

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.

- Il 23/04/2025, verso le ore 17:30, mentre si trovava in vacanza, riceveva una telefonata dal numero *60, corrispondente al centralino dell'intermediario e già memorizzato nella rubrica personale.
- Rispondeva alla chiamata e un interlocutore maschile le comunicava la necessità di provvedere all'aggiornamento di alcuni dati sull'applicazione di home banking del cellulare.
- Sulla base del numero visualizzato, riteneva con certezza di essere in contatto con l'intermediario e seguiva quindi le indicazioni fornite dall'operatore.

- A un certo punto, l'applicazione non risultava più visibile sul cellulare; l'operatore la rassicurava affermando che sarebbe riapparsa a breve e che si sarebbero risentiti l'indomani per ultimare le operazioni.
- La mattina seguente, intorno alle ore 11:00, veniva richiamata dallo stesso numero e dal medesimo interlocutore che le chiedeva i dati della carta debito per collegarla al profilo della nuova app. Comprendeva così che qualcosa non andava e telefonava direttamente all'intermediario: l'operatrice le diceva che era stata vittima di una truffa e passava la chiamata al servizio antifrode. Quest'ultimo le comunicava che erano stati effettuati due bonifici, rispettivamente di € 9.460,00 e € 6.700,00, a favore di soggetti sconosciuti, con i quali non ha mai avuto alcun rapporto.
- A seguito della richiesta di rimborso presentata il 28/04, l'intermediario rispondeva il giorno successivo tramite e-mail, negando il risarcimento con la motivazione che avrebbe tenuto un comportamento colposo.
- Parte ricorrente chiede il risarcimento delle somme indebitamente prelevate.

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

- Parte ricorrente è titolare del conto corrente n. *625 a cui è collegato il servizio "Rapporti a distanza tra Banca e Cliente", c.d. home banking.
- L'istante è caduta vittima di una truffa di spoofing, avendo dato fiducia a una chiamata proveniente dal numero *60, che non è però la modalità ordinaria di contatto in uscita.
- La ricorrente avrebbe seguito le istruzioni di un falso operatore, modificando le impostazioni del proprio account G* per scaricare un'applicazione malevola di terze parti.
- Evidenzia la colpa grave dell'attrice, la quale non si sarebbe insospettita nonostante l'app fosse "sparita" dopo l'aggiornamento e l'operatore avesse fornito spiegazioni assurde sull'interruzione del servizio.
- Le operazioni risultano correttamente autenticate tramite SCA (autenticazione forte) e sono state effettuate dallo smartphone abituale del cliente (Huawei P Smart Pro).
- Il sistema ha inviato regolarmente SMS alert e notifiche push che avrebbero permesso alla ricorrente di bloccare le operazioni, se fosse intervenuta subito.
- Ha effettuato un tentativo di recall dei bonifici, ma la richiesta è stata presentata solo il giorno successivo, quando i bonifici erano ormai irrevocabili secondo la normativa PSD2, avendo superato l'orario di cut-off.
- Rileva che gli importi non erano anomali rispetto allo storico della ricorrente e l'accusa di non aver fornito prove fondamentali, come il link cliccato o il registro chiamate.
- L'intermediario chiede il rigetto del ricorso in quanto infondato.

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

- Ribadisce di non aver mai fornito le proprie credenziali d'accesso o il PIN.
- Contesta la ricostruzione dell'intermediario secondo cui i dati sarebbero partiti dal dispositivo SMART PRO; afferma che, al momento dei fatti, l'app non era più presente o attiva su tale dispositivo.

- Sottolinea come i due bonifici fraudolenti fossero di importi insolitamente elevati rispetto allo storico del conto, che non aveva mai registrato operazioni simili in anni di apertura.
- Nega di aver mai ricevuto gli SMS di notifica push citati dall'intermediario sul proprio numero di cellulare, sostenendo che ciò sarebbe verificabile tramite l'operatore telefonico e un testimone.
- Nonostante la segnalazione dell'illecito sia avvenuta verso le ore 11:30 del 24/04/2025, né l'Ufficio Frodi né il consulente dedicato avrebbero intrapreso azioni concrete per bloccare le transazioni (i bonifici ordinari sono stati eseguiti la sera precedente) fino al 28/04/2025.
- Contesta il fatto che l'intermediario non abbia effettuato alcuna chiamata di verifica per operazioni così rilevanti e che basi la propria difesa solo su report interni, arrivando ad additarla come responsabile per "colpa grave".
- Evidenzia come le comunicazioni ufficiali dell'intermediario esortassero a contattare proprio il numero (*60) da cui è arrivata la telefonata fraudolenta per l'aggiornamento dell'app.

In sede di controrepliche l'intermediario afferma quanto segue.

- Precisa che non è tenuta a verificare preventivamente che le operazioni siano riconducibili all'effettiva volontà del cliente, ma a garantire e assicurare che il processo di esecuzione dell'operazione sia svolto nel rispetto della Strong Customer Authentication, come nel caso concreto è accaduto.
- L'importo dei bonifici oggetto di ricorso non rappresentava un unicum nella pregressa attività bancaria della ricorrente.
- Questa, seguendo acriticamente le indicazioni ricevute al telefono da una persona a lui sconosciuta, ha consentito, sia pur inconsapevolmente, l'installazione sul proprio device di un'applicazione a lui non riferibile, permettendo così al malfattore di carpire le credenziali di accesso all'home banking e di utilizzare da remoto il dispositivo.
- Il fatto di essere stata contattata dal numero *60 avrebbe dovuto insospettire la ricorrente, poiché una banca può solo ricevere telefonate tramite il "numero verde", ma non farle.
- La ricorrente non documenta né le chiamate ricevute, né fornisce il link comunicato dal sedicente operatore sul quale avrebbe cliccato, ovvero non indica l'applicazione di terze parti scaricata.

DIRITTO

Nella presente vicenda parte ricorrente lamenta di essere rimasta vittima di una frode informatica perpetrata tramite una telefonata con la quale un sedicente operatore dell'intermediario la induceva a provvedere all'aggiornamento di alcuni dati sull'applicazione di home banking del cellulare, ciò che consentiva a questo di disporre due bonifici € 9.460,00 e € 6.700,00 a favore di soggetti sconosciuti, dei quali chiede pertanto la restituzione.

Secondo quanto dichiarato dalla stessa nella denuncia sporta all'autorità competente, il 23/04/2025, verso le ore 17:30, mentre si trovava in vacanza, parte ricorrente riceveva una telefonata dal numero *60, corrispondente al centralino dell'intermediario e già memorizzato nella rubrica personale.

Rispondeva quindi alla chiamata e un interlocutore maschile le comunicava la necessità di provvedere all'aggiornamento di alcuni dati sull'applicazione di home banking del cellulare. Sulla base del numero visualizzato riteneva con certezza di essere in contatto con l'intermediario e seguiva quindi le indicazioni fornite dall'operatore. Dopo aver aperto il link dell'applicazione inviatale, l'operatore le comunicava che l'indomani avrebbe ricevuto il PIN per accedere alla nuova app dell'intermediario. La mattina seguente, intorno alle ore 11:00, veniva richiamata dallo stesso numero e dal medesimo interlocutore che le chiedeva i dati della carta di debito per collegarla al profilo della nuova app. Comprendeva così che qualcosa non andava e telefonava direttamente all'intermediario: l'operatrice le confermava che era rimasta vittima di una truffa e passava la chiamata al servizio antifrode. Quest'ultimo le comunicava che erano stati effettuati due bonifici, rispettivamente di € 9.460,00 e € 6.700,00, a favore di soggetti sconosciuti, con i quali non ha mai avuto alcun rapporto. Dichiara altresì che non riusciva ad aprire l'app che era stata disattivata da detto ufficio che aveva anche provveduto a bloccare il conto.

L'intermediario ha riferito di aver effettuato un tentativo di recall dei bonifici, ma la richiesta di revoca è stata presentata solo il giorno successivo, quando i bonifici erano ormai irrevocabili secondo la normativa PSD2, avendo superato l'orario di cut-off.

Dalla documentazione in atti risulta che le operazioni contestate sono n. 2 bonifici, eseguiti in data 23/04/2025, dell'importo di € 9.460,00 e € 6.700,00. Dette operazioni possono essere così sintetizzate:

DATA GG/MM/AA	ORA	TIPOLOGIA	IMPORTO
23/04/2025	17:48	Bonifico	€ 6.700,00
23/04/2025	17:54	Bonifico	€ 9.460,00

Ciò posto in punto di fatto, 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 quanto segue. L'intermediario ha riferito che in fase di accesso all'home banking da app, il sistema di autenticazione prevede: per effettuare il login e le operazioni di inquiry, l'inserimento delle credenziali di sicurezza (numero cliente + PIN, codice statico noto solo al cliente) + codice OTP (One Time Password), codice dinamico generato da Mobile Token- per disporre le operazioni, dopo avere effettuato il login e inserita l'operazione, la stessa deve essere confermata mediante

l'inserimento del PIN + codice OTP generato da Mobile Token. Ha poi precisato che il codice OTP è una password temporizzata valida per un solo utilizzo, in particolare solo per l'operazione richiesta, che viene generata in modo silente dal Mobile Token integrato nell'App che il cliente ha attivato sullo strumento/device che sta utilizzando. Il testo della notifica, che appare sul device e sul quale l'utente deve fare "tap" per autorizzare, indica in chiaro quale operazione/attività si sta autorizzando. Il Mobile Token è una soluzione digitale studiata per garantire i più elevati standard di sicurezza dei pagamenti online: esso permette di generare automaticamente delle password valide per un solo utilizzo (OTP), direttamente sul proprio smartphone (o Tablet), protegge le credenziali di accesso all'Area Clienti e tutte le operazioni dispositive e di pagamento. L'attivazione del Mobile Token è resa possibile esclusivamente attraverso la digitazione delle credenziali di sicurezza (numero cliente + PIN) e del codice OTP inviato al cliente via SMS al cellulare collegato all'home banking, indipendentemente dalla attivazione del servizio SMS Alert. Dai log allegati dall'intermediario emerge la presenza del codice OTP e il corretto inserimento del codice PIN ("PIN inviato: SI", "PIN verificato: Verifica OK").

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.

Da quanto affermato in denuncia, il Collegio rileva che la ricorrente riceveva una telefonata da utenza riferibile all'intermediario, nel corso della quale un operatore, col pretesto di aggiornare i dati sull'applicazione di home banking, le chiedeva di modificare alcune impostazioni del suo account G* per potergli condividere il link di un'altra applicazione. L'intermediario evidenzia come la truffa non avrebbe potuto perfezionarsi senza la collaborazione della ricorrente, che ha consentito, sia pur inconsapevolmente, l'installazione sul proprio device di un'applicazione non riferibile all'intermediario, permettendo, così, al malfattore di carpire le credenziali di accesso all'home banking e di utilizzare da remoto il dispositivo. Il convenuto, pur dando atto che la ricorrente è stato vittima di caller id spoofing (consistente nell'effettuazione di chiamate da utenza telefonica a lui riferibile), ritiene che, nel caso in esame, l'attrice versi in colpa grave, dal momento che è noto che il proprio numero verde possa esclusivamente ricevere chiamate e non farle.

Il Collegio ricorda che, con riguardo alla tecnica fraudolenta del caller id spoofing, l'orientamento condiviso è nel senso di escludere o attenuare la colpa grave dell'utente secondo le circostanze del

caso, in considerazione dell'insidiosità di tali tecniche fraudolente (Collegio di Bologna, n. 4457/2024). Nel caso di specie, il modo in cui la truffa è stata perpetrata si discosta dal vishing classico attuato con modalità tipiche e ampiamente note, dove la colpa grave del cliente è causa sufficiente dell'evento dannoso. Nella presente vicenda, la ricorrente è stata chiamata dal numero verde apparentemente riferibile all'intermediario e ha ricevuto la richiesta di aggiornare l'app. In questa prima fase non le sono state chieste le credenziali degli strumenti di pagamento o di effettuare delle disposizioni, bensì soltanto di collaborare all'aggiornamento della app, ciò che l'istante faceva permettendo così al malfattore di carpire le credenziali di accesso all'home banking e di utilizzare da remoto il device. La ricorrente afferma che a quel punto l'applicazione non risultava più visibile sul suo cellulare, essendo stata manipolata e controllata dal frodatore, quindi non essendo probabilmente visibili neppure gli sms e le notifiche push dei bonifici. Le caratteristiche della collaborazione posta in essere dalla ricorrente seguendo le fraudolente indicazioni del malvivente sono state tali da determinare una percezione erronea della vittima, cosicché la condotta tenuta dalla stessa è caratterizzata sì da colpa, ma non da grave negligenza (cfr. Collegio di Bologna, n. 4457/2024). A conforto di siffatta valutazione il Collegio rileva che l'istante, quando ha ricevuto la seconda telefonata dallo stesso numero, ha prontamente compreso la truffa nel momento in cui le venivano invece chiesti i dati della carta di debito e ha subito chiamato l'intermediario. Questa pronta reazione dell'attrice è connotata da una diligenza tale da averle consentito di impedire la produzione di ulteriori perdite in capo alla stessa. Pertanto, il Collegio ritiene che la condotta della ricorrente sia solamente colposa, per avere la stessa consentito inconsapevolmente il controllo del proprio cellulare a malfattori, avendo scaricato una app non dell'intermediario. Com'è noto, in caso di colpa non grave la disciplina in materia prescrive che le operazioni disconosciute siano totalmente a carico del PSP.

Per tutto quanto sopra esposto, il Collegio ritiene il ricorso meritevole di accoglimento e riconosce il diritto della ricorrente a ottenere dall'intermediario della somma complessiva di € 16.160,00.

PER QUESTI MOTIVI

Il Collegio in accoglimento del ricorso dichiara l'intermediario tenuto in favore della parte ricorrente alla restituzione dell'importo complessivo di euro 16.160,00 (sedicimilacentosessanta/00).

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di Euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di Euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE