

COLLEGIO DI BOLOGNA

composto dai signori:

(BO) TENELLA SILLANI	Presidente
(BO) VELLA	Membro designato dalla Banca d'Italia
(BO) PAGNI	Membro designato dalla Banca d'Italia
(BO) CORRADI	Membro di designazione rappresentativa degli intermediari
(BO) DI NELLA	Membro di designazione rappresentativa dei clienti

Relatore LUCA DI NELLA

Seduta del 31/03/2026

FATTO

La parte ricorrente espone, allega e chiede nel ricorso quanto segue.

- È titolare del conto corrente n. ***3049 acceso presso l'intermediario e della relativa carta di pagamento n. ***5549.
- Il 21/06/2025 riceveva sul proprio cellulare un SMS apparentemente proveniente dall'intermediario concernente una transazione di € 980,00 respinta, con invito a contattare subito il numero 028***211 riconducibile al Servizio Sicurezza.
- Allarmata e convinta della genuinità della comunicazione, contattava senza indugio il numero telefonico indicato e interloquiva con il sedicente operatore L. del servizio di sicurezza dell'intermediario.

- L'interlocutore, mediante raggiri e artifizii, la invitava a comunicare i dati della propria carta di pagamento al fine di bloccare le ulteriori operazioni fraudolente e controllare lo strumento di pagamento.
- Comunicava quindi il numero della carta di credito n. ***5549 con il codice CVV e la scadenza.
- Seguendo le indicazioni del sedicente operatore, accedeva all'home banking tramite app installata sul suo device e notava un pagamento fraudolento di € 577,80 presso l'esercente L.M.I.
- L'interlocutore domandava dell'esistenza di un conto associato, a cui rispondeva affermativamente.
- Insospettita, chiedeva all'interlocutore la sua reale identità e quest'ultimo le confermava di averla truffata.
- Contattava immediatamente la filiale online, raccontando l'accaduto, al fine di bloccare tutti i pagamenti relativi al conto corrente cointestato con la moglie C.S.S. e al suo conto corrente personale.
- Compresa la truffa, sporgeva denuncia in data 25/06/2025 presso i Carabinieri.
- Il 25/06/2025, l'operazione non risultava ancora contabilizzata e l'utenza 028***211 era attiva.
- Il 2/07/2025 disconosceva l'operazione e chiedeva il rimborso nei confronti dell'intermediario, il quale respingeva la richiesta e riaddebitava l'importo con comunicazione dell'11/07/2025 in quanto l'operazione risultava correttamente autorizzata mediante le credenziali personali, in violazione degli obblighi di custodia.
- Il 16/09/2025, il suo legale inviava il reclamo all'intermediario, posto che non ricorreva un proprio comportamento doloso o gravemente colposo.
- In data 1/10/2025 l'intermediario riscontrava negativamente il reclamo in quanto aveva comunicato i propri codici personali, seppur raggiunta da terzi.
- La condotta dell'intermediario risulta illegittima e contraria ai principi normativi e giurisprudenziali.
- Il diniego dell'intermediario risulta illegittimo e infondato sia in fatto sia in diritto.
- L'onere della prova incombe sull'intermediario, il quale deve dimostrare positivamente la colpa grave dell'utente.
- Ha subito una sofisticata frode informatica nota come smishing mista a vishing, con tecniche di ingegneria sociale finalizzate a carpire la sua fiducia.
- L'SMS truffaldino non conteneva link sospetti, bensì simulava una procedura di sicurezza standard tale da ingannare un utente mediamente diligente.
- Successivamente ha ricevuto una telefonata da truffatori esperti nell'impersonare il personale bancario, completando l'artificio.
- L'intermediario è tenuto ad adottare misure idonee a prevenire e individuare le frodi, monitorando le operazioni anomale e provando l'adozione dei sistemi di sicurezza.
- L'intermediario, una volta ricevuta la denuncia, avrebbe dovuto rimborsare definitivamente la somma fraudolentemente sottratta.
- Parte ricorrente chiede, in via principale, la restituzione della somma di € 577,80, oltre interessi legali dalla data dell'illegittimo addebito al saldo; in via subordinata, il riconoscimento del

concorso di colpa dell'intermediario e il rimborso di € 288,90, pari al 50% della somma sottrattale; in ogni caso, il rimborso delle spese della procedura.

Nelle controdeduzioni l'intermediario espone, allega e chiede quanto segue.

- Il 21/06/2025 è stato eseguito un pagamento online di € 577,80 a favore dell'esercente L.M.I.
- Per accedere al servizio di internet banking è richiesto l'inserimento del codice titolare, del PIN e dell'OTP.
- Una volta collegati all'home banking, è necessario l'inserimento del codice OTP al fine di autorizzare le operazioni dispositive.
- Ha ottenuto una specifica certificazione per cui il sistema di gestione offre i massimi livelli di sicurezza nell'utilizzo dei servizi della banca online e dei sistemi di pagamento elettronici.
- Fornisce alla propria clientela ampia informativa concernente i tentativi di truffa.
- Non contatta mai i propri clienti al fine di richiedere codici personali, fermo restando che non inserisce mai link a pagine o applicazioni esterne.
- L'aggiornamento delle app deve avvenire tramite gli store ufficiali e i numeri verdi sono abilitati solo a ricevere le chiamate.
- Le singole operazioni disconosciute sono state eseguite in ragione della corretta autenticazione, registrazione e contabilizzazione, in assenza di anomalie.
- La ricorrente si connette solitamente da app dal proprio device identificato con il codice univoco n. EA13***35CF.
- Alle ore 15:23 del 21/06/2025 è stata disposta con carta n. ***5549 un'operazione di acquisto online di € 577,80 e validata con il codice OTP, inserendo il PIN in risposta alla notifica PUSH.
- Non si tratta di una truffa particolarmente sofisticata in quanto l'SMS civetta, oltre a non risultare conforme ai modelli in uso, proviene da un numero non riconducibile ai propri, in assenza di precedenti messaggi genuini.
- Il numero telefonico indicato nel messaggio non gli è in alcun modo riferibile.
- La ricorrente dichiara in denuncia e nel modulo di disconoscimento di aver comunicato all'interlocutore tutti gli estremi della carta di credito in quanto quest'ultimo doveva effettuare dei controlli.
- La richiesta risulta assolutamente illogica e incongrua, il quanto l'intermediario conosce il numero dello strumento di pagamento concesso a un proprio cliente.
- Il pagamento è avvenuto in un ambiente di commercio elettronico sicuro con autenticazione del titolare, del numero della carta di credito e del relativo CVV.
- La notifica PUSH era "parlante" in quanto riportava l'importo, il beneficiario, la data, l'ora e il numero della carta riferibili all'operazione.
- L'importo di € 577,80 non coincideva con quello riportato nel messaggio truffaldino (€ 980,00).

- L'intermediario chiede, in via principale, il rigetto della domanda in quanto immotivata e infondata; in via subordinata, in caso di accoglimento della richiesta, la ripartizione tra le parti del danno in misura proporzionale alle rispettive responsabilità ai sensi dell'art. 1227 c.c.

In sede di repliche alle controdeduzioni parte ricorrente afferma quanto segue.

- La responsabilità del prestatore di servizi di pagamento rientra nell'alveo del rischio professionale, prevedibile ed evitabile con l'adozione di misure idonee a verificare la riconducibilità delle operazioni alla volontà del cliente.
- L'intermediario deve dimostrare, con elementi precisi e concordanti, la condotta incauta e negligente della ricorrente, integrante la colpa grave.
- Ha subito un attacco combinato di smishing e vishing realizzato con tecniche di ingegneria sociale atte a carpire la sua fiducia, in uno stato di allarme e confusione.
- L'SMS apparentemente proveniva dall'intermediario e si inseriva nel flusso di comunicazioni autentiche in ragione del fenomeno di ID sender spoofing.
- L'SMS civetta simulava una procedura di sicurezza credibile, inducendola a un'azione proattiva tale da rafforzare la percezione di autenticità.
- In uno stato di manipolazione psicologica è stata indotta a comunicare i dati della carta e ad approvare la notifica PUSH, nella convinzione di bloccare le operazioni illecite e non autorizzare le nuove transazioni.
- Il sedicente operatore la induceva ad approvare la notifica in quanto risultava un passaggio tecnico della procedura di storno.
- La differenza di importo ha verosimilmente contribuito alla confusione.
- L'intermediario non ha fornito prove concernenti i sistemi efficaci di fraud detection in tempo reale.
- L'operazione presentava diversi profili di anomalia in ragione delle sue abitudini e del contesto temporale immediatamente successivo a una comunicazione sospetta.
- L'intermediario non ha prodotto evidenze circa l'indirizzo IP di provenienza, la geolocalizzazione del dispositivo o la coerenza dell'operazione con il proprio profilo di rischio.

In sede di controrepliche l'intermediario afferma quanto segue.

- La ricorrente ha incautamente comunicato a terzi sconosciuti i dati della propria carta di credito e personalmente eseguito l'operazione disconosciuta.
- L'attacco combinato da smishing e vishing è da tempo conosciuto e oggetto di opportune informative nei confronti della clientela.
- L'SMS truffaldino proveniva da un numero di cellulare che non gli è riferibile e non risultava inserito all'interno di un flusso di comunicazioni autentiche.
- Non ricorre alcun nesso causale tra il danno lamentato dalla ricorrente e la propria condotta.
- La ricorrente deve dimostrare il carattere singolare della transazione contestata.
- I presunti profili di anomalia non sono documentati dalla ricorrente, bensì risultano smentiti dalla realtà dei fatti.

- Non poteva conoscere le comunicazioni avvenute o in corso tra la ricorrente e gli interlocutori, i quali la stavano contattando da numeri che non gli sono riferibili.
- L'indirizzo IP associato alla validazione della notifica PUSH ricorre nelle tracciatore dei giorni precedenti.

DIRITTO

Nella presente vicenda parte ricorrente lamenta di essere stata vittima di smishing misto a vishing e pertanto chiede la restituzione di € 577,80, oltre agli interessi legali dalla data dell'illegittimo addebito al saldo.

Secondo quanto dichiarato dalla stessa nella denuncia sporta all'autorità competente, il 21/06/2025 parte ricorrente riceveva sul proprio cellulare un SMS apparentemente proveniente dall'intermediario che concerneva una transazione di € 980,00 respinta, con invito a contattare subito il numero 028***211 riconducibile al Servizio Sicurezza. Allarmata e convinta della genuinità della comunicazione, contattava senza indugio il numero telefonico indicato e interloquiva con il sedicente operatore L. del servizio di sicurezza dell'intermediario. L'interlocutore la invitava a comunicare i dati della propria carta di pagamento, al fine di individuare quale fosse per poter bloccare le ulteriori operazioni fraudolente e controllare lo strumento di pagamento. Comunicava quindi il numero della carta di credito n. ***5549 con il codice CVV e la scadenza. Seguendo le indicazioni del sedicente operatore, accedeva all'home banking tramite app installata sul suo device e notava un pagamento fraudolento di € 577,80 presso l'esercente L.M.I. L'interlocutore domandava dell'esistenza di un conto associato, la ricorrente rispondeva affermativamente. Insospettita, a questo punto chiedeva all'interlocutore la sua reale identità e quest'ultimo le confermava di averla truffata. Contattava immediatamente la filiale online, raccontando l'accaduto, al fine di bloccare tutti i pagamenti relativi al conto corrente cointestato con la moglie C.S.S. e al suo conto corrente personale. Le parti non precisano alcunché e non allegano evidenza documentale in ordine al blocco dello strumento di pagamento.

Dalla documentazione in atti risulta che l'operazione contestata consiste in un pagamento online di € 577,80 eseguito con carta n. ***5549 il 21/06/2025 a favore dell'esercente L.M.I., la quale può essere così sintetizzata:

DATA GG/MM/AA	ORA	TIPOLOGIA	IMPORTO
21/06/2025	15:23	Pagamento online	€ 577,80

In sede di repliche, la ricorrente afferma che, in uno stato di manipolazione psicologica, è stata indotta a comunicare i dati della carta e ad approvare la notifica PUSH. Nelle controrepliche, l'intermediario

dichiara che la ricorrente ha personalmente eseguito l'operazione disconosciuta. Si rammenta che i Collegi ABF distinguono tra operazioni autorizzate con l'intervento parziale del pagatore (ad esempio, quando il pagatore autorizza l'operazione precedentemente inserita dal frodatore) e operazioni eseguite per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione). Secondo l'orientamento condiviso, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es., 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. Questo è il caso di in esame. Pertanto, si applicano la PSD2 e il d.lgs. n. 11/2010.

Ciò posto in punto di normativa applicabile, il Collegio ricorda che, secondo la disciplina recata dalla PSD2, è innanzi tutto onere dell'intermediario provare che l'operazione è stata autenticata, correttamente registrata e contabilizzata ex art. 10, d.lgs. n. 11/2010: in caso di mancanza della prova l'intermediario sopporta, in ogni caso, integralmente le conseguenze delle operazioni disconosciute. Qualora venga invece fornita la suddetta prova, occorre valutare se alla parte ricorrente sia imputabile una condotta connotata da dolo o colpa grave in violazione agli obblighi sui di lei gravanti in forza dell'art. 7, essendo altrimenti il rischio di operazioni fraudolente a carico dell'intermediario ai sensi dell'art. 12 d.lgs. n. 11/2010. La prova dei fatti a carico dell'utilizzatore dello strumento di pagamento è posta sull'intermediario dall'art. 10 d.lgs. n. 11/2010.

Il Collegio rileva sul punto quanto segue. L'intermediario afferma, e prova, che la ricorrente si connette prevalentemente da app, usando il device identificato con il codice univoco n. EA13***35CF. Nella descrizione dei fatti, questa ammette di aver effettuato l'accesso all'home banking tramite app installata sul suo device. Con riferimento alla fase prodromica, l'intermediario ha allegato il Foglio Tracciatura. L'intermediario dichiara quindi che alle ore 15:23 del 21/06/2025 veniva disposta l'operazione contestata; tramite il device veniva validata la credenziale dinamica OTP, mediante inserimento del PIN in risposta alla notifica PUSH. Sul punto, l'intermediario ha allegato il foglio delle notifiche PUSH, da cui emerge l'invio di una notifica alle ore 15:23 del 21/06/2025 concernente la richiesta di autorizzazione del pagamento di € 557,80 presso l'esercente L.M.I. L'intermediario precisa che nel testo della notifica PUSH sono chiaramente evincibili l'importo, il beneficiario e lo strumento di pagamento. Con riferimento all'inserimento del PIN, l'intermediario ha allegato il Foglio Validazione OTP. La validazione della credenziale dinamica tramite il device associato al profilo della ricorrente determina la conclusione dell'operazione con esito positivo. Pertanto, secondo il Collegio l'operazione è stata autorizzata mediante credenziale dinamica, rappresentata dal codice univoco OTP generato tramite il device n. EA13***35CF, a seguito della validazione della notifica PUSH ricevuta sullo stesso con inserimento del PIN. L'esecuzione dell'operazione disconosciuta ha rispettato i requisiti della "Conoscenza" (il PIN, noto solo al cliente, con conseguente generazione del codice OTP dinamico) e del "Possesso" (il codice è stato generato tramite app installata sul cellulare del ricorrente).

L'intermediario ha, a questo punto, l'onere di dimostrare la colpa grave dell'attrice. Detta prova del dolo o della colpa grave nella custodia dello strumento di pagamento e nell'uso dello stesso può essere

assolta anche attraverso la presunzione, ossia attraverso l'operazione logica che consente di risalire da un fatto noto ad uno ignoto. La stessa Corte di Cassazione, a tale specifico riguardo, ritiene ammissibile la prova indiziaria della sussistenza della colpa grave (v. Cass. civ., Sez. II, 18 gennaio 2010, n. 654). Si deve allora ricorrere ai fatti noti, ovvero ai c.dd. indizi, che, per assurgere al rango di prova presuntiva, debbono però essere gravi, precisi e concordanti, come previsto dall'art. 2729 c.c.

Siffatta prova della colpa grave consiste, più specificamente, nella prova dei fatti che, in connessione tra loro, possono ragionevolmente condurre a ritenere gravemente negligente la condotta del cliente. Come già scritto, siffatta prova può essere fornita anche per mezzo di presunzioni, purché gli indizi siano gravi, precisi e concordanti ai sensi dell'art. 2729 c.c. Si tratta, in altri termini, di valorizzare le singole e specifiche circostanze relative alle fattispecie di volta in volta sottoposte all'esame dell'ABF, in ordine alle quali è necessario verificare se, alla luce degli elementi costitutivi della fattispecie, stretti in intima connessione tra loro, sia possibile desumere in capo all'utilizzatore un comportamento gravemente colposo.

La fattispecie in esame integra gli estremi di smishing misto a vishing. In sede di denuncia, la ricorrente dichiara di aver ricevuto alle ore 15:18 del 21/06/2025 un SMS proveniente dall'intermediario mediante l'utenza +39 344***755, con cui veniva avvertita di una transazione respinta di € 980,00 e invitata a contattare il servizio clienti al numero 028***211. L'istante contattava l'utenza indicata nel messaggio e interloquiva con il sedicente operatore L., a cui comunicava il numero della sua carta di credito, il codice CVV e la scadenza al fine di controllare lo strumento di pagamento. Successivamente, accedeva all'home banking tramite app e notava un pagamento online di € 577,80 nei confronti dell'esercente L.M.I. Il sedicente operatore domandava altresì l'esistenza di un conto associato, a cui rispondeva affermativamente. A quel punto sospettava della situazione e chiedeva all'interlocutore se era veramente un dipendente dell'intermediario: questi confermava di averla truffata. Parte ricorrente ha allegato l'SMS truffaldino ricevuto alle ore 15:18 del 21/06/2025.

Dall'evidenza documentale risulta che nel testo è riportato il nominativo dell'intermediario e che il mittente dell'SMS è un numero di cellulare privato (+39 344***755). Inoltre, il messaggio civetta non risulta inserito nella chat genuina intrattenuta con l'intermediario. Inoltre, nel ricorso e nelle repliche la ricorrente ammette di aver approvato la notifica PUSH, nella convinzione di bloccare le operazioni illecite e prevenire le successive autorizzazioni. In adesione all'orientamento consolidato, il Collegio ritiene che nel caso di smishing/vishing tradizionale, oramai ampiamente noto, l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e a impedire la truffa. Pertanto, valuta come dimostrata la colpa grave della ricorrente che non avrebbe dovuto rispondere ad un messaggio proveniente da un numero non riferibile all'intermediario e tanto meno avrebbe dovuto comunicare i dati della carta, con i quali il truffatore ha effettuato il pagamento che la ricorrente ha altresì autorizzato, nonostante la notifica PUSH "parlante" (cfr. Collegio di Bologna, n. 14643/2019 e n. 492/2026).

Per tutto quanto sopra esposto, il Collegio ritiene il ricorso non meritevole di accoglimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE