

COLLEGIO DI BARI

composto dai signori:

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

Relatore ESTERNI - FABIO GIROLAMO PORTA

Seduta del 17/12/2025

FATTO

Insoddisfatto dell'esito del reclamo, il ricorrente - titolare di un rapporto di conto corrente abilitato all'operatività on line, intrattenuto dall'omonima ditta individuale presso l'intermediario convenuto - chiede il rimborso delle somme fraudolentemente sottratte da terzi a conclusione di due operazioni di pagamento, a mezzo bonifici istantanei, eseguite in data 26/06/2025, successivamente disconosciute. In particolare, in sede di denuncia sporta (alle ore 14:43 del 26/06/2025) presso le autorità competenti, il ricorrente ha allegato: di avere ricevuto, in pari data (alle ore 13:03), un messaggio - apparentemente proveniente dall'istituto di pagamento che gestisce le carte emesse dall'intermediario convenuto - recante la segnalazione di un addebito anomalo di € 485,20 sul conto in questione e l'invito a contattare il numero "+39344***" per disconoscerlo; di avere risposto alla telefonata proveniente da detta utenza e intrattenuto una conversazione con il chiamante nel corso della quale questi lo avrebbe informato che per ottenere il rimborso era necessario fornire le credenziali di accesso all'APP di home banking; di avere comunicato i codici di accesso richiesti e di avere ricevuto, attraverso un'App di messaggistica istantanea, i QR Code necessari per la generazione dei codici OTP, nel seguito forniti al falso operatore; di non aver chiesto l'aumento dei limiti operativi per i bonifici istantanei; di avere ricevuto via e-mail dall'intermediario, due messaggi di alert contenenti la conferma degli ordini di bonifico controversi; di essersi avveduto che ignoti, all'esito di una truffa perpetrata con artifici e raggiri, hanno carpito le credenziali di accesso all'area riservata di home banking ed eseguito due bonifici, per l'importo complessivo di € 19.100,00, dal medesimo asseritamente non autorizzati. Il ricorrente ha soggiunto di aver denunciato tempestivamente la truffa subito e che, ciò nonostante, l'intermediario non avrebbe revocato le operazioni di pagamento impartite dai malfattori. Alla luce dei superiori rilievi, il

ricorrente deduce la responsabilità dell'intermediario per non avere predisposto adeguate misure di protezione a tutela della clientela nella fruizione dei servizi di pagamento. Pertanto, in relazione alla vicenda occorsa, assumendo che la sofisticatezza della truffa subita valga ad escludere una sua negligenza grave, il ricorrente invoca la tutela dell'Arbitro affinché condanni la convenuta al rimborso della somma sottratta (€ 19.100,00).

Instaurato il contraddittorio, l'intermediario si oppone alla domanda del ricorrente affermando che l'istante è titolare di una ditta individuale intestataria del conto abilitato all'operatività di internet banking - dotato di tecnologia a doppio fattore di autenticazione (SCA) conformemente alla normativa di riferimento - dal quale sono state disposte le operazioni contestate. Rileva che dalle risultanze informatiche in suo possesso non si evince l'intrusione di terzi nei propri sistemi informatici, sicché ritiene che l'accesso del frodatore all'area riservata di home banking sia stato reso possibile unicamente dalla condotta incauta del ricorrente, il quale ha consentito allo sconosciuto interlocutore di impadronirsi dei propri codici personali di sicurezza necessari allo scopo. Osserva che il messaggio civetta ricevuto dal cliente presenta plurimi indici di anomalia, laddove, da un lato, indica quale mittente un istituto di pagamento terzo che gestisce esclusivamente i servizi relativi alle carte di pagamento e non quello di internet banking per mezzo del quale sono state disposte le operazioni; dall'altro contiene l'invito a chiamare un numero a sé non riconducibile per bloccare una presunta operazione di pagamento. Saggiunge che anche il numero dal quale il ricorrente ha ricevuto le ulteriori comunicazioni fraudolente non sarebbe, del pari, a sé riferibile. Evidenzia, inoltre, che le istruzioni impartite dal truffatore nel corso della telefonata truffaldina si palesano illogiche. Afferma, da ultimo, di aver trasmesso al cliente, tramite e-mail, appositi alert in merito alle disposizioni di bonifico poi sconosciute. Tanto premesso, la banca resistente deduce la responsabilità esclusiva per colpa grave del ricorrente, il quale ha ammesso, in sede di denuncia, di avere fornito le credenziali richieste dall'ignoto interlocutore e di aver seguito le istruzioni impartite dal sedicente operatore, che l'ha contattato da una utenza non riconducibile al PSP, senza destare alcun sospetto con riguardo alle procedure richieste, né tener conto dei messaggi di alert coevi ai due pagamenti. Alla stregua delle su esposte argomentazioni, l'intermediario chiede all'Arbitro di pronunciarsi per il rigetto del ricorso in quanto infondato.

DIRITTO

Il ricorrente rivendica il diritto al rimborso dell'importo complessivo di euro 19.100,00, quale controvalore di due operazioni di pagamento addebitate sul conto corrente, abilitato all'operatività on line, intrattenuto dalla omonima ditta individuale presso l'intermediario convenuto, successivamente sconosciute.

Le operazioni oggetto di vertenza risultano eseguite sotto il vigore del d.lgs. 27 gennaio 2010, n. 11, di recepimento della direttiva 2007/64/CE, come modificato dal d.lgs. 218/2017 che ha attuato la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno, e il Regolamento Delegato (UE) n. 2018/389 della Commissione che definisce i requisiti per l'autenticazione forte previsti dalla citata normativa.

Tale disciplina prevede che il rischio di utilizzazione illecita degli strumenti di pagamento ricada in prima battuta sull'intermediario (tenuto a garantire l'affidabilità e la sicurezza complessiva del servizio offerto, in relazione al sistema informatico, organizzativo e di controllo all'uopo adottati) il quale può sottrarsi all'obbligo di rimborso delle somme rivendicate fornendo la prova del dolo o della colpa grave dell'utilizzatore (tenuto alla diligente custodia dello strumento e alla segretezza delle credenziali necessarie per l'autenticazione) ai sensi del combinato disposto degli artt. 7, 10 e 12, comma 4, d. lgs. n. 11/2010, e della Sez. IV, § 2, del Provvedimento Banca d'Italia 5.7.2011. In particolare, l'art. 10 del menzionato decreto legislativo n. 11/2010 stabilisce: "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". Inoltre "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".

Tracciato il quadro normativo di riferimento, come evidenziato nella narrativa del ricorso, il ricorrente ha disconosciuto la paternità di due bonifici istantanei eseguiti a distanza in data 26/06/2025 (€ 14.900,00 alle ore 14:10 ed € 5.000,00 alle ore 14:16) per il complessivo importo di € 19.900,00, a seguito della truffa di cui è rimasto vittima.

L'intermediario resistente ha negato il riaccredito delle somme pretese in restituzione ritenendo il cliente unico responsabile della perdita subita, sul rilievo che gli ordini di bonifico disposti attraverso l'App di internet banking sarebbero stati correttamente impartiti attraverso una procedura di autenticazione e autorizzazione multifattoriale conforme ai requisiti di Strong Customer Authentication. A sostegno della formale regolarità delle operazioni contestate, la resistente ha prodotto i tracciati informatici estratti dai propri sistemi, compendati in tre fogli elettronici denominati "logHubAutenticazione", "logOperazioni" e "NotificheMail". In particolare, nel file "logHubAutenticazione" appaiono i fattori verosimilmente utilizzati in fase di autenticazione (cfr. colonna R – "Cedacri_hubaut.tipo_cred") e autorizzazione (cfr. colonna S – "Cedacri_hubaut.tipo_auth") di ciascuna operazione di pagamento, valorizzati nelle stringhe "OTP_PIN" – "LOGON" e "OTP_SIGNATURE PAYLOAD" – "DISPO".

Ora, seppure le suddette evidenze non risultano corredate da legende esplicative, nondimeno le allegazioni della banca convenuta, in merito ai fattori utilizzati, appaiono corroborate dalle dichiarazioni del ricorrente rilasciate in sede di denuncia presso le autorità competenti, il quale ha ammesso: di aver comunicato allo sconosciuto interlocutore tutte le credenziali di accesso all'APP di home banking e i codici dinamici OTP all'uopo generati per finalizzare le operazioni di pagamento; di avere ricevuto via e mail, dall'intermediario resistente, le notifiche di alert in corrispondenza di ciascuna transazione autorizzata. In proposito, deve rammentarsi che ai fini della prova della SCA possono essere valutate, tra l'altro, eventuali dichiarazioni confessorie del cliente, che assumono valore di prova legale ai sensi dell'art. 2730 c.c. (cfr. ABF Coll. Bari, dec. n. 6764/2025); sicché, in base agli elementi sopra illustrati, nel caso in esame può ritenersi formalmente dimostrato (ex art. 10, d.lgs. n. 11/2010, cit.) il corretto svolgimento della procedura di autenticazione in assenza di malfunzionamenti. Tuttavia, come non si è mancato di sottolineare, "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" (cfr. ABF Coll. Coord. Dec. n. 22745/2019). Sotto questo fronte, la convenuta ha osservato, senza essere smentita, che tanto il numero indicato nel campo mittente del messaggio civetta, quanto quello indicato nel campo mittente della conversazione intercorsa nell'APP di messaggistica istantanea non sono riconducibili ai contatti dell'intermediario resistente. Inoltre non consta che il messaggio civetta si sia inserito nel canale recante precedenti messaggi genuini dell'intermediario. Tali circostanze inducono il Collegio, per un verso, ad escludere la sussistenza di un legittimo affidamento dell'utente circa la genuinità apparente dell'interlocuzione con l'intermediario (cfr. ABF Coll. Milano,

Dec. n. 5431/2024; Coll. Bari, Dec. n. 2663/2023) e, per l'altro, a ravvisare gli estremi di una condotta gravemente negligente del correntista, il quale ha intrattenuto una conversazione con il falso operatore che l'ha contattato da una utenza (numero di cellulare) non riconducibile al PSP e, ciò nonostante, ha dato seguito alle istruzioni ricevute dallo sconosciuto interlocutore, comunicando tutti i codici segreti in suo possesso. Deve quindi concludersi che il ricorrente abbia disatteso l'obbligo posto a suo carico dall'art. 7, d.lgs. n. 11/2010, di diligente custodia e non divulgazione delle credenziali di accesso ai servizi di home banking e delle password dinamiche dispositive generate dall'app bancaria, in tal modo neutralizzando tutti i presidi di sicurezza approntati dall'intermediario, consentendo, seppure all'esito di un raggio, la causazione dell'evento delittuoso. Di conseguenza la domanda volta al rimborso delle somme portate dalle operazioni di pagamento disconosciute non può trovare accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE