

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) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - FABIO GIROLAMO PORTA

Seduta del 23/04/2026

FATTO

La ricorrente - cointestataria di un conto corrente abilitato all'operatività on line intrattenuto presso l'intermediario convenuto - chiede il rimborso del controvalore di una operazione di pagamento a mezzo bonifico bancario disposto in data 19/11/2024, per l'importo di euro 8.700,00, dalla medesima successivamente disconosciuta. In particolare la ricorrente espone: di essere stata contattata (alle ore 16:50 del 19/11/2024) da un sedicente operatore dell'intermediario, attraverso un numero di utenza telefonica riconducibile alla Banca (+3906**60), il quale segnalava la presenza di un'operazione "sospetta" sul suo conto corrente; di avere ricevuto, nel corso della chiamata, una comunicazione via mail, recante intestazione e firme riconducibili alla banca, "nella quale venivano confermate le credenziali dell'operatore al telefono"; di aver seguito le indicazioni del presunto operatore il quale, dopo averle chiesto di appurare l'eventuale sottrazione illecita di somme dal conto, la invitava a disinstallare l'App bancaria e a installare un'apposita App "antivirus"; che per agevolare tale attività, l'operatore effettuava una videochiamata con il cointestatario del conto dal numero "+39351****901" recante il logo ufficiale della banca; che dopo aver completato l'installazione dell'App antivirus, il falso operatore le comunicava che sarebbe stata ricontattata il giorno seguente; che, il giorno successivo, tentava, dapprima, di contattare il numero +39351****901, senza ricevere risposta, e, successivamente, il servizio clienti ufficiale della banca avvedendosi che dal proprio conto corrente era stato disposto un bonifico istantaneo di € 8.700,00 verso l'IBAN IT**8187; di aver sporto denuncia presso le Autorità competenti in data 21/11/2024 e chiesto il rimborso all'intermediario ricevendo riscontro negativo.

Insoddisfatta dell'esito del reclamo, la ricorrente adisce l'Arbitro deducendo la responsabilità della banca convenuta, per colpa in vigilando, sul rilievo che il PSP non avrebbe predisposto sistemi di controllo adeguati atti a intercettare comportamenti anomali o potenzialmente fraudolenti ad opera di terzi (cita Cass. Civ., sent. n. 2950/2017), giacché: i truffatori dimostravano di essere a conoscenza del suo numero di telefono e della relativa e-mail registrata "nei contatti posseduti dalla Banca"; non era stato bloccato tempestivamente il bonifico disposto in favore di un destinatario sconosciuto; l'App della Banca era stata installata dalla ricorrente sul suo device "meno di un mese prima dell'accaduto" e con essa non aveva mai effettuato operazioni; l'ammontare della disposizione fraudolenta (€ 8.700,00) era pressoché pari al saldo (€ 10.000,00) del suo conto corrente. Chiede pertanto: in via principale, che "venga accertata la responsabilità della Banca nella causazione dell'evento descritto e che, per l'effetto, quest'ultima venga condannata al rimborso in favore della ricorrente della somma di € 8.700,00"; in via subordinata, che "venga accertata la maggiore corresponsabilità dell'istituto bancario, per tutte le ragioni esposte in narrativa, con conseguente condanna di quest'ultimo alla refusione nei confronti della ricorrente delle somme proporzionalmente corrispondenti".

Instaurato il contraddittorio, l'intermediario invoca la declaratoria di rigetto del ricorso deducendo che, alla luce delle evidenze e dei tracciati informatici estratti dai propri sistemi, l'operazione disconosciuta sia stata autorizzata con un sistema certificato a doppio fattore di convalida, conforme alla normativa di settore, senza alcuna anomalia di digitazione delle credenziali segrete né malfunzionamenti, secondo quanto evincibile dai log informatici, in atti; questi ultimi documentano le attività effettuate dalla ricorrente (identificata con codice cliente 11*****669) dal proprio device, in data 19/11/2024, e senza variazioni riscontrabili nella "*nomenclatura*" nei giorni antecedenti alla frode.

Deduce pertanto la condotta connotata da "colpa grave" della cliente nella misura in cui ai frodatori è risultato sufficiente chiedere per ottenere il download di un'App sconosciuta e l'esecuzione di istruzioni e comandi ricevuti. Sostiene, inoltre, che i clienti non devono accordare piena fiducia nel "caller ID" visibile sul telefono, in quanto il dato non garantisce che la chiamata sia "partita" dall'utenza apparsa sul display, considerato che è possibile modificare facilmente il mittente di un numero di telefono da parte di terzi. Per cui ove la cliente, piuttosto che indugiare nelle conversazioni telefoniche intrattenute con gli sconosciuti malfattori, avesse controllato con più attenzione tanto la mail pervenutale alle ore 16:56 (recante un "suffisso" errato, connotata da "clamorosi" errori di scrittura presenti nel testo), quanto la sua App originaria o effettuato una chiamata al servizio clienti, avrebbe potuto evitare la frode cagionata con il suo comportamento gravemente negligente. La resistente soggiunge che l'utilizzo delle credenziali segrete per accedere ad App non ufficiali di cui non si sia verificata l'attendibilità, configura un incauto comportamento del titolare degli strumenti di pagamento e una condotta gravemente colposa dell'utilizzatore, che nella specie ha eseguito quanto richiesto da persona sconosciuta al telefono, perdendo così il controllo della sua App e permettendo ai malfattori di agire indisturbati su di essa. Sostiene che, alla luce delle dichiarazioni della cliente, la frode sia stata perpetrata con la tecnica di "phishing", permettendo ai frodatori di carpire le credenziali di sicurezza facendo uso di una app esterna.

Sulla scorta delle superiori considerazioni, stante la sicurezza del sistema di autenticazione forte adottato, l'intermediario ritiene che la frode sia andata in porto per mera negligenza dell'utente nella custodia delle credenziali necessarie per la fruizione a distanza dei servizi di pagamento, sottolineando come l'importo della disposizione di bonifico e la sua causale non potevano destare sospetti, in seno al PSP, sulla natura anomala dell'operazione, giacché apparsa in linea con l'operatività pregressa.

La resistente esclude altresì profili di responsabilità ascrivibili al proprio operato, avendo fornito pronta assistenza alla cliente nel tentativo di recupero dell'operazione di bonifico disconosciuta, non appena ricevuta notizia della frode, seppure con esito negativo.

Conclude chiedendo all'Arbitro di dichiarare il rigetto del ricorso in quanto infondato in fatto e in diritto. Entrambe le parti depositano memorie di replica e di controp replica attraverso cui ribadiscono le rispettive argomentazioni e istanze.

DIRITTO

La domanda formulata dalla ricorrente è relativa all'accertamento del proprio diritto alla restituzione del controvalore di una operazione di pagamento eseguita a mezzo bonifico bancario in data 19/11/2024, per l'importo di euro 8.700,00, successivamente disconosciuta dalla correntista rimasta vittima di una truffa.

La materia è regolata dalle disposizioni del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 218/2017 che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno (PSD2). Le transazioni controverse risultano poste in essere anche sotto la vigenza del Regolamento Delegato (UE) n. 2018/389 della Commissione che definisce i requisiti per l'autenticazione forte previsti dalla citata direttiva.

La disciplina *de qua* prevede che il rischio di utilizzazione fraudolenta degli strumenti di pagamento ricada, in prima battuta, sull'intermediario, il quale può sottrarsi all'obbligo di rimborso delle somme fraudolentemente sottratte fornendo la prova del dolo ovvero della colpa grave dell'utilizzatore (cfr. artt. 7, 10 e 12, co. 4, d. lgs. n. 11/2010; Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011). In particolare, a mente dei commi 1 e 2 dell'art. 10 (d.lgs. n. 11/2010, cit.): "1. Qualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento 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. 2. Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7. È onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente".

Delineato il quadro normativo di riferimento, come evidenziato nella narrativa del ricorso, la ricorrente invoca la restituzione dell'importo di euro 8.700,00, quale controvalore dell'operazione di pagamento a mezzo bonifico bancario eseguita on line e autorizzata alle ore 17:30:02 del 19/11/2024. L'intermediario resistente nega il rimborso in ragione della riscontrata esecuzione in regime di SCA della transazione che occupa, evincibile dai tracciati estratti dai propri sistemi informatici in corrispondenza delle varie fasi di accesso all'app di home banking, autenticazione ed esecuzione dell'operazione di pagamento.

Il rilievo è fondato.

Dall'analisi dei log in atti si evince che: alle ore 17:25:19 del 19/11/2024, la ricorrente ha effettuato l'accesso (da indirizzo IPV4 93.**.*.251) sull'App della banca installata sul dispositivo certificato in uso alla medesima (a52sxq - SM-A528B), mediante inserimento di ID Utente e Password (fattore di conoscenza), utilizzando l'OTP generato da Mobile Token (fattore di possesso); alle ore 17:30:02 ha predisposto e autorizzato l'operazione di bonifico per l'importo di € 8.700,00, con beneficiario IBAN IT**8187 (causale "acquisto rtt22), mediante inserimento del PIN (fattore di conoscenza) e del codice OTP (77345418) generato dal Mobile Token (fattore di possesso).

Sulla scorta delle dichiarazioni delle parti e delle risultanze in atti può dunque concludersi che il processo di autenticazione multifattoriale testé illustrato sia avvenuto in conformità con le regole di Strong customer authentication (SCA), di modo che può considerarsi assolto l'onere della prova posto a carico del PSP del pagatore, ai sensi dell'art. 10, d.lgs. n. 11/2010, in merito all'autorizzazione e alla corretta registrazione della transazione che occupa (cfr. ABF Coll. Bari, Dec. nn. 4215/2025, 11542/2023, 32/2023; Coll. Napoli, Dec. n. 14897/2021; Coll. Milano, Dec. n. 15074/2021).

A tale conclusione non osta il rilievo della ricorrente secondo cui sarebbe stato onere dell'intermediario bloccare tempestivamente il bonifico disposto in favore di un destinatario sconosciuto. Si osserva infatti che, alla luce della normativa applicabile *ratione temporis*, nell'esecuzione di un bonifico bancario, il prestatore di servizi di pagamento dell'ordinante ed il prestatore di servizi di pagamento del beneficiario sono autorizzati a realizzare l'operazione in conformità esclusivamente all'identificativo unico, anche qualora l'utilizzatore abbia fornito al suo prestatore di servizi di pagamento informazioni ulteriori rispetto all'IBAN. In particolare, il prestatore di servizi di pagamento di destinazione del bonifico non è tenuto a verificare la corrispondenza fra il nominativo del beneficiario ed il titolare del conto di accredito identificato tramite l'IBAN fornito dal cliente (cfr. ABF Coll. Coord., Dec. n. 162/2017).

Appurato quanto sopra, occorre ora valutare se sussistono profili di colpa grave imputabili alla ricorrente ove consti che con la propria condotta ella abbia reso possibile ai truffatori di entrare in possesso dei codici dispositivi necessari per perfezionare l'operazione disconosciuta (cfr. ABF Coll. Coord., Dec. n. 22745/2019, n. 3947/2014, 991/2014, 3498/2012; Cass. civ. Sez. I, sent. n. 2950/2017; Cass. Sez. VI-1, ord. n. 9158/2018). A tale ultimo riguardo inducono a ravvisare la colpa grave della ricorrente le dichiarazioni dalla stessa rilasciate in sede di esposto alle autorità competenti e nel ricorso, nella parte in cui afferma di avere intrattenuto una interlocuzione telefonica con il frodatore, prospettando implicitamente un suo legittimo affidamento sulla genuinità della conversazione. Il rilievo, oltre a non essere supportato da elementi utili alla ricostruzione puntuale della truffa denunciata (cfr. ABF Coll. Bari, Dec. n. 175/2025), non appare risolutivo dal momento che la ricorrente produce mera evidenza degli screenshot delle chiamate ricevute, tra l'altro, il 18 novembre 2024, provenienti dalle utenze + 39 06**60 (alle ore 18:47) e 351****901 (alle ore 18:51, con cui il falso operatore avrebbe contattato la ricorrente per aiutarla a disinstallare l'App della banca e installarne una diversa). Al riguardo si osserva che, seppure l'utenza "+ 39 06**60" appaia riconducibile al servizio clienti della banca convenuta, non è tuttavia possibile stabilire il contenuto della conversazione telefonica intrattenuta con il malfattore il giorno prima del pagamento. Peraltro, l'ampio lasso temporale intercorso tra il primo contatto telefonico e il perfezionamento del pagamento avrebbe consentito alla titolare del rapporto di intervenire tempestivamente, eseguendo le opportune verifiche, sì da scongiurare il compimento della frode. Medesime considerazioni valgono anche in relazione alla conversazione intrattenuta con l'utenza 351****901 - in alcun modo riconducibile alla banca - rispetto alla quale la ricorrente non fornisce alcuna evidenza attestante il download dell'App malevola asseritamente scaricata. D'altra parte, anche ove ricorrano gli estremi di una frode perpetrata con la tecnica del c.d. vishing caller ID, l'installazione dell'App di terze parti per il controllo del device del cliente abbinato al rapporto, autorizzata dal suo titolare, sia pure in modo inconsapevole, configura, secondo l'orientamento condiviso dei Collegi territoriali, ipotesi di colpa grave dell'utilizzatore (cfr. ABF Coll. Milano, dec. n. 196/2023; Coll. Roma, Dec. nn. 979/2025; 8747/2024; Coll. Bologna, Dec. nn. 8809/2025, 7883/2025).

Indicativa di una negligenza grave dell'utente è anche la mancanza di adeguata attenzione prestata al contenuto del messaggio di alert e al testo della notifica *push* relativa all'operazione in frode (recante "*Eseguito vs Bonifico, da c/c 16000**003, importo 8700,00, in data 19/11/2024, da Mobile***, beneficiario altra Banca. Info 06**60*") inviata alle ore 17:30 del 19/11/2024 sul device della ricorrente ("Modello del telefono: SM- A528B"), secondo quanto ricavabile dalla documentazione in atti.

In siffatto contesto, il Collegio ravvisa plurimi indizi concordanti che lasciano presumere un'insufficiente custodia dei dati riservati, verosimilmente messi a disposizione dei frodatori, mediante i quali è stato reso possibile il compimento dell'operazione di pagamento in questione (cfr. ABF Coll. Bari, Dec. n. 3157/2022). Alcune censure può dunque essere mossa all'operato della resistente, anche con riguardo alla fase di assistenza prestata alla cliente nel tentativo di recupero dell'operazione di bonifico disconosciuta. In proposito si osserva che, ai sensi dell'art. 17 del D.lgs. n. 11/2010, l'ordine di pagamento, una volta ricevuto dal prestatore di servizi di pagamento del pagatore diviene irrevocabile, sicchè il rimborso dell'operazione è subordinato al consenso del beneficiario, ovvero a un

provvedimento dell'Autorità giudiziaria (cfr. ABF Coll. Bari, Dec. n. 15198/2022; Coll. Milano, Dec. n. 16506/2022; Coll. Roma, Dec. n. 13465/2022).

Nel caso in esame consta che in seguito alla segnalazione inviata dalla cliente, la resistente si sia attivata per il richiamo del bonifico sconosciuto, seppure il PSP beneficiario abbia riscontrato negativamente l'istanza (in data 03/12/2024) a causa di "fondi insufficienti sul conto del beneficiario". Il ricorso non può pertanto trovare accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE