

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) MODICA

Seduta del 19/05/2026

FATTO

La cliente, venuta in contatto con operatore del servizio clienti dell'intermediario, apprendeva di due tentativi di pagamento, bloccati per ragioni di sicurezza; nel corso della chiamata, informava l'operatore che il processo di ripristino del cellulare evidenziava la presenza di un app latente dannosa (T*), che non aveva mai installato; spiegava quindi al proprio interlocutore che nei giorni precedenti aveva cliccato su un link apparso durante uno spot pubblicitario sulla piattaforma T* T*, che aveva temporaneamente alterato le funzioni del cellulare. L'operatore dell'intermediario, il medesimo con cui era già entrata in contatto il 20/12/2025, le consigliava di rivolgersi alle Autorità e fissava un appuntamento per il giorno successivo al fine di reinstallare l'app della banca in sicurezza. In data 23/12/2025, sempre tramite il medesimo operatore, disconosceva le ultime 4 operazioni fraudolente, reinstallava l'app della banca e cambiava tutti i codici; in pari data l'intermediario le riaccreditava provvisoriamente parte delle operazioni disconosciute. In data 29/12/2025 riceveva una nuova comunicazione dell'intermediario, con cui veniva informata che due operazioni fraudolente erano già state stornate, mentre per le altre era in corso un tentativo di recupero.

Chiede la restituzione di € 2.913,12.

L'intermediario afferma che la cliente non ha fornito elementi utili alla ricostruzione della vicenda, limitandosi a disconoscere le operazioni; le operazioni disconosciute risultano effettuate tramite il

dispositivo della cliente e autorizzate mediante biometria; sul proprio sito internet è disponibile un'apposita informativa volta a tutelare la clientela dalle truffe; la cliente è stata vittima di una truffa che esula dalla responsabilità della banca, resa possibile da comportamenti della cliente atti a integrare una fattispecie di negligenza grave.

Chiede il rigetto del ricorso o, in subordine, il riconoscimento di un concorso di colpa.

La cliente replica che: non ha mai ceduto a terzi la carta di credito, il pin e/o le credenziali di accesso al conto corrente; non ha autorizzato le operazioni contestate; non è ravvisabile alcun dolo o colpa grave nella sua condotta, avendo bloccato la carta e sporto querela non appena venuta a conoscenza delle operazioni non autorizzate; l'intermediario ha l'obbligo di attivare sistemi di alert. L'intermediario controreplica che: la cliente non ha chiarito neppure con le repliche in che modo le operazioni disconosciute siano state inserite e confermate tramite il suo device; non ha fornito prova degli asseriti disservizi del suo telefono verificatisi in data 19/12/2025; la cliente è stata allertata tramite push ma ciononostante non si è attivata per bloccare l'operatività in corso, circostanza che avrebbe reso impossibile le operazioni successive alla prima.

DIRITTO

La cliente disconosce una serie operazioni eseguite a valle di una truffa e chiede la restituzione dei relativi importi. Si tratta, in particolare, di n. 8 tra bonifici e pagamenti e-commerce disposti il 16/12/2025 alle ore 15:01 e alle ore 16:42; il 17/12/2025 alle ore 09:53; il 19/12/2025 alle ore 14:21 e alle ore 15:56; il 20/12/2025 alle ore 08:29; 08:56 e 09:27, per un importo complessivo di € 2.953,12.

Le operazioni ricadono sotto il raggio d'azione del D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2). Ai sensi dell'art. 10, comma 1, del d.lgs. n. 11/2010, "Qualora l'utilizzatore di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento 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". L'assolvimento di tale onere è necessario ma non sufficiente, dovendo il prestatore ulteriormente provare, ai fini dell'esonero da responsabilità (art. 10, comma 2, d. lgs. 11/2010), che l'uso indebito del dispositivo sia da ricondurre al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 d. lgs. 11/2010: come chiarito dal Collegio di Coordinamento, "la produzione documentale volta a provare l'autenticazione e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente" (decisione n. 22745/2019). Il Collegio, richiamati gli artt. 97 e 98 della PSD2, l'articolo 10 bis del D. Lgs. 11/2010, le 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 (in particolare il parere dell'EBA del 21 giugno 2019), richiama altresì l'art. 12 del d.lgs. 27.1.2010, n. 11, "Responsabilità del pagatore per l'utilizzo non autorizzato di strumenti o servizi di pagamento": "Salvo il caso in cui abbia agito in

modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente". Il Collegio, ancora, ricorda che, in base all'art. 1, lett. qbis, l'"autenticazione forte del cliente" è definita come "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".

Dai log prodotti con le controdeduzioni risulta che le operazioni di bonifico istantaneo sono state precedute dall'accesso all'app, correttamente autenticata a mezzo SCA tramite App installata sul device certificato, quale fattore di possesso, e Touch id, quale elemento di inerenza. Quanto alla fase esecutiva, dalle evidenze prodotte si evince che le operazioni di bonifico istantaneo sono state autenticate tutte con le medesime modalità, mediante validazione dell'OTP generato, previa validazione con biometria, dall'APP installata sul device abitualmente utilizzato dalla cliente; dunque, mediante i fattori di inerenza (Touch id) e possesso (smartphone da cui è stato generato il codice OTP). Per tutte le operazioni di e-commerce, l'intermediario afferma che le operazioni sono state disposte tramite l'inserimento del codice CVV e l'inserimento del codice OTP generato dal device della cliente. Fornisce conformi evidenze da cui risulta l'impegno dei fattori di inerenza (Touch id, "authType": "Touch") e possesso (smartphone da cui è stato generato il codice OTP).

Il Collegio reputa pertanto fornita piena prova di SCA.

Acclarato l'assolvimento dell'onere probatorio relativo all'autenticazione delle operazioni, il Collegio passa a valutare la condotta tenuta dal cliente, potendosi basare soltanto, a tal fine, sulle scarse dichiarazioni contenute nella denuncia, le quali tuttavia non consentono in alcun modo una sufficiente contestualizzazione dei fatti né chiariscono le modalità della asserita frode: la cliente si limita a dare conto del segmento finale della vicenda, relativa ai contatti con l'intermediario, ma tace sulle origini e dinamiche della truffa in sé. Riferisce soltanto di un malfunzionamento del proprio device (compresa l'app della banca) successiva all'apertura di un link pubblicitario e di essersi accorta dell'utilizzo fraudolento consultando l'estratto conto in data 20/12/2025. Il Collegio, sulla scorta del proprio univoco orientamento, a fronte della prova dell'autenticazione forte da parte dell'intermediario resistente, valuta il mancato circostanziamento degli utilizzi non autorizzati come elemento idoneo a fondare una valutazione in termini di colpa grave della condotta della cliente (Collegio di Milano, decisione n. 7003 del 13 giugno 2024).

La riconosciuta colpa grave, pur a fronte di operazioni accompagnate da piena prova della Sca, non esclude naturalmente che il Collegio, tenuto conto delle peculiarità del caso, possa individuare altri e diversi eventuali profili di responsabilità, per esempio sul versante del rispetto degli obblighi di protezione che gravano, per diritto comune, sul *bonus argentarius*; profili che, nella vicenda in esame, ricorrono.

Per nessuna delle operazioni contestate, infatti, vi è evidenza dell'attivazione di un servizio di alert. L'intermediario, con le controrepliche, riferisce che la cliente è stata allertata tramite push. Il Collegio rileva tuttavia che le notifiche push di cui ha evidenza, inviate al device della cliente, risultano funzionali ad autorizzare le operazioni tramite APP ma non anche a dare comunicazione dell'operazione eseguita. Lo conferma la circostanza che nei "fogli push" allegati non sono riportate le push relative ai

bonifici (che, infatti, vengono inseriti direttamente in App, senza che sia necessaria la convalida della push).

Con riguardo alla mancanza di alert, è sufficiente ricordare che “[f]ra i doveri di protezione dell’utente gravanti sull’intermediario rientra l’onere di fornire il servizio di sms alert o assimilabili da cui l’intermediario può essere esonerato solo dimostrando l’esplicito rifiuto dell’utente ad avvalersene” (Coll. Coord. n. 8553/2019); “non può essere omessa” (ai fini del giudizio di responsabilità dell’intermediario) “la verifica dell’adozione delle misure idonee a garantire la sicurezza del servizio”, avendo la diligenza posta a carico del professionista “natura tecnica che deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento” a norma dell’art. 1176, co. 2, cod. civ. (Cass., n. 13777/2007). La scelta di allocare in capo al fornitore dei servizi di pagamento questo costo organizzativo che, insieme agli ulteriori, indefettibili presidi tecnologici di sicurezza rappresenta un concreto parametro della diligenza dovuta nello svolgimento di una attività non priva di rischi, trova conferma nella giurisprudenza più recente la quale espressamente sussume tali rischi nel paradigma generale del rischio d’impresa, destinato a essere fronteggiato attraverso l’adozione di misure che consentano di verificare se l’operazione sia effettivamente attribuibile al cliente, anche attraverso il servizio di sms – alert; misure che, se non azzerano, di certo concorrono a diminuire in modo rilevante i fenomeni truffaldini (Coll. Coord., nn. 9158/2018; 18045/2019; 26916/2020; 3780/2024). Ne deriva che la mancata attivazione del servizio sms – alert costituisce una carenza organizzativa imputabile all’intermediario che, nel caso, può essere rilevata anche d’ufficio (Coll. Coord., n. 8672/2024). I Collegi territoriali sono unanimi nel ritenere che 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 ovvero di più transazioni ma a distanza di pochi minuti l’una dall’altra, e complessivamente in un arco di tempo limitato, in quanto la ricezione dell’alert non potrebbe limitare, in concreto, il pregiudizio dell’utente.

Nel caso di specie, fra la seconda operazione fraudolenta e le successive sono trascorse diverse ore (circa 16 ore tra la seconda e la terza). L’invio di un alert in corrispondenza, quanto meno, della seconda operazione avrebbe pertanto certamente consentito alla cliente di avvedersi della frode e attivarsi per prevenire o contenere ulteriori perdite. Per tali ragioni, il Collegio reputa che debbano restare a carico dell’intermediario gli importi corrispondenti alle operazioni nn. 3,4,5,6,7,8, per un totale di € 1.563,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l’intermediario corrisponda alla parte ricorrente la somma di € 1.563,00.

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