

COLLEGIO DI BOLOGNA

composto dai signori:

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

Relatore LUCA DI NELLA

Seduta del 20/01/2026

FATTO

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

- Il 29/04/2025 riceveva un SMS fraudolento che, simulando una comunicazione di allerta dell'intermediario, la invitava a contattare un numero telefonico per bloccare una presunta operazione anomala.
- Preoccupata per la sicurezza dei propri risparmi, contattava detto numero, interloquendo con un truffatore che, spacciandosi per un operatore dell'intermediario, la raggirava inducendola a compiere delle operazioni sul proprio dispositivo con la falsa motivazione che fossero necessarie per attivare una procedura di sicurezza.

- Pochi istanti dopo, si avvedeva che la sua buona fede era stata carpita per autorizzare, a sua insaputa e contro la sua volontà, un bonifico istantaneo di € 1.900,00 in favore di un beneficiario a lei totalmente sconosciuto.
- Provvedeva immediatamente a contattare l'intermediario per ottenere il blocco di tutti i suoi strumenti di pagamento e sporgeva denuncia-querela.
- In data 20/06/2025 veniva inoltrato formale reclamo all'intermediario, richiedendo il dovuto rimborso.
- A causa del necessario blocco della sua carta di pagamento, per tutti i mesi successivi è stata privata di qualsiasi strumento di pagamento elettronico, vedendosi costretta, per ogni minima necessità di contante, a recarsi personalmente presso lo sportello della filiale durante gli orari di apertura.
- La difesa dell'intermediario, limitandosi a constatare l'uso delle credenziali, è insufficiente a superare la presunzione di responsabilità a suo carico.
- La condizione di consumatore anziano e non digitalizzato esclude che la sua condotta possa integrare una "colpa grave".
- L'operazione contestata era oggettivamente anomala e avrebbe dovuto attivare i sistemi di sicurezza dell'intermediario, trattandosi del primo e unico bonifico istantaneo disposto, di importo significativo e verso un nuovo beneficiario.
- Il prolungato disagio subito in seguito alla particolarmente gravosa privazione di uno strumento di pagamento costituisce un danno non patrimoniale meritevole di considerazione, essendo esso diretta conseguenza della frode e del successivo rifiuto dell'intermediario di risolvere la questione tempestivamente.
- Parte ricorrente chiede, in via principale, la condanna dell'intermediario alla restituzione della somma di € 1.900,00, oltre interessi legali dal giorno dell'indebito addebito (29.04.2025); in ogni caso, la refusione del contributo versato per l'attivazione della procedura.

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

- La ricorrente è titolare del conto n. *409.
- L'operazione oggetto di contestazione è stata disposta dal device usualmente utilizzato dalla ricorrente per l'operatività online, avente chiave 8f6b8ca17f8d9c22 previo inserimento del PIN, per cui deve qualificarsi come operazione autorizzata ai sensi dell'art. 5, commi 1 e 2, d.lgs. 11/2010.
- Per accedere ai servizi online è richiesto l'inserimento simultaneo del codice Titolare, del codice PIN e del codice O*.
- Il codice O* viene generato:
 - o via software dall'APP, per i clienti che hanno attivato *Smart;
 - o via SMS (inoltrato sul numero di telefono certificato), per i clienti che hanno attivato *SMS;
- Per aumentare ulteriormente il livello di sicurezza di alcune disposizioni di pagamento, oltre alla consueta autenticazione e conferma con codice dinamico, è richiesto al cliente di rispondere alle domande di sicurezza precedentemente censite e/o l'inserimento di un secondo codice inviato via SMS.

- Ha ottenuto la certificazione ISO/IEC 27001 che rappresenta la garanzia che il sistema di gestione adottato è in grado di offrire massimi livelli di sicurezza nell'utilizzo dei servizi della banca online e dei sistemi di pagamento elettronici.
- Ha disposto un'ampia informativa sul proprio sito internet dove viene sempre sottolineato di prestare attenzione alle e-mail, sms e telefonate sospette e di diffidare da link che prevedano l'inserimento di password.
- La ricorrente si connette prevalentemente usando un device "A34" identificato dal codice univoco "8f6b8ca17f8d9c22".
- L'operatività contestata è stata attuata con tale device.
- Il 29/04/2025 alle 21:06:44 da app si evidenzia un accesso dal device in uso alla ricorrente, identificato dal codice univoco "8f6b8ca17f8d9c22" realizzato mediante validazione dell'OTP generato dall'app.
- Alle ore 21:17:25, dalla app installata sul device della ricorrente viene effettuato l'inserimento di un bonifico istantaneo di € 1.900,00 dal conto avente IBAN *409 verso l'IBAN *311 a favore di S.S., la transazione è stata validata tramite inserimento del PIN.
- L'operazione in oggetto è stata autorizzata mediante l'utilizzo di credenziali dinamiche e verifiche di sicurezza e ha rispettato i due requisiti richiesti dalla SCA.
- Ha bloccato due ulteriori tentativi di bonifico, trasmettendo al cellulare certificato del ricorrente alle ore 21:22:11 e 21:28:33 le relative comunicazioni.
- L'operatività disconosciuta è avvenuta tramite l'utilizzo del device con chiave "8f6b8ca17f8d9c22", utilizzato in precedenza dalla ricorrente durante sessioni di operatività dell'esecuzione di operazioni.
- In merito al c.d. "danno da disagio" lamentato dalla ricorrente si rileva che alcuna prova viene fornita in merito sia alla sua esistenza, sia al suo valore.
- Non poteva che considerare autorizzato il pagamento effettuato direttamente dalla ricorrente.
- L'intermediario chiede di non accogliere il ricorso in quanto la richiesta risarcitoria è immotivata e infondata.

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

- Le difese dell'intermediario si fondano su un assunto errato, cioè sulla pretesa di valutare la condotta della ricorrente sulla base di un parametro astratto di "utente digitale esperto", ignorando completamente sia la situazione soggettiva concreta del cliente, sia l'oggettiva anomalia dell'operazione contestata che avrebbe dovuto senz'altro attivare i presidi di sicurezza.
- Non si tratta quindi di negligenza, ma di un consenso estorto con l'inganno a un soggetto vulnerabile.
- Non dispone mai bonifici, quindi non possiede la perizia tecnica necessaria per gestire autonomamente tali strumenti, rendendo palese come l'operazione contestata sia stata possibile solo perché la sua volontà è stata eterodiretta passo dopo passo dal truffatore.
- È inaccettabile che i sistemi di monitoraggio dell'intermediario non abbiano intercettato una deviazione così macroscopica dal profilo transazionale abituale della ricorrente.

- Il fatto che un'operazione così palesemente anomala per tipologia (mai usata prima), importo e beneficiario non abbia generato alcun alert di sicurezza o blocco preventivo costituisce una violazione degli obblighi di diligenza professionale e custodia tecnica.
- La truffa è nota come SMS spoofing.
- Non avendo adottato presidi tecnici capaci di impedire che terzi si inseriscano nel canale di comunicazione riservato o non avendo dismesso l'uso di un canale insicuro, l'intermediario accetta il rischio che la propria clientela venga tratta in inganno.
- La presenza della SCA non giustifica il mancato intervento dei sistemi di fraud detection, i quali avrebbero dovuto bloccare l'operazione in quanto incoerente con il profilo storico della ricorrente.
- La SCA prova l'identificazione del dispositivo e dell'utente, ma non prova la genuina volontà dispositiva: ha eseguito la procedura di autenticazione nella ferma convinzione – indotta dal raggio – di compiere un atto conservativo (blocco conti) e non dispositivo.
- L'intermediario, inoltre, non ha fornito prova rigorosa che la ricorrente, al momento dell'autorizzazione, abbia avuto piena ed effettiva contezza del c.d. dynamic linking (collegamento dinamico tra codice, importo e beneficiario).

In sede di controrepliche l'intermediario afferma quanto segue.

- Non occorre una dimestichezza con strumenti digitali avanzati per effettuare operazioni mediante il servizio di banca online, strumento peraltro che la ricorrente utilizza già da svariato tempo.
- Non gli è dato sindacare né la tipologia di operazioni poste in essere dalla clientela, né la frequenza con cui vengono disposte.
- Non è stata fornita alcuna allegazione a sostegno della possibilità di ricondurre la fattispecie in oggetto alla tipologia dell'SMS spoofing.
- La colpa grave della ricorrente emerge dalle dichiarazioni da lei rilasciate in denuncia.
- Nel nostro ordinamento l'avvenuta autorizzazione esclude, di per sé, il rimborso delle operazioni autorizzate, a prescindere da eventuali coartazioni della volontà del pagatore avvenute a monte del processo autorizzativo.

DIRITTO

Nella presente vicenda parte ricorrente lamenta di essere rimasta vittima di una frode perpetrata tramite un sms apparentemente inviato dall'intermediario e una telefonata, da lei attivata, con la quale un sedicente operatore del convenuto la guidava nella disposizione di un bonifico sul proprio dispositivo a favore di un beneficiario sconosciuto e chiede pertanto il rimborso di € 1.900,00, oltre interessi legali dalla data dell'indebito addebito sul proprio conto di tale somma.

Secondo quanto dichiarato dalla stessa nella denuncia sporta all'autorità competente, parte ricorrente ha ricevuto alle 18:04 del 29.04.2025 un sms da parte di un numero a lei sconosciuto che le notificava un addebito di € 602,10 sulla carta e le indicava un numero da chiamare in caso di anomalie o per reclami. In totale buona fede contattava detto numero e chiedeva spiegazioni sull'sms. Le rispondeva un uomo che si dichiarava essere un operatore dell'intermediario e le chiedeva informazioni sul suo conto corrente. Nello specifico, le suggeriva come bloccare questa pseudo anomalia che veniva riscontrata sul conto. Parte ricorrente forniva al sedicente operatore tutte le informazioni in suo possesso, quindi lo metteva in condizione di accedere al suo conto. Lo stesso giorno alle ore 21:22 riceveva due sms dall'intermediario che la informavano che, per motivi di sicurezza, non è stato possibile portare a termine l'operazione. A questo punto si rendeva conto di essere rimasta vittima di una frode. Il giorno successivo, recatasi in filiale per avere ulteriori dettagli, le veniva spiegato che era stata aggirata e che a causa della truffa aveva inconsapevolmente accreditato la somma di € 1.900,00 a favore di persona a lei ovviamente sconosciuta. L'operatore le riferiva che erano stati bloccati dall'intermediario due ulteriori movimenti fraudolenti. Per motivi di sicurezza l'intermediario le ha bloccato il conto e le carte.

Quanto dichiarato dalla ricorrente in denuncia, nel ricorso e nelle repliche pone la questione della disciplina applicabile, posta dall'intermediario con l'eccezione di inapplicabilità della normativa di cui al d.lgs. n. 11/2010 dal momento che l'operazione in contestazione è stata autenticata dalla ricorrente tramite il device utilizzato abitualmente dalla stessa per l'operatività online. Il Collegio rileva che la ricorrente in denuncia afferma di aver fornito al truffatore tutte le informazioni in suo possesso che le venivano richieste, quindi metteva il truffatore nelle condizioni di accedere al conto bancario; nelle repliche precisa che, non possedendo la perizia tecnica necessaria per gestire autonomamente gli strumenti informatici, l'operazione contestata è stata possibile solo perché la sua volontà è stata eterodiretta passo dopo passo dal truffatore, e dichiara che ha eseguito la procedura di autenticazione nella ferma convinzione, indotta dal raggirò, di compiere un atto conservativo (blocco conti) e non dispositivo. Pertanto, emerge con chiarezza che la ricorrente ha compiuto personalmente l'operazione contestata 'sotto dettatura' con il proprio device. Questo fatto trova conferma nella documentazione esibita dall'intermediario, la quale dimostra che il bonifico è stato disposto tramite app installata sul device utilizzato in precedenti occasioni dalla ricorrente. Ciò acclarato, il Collegio rileva che secondo l'orientamento condiviso sul punto, quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2. In questi casi, dunque, non è configurabile una responsabilità oggettiva del PSP. Il Collegio può comunque rilevare una responsabilità concorrente del PSP, sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode (ad esempio, nei casi di mancata disponibilità, anche temporanea, del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore; di mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, cui il pagatore si sia rivolto esponendo le richieste del frodatore; di mancato rilievo di indizi di frode nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella

convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere).

Individuata la normativa applicabile, occorre valutare la condotta delle parti alla luce del diritto comune. La ricorrente afferma nel ricorso che, il 29/04/2025, è stata vittima di una frode iniziata con la ricezione di un sms ingannevole, apparentemente inviato dal proprio istituto bancario, che segnalava un addebito sospetto di € 602,10. In denuncia dichiara invece che il messaggio proveniva da un numero a lei sconosciuto. Comunque sia, indotta in errore, la vittima ha contattato il numero indicato nel messaggio, parlando con un truffatore che, spacciandosi per un operatore dell'intermediario, l'ha convinta a fornire "informazioni" che gli permettevano di accedere al conto con il pretesto di bloccare l'operazione anomala. A sostegno delle proprie dichiarazioni, la ricorrente allega copia del verbale di denuncia; non risulta invece versata in atti evidenza dell'sms civetta, né della chiamata truffaldina, quindi del numero a cui si è rivolta. Non risulta dunque provato lo spoofing, a cui si richiama la ricorrente. Orbene, l'orientamento consolidato dei Collegi è nel senso di ritenere che in ipotesi di smishing/vishing l'impiego di una media diligenza sia sufficiente a scongiurare il pericolo e a impedire la truffa (v., tra i tanti, Collegio di Bologna n. 14643/2019). Alla medesima conclusione si giunge anche nei casi manipolativi di social hacking, come quello in esame in cui non è accertabile la provenienza della chiamata da un numero falsamente riferibile all'intermediario (cfr. Collegio di Bologna, n. 3082/2025). In queste fattispecie, pertanto, si ritengono sussistenti gli estremi della colpa grave in capo all'utente che comunica le proprie credenziali e password a estranei e collabora attivamente con loro, eseguendone pedissequamente le istruzioni che portano al perfezionamento della frode. Un comportamento improntato sulla diligenza media è sufficiente a evitare gli effetti di siffatte attività illecite, indipendentemente dall'età, dalla dimestichezza con gli strumenti informatici e dalla fragilità del cliente, eccepite dalla ricorrente come circostanze esoneranti dalla colpa grave.

Quanto alla condotta dell'intermediario, il Collegio rileva che allo stesso non sono imputabili fatti fondativi della sua responsabilità, anche solo concorrente. In primo luogo, l'intermediario ha provato l'invio dell'sms alert relativo all'operazione contestata e di aver effettuato un tentativo di recall in data 30/04/2025, non andato però a buon fine. Inoltre, non si riscontrano nel caso in esame gli indicatori di anomalia previsti dal D.M. n. 112 del 2007. La parte ricorrente eccepisce invece che l'operazione presentava indizi di anomalia macroscopici in quanto si trattava della prima disposizione di bonifico istantaneo e l'operazione era di importo elevato e a favore di un beneficiario sconosciuto. Allega, al riguardo, l'estratto conto dal 1°.01.2025 al 25.09.2025. Orbene, il Collegio ritiene che il fatto di aver disposto per la prima volta un bonifico istantaneo di importo elevato nel lasso di tempo di cui all'estratto conto non integri di per sé un indice di anomalia. In generale, si osserva che gli intermediari non sono tenuti al controllo preventivo di un'operazione, se non in circostanze particolari di evidenti anomalie o malfunzionamenti o altre circostanze che inducano dei sospetti sull'operazione: elementi, questi, che non si riscontrano nella fattispecie in esame, caratterizzata peraltro dal fatto che l'operazione è stata disposta dal device della ricorrente. Al contrario, due successivi bonifici sono invece stati bloccati in quanto questi mostravano delle criticità di cui il sistema dell'intermediario ha tenuto conto, reagendo corrispondentemente e trasmettendo alle ore 21:22:11 e 21:28:33 gli sms alert al cellulare certificato della ricorrente, come confermato dalla stessa nella denuncia.

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

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE