

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 28/01/2026

FATTO

Il ricorrente, titolare di un conto corrente abilitato all'operatività on line, intrattenuto presso l'intermediario convenuto, rivendica il rimborso del controvalore (€ 6.990,00) di quattro operazioni di pagamento - due delle quali rappresentate da prelievi cardless presso uno sportello ATM, le altre due da bonifici istantanei - successivamente disconosciute.

In particolare, il ricorrente espone: di aver ricevuto, in data 30/08/2024, un sms proveniente da un'utenza mobile sconosciuta, recante l'invito a contattare un presunto numero verde per disconoscere un pagamento; di aver effettuato la chiamata e di avere ricevuto indicazioni dall'interlocutore sulla necessità di eseguire l'accesso all'app bancaria al fine di ripristinare le condizioni di normalità del conto; di avere "inserito diverse volte il codice di accesso inviato via sms dall'operatore", riscontrando il malfunzionamento dell'applicazione; di essersi recato presso la filiale competente avvedendosi di essere rimasto vittima di una frode attraverso la quale ignoti, impossessatisi delle credenziali di accesso al rapporto, hanno sottratto dal conto la complessiva somma di € 6.990,00, a conclusione di quattro transazioni consistenti in due bonifici bancari (€ 1.990,00 ed € 2.000,00) e due prelievi cardless (€ 1.000,00 ed € 2.000,00); di avere sporto denuncia presso le autorità competenti e chiesto il rimborso all'intermediario ricevendo riscontro negativo.

Esperito infruttuosamente il reclamo, il ricorrente, ascrivendo all'intermediario la responsabilità del danno subito, per non avere questi adottato ogni accorgimento utile a scongiurare il rischio di utilizzo fraudolento nell'uso degli strumenti di pagamento, secondo le prescrizioni dettate in tema di autenticazione forte dal d.lgs n. 11/2010, invoca la tutela dell'Arbitro affinché condanni la convenuta al rimborso della somma sottratta, oltre alla refusione delle spese sostenute.

Instaurato il contraddittorio, l'intermediario si oppone alla domanda del ricorrente rilevando che alla luce dei tracciati informatici estratti dai propri sistemi, le operazioni controverse sarebbero risultate autorizzate, previo accesso ai servizi di home banking, mediante l'inserimento del codice Titolare, del PIN e di un codice OTP dinamico generato dall'app o via sms. In particolare, l'intermediario evidenzia che, in data 30/08/2024: alle ore 17:47, il cliente ha eseguito l'accesso alla propria area riservata dal suo device (fattore di possesso) con inserimento del codice PIN (fattore di conoscenza); alle ore 18:03 e 18:04 ha eseguito due prelievi cardless, entrambi tramite inserimento dei codici OTP generati da app, previo inserimento del PIN; con le stesse modalità, alle ore 18:09 e 18:12 ha autorizzato due bonifici istantanei, senza alcuna anomalia riscontrata nella digitazione delle credenziali o malfunzionamenti delle apparecchiature.

L'intermediario deduce pertanto la colpa grave del cliente (ex art. 7, co. 2, d.lgs. n. 11/2010) in relazione alla non corretta custodia delle credenziali segrete in suo possesso, essenziali per il corretto utilizzo dei servizi di pagamento on line, rilevando che il ricorrente non ha prodotto evidenza tanto dell'sms, quanto della telefonata ricevuta da una utenza in alcun modo riferibile alla banca. Conclude, dunque, per il rigetto del ricorso; in subordine, chiede di ripartire il danno tra le parti in proporzione alle effettive responsabilità, con applicazione della franchigia di € 50,00 contemplata dalla normativa applicabile in subiecta materia.

In sede di repliche e controrepliche le parti insistono per l'accoglimento delle rispettive conclusioni.

DIRITTO

Il ricorrente invoca l'accertamento del diritto al rimborso del controvalore di quattro operazioni di pagamento addebitate sul conto detenuto presso la resistente, eseguite a distanza, in data 30 agosto 2024, usufruendo del servizio di home banking, consistenti in due prelievi di denaro contante da ATM (€ 1.000,00 alle ore 18:03 ed € 2.000,00 alle ore 18:04) e due bonifici istantanei (€ 2.000,00 alle ore 18:09 ed € 1.990,00 alle ore 18:12) formalmente disconosciuti.

La materia trova precipua regolamentazione nelle disposizioni 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 Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 sui servizi di pagamento nel mercato interno (PSD2). L'operazione controversa risulta posta 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 direttiva. 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 trafugate 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. L'art. 10 del citato decreto legislativo n. 11/2010 stabilisce infatti: "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, nella fattispecie in esame l'intermediario documenta che le operazioni disconosciute sono state autorizzate mediante app dal device n. "48***cb" certificato dal cliente in data 30/08/2024.

In particolare, a sostegno della regolarità formale delle transazioni contestate, l'intermediario produce talune evidenze estratte dai propri sistemi informatici, dalle quali sembra evincersi: a) che per l'accesso all'area riservata effettuato alle ore 17:47, utilizzando il device certificato contraddistinto dal codice univoco "48***cb" (fattore di possesso), il sistema ha richiesto l'inserimento di un PIN (attestato dalla stringa "authtype: PIN" presente nella descrizione del contenuto della colonna R, quale fattore di conoscenza); b) che le operazioni di prelievo cardless sono state disposte attraverso l'APP installata sul device del ricorrente ("48***cb"), alle ore 18:03 e alle ore 18:04 del 30/08/2024, per gli importi di € 2.000,00 ed € 1.000,00 mediante validazione del codice OTP generato dalla stessa APP (stringa "checkotpmobile" valorizzata nella colonna J del log prodotto, quale fattore di possesso) previo inserimento del PIN (confermato dalla stringa "authtype: PIN" valorizzato nella colonna R, quale fattore di conoscenza);

c) che, analogamente, i bonifici istantanei sono stati disposti dall'APP installata sul device del ricorrente ("48***cb"), alle ore 18:09 e alle ore 18:12 del 30/08/2024, per gli importi di € 2.000,00 ed € 1.990,00 mediante validazione del codice OTP generato dalla stessa APP (stringa "checkotpmobile" valorizzata nella colonna J del log prodotto, quale fattore di possesso) previo inserimento del PIN (confermato dalla stringa "authtype: PIN" valorizzato nella colonna R, quale fattore di conoscenza).

Sulla scorta delle risultanze in atti può affermarsi che il processo di autenticazione multifattoriale testé illustrato sia avvenuto in regime di SCA, di modo che può considerarsi assolto l'onere della prova posto a carico del PSP, ai sensi dell'art. 10, d.lgs. n. 11/2010, in merito all'autorizzazione e alla corretta registrazione delle transazioni che occupano (cfr. ABF Coll. Bologna, Dec. n. 206/2025; Coll. Bari, Dec. n. 5831/2023).

Pur tuttavia, in coerenza con i principi del processo civile sull'onere della prova, la formale regolarità di una operazione di pagamento, di per sé, non soddisfa l'onere probatorio, essendo altresì necessario che l'intermediario provveda specificamente a indicare una serie di circostanze di fatto che caratterizzano le modalità esecutive dell'attività contestata, dalle quali possa trarsi la dimostrazione, in via presuntiva, della colpa grave dell'utente, ravvisabile ove consti che con la propria condotta egli abbia reso possibile ai truffatori di entrare in possesso dei codici dispositivi necessari per il perfezionamento dei pagamenti (cfr. ABF Coll. Coord., Dec. nn. 22745/2019, 3947/2014, 3498/2012, 991/2014. Nella giurisprudenza di legittimità, cfr. Cass. civ. n. 2950/2017, n. 9158/2018).

Nel caso in esame, come anche rilevato dall'intermediario resistente, il ricorrente non ha procurato evidenza del messaggio civetta ricevuto. Ora, sebbene tale carenza probatoria non consente al giudicante di accertare *per tabulas* se risultino o meno integrati gli estremi di un legittimo affidamento dell'utente circa la genuinità dell'interlocuzione con l'intermediario, sul punto assume rilevanza decisiva la dichiarazione rilasciata dal ricorrente (in sede di denuncia e nel ricorso) di aver ricevuto il messaggio esca da un'utenza mobile sconosciuta - pertanto non riconducibile all'intermediario - recante l'invito a contattare un numero verde parimenti non riferibile a un canale ufficiale dell'intermediario. Queste circostanze inducono a ritenere che il ricorrente sia rimasto vittima di c.d. phishing tradizionale, sicchè "l'assenza di cautela dell'utente appare difficilmente scusabile, trattandosi di fenomeni diffusamente noti, che qualunque utente dotato di normale avvedutezza e prudenza, come si ritiene siano quelli avvezzi all'uso del cd. home banking, deve essere in grado di individuare, non facendosi trarre in inganno" (cfr. ABF Coll. Coord., dec. nn. 1820/2013, 3498/2012). Il descritto contesto, in applicazione degli artt. 7, comma 1, lett. a), e 12, comma 4, d.lgs. n. 11/2010, integra una tipica ipotesi di colpa grave dell'utilizzatore (cfr. ABF Coll. Coord., Dec. n. 5304/2013).

Nondimeno, è stato chiarito come l'obbligo a carico dell'utente dello strumento di pagamento di tempestiva segnalazione del suo utilizzo indebito (previsto dall'art. 7, lett. *b*, d.lgs. 11/2010, cit.) sia strettamente correlato all'obbligo in capo all'intermediario di assicurare che siano sempre disponibili strumenti adeguati affinché il cliente possa eseguire tale comunicazione (ex art. 8, lett. *c*). In particolare, fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene (cfr. ABF Coll. Coord., Dec. n. 24366/2019); per cui "la mancata prova dell'attivazione del servizio di *sms alert* da parte dell'intermediario rappresenta una violazione al corretto adempimento degli obblighi posti a suo carico" (cfr. ABF Coll. Coordinamento, Dec. n. 8672/2024).

Nella fattispecie in esame, le quattro operazioni sono state poste in essere nel seguente ordine: la prima di € 2.000,00 alle ore 18:03; la seconda di € 1.000,00 alle ore 18:04; la terza di € 2.000,00 alle ore 18:09; la quarta di € 1.990,00 alle ore 18:12. Ora, considerata la tempistica, il Collegio osserva che ove fosse stato attivo il servizio di sms alert, le prime tre operazioni, eseguite nell'arco di sei minuti, sarebbero state inevitabili, dunque, per esse, alcuna responsabilità può essere ascritta all'operato dell'intermediario. Diversamente è a dirsi con riferimento all'ultima operazione di € 1.990,00 avvenuta in un arco temporale sufficientemente distanziato dalla prima (cfr. ABF Coll. Bari, Dec. n. 416/2024). In questo caso, l'attivazione del servizio di "alert" avrebbe verosimilmente consentito al ricorrente di avere contezza più immediata dei movimenti, offrendo al medesimo la possibilità di attenuare il pregiudizio patrimoniale risentito (cfr. ABF Coll. Bari, Dec. n. 10735/2023; Coll. Napoli, Dec. n. 8838/2022). Pertanto in relazione all'operazione di € 1.990,00 eseguita alle ore 18:12, l'intermediario non può andare esente da responsabilità ed è tenuto alla restituzione del corrispondente importo (cfr. ABF Coll. Bari, Dec. nn. 416/2024, 10010/2023, 15207/2022).

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 1.990,00.

Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE