

COLLEGIO DI MILANO

composto dai signori:

(MI) TINA	Presidente
(MI) DELL'ANNA MISURALE	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) DELL'ANNA MISURALE

Seduta del 04/09/2025

FATTO

La cliente, con ricorso del 29 aprile 2025 afferma quanto segue:

- è titolare del conto corrente bancario accesso presso l'intermediario convenuto;
- è stata vittima di una frode informatica in data 10.3.2025, quando sono stati fraudolentemente disposti due bonifici, pari all'integrale disponibilità del conto corrente, da parte di soggetti terzi rimasti anonimi, mediante l'utilizzo delle credenziali di accesso al servizio di home banking autonomamente possedute da tali soggetti e previa installazione dell'applicazione su un nuovo dispositivo *smartphone*;
- non ha ricevuto alcun messaggio di alert;
- le operazioni realizzate dai truffatori non rispecchiavano la normale operatività del conto e avrebbero dovuto determinare la sospensione della transazione e l'effettuazione tempestiva di una segnalazione di operazione sospetta alla competente UIF presso Banca d'Italia;
- nel riscontro al reclamo l'intermediario non ha assolto l'onere della prova relativo alla sussistenza di una colpa grave, in particolare omettendo di far luce sull'intervenuta modifica del dispositivo di verifica dell'identità (c.d. doppio fattore) e sull'intervenuta trasmissione dei codici OTP ad un nuovo numero di cellulare.

Chiede, pertanto, il rimborso dei bonifici disconosciuti.

L'intermediario, riportato il fatto, afferma quanto segue:

- le transazioni oggetto del ricorso sono state perfezionate nel rispetto delle procedure di sicurezza previste dalla banca e con la collaborazione attiva, pur se inconsapevole, della cliente;
- nel caso di specie, difatti, la cliente è stata vittima di una frode avviata tramite l'effettuazione di una chiamata da parte del malfattore, in occasione della quale ha finito per comunicare le proprie credenziali statiche al di fuori del circuito dell'intermediario, permettendo l'effettuazione delle operazioni di bonifico oggetto di contestazione;
- la truffa in questione sarebbe stata evitata se la cliente avesse prestato attenzione agli avvisi diramati dall'intermediario;
- la denuncia contiene una dichiarazione confessoria della ricorrente laddove si ammette di avere *"seguito le istruzioni dell'operatore"*, sebbene nel ricorso la ricorrente asserisca di non avere fornito al frodatore *"né le proprie credenziali né codici OTP"*;
- il comportamento della ricorrente è qualificabile come gravemente colposo in quanto ha fornito ai malfattori le credenziali per portare a termine la frode.

Chiede, pertanto, il rigetto del ricorso.

La cliente con le repliche eccepisce che i file dell'accertamento tecnico trasmessi con le controdeduzioni contengono dati di cui non solo è sconosciuta l'origine, ma che sono stati anche oggetto di plurime modifiche da parte di diversi soggetti e pertanto sono privi di attendibilità.

L'intermediario richiama le conclusioni già formulate in sede di controdeduzioni, precisando al contempo che i documenti depositati sono redatti dalla funzione antifrode della banca e riportano la tracciatura tecnica delle operazioni effettuate dal cliente.

DIRITTO

La controversia ha ad oggetto una truffa perpetrata attraverso l'utilizzo di strumenti di pagamento.

Nella specie, sono state disconosciute n. 2 operazioni per un importo complessivo di € 7.415,00. In particolare, si tratta di due bonifici eseguiti in data 10 marzo 2025, alle ore 12:51 e 13:29.

È in atti la denuncia del cliente presentata in data 11/03/2025.

Viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate.

Le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27.1.2010, n. 11.

In particolare, le fonti normative applicabili alla fattispecie sono rinvenibili negli artt. 97 e 98 della PDS2, 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 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.

Quanto al primo profilo evidenziato, l'intermediario offre puntuale prova dell'esistenza del doppio fattore di autenticazione per ogni fase di esecuzione delle operazioni.

In particolare, con riferimento all'enrollment dall'analisi dei log si ricava che questo si conclude positivamente con l'inserimento: di userid e la password mnemonica, vale a dire con OTP-SMS di sicurezza inviato al numero di cellulare certificato e OTP mail inviata all'indirizzo certificato.

Per quanto attiene alla fase di accesso al conto, dalle evidenze prodotte si ricava che l'accesso è stato autorizzato mediante ricorso a un elemento di conoscenza (la password) e a un elemento di possesso (OTP Software).

Infine, con riferimento all'esecuzione delle due operazioni contestate l'autenticazione è avvenuta con sblocco del token App mediante inserimento del PIN, che ha generato un codice "OTP-token" validato dai sistemi dell'intermediario. Dai log prodotti in atti non è possibile risalire all'avvenuto inserimento del PIN ai fini dello sblocco del token, tuttavia, dalle evidenze in atti è ricavabile, sia per l'una che per l'altra operazione, l'utilizzo del codice OTP (fattore di possesso) effettuato nella stessa sessione di login aperta con le modalità sopra descritte.

In merito al primo fattore l'EBA ammette che possa essere riutilizzato il fattore impiegato per il login (Q&A EBA 2018_4141).

Nel caso di specie, il riutilizzo riguarda il fattore di conoscenza (password) inserito in fase di login e dunque da reputarsi sussistente.

Valutato positivamente assolto l'onere della prova con riferimento alla SCA, deve procedersi alla verifica del profilo soggettivo, dovendosi accertare l'eventuale colpa grave del cliente.

Ebbene, la ricorrente riferisce di essere stata contattata telefonicamente apparentemente dal servizio antifrode dell'intermediario e di avere "seguito le istruzioni dell'operatore", sebbene nel ricorso asserisca di non avere fornito al frodatore "né le proprie credenziali né codici OTP".

Sta di fatto che non risulta allegata alcuna evidenza della chiamata ricevuta dalla cliente. Peraltro, il numero indicato in denuncia risulta segnalato su Google come truffaldino.

La cliente allega, tuttavia, evidenza di un messaggio ricevuto da un'utenza non nota e dalla stessa classificata come riconducibile al servizio antifrode dell'intermediario. Ma dall'analisi del messaggio emerge che: la chat in cui è inserito il messaggio civetta non riporta comunicazioni precedenti o genuine dell'intermediario; il contatto è pervenuto da un numero non utilizzato in precedenza e salvato per la prima volta nella rubrica della ricorrente in questa occasione; il messaggio relativo al finto blocco è successivo alla ricezione della chiamata da cui ha avuto inizio la truffa, che in denuncia la cliente colloca alle 12:18.

Sulla base di quanto sopra prodotto la fattispecie appare riconducibile al *vishing*.

Al riguardo, i Collegi sono unanimi nel ritenere che la mancata allegazione, da parte del cliente, del messaggio civetta (ovvero, per il *vishing*, del registro delle chiamate) debba

determinare il rigetto del ricorso, in quanto non consente di verificare se il mittente/chiamante risulti riconducibile all'intermediario e, pertanto, se sia configurabile un legittimo affidamento dell'utente circa la genuinità del messaggio o della telefonata ricevuti.

Vi è però che nel caso di specie la cliente abbia contestato di non avere ricevuto i messaggi di alert relativi alle operazioni disconosciute.

In effetti, dato il lasso temporale intercorso tra la prima operazione e la seconda (quasi 40 minuti), l'invio dell'SMS alert relativo alla prima operazione avrebbe potuto consentire di bloccare il conto impedendo l'esecuzione della seconda.

L'intermediario non produce evidenza delle notifiche di natura informativa (ad eccezione dell'invio di alert per l'*enrollment* dell'app su un nuovo dispositivo).

I Collegi sono unanimi nel ritenere che la mancata attivazione del servizio di sms-alert (o altro assimilabile, come notifica tramite app dell'intermediario oppure e-mail, con una valutazione di equivalenza da condurre caso per caso) costituisce in genere un profilo di responsabilità dell'intermediario.

Ne segue che nel caso di specie deve procedersi al rimborso della seconda operazione ammontante ad € 415,00.

PER QUESTI MOTIVI

Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 415,00.

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

Firmato digitalmente da
ANDREA TINA