

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) MODICA	Membro designato dalla Banca d'Italia
(MI) RIZZO	Membro designato dalla Banca d'Italia
(MI) SANTARELLI	Membro di designazione rappresentativa degli intermediari
(MI) GILIBERTI	Membro di designazione rappresentativa dei clienti

Relatore (MI) RIZZO

Seduta del 18/12/2025

FATTO

La cliente, nel ricorso, afferma quanto segue:

- alle ore 18.53 del 07/07/2025, riceveva n. 2 notifiche di transazione sul suo conto presso l'intermediario a favore dell'attività di e-commerce Z*. Tali transazioni venivano poi annullate;

- riceveva, quindi, alle ore 18.56 una chiamata dal numero +370* che pareva provenire dall'intermediario in quanto, copiando e incollando il numero in internet, verificava che lo stesso corrispondeva al numero di assistenza clienti dell'intermediario. Riceveva poi un SMS dal medesimo numero, con il quale le veniva comunicata l'associazione di un nuovo dispositivo alla sua APP;
- alle ore 18.57 rispondeva alla chiamata, con la quale un sedicente operatore antifrode dell'intermediario la informava di tentativi di pagamento all'estero, in sospeso in quel momento. Le chiedeva se si fosse recata in un paese estero, se avesse effettuato pagamenti su siti strani o non sicuri. Rispondeva negativamente e faceva presente di non possedere carta fisica ma solo l'APP e la carta virtuale salvata sul telefono in un wallet;
- il sedicente operatore le chiedeva, quindi, di procedere a bloccare i pagamenti sospetti, confermandoli. Sull'APP non vedeva alcun pagamento e lo faceva presente. Il sedicente operatore sosteneva che erano stati bloccati in automatico e che le avrebbe inviato le transazioni una alla volta da confermare, per poi bloccarle immediatamente;
- la prima transazione per la quale le veniva richiesta la conferma era per 1,00 €. Alla sua domanda scettica sul perché le venisse richiesto di cliccare su "conferma" invece che su "rifiuta", il sedicente operatore rispondeva che serviva per comunicare al sistema che stava confermando di non essere stata lei ad effettuare la spesa. Cliccava quindi su "conferma" e, come anticipato dal sedicente operatore, le arrivava subito un SMS dal numero dell'intermediario – lo stesso dal quale aveva ricevuto i codici della sua carta allorché aveva aperto il conto in data 05/12/2023 - che le comunicava il blocco dell'operazione di € 1,00;
- il sedicente operatore le chiedeva poi di procedere col blocco della seconda transazione per € 440,00 €, per la quale riceveva una notifica e confermava. Riceveva subito ulteriore SMS di conferma del blocco dell'operazione. Alla sua rimostranza nel non visualizzare i blocchi mentre i pagamenti risultavano effettuati, il sedicente operatore la rassicurava di nuovo, sostenendo che fosse per via dei tempi del sistema;
- a quel punto riceveva ulteriore SMS dal numero dell'intermediario con il quale lo stesso si scusava per il disagio nella visualizzazione del saldo disponibile e la pregava di seguire le istruzioni dell'operatore antifrode;
- il sedicente operatore le chiedeva, quindi, di caricare i soldi sul conto. All'uopo, riceveva un SMS con il quale veniva pregata di effettuare una simulazione di ricarica per 1.500,00 euro. Controllava di nuovo per sicurezza in internet il numero dal quale stava ricevendo la chiamata e verificava che corrispondesse a quello dell'intermediario. Procedeva dunque con la ricarica del conto presso l'intermediario via wallet A* Pay. Riceveva un SMS con il quale le veniva chiesto di effettuare di nuovo l'operazione in quanto risultava un errore di sistema. I messaggi erano scritti in modo poco chiaro, con frasi disordinate e prive di punteggiatura corretta. Il sedicente operatore le chiedeva di chiudere e riaprire l'APP. Eseguiva la richiesta e verificava il saldo di € 1.500,00 €;

- il sedicente operatore procedeva con ulteriore transazione dell'importo di € 703,50. Riceveva una richiesta di conferma che cliccava e riceveva SMS di annullamento del pagamento;
- procedevano con ulteriore transazione, questa volta per € 600,00;
- mentre attendeva le notifiche, notava nomi di esercenti a lei sconosciuti. Chiedeva lumi al sedicente operatore, il quale rispondeva che si trattava di giri di conti e la tranquillizzava sostenendo di avere tutto sotto controllo;
- ricevute le notifiche, procedeva. La seguente operazione era per € 154,00 €. Ad ogni sua rimostranza e dubbio, il sedicente operatore la rassicurava;
- il sedicente operatore le chiedeva, quindi, di provare a eseguire un'altra ricarica per il massimale. L'operazione non andava a buon fine in quanto risultavano fondi insufficienti e errore di sistema. Il sedicente operatore si spazientiva e si rivolgeva a lei con tono quasi minaccioso. Le chiedeva poi di provare ad eseguire un'altra ricarica per € 1.000,00, che non andava a buon fine. Nei messaggi ricevuti veniva riportato un errore di sistema e le veniva richiesto di riprovare tramite bonifico;
- il sedicente operatore le richiedeva, dunque, di confermare una transazione per € 1,00 € e le chiedeva se avesse ricevuto una mail di conferma dei blocchi. Controllava: stava accadendo tutto quello che le riferiva lui. Quindi, le chiedeva di cliccare su "rivedi pagamento" nella e-mail per attivare il Bypass di sistema: avrebbe dovuto rispondere a delle domande nelle cui risposte la avrebbe guidata, poi avrebbe dovuto visionare n. 5 video. Eseguita quella che le veniva richiesto. Non condivideva mai lo schermo. Finita la procedura, il sedicente operatore la avvisava che avrebbe ricevuto una mail per la conferma dell'identità, e così infatti accadeva. Il sedicente operatore chiedeva di procedere con la conferma dell'identità e il riconoscimento facciale. Procedeva ad effettuarla;
- dopodiché riprendeva la chiamata e vedeva dall'APP che le erano stati stornati 945,79 €;
- procedevano con un'ulteriore transazione, per € 300,00, con la medesima modalità delle precedenti;
- in seguito, proseguivano nuovamente con la procedura del Bypass, per la quale riceveva anche un SMS di richiesta onde evitare un blocco del suo account. Di nuovo veniva guidata passo per passo dal sedicente operatore;
- seguivano ulteriori n. 2 transazioni, da € 300,00 € e € 740,00 rispettivamente;
- a quel punto, il suo telefono aveva la batteria quasi completamente scarica e, dato che stava tornando dal lavoro, il sedicente operatore le proponeva di richiamarla più tardi. Arrivata a casa, metteva il telefono in carica e attendeva la chiamata, che non arrivava;
- scriveva allora in chat all'assistenza clienti dell'intermediario. Le rispondeva il Bot al quale chiedeva di parlare con un operatore. Si avvedeva quindi di essere stata vittima di una truffa in quanto, aspettando di essere messa in comunicazione con l'operatore, eseguiva delle ricerche sul sito dell'intermediario e si accorgeva che il numero da cui era stata contattata corrisponde a una linea telefonica automatizzata che non è in grado di mettere in contatto il cliente con un agente umano. L'operatore, quando le rispondeva, confermava la truffa;

- l'accesso al suo conto è protetto da face id e da codice di accesso non salvato sul suo telefono ma memorizzato nelle note del suo pc portatile. L'account del pc portatile è completamente diverso da quello del telefono. È impossibile sia che qualcuno abbia avuto accesso al suo codice per errore o disattenzione da parte sua sia che qualcuno abbia potuto clonare fisicamente la carta;
- le operazioni sono state autorizzate da lei dietro manipolazione continua e in stato di confusione e ansia;
- l'importo complessivo sottratto è pari a € 2.939,00. Alcuni bonifici risultano effettuati e poi rimbalzati o stornati, altri sono andati a buon fine;
- ha ricevuto un totale di cinque chiamate dal numero ufficiale associato all'intermediario, lo stesso con cui la banca comunica tramite SMS, da cui ha ricevuto in passato codici della carta e notifiche ufficiali;
- le comunicazioni di sicurezza dell'intermediario sono arrivate solo dopo aver già autorizzato i primi pagamenti. Il sedicente operatore telefonico conosceva nei dettagli l'intero flusso di sicurezza e le domande di verifica personali. Ciò dimostra un livello di accesso e conoscenza anomala dei sistemi di sicurezza dell'intermediario, che ha reso del tutto inefficaci i meccanismi di protezione della banca.

La ricorrente domanda, quindi, il rimborso integrale dell'importo sottratto; e lo svolgimento, da parte dell'intermediario convenuto, di accertamenti interni volti alla protezione della clientela dalle vulnerabilità emerse.

Nelle controdeduzioni, l'intermediario convenuto, riportato il fatto, afferma quanto segue:

- il ricorso è irricevibile in quanto le operazioni di pagamento contestate non possono considerarsi quali operazioni non autorizzate: la stessa cliente nell'allegato al ricorso denominato "Denuncia - Documenti Google" afferma di aver autorizzato le operazioni. Pertanto, non è applicabile il regime di responsabilità per le operazioni di pagamento non autorizzate di cui alla direttiva 2015/2366/EU ("PSD2") e al D.lgs. n. 11/2010 e, quindi, l'intermediario è esonerato dalla prova di autenticazione ai sensi del citato decreto. Non ravvisa neppure indizi di negligenza e/o responsabilità propria in merito ai sistemi di alert predisposti. Ha inviato, durante l'esecuzione delle operazioni contestate, degli alert di frode in cui dava avviso: a) che era stata rilevata una potenziale truffa e che per tale ragione alcuni pagamenti erano stati rifiutati; b) che se il pagamento fosse stato ritenuto legittimo dalla cliente, la stessa avrebbe potuto sbloccarlo manualmente (invero è proprio in ragione di tali alert che la cliente ha dovuto eseguire la procedura di Bypass che comportava una revisione dei pagamenti);
- la cliente è stata vittima di impersonation scam;
- le operazioni sono state correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali;
- sussiste la colpa grave della cliente in quanto le transazioni avvenute sul sito di Z* – cd. transazioni civetta – vengono normalmente poste in essere dai truffatori in modo del tutto autonomo, senza alcuna cooperazione né con l'utente né con l'intermediario. I truffatori

riescono a carpire da differenti siti i dati che gli utenti inseriscono quando effettuano transazioni su siti web poco affidabili. Una volta in possesso di tali dati, i truffatori riescono a eseguire transazioni civetta senza che sia richiesta l'esecuzione di una forma di autenticazione forte, in considerazione del fatto che l'importo è inferiore a € 30,00 (le transazioni effettuate presso il merchant Z* erano di importo pari a € 22,90 ciascuna) e rientra, pertanto, nelle operazioni di modesta entità per le quali, ai sensi dell'art. 16 del Regolamento UE 2018/389, non è previsto l'obbligo di autenticazione forte del cliente. Gli SMS ricevuti dalla cliente – apparentemente provenienti dall'intermediario – presentano evidenti errori grammaticali e differenze stilistiche rispetto ai messaggi genuini, come peraltro affermato dalla cliente. La cliente ha dato seguito alle richieste anomale del suo interlocutore: autorizzando al fine di bloccare (palese controsenso) le operazioni contestate; ricaricando il conto al fine di effettuare una simulazione; continuando a confermare le operazioni, nonostante avesse constatato nomi sconosciuti di merchant presso i quali tali operazioni venivano effettuate. In aggiunta, il numero dal quale la cliente è stata contattata è utilizzato dall'intermediario soltanto per permettere il blocco delle carte da parte dei clienti, così come la stessa cliente ha avuto modo di constatare. La cliente non ha nemmeno provveduto, durante la telefonata con il truffatore, a contattare gli operatori dell'intermediario mediante la chat presente nell'applicazione, posto che la stessa nutrisse dei sospetti sulle richieste dell'interlocutore e fosse a conoscenza del fatto che la chat è il canale ufficiale dell'assistenza clienti dell'intermediario.

L'intermediario convenuto domanda, quindi, il rigetto del ricorso in quanto infondato in fatto e in diritto.

DIRITTO

Oggetto della presente controversia sono sei operazioni contestate, per un importo complessivo di euro 2.939,85, poste in essere il 07/07/2025. Alla data delle operazioni (v. infra, par. 2) trovava applicazione il D.lgs. 27 gennaio 2010, n. 11 come modificato dal D.lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD II), entrato in vigore il 13/01/2018.

Rileva il Collegio come la cliente, nel ricorso, affermi – forse per errore – che le sono stati sottratti € 2.939,85, mentre nel reclamo contesta un totale di spese per € 2.937,85, cifra esattamente corrispondente all'evidenza delle operazioni prodotta agli atti dalla parte resistente.

È agli atti la denuncia della cliente presentata in data 11 luglio 2025.

Quanto all'autenticazione forte, corretta registrazione e contabilizzazione delle operazioni contestate, dall'esame dei log informatici prodotti agli atti dall'intermediario convenuto emerge che tutte le operazioni sono state autenticata tramite protocollo 3DS, attraverso i fattori del riconoscimento biometrico e della notifica push inviata e confermata in app. La procedura di autenticazione seguita risulta, pertanto, conforme a quanto previsto dall'art. 10 del D.lgs. n. 11 del 2010.

Quanto alla condotta delle parti e ai profili rilevanti per la valutazione di sussistenza della colpa, dall'esame delle evidenze agli atti risulta che: la denominazione della chat in cui si inserivano i messaggi truffaldini è riferibile all'intermediario; nella medesima chat sono presenti messaggi genuini dell'intermediario antecedenti a quello civetta; detto messaggio civetta contiene errori di punteggiatura

e grammaticali (“se non e lei”), così come i messaggi truffaldini successivi; nella chat sono presenti messaggi parlanti relativi alle operazioni contestate e gli stessi sono seguiti da messaggi truffaldini che ne indicano il blocco.

Da tutto quanto precede consegue una qualificazione della fattispecie come spoofing.

Considerato che le chiamate ricevute sono riconducibili all’intermediario – e pertanto sono identificabili, per precisione, come ID caller spoofing; che la cliente dichiara espressamente di avere verificato più volte la riconducibilità del numero all’intermediario durante la telefonata con il truffatore; che il numero, effettivamente, corrisponde a una linea telefonica automatizzata dell’intermediario che non è in grado di mettere in contatto il cliente con un agente umano, ma di ciò la cliente dichiara di essersi accorta solo una volta che la truffa si era consumata; il giudizio sulla colpa della ricorrente merita un’attenuazione che tenga conto dell’apporto causale rappresentato dalla compromissione dei sistemi informativi dell’intermediario e dell’effetto decettivo che tale compromissione ha determinato nella ricorrente. Ne consegue, ex art. 1227 c.c., una divisione della responsabilità fra le parti nella misura di un terzo imputabile all’intermediario e due terzi riconducibili, causalmente, alla ricorrente.

Quanto alla domanda di accertamenti interni proposta dalla ricorrente, il Collegio rammenta come le “Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari” circoscrivono la competenza dell’ABF alle questioni “aventi ad oggetto l’accertamento di diritti, obblighi e facoltà” in relazione ad operazioni bancarie e finanziarie. La domanda spiegata non merita, pertanto, accoglimento.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l’intermediario corrisponda alla parte ricorrente la somma di € 980,00.

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