

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) LEMME	Membro designato dalla Banca d'Italia
(BO) MIRABELLI	Membro di designazione rappresentativa degli intermediari
(BO) TRAVERSI	Membro di designazione rappresentativa dei clienti

Relatore STEFANO TRAVERSI

Seduta del 13/01/2026

FATTO

Con ricorso ritualmente proposto in data 01/08/2025, parte ricorrente deduce e allega che in data 25 luglio 2025, intorno alle ore 18:20, riceveva sul proprio telefono cellulare una chiamata proveniente dal numero 05**, ritenuto riconducibile al centralino dell'intermediario resistente. Il soggetto che la contattava si qualificava come operatore della banca e la informava della presenza di un presunto bonifico sospetto dell'importo di euro 1.490,00, rappresentando la necessità di procedere con urgenza allo storno dell'operazione.

La ricorrente espone che, inizialmente, rifiutava di comunicare il proprio codice utente di accesso all'home banking; tuttavia, a seguito delle insistenti richieste dell'interlocutore, che faceva riferimento a possibili iniziative giudiziarie, forniva il codice utente e, successivamente, anche il codice OTP ricevuto poco dopo tramite SMS. Dopo circa trenta minuti di conversazione telefonica, grazie all'arrivo presso l'abitazione del figlio, la ricorrente si avvedeva che dal proprio servizio di home banking risultavano disposti tre bonifici, rispettivamente di euro 969,00, euro 970,00 ed euro 10,00, per un importo complessivo di euro 1.949,00. In data 28 luglio 2025, la ricorrente sporgeva formale denuncia alle competenti Autorità.

L'intermediario resistente eccepisce, in primo luogo, che la ricorrente ha attivato il servizio di internet banking in data 7 agosto 2020 e che tutte le fasi rilevanti della vicenda, inclusa l'esecuzione dei bonifici contestati, sono state autorizzate mediante Strong Customer Authentication (SCA).

Secondo la banca, l'elemento centrale della frode risiede nel positivo completamento, con la collaborazione attiva della ricorrente, della procedura di recovery, vale a dire della procedura di abbinamento di un nuovo dispositivo al servizio di internet banking in sostituzione di quello precedentemente utilizzato.

In particolare, l'intermediario evidenzia che il token M**, costituente il fattore di possesso, risultava associato dal 25 dicembre 2023 e fino al giorno della frode all'idtoken n. **189, utilizzato regolarmente per tutte le operazioni sino all'evento contestato.

La ricorrente avrebbe effettuato l'accesso all'app di mobile banking mediante le consuete credenziali personali (username e password) e, successivamente, avrebbe avviato una procedura di rigenerazione della password, completata attraverso l'utilizzo di un secondo fattore SCA.

Il frodatore, secondo la ricostruzione dell'intermediario, avrebbe quindi avuto accesso all'app inserendo correttamente l'OTP comunicato dalla ricorrente, completando la procedura di recovery e disponendo infine i bonifici contestati. L'intero processo sarebbe stato integralmente presidiato da SCA e accompagnato da comunicazioni informatiche "parlanti", idonee a chiarire la natura e la finalità delle operazioni in corso.

L'intermediario ravvisa numerosi profili di grave negligenza in capo alla ricorrente, tra cui la comunicazione del codice utente e dell'OTP a un soggetto terzo, nonché – presumibilmente – della password temporanea, del codice di completamento della recovery inviato via e-mail e di ulteriori codici SMS. Le comunicazioni inviate alla cliente sarebbero state chiare e inequivoche nel descrivere le operazioni in atto.

La banca sottolinea inoltre come la minaccia di querela riferita dalla ricorrente costituisca un ulteriore indice della palese natura fraudolenta della vicenda, rilevando che si tratta di una tipologia di truffa ampiamente nota, rispetto alla quale l'adozione di una media diligenza sarebbe sufficiente a evitare il danno. A ciò si aggiunge che l'intermediario avrebbe predisposto massicce campagne informative sui propri canali di comunicazione.

Nelle repliche la ricorrente, nel ribadire quanto già dedotto in ricorso, ha replicato che il proprio numero di cellulare indicato nelle controdeduzioni non corrisponde alla realtà. Ha inoltre rappresentato che il beneficiario del bonifico di euro 10,00, suo conoscente, l'ha contattata direttamente per ringraziarla e che la stessa non ha mai accettato la restituzione in contanti della somma.

La ricorrente riferisce di aver inviato numerose e-mail al servizio clienti dell'intermediario, ricevendo sempre riscontri negativi. Aggiunge che la resistente le ha proposto di definire transattivamente il ricorso mediante il pagamento della somma di euro 780,00, importo inferiore rispetto a quello di 850/900 euro prospettato in precedenza dallo studio legale nel corso di contatti telefonici.

Alla luce delle contraddizioni riscontrate tra le comunicazioni telefoniche e quelle via e-mail, la ricorrente afferma di aver deciso di non accettare la proposta transattiva, evidenziando altresì di non

aver ricevuto alcun riscontro scritto in merito alla restituzione dei tre bonifici e che solo dopo circa 43 giorni le sarebbe stata proposta la restituzione parziale della somma contestata.

Nelle controrepliche, l'intermediario, richiamando integralmente le controdeduzioni già depositate, ribadisce che tutte le operazioni sono state eseguite nel rispetto della SCA e che molteplici elementi fattuali dimostrerebbero la colpa grave della ricorrente.

La banca afferma di aver tentato il recupero delle somme, senza esito favorevole, e rileva che la ricorrente non ha formulato specifiche contestazioni alla ricostruzione dei fatti proposta nelle controdeduzioni, con conseguente applicazione del principio di non contestazione. La difformità del numero di cellulare segnalata dalla ricorrente viene ricondotta a un mero rifiuto materiale, precisando che a pagina 3 delle controdeduzioni il numero risulta correttamente indicato e coincidente con quello della cliente.

Secondo l'intermediario, la ricorrente avrebbe seguito in modo acritico le indicazioni di un soggetto che si è atteggiato in maniera palesemente incompatibile con il ruolo di responsabile antifrodi, ignorando al contempo i messaggi genuini ricevuti. La condotta dell'interlocutore avrebbe dovuto apparire anomala, inducendo quanto meno a interrompere immediatamente la conversazione.

Viene ribadito che non è provato che la chiamata provenisse da una numerazione riconducibile alla banca e che le operazioni risultano correttamente autenticate, come emerge dai log prodotti in atti. Con riferimento al bonifico di euro 10,00, l'intermediario osserva che la ricorrente avrebbe avuto la concreta possibilità di rientrare in possesso della somma, sia tramite i canali formali dell'intermediario del beneficiario, sia mediante la restituzione diretta da parte di quest'ultimo, e che la scelta di non avvalersene non può essere imputata alla banca.

Infine, l'intermediario precisa che è stato fornito riscontro scritto alla cliente e che la proposta transattiva formulata si fondava esclusivamente su valutazioni di convenienza negoziale, senza alcun riconoscimento di responsabilità.

DIRITTO

Le operazioni contestate sono state poste in essere sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD2), che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

La controversia concerne anzitutto la valutazione sulla validità delle operazioni di pagamento disconosciute e la conformità del sistema di sicurezza adottato dall'intermediario alla disciplina sopra richiamata.

Dagli atti emerge che le operazioni contestate sono state precedute da una procedura di accesso e di enrollment di un nuovo dispositivo, articolata secondo una sequenza cronologica definita: accesso all'applicazione mediante credenziali personali già in uso, avvio della procedura di rigenerazione della

password, assegnazione di una password temporanea, conferma mediante codice OTP, nonché ulteriori comunicazioni informative inviate ai recapiti certificati dell'utente.

Il Collegio è consapevole dell'esistenza di un orientamento giurisprudenziale che ha ritenuto non soddisfatto il requisito della SCA in processi di autenticazione caratterizzati dall'inserimento di una password temporanea e di un OTP inviati tramite il medesimo canale (SMS), riconducendo entrambi i fattori alla categoria del possesso (cfr. Collegio di Milano, decisioni n. 3478/2023 e n. 2223/2023; Collegio di Torino, decisione n. 1971/2024; Collegio di Palermo, decisione n. 2735/2023).

Questo Collegio ritiene tuttavia di aderire all'orientamento espresso dal Collegio di Bologna nelle decisioni n. 3540/2023, n. 6405/2023 e, da ultimo n. 1131/2025, secondo cui, nell'ambito delle procedure di recupero o rigenerazione delle credenziali e della successiva operatività, la password temporanea può qualificarsi come elemento di conoscenza ai fini della Strong Customer Authentication in coerenza con una lettura funzionale della PSD2.

In tale prospettiva, ritiene che l'invio della password temporanea possa configurare un elemento di conoscenza "estemporaneo", funzionalizzato a consentire l'accesso iniziale e il successivo cambio della password. Ne consegue che OTP e password temporanea, pur essendo entrambi trasmessi tramite il medesimo canale, assolvono a funzioni differenti: l'OTP è preordinato alla convalida tecnica di uno specifico passaggio autorizzativo, mentre la password temporanea, una volta acquisita e digitata dall'utente, opera come informazione conosciuta dal medesimo.

Alla luce di tale impostazione, il processo di autenticazione va valutato nel suo complesso, tenendo conto della sequenza e della funzione dei fattori impiegati.

In ordine alla valutazione dell'onere della prova e sulla condotta dell'utilizzatore, con riferimento alla dedotta provenienza della chiamata da una numerazione che la ricorrente assume riconducibile all'intermediario resistente, il Collegio rileva che tale circostanza non risulta adeguatamente provata.

In atti non sono stati prodotti riscontri oggettivi quali a titolo esemplificativo, un estratto delle chiamate in ingresso rilasciato dall'operatore telefonico, ovvero la stampa del registro chiamate del dispositivo idonei a confermare l'effettiva ricezione di una chiamata proveniente dalla numerazione indicata, né elementi che consentano di attribuire tale utenza alla disponibilità dell'intermediario.

La sola schermata prodotta, in assenza di ulteriori verifiche tecniche, non consente, né sotto il profilo logico né sotto quello tecnico, di ricondurre la paternità della telefonata all'istituto resistente, tenuto conto, peraltro, della notoria possibilità di alterazione del numero chiamante, nonché della mancanza di ogni collegamento con pregresse comunicazioni con l'intermediario idonee a consentirne la necessaria contestualizzazione.

Rileva infine che il contenuto della comunicazione, come descritto dalla ricorrente, non risulta di per sé idoneo a integrare un elemento oggettivo di riferibilità del contatto all'intermediario resistente.

In assenza di elementi idonei a fondare un affidamento qualificato sull'origine della comunicazione, la valutazione deve pertanto concentrarsi sul comportamento tenuto dall'utilizzatore nella gestione delle proprie credenziali di sicurezza, avendo comunicato a soggetti terzi una pluralità di credenziali e codici di sicurezza necessari al completamento delle procedure di accesso e alla disposizione delle operazioni contestate.

Tale comportamento, valutato in termini oggettivi, integra una violazione degli obblighi di custodia delle credenziali di sicurezza posti a carico dell'utilizzatore dall'art. 7 del d.lgs. n. 11/2010 e assume rilievo ai sensi dell'art. 12 del medesimo decreto, con conseguente imputazione della perdita all'utilizzatore, non emergendo profili di responsabilità imputabili all'intermediario resistente.

Alla luce delle considerazioni che precedono, deve pertanto escludersi la sussistenza di profili di responsabilità in capo all'intermediario resistente in relazione alle operazioni contestate.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE