

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 20.11.2025, il consumatore espone di aver ricevuto, intorno alle ore 11:15 del 13.11.2025, una telefonata da un soggetto il quale, qualificatosi come operatore dell'intermediario, lo informava di un cambio di applicazione per motivi di sicurezza e che un suo collaboratore lo avrebbe ricontattato a breve. Alle ore 11:45 circa il ricorrente veniva effettivamente richiamato da un'altra utenza: durante tale seconda chiamata l'interlocutore lo guidava nell'installazione

di una nuova applicazione, facendogli ricevere tramite messaggio WhatsApp — proveniente da un ulteriore numero — un file in formato APK (*Android Package Kit*) da installare sul proprio dispositivo. Completata l'installazione, il presunto operatore invitava il ricorrente ad accedere alla vecchia applicazione e, salutandolo, lo informava che il giorno successivo sarebbe stato ricontattato per un ultimo aggiornamento. Insospettito dell'accaduto, il ricorrente verificava la propria situazione contabile sull'applicazione autentica dell'intermediario e si avvedeva di essere stato vittima di una frode: riscontrava infatti due giroconto — rispettivamente di € 800,00 ed € 2.900,00 — da una sua carta libretto verso una sua carta prepagata, nonché quattro movimenti in uscita da quest'ultima tutti a favore dello stesso beneficiario dell'importo di € 2.850,00, € 100,00, € 50,00 ed € 207,70. Il ricorrente procedeva immediatamente al blocco di entrambe le carte e presentava denuncia presso le Autorità; inoltrava reclamo all'istituto di pagamento in data 14.11.2025, che veniva riscontrato negativamente. Con il ricorso ha domandato il rimborso integrale delle operazioni disconosciute.

Con le controdeduzioni, l'istituto di pagamento ha qualificato la fattispecie come "*Card Relay Attack*", schema di frode nel quale il cliente viene inizialmente avvicinato tramite un *phishing* tradizionale, che poi si concretizza attraverso l'installazione sul *device* della vittima di un'applicazione malevola che consente agli attaccanti di veicolare il flusso di una transazione *contactless* verso un dispositivo mobile in loro possesso che, a sua volta, dialoga con un terminale POS o ATM permettendo di finalizzare l'operazione di pagamento. Precisa che le operazioni contestate sono state correttamente contabilizzate, registrate e autenticate con il corretto inserimento delle credenziali e che non sono stati rilevati malfunzionamenti o intrusioni nei propri sistemi informatici. Ritiene che sussiste la colpa grave del ricorrente per aver seguito le istruzioni di terzi sconosciuti contattati tramite numeri non riconducibili all'istituto, avendo verosimilmente comunicato il PIN ai frodatori.

DIRITTO

Le operazioni contestate rientrano 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.

Le operazioni disconosciute sono quattro transazioni eseguite in data 13.11.2025, tutte verso il medesimo beneficiario, dell'importo rispettivamente di € 2.850,00, di € 100,00, di € 50,00 ed € 207,70. Occorre rilevare che il valore dell'ultima transazione all'interno del log informatico prodotto dall'intermediario è indicato in € 205,95.

Le prime tre sono state eseguite nel giro di otto minuti (ore 11:21, 11:28 e 11:29), mentre la quarta è successiva di circa un'ora (ore 12:32).

Risulta che nel corso della truffa sono state effettuate due operazioni di giroconto di € 800,00 ed € 2.900,00 da una carta libretto verso la carta prepagata, entrambe intestate al ricorrente e accese presso lo stesso prestatore, allo scopo di creare su quest'ultima la provvista per le transazioni poi disconosciute.

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 fondamento normativo risiede nell'art. 15 del Regolamento Delegato UE n. 2018/389, che autorizza il mancato ricorso alla SCA quando pagatore e beneficiario coincidono e i conti sono radicati presso il medesimo prestatore, in ragione del basso livello di rischio riconducibile a tale tipologia operativa, come esplicitato dal Considerando n. 10 del Regolamento.

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. Poiché tali giroconti non sono stati oggetto di contestazione e di richiesta di rimborso da parte del ricorrente, l'analisi della SCA si concentra sulle quattro transazioni disconosciute.

Al fine di comprendere le modalità di autenticazione delle operazioni contestate, risulta opportuno chiarire la tecnica utilizzata dai truffatori, nota come *“Card Relay Attack”*.

Essa si articola in una fase iniziale di ingaggio del cliente tramite chiamata o messaggio apparentemente proveniente dall'istituto di pagamento, cui segue l'induzione ad installare un'applicazione malevola sul proprio dispositivo. Tale applicazione, sfruttando la tecnologia NFC, consente agli aggressori di emulare la carta di pagamento della vittima su un proprio terminale e di effettuare transazioni *contactless* presso POS o ATM, senza che i malfattori debbano mai entrare fisicamente in possesso della carta, a condizione che questa risulti salvata sul dispositivo mobile della vittima.

Nel caso in esame risulta documentato che il ricorrente aveva registrato la propria carta sull'applicazione dell'istituto sin dall'aprile 2025, unitamente all'*enrollment* della stessa App sul *device* del cliente.

Dai log prodotti dal resistente risulta che ciascuna operazione di pagamento è stata autenticata tramite la combinazione di lettura *contactless* della carta — fattore di possesso, come risultante dalla dicitura "C" nella colonna "*Input Mode*" dei log — e corretto inserimento del PIN — fattore di conoscenza, come indicato dalla dicitura "PIN" nella colonna "Dati Autorizzazione" e dal codice di *action code* "0" che nella legenda corrisponde all'inserimento corretto del PIN. Con specifico riguardo alla conoscenza del PIN da parte dei frodatori, l'intermediario ha prodotto evidenza documentale attestante che il ricorrente aveva effettuato il recupero del PIN della propria carta direttamente tramite l'applicazione autentica, nel medesimo frangente temporale in cui si svolgeva l'interazione con i frodatori, e che tale operazione risulta eseguita dallo stesso *device* identificativo — corrispondente al dispositivo sul quale la carta era stata genuinamente registrata — con il quale erano state poi ricevute le notifiche *push* relative alle operazioni contestate. Ciò avvalorava la ricostruzione secondo cui il PIN sarebbe stato comunicato dal ricorrente ai frodatori durante la chiamata.

Alla luce delle evidenze documentali, deve pertanto ritenersi che l'intermediario abbia fornito prova dell'autenticazione forte delle operazioni, mediante combinazione di elementi di possesso e conoscenza, nonché della loro corretta registrazione e contabilizzazione.

Quanto alla condotta del ricorrente, nella denuncia e nel ricorso, egli riferisce di avere ricevuto una chiamata dal numero **967 in cui, un soggetto qualificatosi come operatore dell'intermediario, lo avvisava di un cambio di applicazione in atto presso l'intermediario per motivi di sicurezza, indicando che sarebbe stato chiamato da lì a breve da un altro operatore. Riceveva infatti un'altra chiamata dal numero **230 in cui veniva invitato ad installare una nuova applicazione, per la quale riceveva tramite messaggio Whatsapp proveniente da numero **578 un file APK (*Android Package Kit*), un formato di file utilizzato per installare applicazioni su dispositivi *android*. Dopo essersi assicurato che il cliente avesse installato questa app, il presunto operatore al telefono gli chiedeva di rieseguire l'accesso alla "vecchia applicazione".

Nessuno dei numeri con cui il ricorrente è entrato in contatto è riconducibile all'intermediario. Inoltre, il ricorrente non produce evidenza in merito alle chiamate e al messaggio ricevuti, e neppure riguardo all'applicazione che ha installato. Tuttavia, come affermato dall'intermediario in sede di controdeduzioni, è molto probabile che si tratti di un'applicazione, come altre presenti sul mercato, che consente il controllo da remoto del dispositivo su cui è stata installata. Per acquisire il controllo da remoto è necessario/sufficiente inserire l'ID univoco fornito dall'applicazione. Il truffatore, pertanto, una volta convinto il cliente a scaricare l'applicazione, visualizzerebbe in modo automatico tutti i messaggi provenienti dall'intermediario (contenenti ad es. le notifiche *push*, gli OTP ovvero gli *alert* relativi all'avvenuta operazione di pagamento), eseguendo le operazioni fraudolente senza la necessità di contattare ulteriormente il cliente ovvero richiedere informazioni aggiuntive. Tali applicazioni non recano alcuna indicazione riferibile all'intermediario e sono direttamente scaricabili da parte di ogni utente.

Come stabilito in fattispecie analoghe, deve ritenersi che il cliente sia stato vittima di *smishing* misto a *vishing* 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). Inoltre, secondo orientamento consolidato di questo Collegio,

versa in colpa grave l'utente che, seguendo le istruzioni ricevute da soggetti terzi, installi un'applicazione malevola idonea a consentire ai malfattori di carpire le sue credenziali o di assumere il controllo del suo dispositivo (*ex multis*, Collegio di Milano, decisioni nn. 7036/2025 e 196/2023).

Ciò nondimeno, pur in presenza di una colpa grave del cliente, il Collegio è chiamato a valutare anche la condotta dell'intermediario alla luce dell'operatività concretamente posta in essere e degli obblighi di controllo e monitoraggio gravanti sul prestatore dei servizi di pagamento.

Come noto, la necessità che gli intermediari operanti nel settore si dotino di sistemi di monitoraggio capaci di intercettare elementi sintomatici di un rischio di frode rispetto a operazioni c.dd. sospette si evince dalle indicazioni contenute nel D.M. 30 aprile 2007, n. 112, adottato in attuazione della legge 17 agosto 2005, n. 166 (recante "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento").

In particolare, l'art. 8 del D.M. 112/2007 identifica i casi di frode che vanno segnalati all'Ufficio Centrale Antifrode dei Mezzi di Pagamento del Ministero dell'Economia e delle Finanze (UCAMP) per consentire un monitoraggio del mercato delle carte di pagamento.

Nel caso di specie, sulla base delle evidenze in atti, risulta integrato l'indice di anomalia espressamente previsto dal D.M. 112/2007, art. 8, lett. a), punto 2, che individua quale fattispecie rilevante, ai fini del monitoraggio delle frodi, la presenza di tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle ventiquattro ore presso un medesimo punto vendita. Sono state infatti eseguite nel giro di 8 minuti 3 operazioni di pagamento POS (contactless) presso il medesimo esercente.

Secondo l'orientamento costante dei Collegi, le previsioni del D.M. n. 112/2007 non hanno valore precettivo diretto in materia di disconoscimento delle operazioni di pagamento, né determinano automaticamente l'obbligo di rimborso di un numero predeterminato di transazioni. Esse costituiscono tuttavia un parametro qualificato per la formulazione di un giudizio in concreto sulla diligenza tecnica dell'intermediario e sull'adeguatezza dei presidi di prevenzione delle frodi. In presenza di un indice di anomalia come quello sopra descritto, anche laddove sia stata accertata la colpa grave dell'utilizzatore, la ripartizione della responsabilità tra le parti deve essere determinata con un giudizio sintetico che tenga conto della condotta complessiva dell'istituto e di tutti gli altri elementi del caso. La base di calcolo è costituita dall'intero ammontare degli importi disconosciuti, senza esclusioni, procedendo a una distribuzione in concreto del concorso di colpa.

Nel caso di specie, tenuto conto, da un lato, dell'assenza di qualsiasi intervento automatico di blocco o di segnalazione, a fronte di un rischio di frode oggettivamente elevato e riconducibile a uno schema tipico di truffa e, dall'altro, della condotta gravemente imprudente del cliente, che ha installato un'applicazione malevola su indicazione di soggetti sconosciuti, il Collegio ritiene che siano da rimborsare le ultime due operazioni, eseguite alle ore 11:29 e alle ore 12:32 di importo pari rispettivamente ad € 50,00 ed € 207,70 per un totale di € 257,70, arrotondato a € 258,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 258,00.

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