

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) DELL'ANNA MISURALE

Seduta del 19/05/2026

FATTO

La cliente, con ricorso del 19 gennaio 2026, afferma che:

- in data 06/12/2025 veniva eseguita, tramite M**B***, un'operazione non autorizzata di € 5.000,00 a seguito di una truffa mediante smishing/vishing;
- ha ricevuto un sms apparentemente proveniente dall'intermediario, che conteneva un numero di telefono;
- contattava il numero di telefono indicato nell'sms, interloquendo inizialmente con sedicenti operatori dell'intermediario e successivamente con sedicenti appartenenti alle forze dell'ordine;
- i truffatori la inducevano a confermare un'operazione asseritamente necessaria a mettere in sicurezza il conto;
- non ha comunicato il PIN, la password o l'OTP.

Chiede, pertanto, la restituzione integrale della somma indebitamente sottratta, oltre alle spese di procedura.

L'intermediario, con le controdeduzioni, riportato il fatto, afferma quanto segue:

- l'operazione contestata risulta essere stata correttamente autenticata in app, utilizzando il dispositivo mobile in esclusivo possesso della ricorrente ed unicamente associato al suo conto;
- l'operazione è stata disposta nell'ambito di una sessione di accesso al conto in app, avviata dalla ricorrente mediante l'inserimento delle credenziali personali;
- l'operazione è stata autorizzata tramite convalida della notifica push riepilogativa del pagamento e confermata mediante l'inserimento del codice PIN;

- la cliente ha seguito le istruzioni dei frodatori, comunicando i dati della propria carta e autorizzando personalmente le transazioni successivamente disconosciute, nonostante fosse stata informata dei rischi legati al phishing tramite apposite campagne antifrode;
- il caso in esame non rientra nel regime di protezione previsto dal D. Lgs. n. 11/2010 per le operazioni non autorizzate;
- si è attivato per stornare l'operazione disconosciuta, tuttavia non ha potuto revocarla in quanto trattandosi di pagamento istantaneo disposto all'interno dello stesso istituto, l'importo era stato già trasferito e prelevato dal soggetto beneficiario;
- sussiste la colpa grave della cliente in quanto ha seguito le istruzioni del frodatore fino ad autorizzare l'operazione fraudolenta;
- le richieste avanzate dal frodatore presentavano carattere palesemente anomalo;
- negli screenshot prodotti dalla cliente appare il nominativo dell'intermediario ma non il relativo numero di telefono;
- il messaggio civetta non riporta la data della presunta operazione illecita e presenta ulteriori indizi di anomalia;
- anche la comunicazione intercorsa tramite WhatsApp tra la cliente e i truffatori presenta profili di evidente anomalia;
- non sono stati riscontrati malfunzionamenti né intrusioni nei propri sistemi informatici;
- nel corso della telefonata, l'app ha mostrato una notifica antifrode volta a segnalare un possibile tentativo di truffa telefonica;
- tale notifica si attiva in caso di apertura dell'app durante una chiamata;
- la ricorrente è stata vittima di una tipologia di truffa denominata social hacking.

Chiede, pertanto, il rigetto del ricorso.

La cliente replica che l'operazione non può ritenersi autorizzata, in quanto il proprio consenso è stato viziato da dolo. Sottolinea il carattere sofisticato della truffa e l'inadeguatezza dei presidi di sicurezza adottati dall'intermediario. In via subordinata, chiede l'applicazione del principio di responsabilità concorrente dell'intermediario, con conseguente condanna al rimborso proporzionale del danno subito, comunque non inferiore al 50% dell'importo sottratto.

L'intermediario, con le controrepliche, riportandosi alle conclusioni in atti, sottolinea che un'operazione di pagamento è autorizzata se il pagatore presta il proprio consenso secondo le forme tecniche e contrattuali pattuite; nel caso di specie, la documentazione prodotta in sede di controdeduzioni, unitamente alle dichiarazioni rese dalla ricorrente in sede di denuncia, confermano che l'operazione è stata correttamente predisposta e autorizzata dalla medesima. Ribadisce che un utente mediamente diligente, rilevata l'inesistenza del pagamento segnalato in un SMS connotato da evidenti indizi di anomalia e, contestualmente, la presenza nell'app di una richiesta di autorizzazione per un importo diverso e superiore, avrebbe dovuto interrompere l'operazione e contattare la banca tramite i canali ufficiali. L'intermediario insiste per il rigetto del ricorso.

DIRITTO

La controversia ha ad oggetto il disconoscimento di un'operazione eseguita *online* tramite funzione M**B***, dell'importo di € 5.000,00, in data 06/12/2025.

È in atti la denuncia della cliente presentata lo stesso giorno.

Dalle dichiarazioni rese dalla cliente nella denuncia risulta che la stessa ha comunicato ai truffatori i dati sensibili della propria carta e confermato (tramite notifica push) l'esecuzione dell'operazione fraudolenta, credendo che servisse a fermare una frode a suo danno.

Non per questo può reputarsi fondato il rilievo dell'intermediario secondo il quale al caso in esame non si applicherebbe il regime di protezione previsto dal d. lgs., n. 11/2010 per le operazioni non autorizzate.

Invero, secondo l'orientamento dei Collegi, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad esempio come nel caso di specie con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP.

Pertanto, si procederà di seguito ad esaminare la prova di autenticazione delle operazioni ai sensi del D.Lgs. 11/2010.

Le fonti normative applicabili alla fattispecie in esame sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10 bis del D. Lgs. n. 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 è richiesta l'autenticazione forte (SCA) 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.

Al riguardo, giova precisare che l'art. 10 del D.lgs. n. 11/2010 prevede un particolare regime di ripartizione dell'onere probatorio, che, come noto, si articola in una precisa e graduata sequenza così riassumibile: in prima battuta (comma 1), il prestatore di servizi di pagamento deve provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti; quindi, assolto con successo questo primo onere, necessario ma di per sé ancora insufficiente a dimostrare che l'operazione sia stata effettivamente autorizzata dal titolare, il prestatore deve ulteriormente dimostrare, ai fini dell'esonero dalla responsabilità (comma 2) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.

Ebbene, con riferimento alla fase di accesso all'APP, l'intermediario afferma quanto segue.

L'operazione sconosciuta veniva eseguita all'interno di una sessione di login *in-APP* avviata dalla cliente il giorno 06/12/2025 alle ore 15:01 UTC (16:01 ora locale) tramite SCA, ossia mediante l'inserimento delle credenziali personali - indirizzo e-mail di registrazione e password – (fattore di conoscenza) e l'utilizzo dell'APP installata sul dispositivo mobile personale della cliente, associato in via esclusiva al suo conto (fattore di possesso).

Al riguardo produce evidenze che comprovano che il *login* è avvenuto tramite: inserimento delle credenziali personali del cliente, quali indirizzo e-mail di registrazione e *password* (fattore di

conoscenza - *LOGIN_WITH_PASSWORD*); nell'APP installata sul dispositivo mobile associato in via esclusiva al conto avente device token *80f9 (fattore di possesso - *MFA_OSC*) dal 09/03/2025.

Con riferimento all'operazione contestata di € 5.000,00 l'intermediario afferma che la funzione *M**B**** è un sistema di trasferimento istantaneo di denaro tra utenti utilizzatori dell'app N**. Per la disposizione di un'operazione di pagamento online attraverso *M**B****, il cliente che voglia effettuarla deve selezionare un contatto dalla sua lista utenti, inserire l'importo del pagamento e un'eventuale causale e immettere il PIN di conferma da lui stesso creato (fattore di conoscenza). A questo punto, al cliente viene presentata una schermata riepilogativa del pagamento in cui viene richiesto di confermare l'operazione *M**B**** tramite una notifica *push* dal dispositivo associato (fattore di possesso).

L'intermediario afferma che l'operazione è stata autorizzata all'interno della predetta sessione di login alle ore 15:03 UTC (16:03 ora locale) del 06/12/2025 in seguito a: immissione del codice PIN di conferma (fattore di conoscenza - *PIN Validation*); convalida della *push* generata in app (fattore di possesso).

Al riguardo l'intermediario produce evidenze che comprovano la validazione del codice pin inserito (elemento di conoscenza) sul device con token *80f9 (elemento di possesso).

Successivamente è stata altresì inviata e confermata in app una *push* (elemento di possesso).

Sulla base delle evidenze prodotte risulta che l'operazione è stata autenticata tramite: convalida del PIN di conferma (*PIN Validation* - fattore di conoscenza); convalida della relativa notifica *push* generata in-APP (fattore di possesso).

Può dunque passarsi ad esaminare la condotta della cliente per verificare se sussiste la sua colpa grave.

Ebbene, non può non ricordarsi a tal proposito che la cliente dichiara in denuncia di aver confermato essa stessa l'operazione oggetto di ricorso, seppur inconsapevolmente in quanto convinta di stornare un'operazione fraudolenta.

Ebbene, le modalità della truffa non giustificano un simile comportamento.

La cliente, in data 06/12/2025 alle ore 15:26, riceveva un SMS apparentemente proveniente dall'intermediario, con il quale veniva informata di un tentativo di pagamento di 2.168,64 (senza indicazione di valuta) dal proprio conto presso intermediario diverso da quello convenuto e invitata a contattare il servizio clienti al numero *669 qualora non riconoscesse l'operazione.

Sulla base della evidenza del messaggio civetta prodotto risulta che: la chat in cui è inserito il messaggio è solo a un occhio disattento riferibile all'intermediario non riportandone correttamente la denominazione; nella medesima chat non sono presenti messaggi genuini dell'intermediario antecedenti a quello civetta, bensì ulteriori messaggi truffaldini ricevuti negli anni precedenti ai quali invece la cliente non aveva dato seguito; la somma oggetto del presunto pagamento è priva di valuta; il numero di telefono contenuto nel sms non è riconducibile al servizio clienti dell'intermediario.

La cliente produce, altresì, una comunicazione WhatsApp con i truffatori, in relazione alla quale tuttavia non fornisce alcuna spiegazione, ma dalla quale si evincono messaggi sgrammaticati.

La cliente riferisce di aver contattato il numero di telefono indicato nel sms civetta, al quale rispondeva un soggetto che la informava di un tentativo di frode in corso e della necessità di confermare, tramite app, lo storno di € 5.000,00. Tale numero, tuttavia, non risulta riconducibile all'intermediario convenuto e pertanto la fattispecie è qualificabile alla stregua di un banale *vishing*, cui la cliente avrebbe potuto agevolmente sottrarsi con l'uso dell'ordinaria diligenza e prudenza.

Infine, vi è da rilevare che non vi è evidenza dell'attivazione di un servizio di sms-alert. Tuttavia, la mancata attivazione ovvero il mancato funzionamento del servizio di sms-alert (o di servizio assimilabile) è irrilevante nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta come nel caso di specie, in quanto la ricezione dell'alert non avrebbe potuto limitare, in concreto, il pregiudizio dell'utente.

Infine, soltanto per scrupolo e completezza, si osserva che non rientra nei compiti di questo Arbitro stabilire che l'intermediario *“debba collaborare con le autorità competenti fornendo tutta la documentazione e informazioni disponibili dell'operazione contestata e del beneficiario del pagamento per integrazione della denuncia”*.

Tutto quanto esposto deve concludersi per l'infondatezza delle domande.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE