

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BARTOLINI	Membro designato dalla Banca d'Italia
(BA) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) ROBUSTELLA	Membro di designazione rappresentativa dei clienti

Relatore CARMELA ROBUSTELLA

Seduta del 30/03/2026

FATTO

Parte ricorrente riferisce di aver subito la perdita di una somma pari a € 4.990,00, sottratta mediante un'operazione fraudolenta (bonifico istantaneo) eseguita in data 08/07/2025 sul conto aziendale intestato presso l'intermediario B. Sostiene che la frode informatica è riconducibile a un "attacco di social engineering" condotto a danno del rappresentante legale, nonché socio e amministratore della società, che è stato contattato da un numero telefonico apparentemente riconducibile a quello ufficiale del servizio clienti dell'intermediario A, da cui riceveva notizia di tentativi di frode tanto sul conto a lui intestato quanto sul conto aziendale. Aggiunge che, al fine di "bloccare la frode", il presunto operatore invitava il rappresentante legale a installare un'app sul proprio dispositivo tramite un link inviato da un'utenza cellulare su un'app di messaggistica istantanea e lo guidava nell'avvio dell'app, causando un blocco temporaneo del dispositivo e la visualizzazione di un messaggio di scansione antivirus. Riferisce di aver contattato, nel mentre, da altra utenza il servizio clienti dell'intermediario A, al numero di telefono di cui sopra, il cui operatore lo informava della truffa in atto e del prelievo, tramite un bonifico, dell'importo di € 13.000,00 dal suo conto, annullato grazie all'intervento dell'operatore. Sostiene, però, che gli autori della frode riuscivano comunque ad accedere al conto aziendale tramite l'applicazione dell'intermediario B installata sul dispositivo del legale rappresentante e ad autorizzare un bonifico istantaneo di € 4.990,00. Aggiunge che lo stesso non riusciva a bloccare la suddetta

operazione e a richiamare il predetto bonifico in tempo, ma riusciva a ottenere la distinta e l'IBAN del beneficiario.

Di seguito riferisce che, in data 09/07/2025, il legale rappresentante provvedeva a sporgere denuncia e, in pari data, si recava presso un ufficio dell'intermediario B, ove veniva invitato a presentare modulo di richiesta di tentativo di richiamo del bonifico.

Contesta all'intermediario A di non essere riuscito a evitare che il numero del servizio clienti fosse oggetto di spoofing, consentendo agli autori della frode di convincere il legale rappresentante della legittimità della telefonata. Evidenzia che nessuna prova è stata fornita circa i controlli di sicurezza delle linee o l'eventuale compromissione del canale telefonico. Ritiene che, per il tramite della telefonata di spoofing, sia stato verosimilmente introdotto nell'apparecchio mobile della vittima un malware in grado di confermare la disposizione di bonifico a favore del truffatore.

Si duole invece nei confronti dell'intermediario B per non essere riuscito a impedire agli autori della frode di utilizzare l'applicazione installata sul dispositivo del ricorrente per autorizzare il bonifico fraudolento.

Rileva, altresì, che tale intermediario – a fronte di un bonifico istantaneo con causale generica e anomala – non ha applicato alcun filtro antifrode né ha attivato meccanismi di conferma o allerta, come previsto dagli standard di sicurezza più aggiornati.

Lamenta inoltre che l'intermediario B non ha fornito alcuna informazione circa le modalità con cui avrebbe monitorato l'autenticità dell'operazione in parola, disposta dai truffatori tramite tecniche di vishing, spoofing dell'ID chiamante e installazione sul dispositivo della vittima di un malware atto a confermare la disposizione di bonifico attraverso l'app, né ha fornito alcuna prova in ordine ai propri sistemi di sicurezza.

L'intermediario A precisa che, nel corso della frode, sono stati eseguiti due bonifici: il primo (dell'importo di € 13.000,00) a valere sul conto corrente detenuto dal rappresentante legale della società ricorrente presso di essa e il secondo (dell'importo di € 4.990,00) a valere sul conto corrente detenuto dalla ricorrente presso altro intermediario. Segnala che il primo bonifico eseguito presso la resistente è stato prontamente annullato, non comportando alcuna perdita patrimoniale per il rappresentante legale.

Eccepisce preliminarmente il difetto di legittimazione attiva della società ricorrente, non intrattenendo alcun rapporto giuridico con quest'ultima, nemmeno sotto il profilo del contatto sociale, e non rientrando pertanto nella nozione di cliente di cui alle Disposizioni ABF.

Evidenzia, inoltre, che la società ricorrente è carente di interesse ad agire, non essendo la titolare del conto corrente su cui è stato addebitato – solo in origine, in quanto annullato – il bonifico di € 13.000,00 e non avendo subito alcun danno dalla vicenda in esame.

Evidenzia, inoltre, che la ricostruzione della vicenda risulta sprovvista di supporto probatorio in merito alla chiamata civetta ricevuta dal rappresentante legale della ricorrente; al fatto che la chiamata proveniva presumibilmente dalla numerazione ufficiale della scrivente; al messaggio istantaneo ricevuto dal rappresentante legale, contenente un link per scaricare un'applicazione; alla riconducibilità del link e dell'app all'intermediario.

Richiama l'orientamento dei Collegi secondo cui la mancata allegazione, da parte del cliente, del messaggio civetta ovvero, per il vishing, del registro delle chiamate deve determinare il rigetto del ricorso, in quanto non consente di verificare se il mittente/chiamante risulta riconducibile all'intermediario e, pertanto, se è configurabile un legittimo affidamento dell'utente circa la genuinità del messaggio o della telefonata ricevuti (cfr. Collegio di Milano, decisione n. 6153 del 24 giugno 2025; così anche Collegio di Palermo, decisione n. 6042 del 20 giugno 2025).

Segnala, in ogni caso, che quella descritta dal ricorrente si configurerebbe come una delle varianti del phishing, denominata vishing, eseguita con la tecnica di "caller ID spoofing", per la quale esistono

comunemente in commercio servizi offerti da siti internet che consentono di effettuare telefonate scegliendo il numero con cui il mittente della telefonata intende presentarsi al destinatario, il quale viene pertanto indotto a credere che il numero che compare sia quello autentico. Evidenza, pertanto, che non vi è stata alcuna manomissione dei sistemi della banca.

Rileva il comportamento gravemente colposo tenuto dal ricorrente nella vicenda in oggetto, avendo scaricato un'applicazione mediante un link ricevuto tramite messaggistica istantanea da un numero di cellulare. Fa presente che tale app è probabilmente riconducibile a un'applicazione di controllo da remoto (c.d. di mirroring).

Sostiene che il cliente, dopo aver scaricato detta applicazione e mentre quest'ultima era operativa, ha provveduto ad accedere alla propria area riservata di home banking dalla propria app, dando così la possibilità al frodatore di carpire i codici di accesso nell'atto della digitazione e operare indisturbato all'interno della stessa.

Richiama l'orientamento dei Collegi secondo cui deve essere generalmente riconosciuta la colpa grave dell'utente che, su indicazione di ignoti truffatori, installi incautamente un'applicazione non meglio identificata sul device utilizzato per l'accesso ai servizi di mobile banking, consentendo così la compromissione del device stesso, ovvero il suo possibile accesso e controllo da remoto per disporre pagamenti (in tal senso cfr. ABF, Collegio di Roma, decisioni n. 4317/2024 e n. 7806/2023).

Rileva, inoltre, che dalla ricostruzione di controparte emergerebbe la circostanza per cui i malfattori hanno avuto modo di operare contestualmente sia sul conto corrente detenuto dal cliente presso la scrivente sia sul rapporto detenuto dalla società ricorrente presso altro intermediario. Sostiene che l'utilizzo ravvicinato di più strumenti di pagamento (in questo caso due aree personali di home banking) è un altro elemento presuntivo della condotta gravemente colposa dell'utente.

Fa presente, inoltre, che nella chiamata intercorsa con il servizio clienti il rappresentante legale ha comunicato incautamente a terzi i codici della tessera a "battaglia navale" a sue mani (e cioè la matrice dispositiva).

Chiarisce, infine, che il cliente è stato sensibilizzato sulla tematica tramite un'assidua campagna antiphishing a cadenza periodica, che è stata dispiegata con invio mirato di e-mail informative e con la pubblicazione di campagne di sensibilizzazione nell'area personale di home banking e nell'app.

Chiede, pertanto, di dichiarare la domanda della società ricorrente inammissibile e, in alternativa, di rigettarla.

L'intermediario B rappresenta che l'operazione è stata correttamente autenticata, registrata e contabilizzata, in assenza di malfunzionamenti o compromissioni dei sistemi.

Precisa che l'operazione di bonifico è stata eseguita con l'inserimento del codice *ID, al ricevimento della notifica in app.

Dichiara, altresì, che dalla documentazione allegata è evincibile l'enrollment della carta di pagamento di titolarità dell'istante al sistema autorizzativo di tipo dinamico funzionante mediante invio, con SMS, della password dinamica sul numero di cellulare indicato in denuncia, nonché la fase di log-in, risultando che in data 08/07/2025 il ricorrente si è autenticato in home banking mediante autenticazione con *ID.

Rappresenta che, ai fini dell'utilizzo della procedura di autenticazione forte, è necessario, in via preventiva, installare l'app dell'intermediario sul device; associare lo strumento di pagamento; configurare il codice *ID attraverso l'inserimento delle credenziali di accesso ai servizi di Internet banking (username e password), dei dati dello strumento di pagamento utilizzato per effettuare i pagamenti online (ossia, nel caso della carta, PAN, CVV2, data di scadenza), della password dinamica "usa e getta" (OTP) inviata via SMS sul numero di cellulare fornito dal cliente e associato allo strumento di pagamento in modo sicuro.

Afferma, inoltre, che “l’operazione disconosciuta, tenuto conto della modalità con cui è stata autorizzata, poteva essere eseguita soltanto dal titolare del rapporto [...], che è in possesso del device su cui è inviata la notifica in app per l’inserimento del codice di sicurezza «*ID», o, in ultima istanza, da un terzo a cui potrebbero essere state fornite, anche inconsapevolmente, nell’ambito di uno schema fraudolento di phishing tradizionale, i codici di sicurezza e la password dinamica necessari per l’abilitazione di tale procedura di autenticazione, consentendo quindi con ciò, da un lato, la violazione del sistema di autenticazione informatica c.d. «a due fattori», attualmente reputato più sicuro e affidabile, e, dall’altro, configurando una grave violazione degli obblighi di custodia posti al riguardo in capo al titolare dello strumento di pagamento dalle disposizioni di legge e contrattuali in materia”.

Al contempo, dichiara che “[i]n relazione all’operazione in oggetto l’utenza telefonica collegata alla posizione del ricorrente non sembra aver ricevuto alcuna modifica”, sostenendo che “questo elemento è rilevante poiché dimostra che l’operazione è stata eseguita integralmente dal cliente stesso (e non tramite un dispositivo terzo)”.

Procede a illustrare il funzionamento del codice *ID.

Sottolinea che tale sistema è rispondente ai requisiti previsti dalla normativa in vigore ai fini della SCA, essendo presenti un fattore di conoscenza (il codice statico scelto dall’utente) e un fattore di possesso (l’utilizzo dell’app previamente associata a uno specifico dispositivo). Saggiunge che è possibile utilizzare il fattore di conoscenza solo sul device su cui il prodotto finanziario è stato precedentemente abilitato e che, in caso di possesso del device ma non del codice e di errato inserimento di esso per più di cinque volte, è prevista una procedura di blocco del codice. Richiama, sul punto, la decisione n. 4824/22 del Collegio di Napoli, che ha riconosciuto la conformità del codice *ID all’obbligo di autenticazione a doppio fattore.

Evidenzia che parte ricorrente, tramite l’installazione di un software di dubbia provenienza, ha permesso al frodatore di predisporre l’operazione per cui oggi si discute.

Saggiunge che, senza un’idonea allegazione documentale, è impossibile valutare l’eventuale specifica insidiosità di un presunto messaggio ricevuto dal cliente, ritenendo la credulità del ricorrente “non scusabile”, in quanto le modalità con cui la truffa sarebbe stata perpetrata rientrano tra quelle più diffuse, che qualunque cliente dotato di normale avvedutezza e prudenza, riconducibile alla diligenza del buon padre di famiglia, deve essere in grado di individuare, non facendosi trarre in inganno.

Segnala che il servizio di alert è attivo di default in app.

Precisa di condurre campagne informative antifrode sui canali digitali o fisici, trasmettendo avvisi relativi a possibili comportamenti anomali che l’intermediario non è solito tenere e svolgendo azioni di sensibilizzazione della clientela.

Chiede, pertanto, di rigettare la domanda.

Il ricorrente, in sede di repliche, fa presente che, sebbene non intrattenga un rapporto di conto corrente con l’intermediario A, la legittimazione passiva discende dal ruolo causalmente rilevante svolto dallo stesso nella genesi della frode.

Fa presente, infatti, che il contatto fraudolento è avvenuto mediante spoofing del numero telefonico ufficiale dell’intermediario, circostanza che ha indotto il legale rappresentante a confidare nella provenienza bancaria della comunicazione.

Segnala che l’utilizzo del numero ufficiale dell’intermediario rientra nell’area di rischio a esso imputabile e integra un deficit dei presidi di sicurezza e di prevenzione delle frodi, non potendo qualificarsi come evento del tutto estraneo alla sua sfera di controllo.

Segnala, inoltre, che, nel riscontrare il proprio reclamo, l’intermediario A non ha formulato alcuna eccezione di difetto di legittimazione passiva e che tale circostanza è stata ritenuta dal Collegio di Bologna significativa nel respingere l’eccezione dell’intermediario (cita decisione n. 7832/23).

Fa presente che la circostanza che uno dei due bonifici sia stato bloccato non interrompe il nesso causale, ma conferma che: la frode era già in atto; il contatto fraudolento aveva già prodotto i suoi effetti sul piano psicologico e operativo; l'azione dei truffatori era coordinata e seriale.

Evidenzia che l'intermediario A non ha mai prodotto alcuna documentazione tecnica relativa al numero verde; non ha fornito log, tracciati, audit, controlli o certificazioni sulla sicurezza del canale telefonico; non ha dimostrato di aver svolto verifiche sul traffico in entrata/uscita; non ha prodotto documenti sulla gestione del traffico IVR, sui sistemi anti-spoofing, sui controlli sul caller ID e sugli audit di sicurezza del canale telefonico.

Fa presente che la giurisprudenza ABF non configura alcun automatismo tra installazione di un'app e colpa grave e che la valutazione deve essere effettuata caso per caso, tenendo conto del contesto complessivo della frode, del grado di sofisticazione e del comportamento dell'intermediario.

Osserva che la circostanza che i truffatori abbiano operato su più rapporti non dimostra una maggiore imprudenza del cliente, ma l'elevato grado di sofisticazione e pervasività dell'attacco.

Quanto allo stralcio della conversazione telefonica riprodotta dall'intermediario A, segnala che non è corredato dalla registrazione integrale e non consente di ricostruire il contesto, le domande e le modalità di interlocuzione.

Il ricorrente evidenzia che il documento allegato sub 1) dall'intermediario B si limita a riportare dati meramente contabili e descrittivi dell'operazione (importo, data, ora, canale app, causale, codice operazione), ma non fornisce alcuna prova tecnica idonea a dimostrare le modalità concrete di autenticazione dell'operazione; l'assenza di interferenze esterne sul dispositivo utilizzato; l'integrità dell'ambiente di sicurezza al momento della disposizione; l'effettiva riconducibilità della volontà dispositiva al correntista.

Segnala che l'intermediario B si limita a produrre evidenze che attestano l'avvenuta sequenza tecnica di autenticazione, ma non dimostra in alcun modo che tale sequenza sia stata realizzata direttamente e consapevolmente dalla ricorrente, né che il dispositivo fosse nella sua esclusiva disponibilità al momento dell'operazione.

Richiama l'orientamento dell'ABF, secondo cui la mera evidenza contabile dell'operazione non è sufficiente a dimostrare la legittima autorizzazione della stessa, né tantomeno la sussistenza di dolo o colpa grave dell'utente, occorrendo un *quid pluris* rappresentato da log di sicurezza, tracciati di autenticazione, evidenze antifrode e analisi delle anomalie (cfr. art. 10 d.lgs. 11/2010; art. 74 PSD2).

Ritiene che la fattispecie oggetto di ricorso sia riconducibile allo spoofing e non al phishing, come invece affermato dall'intermediario B, in ragione del contatto telefonico diretto, dell'utilizzo di un numero coincidente con quello ufficiale del servizio clienti dell'intermediario A, della creazione di un contesto di urgenza e pericolo imminente e della successiva veicolazione del malware tramite canale apparentemente istituzionale. Dichiara di allegare lo screenshot della telefonata ricevuta il 08/07/2025 dal numero ufficiale del servizio clienti dell'intermediario A, nonché il messaggio istantaneo contenente il link per l'installazione dell'applicazione, dal quale risulta che il numero mittente è associato al logo dell'intermediario A, la cui dicitura compare nella parte inferiore.

Precisa che nel corpo del messaggio compare l'indicazione "Questo messaggio è stato eliminato", in quanto, a seguito dell'avvio dell'applicazione malevola e del conseguente blocco temporaneo del dispositivo, il contenuto non risultava più visualizzabile.

Fa presente che un malware ingannevole, diffuso tramite il link, ha agito direttamente sul dispositivo del rappresentante legale, consentendo l'esecuzione dell'operazione e neutralizzando qualsiasi alert o misura di sicurezza ordinaria. Ritiene che la mancanza di un blocco o malfunzionamento della SIM non possa costituire elemento a carico della ricorrente.

Fa presente di non aver mai contestato l'inadempimento, né preteso l'introduzione di un obbligo astratto di monitoraggio generalizzato, ma di contestare l'assenza di misure adeguate di prevenzione del rischio; la mancata dimostrazione dell'integrità del sistema in presenza di una frode conclamata; l'assenza di qualsiasi verifica rafforzata a fronte di elementi oggettivi di rischio, quali bonifico istantaneo unitamente a primo beneficiario, causale generica e contesto di compromissione del device.

L'intermediario A, in sede di controrepliche, ribadisce che, nella vicenda in oggetto, la ricorrente non è né titolare di un rapporto con la scrivente, né l'ordinante del bonifico eseguito presso la resistente e poi tempestivamente annullato, né il beneficiario del medesimo.

Segnala che l'esecuzione del bonifico oggetto del presente ricorso è stata possibile solo grazie al contegno gravemente colposo del legale rappresentante.

In particolare, evidenzia che quest'ultimo ha dato seguito alle istruzioni pervenute mediante messaggio proveniente da un numero di cellulare non riferibile alla banca su un'applicazione di messaggistica istantanea non utilizzata dalla stessa.

Osserva, in ogni caso, che non è possibile valutare il tenore del messaggio (essendo stato cancellato), né verificare se il link presumibilmente contenuto in tale messaggio e l'app malevola scaricata fossero riferibili alla scrivente.

Sostiene che il legale rappresentante ha anche comunicato al frodatore tutti i codici necessari all'esecuzione del bonifico presso l'intermediario B, senza i quali l'operazione non sarebbe stata possibile.

In sede di controrepliche, l'intermediario B si riporta a quanto già eccepito e controdedotto, insistendo per il rigetto del ricorso, ritenuto infondato in fatto e in diritto.

DIRITTO

Nel presente ricorso, parte ricorrente chiede il rimborso di € 4.990,00, oltre interessi legali dal giorno dell'operazione al saldo, corrispondente a un bonifico effettuato da terzi malfattori, in data 08/07/2025 a valere sul proprio conto aziendale intrattenuto presso l'intermediario B.

Il Collegio rileva che nell'ambito della operatività fraudolenta di cui è causa sono stati eseguiti in pari data (08/07/2025):

- un bonifico di € 13.010,00 a valere sul rapporto di conto corrente intrattenuto dal legale rappresentante della società ricorrente con l'intermediario A, tempestivamente annullato da quest'ultimo a seguito della segnalazione del cliente;
- un bonifico di € 4.990,00 a valere sul conto corrente intrattenuto dalla società ricorrente con l'Intermediario B.

Oggetto del ricorso, proposto dalla società per il tramite del legale rappresentante, è il solo bonifico di € 4.990,00.

Il Collegio, in via preliminare, esamina l'eccezione di difetto di legittimazione attiva della società ricorrente sollevata dall'intermediario A, il quale evidenzia di non intrattenere alcun rapporto giuridico con la stessa, neppure sotto il profilo del contatto sociale, con conseguente esclusione della qualifica di cliente ai sensi delle Disposizioni ABF. L'intermediario A sottolinea, inoltre, che la società sarebbe priva di interesse ad agire in relazione al bonifico di € 13.010,00, in quanto addebitato sul conto personale del legale rappresentante e, in ogni caso, successivamente annullato.

Il Collegio osserva anzitutto che le domande rivolte all'intermediario A con il presente ricorso riguardano:

- l'accertamento della responsabilità in relazione al bonifico di € 4.990,00, con conseguente riconoscimento della relativa somma;

- la richiesta di documentazione tecnica (“log, procedure di sicurezza e [...] verifica completa degli accessi, connessioni e operazioni effettuate tramite il numero verde 02*, incluse eventuali anomalie o accessi sospetti il giorno 08.07.2025”).

In sede di repliche, la ricorrente contesta l’eccezione sollevata dall’intermediario A, evidenziando che, sebbene non intrattenga con esso un rapporto di conto corrente, la legittimazione passiva discende dal ruolo causalmente rilevante svolto nella genesi della frode. Rileva, infatti, che il contatto fraudolento è avvenuto mediante spoofing del numero telefonico ufficiale dell’intermediario A, circostanza che ha indotto il legale rappresentante a confidare nella provenienza bancaria della comunicazione.

La ricorrente segnala, inoltre, che, nel riscontro al reclamo, l’intermediario A non aveva sollevato alcuna eccezione di difetto di legittimazione passiva e che tale omissione è stata ritenuta dal Collegio di Bologna significativa ai fini del rigetto dell’eccezione dell’intermediario (decisione n. 7832/23).

Sul punto, il Collegio rileva che la pronuncia n. 7832/23 del Collegio di Bologna, richiamata dal ricorrente, concerne una diversa fattispecie, relativa alla sussistenza o meno della legittimazione passiva dell’intermediario collocatore in ordine alle richieste di rimborso di somme sottratte a seguito dell’utilizzo fraudolento di uno strumento di pagamento.

Con riferimento alla richiesta di riconoscimento della somma di € 4.990,00, addebitata sul conto intrattenuto con l’intermediario B e che la ricorrente pretende anche dall’intermediario A, il Collegio rileva che, in casi analoghi, i Collegi hanno ravvisato il difetto di legittimazione passiva in capo agli intermediari i cui contatti ufficiali erano stati oggetto di spoofing, quando le operazioni disconosciute erano state eseguite su conti accesi presso altri intermediari (cfr. infra, Collegio di Palermo, decisione n. 12433/24; Collegio di Torino, decisione n. 6014/24). Ne consegue che l’eccezione sollevata deve essere accolta.

Quanto alla richiesta documentale avanzata nei confronti dell’intermediario A, si osserva che quest’ultimo, nelle proprie controdeduzioni, ha allegato i log relativi all’operazione di € 13.010,00 eseguita sul conto del legale rappresentante, operazione che, peraltro, non ha prodotto alcun addebito essendo stata annullata. Con riguardo, invece, agli “accessi, connessioni e operazioni effettuate tramite il numero verde” oggetto di spoofing, l’intermediario A ha chiarito che non vi è stata alcuna manomissione dei sistemi della banca, precisando che “esistono invero comunemente in commercio dei servizi offerti da siti internet che consentono di effettuare delle telefonate scegliendo il numero con cui il mittente della telefonata intende presentarsi al destinatario, il quale viene pertanto indotto a credere che il numero che compare sia quello autentico”.

Passando al merito del ricorso, il Collegio rileva innanzitutto che l’operazione contestata – un bonifico istantaneo, eseguito in data 08/07/2025, dell’importo di € 4.990,00 – è stata disposta 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), entrata in vigore il 13 gennaio 2018.

Ciò premesso, il Collegio rileva che il ricorrente, nella denuncia presentata in data 19/07/2025, ha descritto i fatti in termini sostanzialmente coincidenti con quanto esposto nel ricorso.

L’intermediario B ha prodotto, a supporto delle proprie difese, una ricostruzione generale del sistema di autenticazione adottato. In particolare allega:

- i log di accesso all’app business e di disposizione del bonifico istantaneo;
- una legenda esplicativa dei campi tecnici;
- la descrizione del processo di autenticazione forte applicato alle operazioni dispositive da app;
- l’attestazione che l’operazione è stata eseguita dal medesimo deviceID abitualmente utilizzato dalla ricorrente;
- l’assenza di variazioni dell’utenza certificata/numero di telefono associato al profilo;

- la conferma dell'avvenuto superamento di tutte le fasi di autenticazione previste (fattori di conoscenza e possesso/inerenza).

Alla luce dei criteri individuati anche in sede ABF (produzione di tracciature informatiche, evidenza dell'invio e utilizzo di codici di autorizzazione, log che documentano l'inserimento delle credenziali e dei codici dispositivi sul numero associato all'utente), tale documentazione è idonea a dimostrare che l'operazione è stata correttamente autenticata e non è frutto di un malfunzionamento dei sistemi dell'intermediario.

Il Collegio rammenta che la prova della regolarità formale dell'operazione contestata non è sufficiente ad attribuirne le conseguenze patrimoniali in capo al titolare dello strumento di pagamento, dovendo l'intermediario provare anche i fatti idonei a integrare il dolo o la colpa grave dell'utilizzatore. Questo aspetto risulta enfatizzato, a seguito della novella del 2017 (d.lgs. n. 218/2017), che ha introdotto nell'art. 10, co. 2, la disposizione sopra riportata, in tema di onere della prova del dolo o della colpa grave dell'utente. La prova in questione, evidentemente, non può coincidere con quella della mera regolarità formale delle operazioni, pena un'interpretazione abrogante della disposizione. Sul punto si è, da ultimo, pronunciato il Collegio di Coordinamento, nella decisione n. 22745 del 10/10/2019, nella quale è stato enunciato il principio secondo cui "la previsione di cui all'art. 10, comma 2, del d.lgs. n.11/2010 in ordine all'onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell'utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l'"autenticazione" e la formale regolarità dell'operazione contestata non soddisfa, di per sé, l'onere probatorio, essendo necessario che l'intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell'utente [...].

Nel caso di specie, il Collegio rileva che parte ricorrente allega – sia pure solamente in sede di repliche – uno screenshot da cui si evince la chiamata ricevuta alle 16.48 del 08/07/2025 (giorno della frode), con durata di un'ora e 19 minuti (il bonifico disconosciuto risale alle 17.47, collocandosi dunque nel corso di tale telefonata). Tuttavia, il Collegio constata che l'utenza telefonica da cui è giunta la chiamata è il numero per l'assistenza su conti dell'Intermediario A e che, tuttavia, l'operazione oggetto di ricorso è un bonifico eseguito sul conto intestato alla società ricorrente presso l'Intermediario B. La ricorrente produce altresì in sede di repliche uno screenshot della chat in cui avrebbe ricevuto il link fraudolento. Il Collegio osserva, tuttavia, che il mittente è un numero di cellulare, che reca nell'immagine profilo il logo dell'Intermediario A e il nome di questo nella sola descrizione. Non è visibile, peraltro, il link fraudolento in quanto, secondo il ricorrente, "a seguito dell'avvio dell'applicazione malevola e del conseguente blocco temporaneo del dispositivo, il contenuto del messaggio non risultava più visualizzabile".

Sulla base di questi fatti deve ritenersi che la ricorrente non si è limitata a subire un mero furto di credenziali, ma ha attivamente installato, su indicazione di un interlocutore telefonico, un'applicazione di controllo remoto che consentiva a terzi di operare sul proprio smartphone, sul quale era installata l'app business dell'intermediario B, e quindi di interagire con il sistema di autenticazione. Tale condotta ha reso possibile, per il soggetto malintenzionato, disporre del device registrato, delle credenziali di accesso e dei codici dispositivi, vanificando di fatto le misure di sicurezza predisposte dall'intermediario, che si fondano proprio sull'esclusività del controllo del device e delle credenziali da parte dell'utente.

Pur tenendo conto della sofisticatezza della truffa (caller ID spoofing del numero del servizio clienti dell'intermediario A e tono apparentemente professionale dell'interlocutore), la scelta di installare un'app di controllo remoto sul device utilizzato per l'operatività bancaria, senza alcuna verifica autonoma presso i canali ufficiali degli intermediari coinvolti, integra un livello di imprudenza che, alla

luce degli standard ormai consolidati di sicurezza nell'uso dei servizi di pagamento digitali, appare qualificabile come colpa grave.

Accertata la colpa grave del ricorrente, il Collegio ricorda che l'art. 8 del D.M. 112/2007 individua i casi di frode che, ai fini della stessa normativa, devono essere segnalati all'Ufficio Centrale Antifrode dei Mezzi di Pagamento del Ministero dell'Economia e delle Finanze (UCAMP), al fine di consentire il monitoraggio del mercato delle carte di pagamento.

Secondo gli orientamenti recentemente condivisi dai Collegi, le disposizioni di cui all'art. 8 – mai modificate, nonostante la significativa evoluzione degli strumenti di pagamento – non hanno un valore precettivo diretto nella materia qui in esame, ma costituiscono utili indici per individuare anomalie e scenari di frode, anche ai sensi dell'art. 2 del Regolamento EBA n. 2018/389, che impone agli intermediari di predisporre meccanismi idonei a rilevare operazioni di pagamento non autorizzate o fraudolente.

Ne consegue che, ad avviso dei Collegi, una volta accertata la colpa grave del cliente, qualora ricorra uno dei seguenti indici di frode:

- (i) sette o più richieste di autorizzazione nelle 24 ore sulla medesima carta di pagamento, di cui al punto 1, lett. b), del citato art. 8;
- (ii) tre o più richieste di autorizzazione sulla stessa carta, nelle 24 ore, presso il medesimo punto vendita, di cui al punto 2, lett. a), del medesimo art. 8;
- (iii) due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta minuti, di cui al punto 3, lett. b), del medesimo art. 8;

deve essere riconosciuto un concorso di colpa anche in capo al prestatore di servizi di pagamento (PSP), poiché l'inerzia dell'intermediario in presenza di situazioni che la normativa richiamata qualifica come rischio di frode integra una disfunzione organizzativa che comporta responsabilità per le operazioni non autorizzate.

Il Collegio rileva tuttavia che, nel caso di specie, nessuno dei suddetti indici risulta integrato.

Va peraltro ricordato che i Collegi hanno ritenuto possibile valorizzare anche ulteriori indici di frode, diversi da quelli previsti dal D.M. 112/2007, quando l'operatività risulti anomala rispetto alle movimentazioni storiche del ricorrente (ad esempio quanto a numero, tipologia, importo, tempistica di esecuzione e riconducibilità delle operazioni al medesimo beneficiario), purché tali anomalie emergano con sufficiente evidenza.

Nel caso in esame, il ricorrente individua l'anomalia dell'operazione nella "causale generica e anomala" e, nelle repliche, segnala ulteriori profili, quali la natura di bonifico istantaneo e la novità del beneficiario. Si osserva, tuttavia, che il Collegio di Bari, con decisione n. 9567/25, ha escluso l'esistenza di "un «dovere generale di monitorare la regolarità delle operazioni ordinate dal cliente» in mancanza delle ipotesi di rischio di frode tipizzate dall'art. 8 del D.M. n. 112/2007 (così anche ABF Torino, nn. 10071/24 e 794/25)".

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE