisi dell'autenticazione forte si concentra sull'operazione contestata di € 230,00 che ha causato la perdita patrimoniale definitiva e non si estende all'operazione di giroconto, seppure documentata dall'intermediario.

Dai log prodotti in atti, risulta che la carta del ricorrente era correttamente inserita e attiva nell'applicazione dell'intermediario, con *enrollment* originario effettuato in data ampiamente anteriore ai fatti per cui è causa, e con il numero di cellulare associato coincidente con quello indicato nella denuncia. Il codice OTP necessario per completare l'operazione è stato ricevuto sul telefono del ricorrente ed è stato evidentemente da questi comunicato al frodatore nel corso della chiamata, circostanza comprovata anche dalle evidenze dei messaggi OTP allegati agli atti.

Un profilo di particolare rilievo riguarda l'attivazione dell'applicazione dell'intermediario su un secondo dispositivo, avvenuta poco prima dell'esecuzione dell'operazione contestata. L'intermediario ha documentato che tale attivazione è stata completata tramite inserimento delle credenziali di accesso — fattore di conoscenza rilevabile dalla voce *'grant:password'* nei log — e di un codice OTP inviato al numero certificato del ricorrente e da questi evidentemente comunicato al frodatore — fattore di possesso.

Tuttavia, dall'analisi dei log informatici relativi all'operazione contestata emerge che il *device* identificativo associato alla fase di autorizzazione corrisponde a quello del dispositivo originariamente

collegato al conto del ricorrente, e non a quello del secondo dispositivo successivamente attivato. Ciò consente di concludere che, malgrado l'avvenuto *enrollment* di un ulteriore dispositivo ad opera del frodatore, l'operazione contestata è stata validata dall'applicazione installata sul dispositivo del ricorrente, mediante notifica *push* quale fattore di possesso, confermata con l'inserimento del codice identificativo personale quale fattore di conoscenza.

Quanto alla condotta dell'utente, il ricorrente ha affermato di aver ricevuto un messaggio di testo apparentemente proveniente dall'intermediario, che lo invitava a contattare un numero per bloccare una transazione sospetta. Dall'esame del messaggio prodotto agli atti emerge tuttavia che esso presenta elementi che avrebbero dovuto indurre il destinatario ad assumere un atteggiamento di cautela: il testo proveniva da un numero che non era in alcun modo riconducibile all'intermediario, non era inserito in una *chat* contenente precedenti messaggi genuini dell'intermediario, indicava come numero di assistenza clienti un recapito privo di qualsivoglia collegamento con l'intermediario, e recava altresì un evidente errore grammaticale nella parola 'ALLERT', scritta con due lettere 'L'. Tutti questi elementi avrebbero dovuto richiamare l'attenzione del ricorrente, il quale ha invece provveduto a contattare il numero indicato nel messaggio e a seguire le istruzioni impartite dall'interlocutore, modificando le proprie credenziali di accesso e comunicando i codici OTP ricevuti. Va altresì rilevato che l'orario indicato nel messaggio prodotto agli atti risulta difforme rispetto a quello della truffa ricostruito dalla documentazione tecnica, e il giorno della settimana risulta diverso da quello del giorno 11.11.2025, che era un martedì e non un lunedì come risulterebbe dal messaggio.

Come stabilito in fattispecie analoghe, deve ritenersi che il cliente sia stato vittima di *smishing* per propria colpa e non sia ravvisabile il c.d. *spoofing*, configurabile quando sussistono elementi tali da far ritenere un legittimo affidamento da parte dell'utilizzatore sulla genuinità dei contatti ricevuti con i truffatori e che avrebbe potuto comportare un concorso di colpa tra le parti (cfr. Collegio di Milano, decisioni nn. 1108/2023 e 2036/2023).

Con riguardo al profilo del servizio di notifica delle operazioni eseguite, dagli atti risulta che l'intermediario ha documentato l'attivazione di default delle notifiche *push* nell'applicazione e ha prodotto evidenza del fatto che la notifica *push* relativa all'operazione contestata è stata indirizzata al dispositivo del ricorrente, ovvero al dispositivo sul quale l'operazione è stata autorizzata. Il servizio di notifica *push* deve essere valutato ai fini dell'equiparabilità al servizio di sms-alert.

Ritenuto pertanto che non sussistono profili di responsabilità autonoma dell'intermediario relativi al sistema di notifica delle operazioni e risultando accertata l'autenticazione forte dell'operazione nonché la colpa grave dell'utilizzatore, il ricorso deve essere rigettato.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE