

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 FRANCESCO VELLA

Seduta del 31/03/2026

FATTO

Parte ricorrente, premesso di essere titolare di un conto corrente presso l'intermediario convenuto, come di seguito ricostruisce i fatti accaduti. In data 21/10/2025 era contattata telefonicamente da un soggetto qualificatosi come operatore antifrode della banca, che segnalava presunti accessi abusivi e la induceva ad accedere all'app di mobile banking e ad autorizzare un aumento del limite dei bonifici fino a € 20.000,00, presentandolo come misura di sicurezza. Precisa di non aver mai comunicato a terzi credenziali personali (PIN, password, OTP), limitandosi ad autorizzare l'innalzamento del massimale. Subito dopo la chiamata veniva eseguito un bonifico di € 20.000,00 verso un beneficiario sconosciuto, mai autorizzato. Sporgeva immediata denuncia-querela e disconosceva l'operazione presso la banca, presentando quindi reclamo con il quale chiedeva il rimborso dell'importo sottratto, che la banca negava, sostenendo la corretta autorizzazione dell'operazione, senza provare la sua

colpa grave. Argomenta che ai sensi del D. Lgs. n. 11/2010, la banca è tenuta a rimborsare le operazioni non autorizzate e a dimostrare l'eventuale frode o colpa grave dell'utente e, nel caso concreto, l'intermediario non ha fornito prova della riconducibilità dell'operazione alla cliente né della sua colpa grave. Infatti la sua condotta non integra colpa grave, in quanto: non vi è stata comunicazione di credenziali; la truffa era sofisticata e idonea a ingannare un utente diligente; l'autorizzazione prestata riguardava un'operazione diversa (aumento del limite) rispetto al bonifico fraudolento. Aggiunge che la banca è inoltre responsabile per carenze nei sistemi di sicurezza, non avendo bloccato o segnalato un'operazione anomala di elevato importo verso beneficiario sconosciuto e l'intermediario non ha dimostrato la conformità e sicurezza del sistema di autenticazione forte (SCA), né prodotto adeguati log informatici e, pertanto, la responsabilità dell'operazione fraudolenta deve ricadere su quest'ultimo e il ricorso, con il quale si chiede il rimborso dell'operazione fraudolenta subita, deve essere accolto.

L'intermediario nelle controdeduzioni sostiene che il ricorso deve essere respinto in quanto il bonifico di € 20.000,00 è stato disposto direttamente dalla cliente tramite la propria App, dopo aver volontariamente innalzato i limiti operativi. Tanto premesso, in via preliminare parte resistente eccepisce che il ricorso sarebbe inammissibile per assenza di un reclamo preventivo, che non risulta agli atti. Nel merito, dichiara che la ricostruzione della controparte è generica e priva di prove, in quanto non vengono forniti elementi sulla telefonata ricevuta né sul numero chiamante. Inoltre, l'innalzamento dei massimali è stato effettuato autonomamente dalla cliente mediante autenticazione forte (PIN e riconoscimento biometrico) e le evidenze informatiche dimostrano che il bonifico è stato eseguito dalla cliente tramite App (canale 016) ed autorizzato correttamente. Evidenzia inoltre che dalla denuncia emerge che la cliente è stata contattata da un numero non riconducibile alla banca, ha interagito con il truffatore per due giorni senza effettuare verifiche, ha disposto autonomamente il bonifico dopo aver aumentato i limiti, non ha contattato il servizio clienti né verificato la veridicità delle comunicazioni ricevute e il telefono utilizzato è sempre rimasto nella sua disponibilità. Osserva che la truffa subita rientra in fenomeni noti di vishing e SMS spoofing, caratterizzati da messaggi palesemente anomali e riconoscibili. L'SMS ricevuto presentava elementi evidenti di falsità (numero non riconducibile alla banca, errori, contenuto generico), che avrebbero dovuto insospettire la cliente, la quale non ha effettuato alcuna verifica preventiva (motori di ricerca, contatto banca, confronto con terzi). Evidenzia altresì che vi è incoerenza tra il contenuto dell'SMS (bonifico di € 1.750,00) e l'operazione disposta (€ 20.000,00), che il bonifico era ordinario ma verso un IBAN dell'intermediario, quindi di fatto immediatamente accreditato e non revocabile e, inoltre ha inviato una notifica di alert al momento dell'operazione. Conclude che secondo l'orientamento ABF, quando l'operazione è eseguita direttamente dal cliente con autenticazione completa, essa deve considerarsi autorizzata e non emergono profili di responsabilità della banca né carenze nei sistemi di sicurezza, non risultano anomalie tecniche, intrusioni o vulnerabilità del sistema, il sistema utilizzato rispetta i requisiti di autenticazione forte (SCA), oltre al fatto che l'intermediario può valutare solo la correttezza formale dell'autorizzazione e non le motivazioni soggettive del cliente.

Parte resistente chiede il rigetto del ricorso.

La ricorrente replica che le controdeduzioni dell'intermediario sono infondate e in parte contraddittorie e non scalfiscono la fondatezza del ricorso. Infatti, l'eccezione di inammissibilità per mancanza di reclamo preventivo è pretestuosa, poiché il "Modulo Disconoscimento Importo" costituisce a tutti gli

effetti un reclamo scritto e contiene l'identificazione del cliente, la contestazione dell'addebito e la richiesta di rimborso. Inoltre, la banca ha risposto con e-mail di rigetto del 22/10/2025, dimostrando di aver ricevuto ed esaminato il reclamo. Prosegue dichiarando che l'intermediario ha invertito illegittimamente l'onere della prova, che grava invece sulla banca ai sensi del D.Lgs. 11/2010, e non ha dimostrato correttamente l'applicazione della SCA, in quanto i log prodotti sono generici e privi di tracciatura tecnica dettagliata, manca prova dei due fattori di autenticazione indipendenti, manca prova del collegamento dinamico tra autorizzazione, importo e beneficiario, manca prova della SCA relativa all'innalzamento dei massimali. Argomenta che la mera produzione di log informatici non è sufficiente a dimostrare né l'autorizzazione né la colpa grave della cliente, in relazione alla quale la banca non ha fornito elementi concreti idonei a provarla, neppure in via presuntiva. Ancora, responsabilità dell'intermediario emerge anche per violazione della diligenza dell'accorto banchiere, in quanto: la sequenza operativa registrata costituisce uno schema tipico di frode e vi sono molteplici indici di anomalia (errore PIN, accesso ravvicinato, aumento massimale, bonifico di pari importo al limite, beneficiario nuovo), che i sistemi della banca non hanno rilevato né bloccato, e la mancata attivazione di sistemi antifrode adeguati integra una grave negligenza dell'intermediario. Argomenta ancora che l'operazione deve qualificarsi come non autorizzata, poiché la volontà della cliente è stata viziata da raggirio (vishing) e la cliente ha autorizzato solo l'aumento del massimale, non eseguito il bonifico. Conclude che non sussiste una sua colpa grave in quanto non ha comunicato credenziali personali (PIN, password, OTP) ed è stata vittima di una truffa sofisticata e insidiosa, posto che le tecniche di vishing sono idonee a ingannare anche utenti diligenti. Infatti, la giurisprudenza e l'ABF escludono la colpa grave in presenza di frodi basate su social engineering, specie in assenza di comunicazione di credenziali.

Nelle controrepliche la resistente richiama integralmente le precedenti difese e i documenti già prodotti e ribadisce di aver provato, tramite evidenze informatiche, la corretta autenticazione e autorizzazione del bonifico disposto dalla cliente tramite App. Sostiene che anche l'innalzamento dei massimali è stato effettuato direttamente e consapevolmente dalla cliente e ribadisce che è stata applicata correttamente la SCA, basata su un fattore di possesso (App sul cellulare della cliente) ed fattore di conoscenza (MPIN noto solo alla cliente). Evidenzia che la cliente stessa, in denuncia, ammette di aver eseguito le operazioni su indicazione del truffatore. Pertanto, la frode è stata resa possibile dal comportamento della cliente, che ha seguito le istruzioni del truffatore, configurando un concorso colposo grave. Dichiaro che tutti i sistemi di sicurezza della banca erano attivi e funzionanti, senza violazioni o anomalie tecniche ed evidenzia di aver adottato misure informative e preventive (avvisi, e-mail, sito) per mettere in guardia i clienti dalle truffe. Contesta infine la condotta della cliente per non aver effettuato verifiche sul messaggio e sul numero chiamante, né aver contattato la banca o terzi.

DIRITTO

Il Collegio esamina in primo luogo l'eccezione preliminare eccepita dall'intermediario, relativa all'inammissibilità del ricorso per mancanza di reclamo. L'eccezione non merita accoglimento. In base al paragrafo 1 (Avvio del procedimento), Sezione VI delle "Disposizioni sui sistemi di risoluzione stragiudiziale delle controversie in materia di operazioni e servizi bancari e finanziari della Banca d'Italia, che regolano il funzionamento dell'ABF", il ricorso all'ABF deve essere preceduto da un reclamo

preventivo all'intermediario, circostanza che indica una vera e propria condizione di procedibilità del ricorso (Collegio di Coordinamento, decisione n. 5304/2013). La definizione di reclamo è contenuta alla Sezione I del medesimo provvedimento, il cui paragrafo 3 (Definizioni), definisce quale reclamo "ogni atto con cui un cliente chiaramente identificabile contesta in forma scritta (es. lettera, fax, email) all'intermediario un suo comportamento anche omissivo". Nel modulo del ricorso odierno, la data del reclamo viene indicata al 21/10/2025, come pure si indica che l'intermediario vi ha fornito riscontro nel termine di 15 giorni. Parte ricorrente in sede di repliche, afferma che "la documentazione relativa alla denuncia sporta, include non solo il verbale di denuncia-querela, ma anche il "Modulo Disconoscimento Importo (CLAIM FORM)" (Id. Pratica: 959) presentato dalla cliente presso la filiale in data 21/10/2025," e produce anche la corrispondenza intercorsa con l'intermediario. In base al costante orientamento dell'ABF, il reclamo non deve rivestire alcuna particolare forma rituale, come pare al contrario indicare la comunicazione della banca in atti, ma è solo necessario che contenga una contestazione di un comportamento, seppure omissivo. Il reclamo ha infatti in questo sistema di risoluzione delle controversie la funzione di consentire all'intermediario, in sede di risposta, versata in atti, di giungere ad una composizione della controversia insorta già nella sua fase iniziale, prima che si instauri un vero e proprio contenzioso. In particolare, per quanto attiene le operazioni disconosciute, secondo l'orientamento costante dei Collegi, il modulo di disconoscimento di una operazione ha valore di reclamo ed il rigetto della richiesta di rimborso costituisce rigetto del reclamo.

Ciò posto, parte ricorrente contesta un'operazione di bonifico eseguita tramite l'app dell'intermediario convenuto in data 21/10/2025 di importo pari a € 20.000,00. L'intermediario specifica che i bonifici infra-banca hanno un'esecuzione in tempo reale e sono caratterizzati dalla non annullabilità.

Il Collegio in primo luogo precisa che l'operazione contestata è disciplinata dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del d.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

L'art. 12 del d. lgs. n. 11/2010 regola il regime della responsabilità a fronte dell'utilizzo non autorizzato di strumenti e servizi di pagamento. La disposizione, con un evidente *favor* nei confronti dell'utilizzatore, opera uno spostamento della responsabilità in capo al prestatore dei servizi di pagamento in caso di utilizzo fraudolento, estendendola a tutte le ipotesi di violazione degli obblighi di custodia e sicurezza non caratterizzate da frode, dolo o colpa grave. Ne consegue che, nel caso in esame, al fine di escludere la responsabilità della parte ricorrente, è necessario escludere che il suo comportamento possa configurarsi quale colpa grave. Sul punto deve essere richiamato l'art. 7, comma 3 del d. lgs. n. 11/2010, in base al quale l'utente "adotta tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate".

Tuttavia, ai sensi del 1° comma dell'art. 10 del d. lgs. n. 11/2010, nel caso di un'operazione di pagamento disconosciuta, il prestatore del servizio è tenuto a "provare che l'operazione di pagamento 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".

Deve ancora richiamarsi l'art. 10 bis, comma 1, del d. lgs. n. 11/2010, il quale, recependo l'art. 98 della direttiva UE 2015/2399, sancisce l'obbligo per i prestatori di servizi di pagamento di applicare "l'autenticazione forte del cliente" nei casi in cui questi acceda al proprio conto di pagamento on line, effettui un'operazione o "qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi".

Quanto all'esecuzione dell'operazione oggetto della controversia, le evidenze informatiche disposte dalla banca confermano il fatto che la transazione è stata eseguita dalla cliente attraverso la propria APP, installata sul proprio cellulare (canale 016), il 21/10/2025 e dalla stessa debitamente autorizzata alle ore 00:15 alla propria APP a cui si era collegata con doppio fattore autenticazione PIN (in possesso solo della ricorrente) e fattore biometrico Fingerprint. Si tratta di documentazione che il Collegio ritiene idonea a dimostrare la corretta autenticazione a doppio fattore dell'operazione contestata.

Il Collegio oltre a ciò è però tenuto, al fine di attribuire le conseguenze patrimoniali della frode al titolare dello strumento di pagamento (cfr. Collegio di Coordinamento, decisione n. 22745/2019), a valutare la sussistenza o meno della colpa grave dello stesso ed ogni altro fatto, in base a tutte le circostanze allegate. In sintonia con l'orientamento espresso sul punto dalla Corte di Cassazione, l'uniforme giurisprudenza dell'ABF qualifica la colpa grave come "un comportamento consapevole dell'agente che, senza volontà di arrecare danno agli altri, operi con straordinaria e inescusabile imprudenza o negligenza, omettendo di osservare non solo la diligenza media del buon padre di famiglia, ma anche quel grado minimo ed elementare di diligenza generalmente osservato da tutti" (cfr. per una simile prospettiva, in tema di gravità della colpa, Cass. civ., 19 novembre 2001, n. 14456; Collegio di Milano, decisioni n. 40/2012 e n. 2310/2011; Collegio di Roma, decisioni n. 2157/2011 e n. 712/2010). Si tratta, evidentemente, non di una semplice distrazione o negligenza, bensì di "un comportamento abnorme e, in quanto tale, non scusabile". Nel caso in specie la frode subita dalla ricorrente è inquadrabile nello schema del c.d. sms spoofing e l'intermediario deduce la colpa grave della cliente evidenziando come il bonifico di € 20.000,00 sia stato disposto direttamente dalla stessa tramite la propria App, dopo aver volontariamente innalzato i limiti operativi.

La colpa grave della cliente sarebbe presuntivamente ricavabile dalla sua collaborazione con il truffatore - con cui ha interloquito per due giorni senza effettuare verifiche e senza contattare i servizi di assistenza della banca - e dal non aver prestato la dovuta attenzione al fatto che vi fosse incoerenza tra il contenuto dell'SMS (bonifico di € 1.750,00) e l'operazione disposta (€ 20.000,00), evidenziando altresì che l'operazione veniva disposta alle ore 00.15 e la ricorrente avrebbe potuto effettuare il cut off fino alle 20.00. D'altra parte, la ricorrente contesta le deduzioni avverse in merito alla propria condotta gravemente colposa ed alla prova che l'intermediario assume aver fornito in merito. In particolare, evidenzia che non vi è stata comunicazione di credenziali e che la truffa era sofisticata e idonea a ingannare un utente diligente e che l'autorizzazione prestata riguardava un'operazione diversa (aumento del limite) rispetto al bonifico fraudolento.

Con riguardo alle fattispecie di sms spoofing, l'orientamento condiviso dal Collegio ABF è nel senso di ritenere che quando il cliente è vittima di questo tipo di truffa non può essere in genere ravvisata una sua colpa grave, salvo che il messaggio civetta presenti indici di inattendibilità o anomalia che dovrebbero allertare l'utente avveduto.

Nel caso in esame, la ricorrente ha essa stessa disposto le due operazioni che hanno consentito la truffa - come emerge dal fatto che sono state autorizzate dal device in suo possesso -, incautamente seguendo le istruzioni ricevute al telefono da uno sconosciuto, dando seguito a messaggi ricevuti da un'utenza non riconducibile alla resistente e redatti in modo generico e con errori, ed ha ricevuto peraltro anche un sms di alert, dalla stessa parte ricorrente versato in atti, che la informava della transazione che aveva disposto, ciò che avrebbe potuto e dovuto allarmarla ed indurla a contattare la banca, così da procedere in tempo utile al blocco dell'operazione. Considerati tutti questi elementi, il Collegio ritiene che la parte ricorrente abbia agito senza quel minimo di prudenza che avrebbe scongiurato la truffa e sia pertanto chiamata a sopportare l'intera perdita subita.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE