

COLLEGIO DI TORINO

composto dai signori:

(TO) LUCCHINI GUASTALLA	Presidente
(TO) BARENGHI	Membro designato dalla Banca d'Italia
(TO) GRECO	Membro designato dalla Banca d'Italia
(TO) SPENNACCHIO	Membro di designazione rappresentativa degli intermediari
(TO) D'ANGELO	Membro di designazione rappresentativa dei clienti

Relatore MAURILIO D'ANGELO

Seduta del 09/03/2026

FATTO

Con ricorso dell'11.11.2025 (preceduto da rituale reclamo, negativamente riscontrato dall'intermediario), l'istante si è rivolto a codesto Collegio rappresentando che in data 15.09.2025 alle ore 12.16 riceveva sul proprio cellulare un SMS, proveniente dal nr. 379*****505 e apparentemente riferibile a un intermediario terzo, con cui veniva segnalata una richiesta di autorizzazione di pagamento di € 4.800,00 e l'invito a contattare il numero 02****49 nel caso di disconoscimento di tale richiesta di autorizzazione.

Contattava il numero indicato e un interlocutore, qualificatosi come operatore della banca, la informava di un tentativo di pagamento da dispositivo non autorizzato.

Accedeva alla propria area personale del conto senza rilevare movimenti sospetti.

Dopo aver comunicato al suo interlocutore la località in cui si trovava, veniva informata che sarebbe stata contattata dalla stazione locale dei Carabinieri.

Alle ore 12.37, infatti, riceveva una chiamata dal numero 01***200, apparentemente riconducibile alla menzionata Stazione dei Carabinieri, da un soggetto qualificatosi come Maresciallo B.A., addetto al contrasto frodi informatiche.

Il sedicente Maresciallo dichiarava di essere impegnato in indagini su frodi riguardanti l'intermediario resistente e si offriva di assisterla, invitandola inizialmente a recarsi presso una sede della banca e successivamente presso una diversa sede della stessa banca.

Mentre si recava nella filiale indicata, veniva istruita ad effettuare un bonifico urgente di € 24.900,00 con causale "giroconto personale" su un conto corrente a sé intestato presso un altro istituto bancario.

In tale contesto, eseguiva il bonifico come richiesto e, su indicazione dell'interlocutore, inviava tramite WhatsApp la fotografia della ricevuta di pagamento al numero 35***20.

La conversazione telefonica con il sedicente Maresciallo non veniva mai interrotta fino alle ore 16.36, quando veniva preannunciato un ulteriore contatto da numero privato.

Riceveva quindi una nuova chiamata dal numero 35***55, nel corso della quale veniva informato dell'imminente intervento di un Ufficiale Giudiziario per la verbalizzazione dell'operazione e la consegna delle credenziali, poi rinviato al giorno successivo.

Rientrato, si recava presso la locale Stazione locale dei Carabinieri ed apprendeva che non esisteva alcun Maresciallo B.A., non riuscendo più a ricontattare l'interlocutore.

Alle ore 20.10 contattava il servizio clienti al numero 02***41 e provvedeva a bloccare il conto corrente, comprendendo di essere stato vittima di truffa.

Il giorno successivo sporgeva denuncia querela contro ignoti.

In data 19.9.2025 presentava reclamo via PEC sia all'intermediario resistente che alla banca ricevente, chiedendo la restituzione della somma bonificata.

Entrambe le banche negavano responsabilità, ma la banca beneficiaria forniva le generalità e il codice fiscale dell'intestatario del conto destinatario del bonifico.

In data 10 ottobre 2025 integrava la precedente querela indicando il sig. E.M. quale effettivo intestatario del conto corrente presso cui era stato disposto il bonifico.

La contabile del bonifico del 15/9/2025 indicava sé stessa quale beneficiaria del pagamento (che aveva infatti come causale "giroconto personale"), ma in realtà il conto IBAN apparteneva ad un terzo soggetto: risultava cioè una totale difformità tra il nominativo indicato nell'ordine di bonifico e l'intestatario effettivo dell'iban.

Lamentava che l'intermediario avesse eseguito il bonifico senza verificare la corrispondenza tra IBAN e nome del beneficiario, in violazione dei doveri di diligenza e buona fede (artt. 1176, co. 2, e 1375 c.c.), della normativa PSD2 (Direttiva UE 2015/2366) e del Regolamento UE 2024/886.

In particolare, il Regolamento UE 2024/886, pubblicato il 19 marzo 2024 ed efficace dall'8 aprile 2024, imponeva già l'obbligo di predisporre il servizio di verifica del beneficiario (VOP), sicché il termine del 9 ottobre 2025 costituiva solo il limite massimo di adeguamento e non il *dies a quo* dell'obbligo.

Il Regolamento UE 2024/886, infatti, è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea del 19 marzo 2024, acquisendo quindi piena efficacia giuridica il ventesimo giorno successivo alla pubblicazione (8 aprile 2024) secondo il principio generale stabilito dall'art.297 TFUE, così come evincibile anche dai considerando 20 e 28 del regolamento.

Nel caso di specie la banca resistente ha autorizzato i clienti rispettivamente ad effettuare e ricevere operazioni urgenti senza contestualmente attivarsi per fornire ai consumatori il Servizio VPO.

Seppure sia certamente vero che è stato concesso alle banche termine fino al 9 ottobre per implementare il Servizio di verifica del beneficiario (VOP), questo intervallo temporale di oltre 18 mesi tra l'entrata in vigore del regolamento e l'ultima data utile per le banche per adeguarsi ad esso non può andare a detrimento del consumatore.

La banca, pur avendo comunicato al cliente l'imminente attivazione del servizio VOP, ha consentito operazioni urgenti senza attivare contestualmente tale presidio di sicurezza.

Secondo la giurisprudenza ABF (es. decisione n. 2728/2021), l'intermediario deve adottare sistemi di controllo dell'identità del beneficiario e può essere corresponsabile se l'assenza di controlli contribuisce alla perdita; sussiste, poi, responsabilità anche da "contatto sociale qualificato", in quanto la banca, ingerendosi nell'operazione allo sportello, era tenuta a obblighi di protezione e collaborazione verso il cliente.

In base a tale principio si ritiene configurabile la responsabilità della banca per aver eseguito l'erroneo bonifico senza effettuare le opportune verifiche tra l'intestatario dell'Iban e il destinatario del bonifico, vista la macroscopica incongruenza tra l'operazione voluta e ordinata (bonifico a sé stesso) e quella effettivamente eseguita (bonifico a terzi). L'operazione non è stata eseguita autonomamente online, ma con intervento dell'operatore di filiale, su modulo predisposto dalla banca che richiedeva nominativo del beneficiario, IBAN e causale, dati che non potevano essere ignorati.

L'importo era anomalo rispetto all'operatività abituale del cliente e ha quasi azzerato il conto, circostanza che avrebbe dovuto indurre la banca a effettuare ulteriori verifiche.

Ha chiarito che non ha agito con dolo o colpa grave, essendo stato vittima di una truffa sofisticata attuata mediante spoofing telefonico e falsa qualificazione dell'interlocutore come appartenente all'Arma dei Carabinieri.

La banca avrebbe dovuto almeno segnalare l'evidente anomalia tra beneficiario indicato e intestatario effettivo dell'IBAN, sospendendo o rifiutando l'operazione a tutela del cliente. Pertanto, ha richiesto la restituzione della somma di € 29.400,00, corrispondente all'importo dell'operazione di pagamento effettuate a seguito di truffa perpetrata ai suoi danni, oltre agli interessi legali e spese di procedura.

Nel costituirsi con apposite controdeduzioni, l'intermediario ha rappresentato che il ricorrente in data 15 settembre 2025 si recava personalmente presso la filiale dell'intermediario chiedendo l'esecuzione di un bonifico di € 24.900 su IBAN da lui indicato, firmando il relativo modulo.

L'operazione veniva eseguita previa identificazione del cliente allo sportello e seguita dall'invio dell'SMS alert; solo in serata il cliente aveva segnalato la frode, chiedendo il richiamo del bonifico, cui la banca aveva dato seguito senza esito positivo.

Il ricorso all'ABF è infondato poiché l'operazione è stata personalmente disposta, autorizzata e autenticata dal cliente, rientrando nei casi di "*social hacking*" (pagamento eseguito dal cliente sotto dettatura del truffatore) e non nelle operazioni non autorizzate ex art. 10 d.lgs. 11/2010.

Il consenso del pagatore era presente, seppure viziato da raggiro, e pertanto non opererebbe il regime di rimborso previsto per le operazioni prive di autorizzazione.

La responsabilità è ascrivibile esclusivamente al cliente, che ha agito con colpa grave dando seguito a plurimi segnali di anomalia (SMS da numero sconosciuto, contatti telefonici sospetti, richiesta di bonifico urgente per "mettere al sicuro" somme, invio ricevuta via WhatsApp).

La banca ha svolto regolare attività informativa e campagne di sensibilizzazione contro phishing e frodi, anche tramite comunicazioni dirette al cliente.

In proposito, non sussiste un obbligo dell'intermediario di bloccare o monitorare operazioni solo perché atipiche rispetto alla consueta operatività, né la banca potrebbe impedire al cliente di disporre liberamente delle proprie somme in assenza di specifici indici di frode. L'operatore di filiale si è limitato a eseguire un ordine conforme alle istruzioni impartite e sottoscritte dal cliente, senza elementi oggettivi che imponessero un rifiuto.

Il bonifico non è stato disposto in modalità istantanea e, pertanto, non troverebbe applicazione il servizio di verifica del beneficiario (VOP), attivato dalla banca solo a decorrere dal 9 ottobre 2025.

Ricevuto l'ordine, lo stesso è divenuto irrevocabile ai sensi della normativa vigente; ciononostante, la banca si è attivata per il recall presso l'istituto beneficiario, che ha tuttavia rifiutato la restituzione delle somme.

Nel replicare alle controdeduzioni, la parte ricorrente ha precisato che il bonifico non è stato disposto *“liberamente e personalmente”*, poiché la sua volontà era viziata dalla truffa e l'operazione è stata materialmente eseguita allo sportello da un operatore dell'intermediario.

Ha rilevato che l'operatore di filiale avrebbe dovuto verificare la corrispondenza tra intestatario dell'IBAN e nominativo del beneficiario, trattandosi di controlli doverosi e non effettuati.

La giurisprudenza richiamata dalla banca sarebbe inconferente, riguardando casi di operazioni interamente eseguite online dal cliente con credenziali personali, situazione diversa da quella in esame.

Oltretutto, la partecipazione attiva del ricorrente si sarebbe esaurita nel momento in cui ha comunicato i dati allo sportello, spettando poi alla banca il controllo formale e sostanziale dell'operazione.

Il termine del 9 ottobre 2025 costituirebbe solo il limite massimo per l'adeguamento al sistema di verifica del beneficiario (VOP), ma non escluderebbe la responsabilità della banca nel periodo transitorio successivo all'entrata in vigore del Regolamento.

Nella circostanza, la banca avrebbe introdotto bonifici urgenti senza attivare contestualmente adeguati sistemi di sicurezza, assumendosi il rischio delle conseguenze. Ha evidenziato che le campagne informative richiamate dall'intermediario sarebbero generiche, non specifiche rispetto alla tecnica di *“social hacking”* e comunque inidonee a esonerare la banca dall'obbligo di controlli tecnici.

L'SMS alert successivo all'operazione non avrebbe alcuna reale funzione protettiva, essendo intervenuto a bonifico già disposto e se il sistema di verifica del beneficiario fosse stato attivo, l'operazione non sarebbe stata eseguita, poiché sarebbe emersa la difformità tra giroconto a sé stesso e bonifico verso terzi.

Inoltre, ritiene che il periodo compreso tra l'entrata in vigore del Regolamento europeo e il termine ultimo di adeguamento non può tradursi in un vuoto di tutela a danno del consumatore.

In sede di controrepliche, l'intermediario ha ribadito che il ricorrente ha seguito pedissequamente le istruzioni dei truffatori, nonostante fossero anomale e contraddittorie (spostamenti tra filiali e richiesta di bonifico *“per mettere al sicuro”* il denaro).

Il bonifico è stato richiesto personalmente dal cliente, regolarmente identificato, e sottoscritto; pertanto, l'operatore di sportello non poteva che darvi esecuzione.

Inoltre, non vi erano elementi oggettivi che consentissero alla banca di percepire la truffa, trattandosi di un'operazione formalmente autorizzata dal titolare del conto.

Ha chiarito che alla data del 15 settembre 2025 (anteriore al 9 ottobre 2025), la normativa vigente in ambito SEPA non imponeva agli intermediari la verifica di corrispondenza tra IBAN e nominativo del beneficiario; al contrario, ai sensi dell'art. 24 d.lgs. 11/2010, il prestatore di servizi di pagamento è tenuto a eseguire l'operazione esclusivamente in base all'identificativo unico (IBAN) fornito dal cliente, con esenzione da responsabilità in caso di difformità rispetto al nome indicato.

L'eventuale incongruenza tra IBAN e intestazione avrebbe potuto essere rilevata, all'epoca dei fatti, solo dalla banca del beneficiario.

Al riguardo, la responsabilità dell'errore nell'indicazione dell'IBAN ricade sul disponente; la banca dell'ordinante è coperta da una clausola di esenzione se esegue correttamente l'operazione secondo l'IBAN fornito.

In altri termini, quanto accaduto dipende esclusivamente dalla condotta autonoma del ricorrente, che ha disposto il bonifico indicando l'IBAN poi contestato.

Una volta ricevuta la segnalazione della frode, la banca ha attivato tempestivamente la procedura di recall, ma la restituzione delle somme è subordinata al consenso del beneficiario, che nel caso di specie è stato negato.

DIRITTO

L'operazione contestata consiste in n.1 bonifico SEPA di importo pari a € 24.900,00, eseguito in data 15/09/2025.

La ricevuta della richiesta di bonifico (allegata in atti) risulta compilata digitalmente (dall'addetto allo sportello seguendo le indicazioni del cliente, in base a quanto riferito dal ricorrente e non contestato), ma sottoscritta a mano dall'odierno ricorrente.

La parte ricorrente ha riferito nel ricorso e nella denuncia che, per quanto sia stata vittima di un raggirio da parti di terzi, ha personalmente disposto l'operazione oggetto del presente ricorso.

In particolare, in data 15/09/2025 alle ore 12.16 il ricorrente riceveva un messaggio che segnalava un presunto tentativo di pagamento non autorizzato. Contattava il numero indicato nel messaggio e avviava una conversazione con un interlocutore che si presenta come operatore di una banca. Quest'ultimo gli riferiva che c'era stata una richiesta di pagamento dal suo conto e lo invitava a verificare la sua lista dei movimenti, su cui però parte ricorrente non notava transazioni sospette. Dopo avergli chiesto dove si trovasse, il sedicente operatore lo informava che sarebbe stato ricontattato dai Carabinieri del posto. Difatti, alle 12.37 veniva contattato da un sedicente maresciallo dei Carabinieri. Con vari pretesti e pressioni, il truffatore convinceva l'utente a effettuare un bonifico urgente a favore di sé stesso (giroconto) su un conto radicato presso un intermediario terzo, dettandogli un IBAN. Tale operazione veniva presentata come misura di sicurezza. Il ricorrente eseguiva il bonifico di € 24.900,00 presso uno sportello dell'intermediario. Successivamente, il truffatore richiedeva anche l'invio della ricevuta di esecuzione del bonifico tramite WhatsApp. Il malfattore ha poi continuato a contattare la vittima tramite numeri diversi, simulando ulteriori passaggi procedurali, fino a quando l'utente si avvedeva della truffa e si rivolgeva alla propria banca e ai Carabinieri.

Nel caso di specie l'intermediario ha espressamente eccepito l'inapplicabilità della PSD2.

In tale contesto – e secondo gli orientamenti condivisi dei Collegi - 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. Rientrano in questa fattispecie le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, senza la consapevolezza di disporre una transazione (ad esempio, le c.d. operazioni "sotto dettatura").

Trattandosi di operazione eseguita personalmente dal cliente allo sportello fisico dell'intermediario – e considerata l'espressa contestazione mossa dalla ricorrente in proposito - potrebbe doversi valutare la condotta dell'operatore di banca quale eventuale fattore causale concorrente al realizzarsi della frode.

In particolare, rispetto all'obbligo di verificare la corrispondenza tra iban ed effettivo intestatario del conto il ricorrente, nel ricorso, afferma che la ricevuta dell'operazione evidenziava quale beneficiario del bonifico sé medesimo.

Pertanto, contesta all'intermediario di non aver verificato la corrispondenza tra il beneficiario dell'operazione indicato (sé stesso) e l'effettivo intestatario del conto corrente destinatario.

Sul punto, si rammenta che dalla distinta di bonifico in atti il beneficiario del pagamento risulta il ricorrente stesso e la causale – coerentemente – risulta essere "giroconto personale".

Con riferimento alla verifica della corrispondenza tra iban e beneficiario, l'intermediario ha eccepito che il regolamento UE n. 886/2024 – cui accenna il ricorrente - è applicabile ai soli bonifici istantanei e solo a partire dal 09/10/2025, aggiungendo comunque che solo l'istituto di credito beneficiario poteva effettuare tale controllo di corrispondenza.

Il bonifico disconosciuto – ed in disamina - risale al 15/09/2025.

Il riferimento delle parti è all'introduzione dell'art. 5 quater nel Regolamento UE n. 2012/260, ad opera dell'art. 1 del Regolamento UE 2024/886: viene infatti introdotto l'obbligo per i PSP di implementare per il pagatore un servizio di verifica del beneficiario al quale intende eseguire un pagamento.

Come evincibile dal comma 9, il nuovo Regolamento del Parlamento Europeo e del Consiglio (n. 2024/886) sui bonifici istantanei in euro non è applicabile al caso di specie, in quanto l'obbligo di implementare tale servizio di verifica ha quale termine ultimo la data del 9 ottobre 2025, non potendosi quindi individuare responsabilità dei PSP per la mancata implementazione prima di tale momento.

Sul punto, la giurisprudenza dell'Arbitro (a partire dalla decisione del Collegio di Coordinamento n. 162/2017) e della Corte di giustizia dell'Unione europea (sentenza 21 marzo 2019, causa C-245/18, Tecnoservice Int.) ha costantemente affermato che, nell'ambito del sistema SEPA, il codice IBAN rappresenta l'unico identificativo vincolante per l'esecuzione dei pagamenti, e che gli intermediari non sono tenuti a verificare la congruità tra tale identificativo e il nominativo del beneficiario.

Lo stesso orientamento della giurisprudenza di legittimità non ha modificato tale quadro interpretativo, confermando che il prestatore di servizi di pagamento non è gravato da un dovere di controllo sulla corrispondenza IBAN/nome del beneficiario.

Solo con l'entrata in vigore del Regolamento (UE) 2024/886 sui bonifici istantanei è stato introdotto l'obbligo per i PSP di effettuare il c.d. check IBAN, disposizione, tuttavia, non applicabile al caso di specie, in quanto il comma 9 dell'art. 5 quater prevede

espressamente: “I PSP situati in uno Stato membro la cui moneta è l'euro si conformano al presente articolo entro il 9 ottobre 2025”.

Non ricorrono pertanto i presupposti per l'applicazione della disciplina in materia di operazioni non autorizzate né, in via sussidiaria, elementi idonei a fondare una responsabilità concorrente dell'intermediario ai sensi dell'art. 1227 c.c..

Alla luce di quanto sopra esposto, il Collegio ritiene che il ricorso non possa essere accolto.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE