

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) GIGLIOTTI	Membro designato dalla Banca d'Italia
(NA) COCCIOLI	Membro designato dalla Banca d'Italia
(NA) MIOLA	Membro di designazione rappresentativa degli intermediari
(NA) VERDICCHIO	Membro di designazione rappresentativa dei clienti

Relatore GIANFRANCO COCCIOLI

Seduta del 10/02/2026

FATTO

Il ricorrente evidenzia di aver subito il 26.02.2025 una truffa *online* che l'ha spinto al perfezionamento di tre bonifici per un importo complessivo pari a 31.700 euro.

Nella denuncia deduce che, avendo investito su una piattaforma di criptovalute e volendo sboccare i relativi fondi, gli era stato riferito, da persona spacciata per consulente, che doveva effettuare alcuni bonifici.

Soggiunge che il 5 febbraio 2025, dopo avere eseguito un bonifico di 10 euro su suggerimento del consulente, gli era stato riferito che il denaro risultava sbloccato, ma che sarebbe stato riaccreditato nei giorni successivi.

Senonché il 26 febbraio 2025, chiamato per avviare una "*procedura guidata di trasferimento*", era richiesto di condividere l'accesso tramite l'applicazione ***desk* al fine di accelerare l'esecuzione dei bonifici.

In realtà, dopo un controllo sul conto, si è avveduto che i bonifici erano stati non accreditati, come promesso dal consulente, ma addebitati.

In relazione a quanto dedotto, invoca la responsabilità della banca che, a fronte di tali operazioni, non ha attivato la procedura antifrode.

Insoddisfatto della prodromica interlocuzione con l'intermediario, si rivolge al Collegio al quale chiede il risarcimento del danno patrimoniale, pari all'importo delle operazioni disconosciute, oltre agli interessi, alla rivalutazione monetaria, al danno morale "*per non esser stato protetto dalla banca*" e, infine, al

riconoscimento delle spese di assistenza difensiva.

Si è costituita la resistente che, ricostruita la vicenda, deduce che si è fuori dal perimetro applicativo dell'art. 10 d. lgs 11/2010, dal momento che i bonifici sono stati disposti consapevolmente dal ricorrente che ha agito in concorso con un interlocutore telefonico, rimasto sconosciuto.

In subordine, deduce che è stata correttamente applicata la procedura di autenticazione forte, anche per l'operazione di svincolo della provvista, né le analisi tecniche dei log, relativi agli indirizzi IP e ai dispositivi utilizzati dal cliente, hanno evidenziato difformità rispetto alle consuete modalità operative.

Invero, anche il rapporto di conto corrente beneficiario dei tre bonifici eseguiti dal ricorrente il 26 febbraio 2025 è il medesimo conto in favore del quale il ricorrente ha disposto un bonifico in data 5 febbraio 2025, che non ha mai disconosciuto.

Precisa altresì che la linea di deposito originariamente costituita e successivamente svincolata dal soggetto fraudolento, presentava le caratteristiche delle cosiddette linee "svincolabili" che, in conformità alla disciplina contrattuale del Conto Deposito di esso intermediario, prevedono la possibilità per il cliente di rientrare in qualsiasi momento nella disponibilità dei fondi, rinunciando al riconoscimento degli interessi che sarebbero stati riconosciuti al termine del periodo di vincolo, a fronte di un tasso di interesse generalmente inferiore.

Ritiene quindi che il ricorrente abbia adottato una condotta gravemente negligente, imprudente e imperita, poiché ha seguito pedissequamente tutte le istruzioni che gli sono state fornite dai frodatori, senza nemmeno avvedersi degli alert inviati nel frattempo da parte di esso intermediario.

Dunque, alla luce della prova dell'avvenuta SCA, nonché della violazione da parte del cliente dell'obbligo di diligenza nella custodia delle credenziali di accesso e dei dispositivi abilitati, violazione aggravata dall'eventuale installazione del software di controllo remoto **desk, che potrebbe aver consentito ai malfattori di operare direttamente sul terminale del cliente, risulta comprovata la genuinità delle operazioni oggetto di contestazione.

Infatti, qualora il ricorrente avesse consentito a persone terze di accedere e controllare il proprio *device* mediante l'installazione del software di controllo remoto ***desk, il comportamento del ricorrente configurerebbe una evidente e grave violazione dei criteri minimi di diligenza imposti in materia di custodia delle credenziali di accesso. Tale tipologia di applicazioni, infatti, consente l'accesso integrale ai file presenti sul dispositivo, inclusi quelli contenenti dati sensibili e funzionali all'autenticazione nell'home banking, esponendo così il sistema a rischi di compromissione da parte di soggetti non autorizzati (cfr. decisione N. 3309/2025 del Collegio di Milano).

Inoltre, secondo l'orientamento condiviso tra i Collegi, nelle contestazioni di utilizzi fraudolenti online di strumenti di pagamento in cui l'intermediario offre, come nel caso specifico, la prova della SCA, le mancate allegazioni del cliente sulle circostanze di fatto della frode rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del cliente medesimo.

Più in particolare, i Collegi sono unanimi nel ritenere che la mancata allegazione, da parte dei clienti, del registro delle chiamate, come nel caso in oggetto, debba determinare il rigetto del ricorso, in quanto non consente di verificare se il chiamante risulti riconducibile all'intermediario e, pertanto, se sia configurabile un legittimo affidamento dell'utente circa la genuinità delle comunicazioni ricevute.

Il ricorrente, nelle repliche, si oppone a quanto dichiarato dalla banca, chiarendo di aver eseguito un unico bonifico di 10,00 euro. Al contrario, gli altri bonifici non sono stati autorizzati, analogamente alla attività di costituzione della provvista.

Ciò posto, invoca la responsabilità dell'intermediario che non ha attivato alcun sistema, neanche di *alert*, per evitare il compimento della truffa.

Ricostruita la normativa applicabile alla fattispecie, ritiene che la banca non abbia provato la corretta autenticazione del cliente né abbia tenuto conto delle nuove tecniche di frode, come lo *spoofing*, che escludono la colpa grave del cliente.

Ritiene quindi che il comportamento della Banca sia stato gravemente negligente. Cita al riguardo la decisione n. 11117/24 del Collegio di Milano, che ha affermato un principio fondamentale, ovvero che le banche sono tenute a monitorare le operazioni dei clienti non solo in base a parametri tecnici, ma anche in funzione delle caratteristiche delle transazioni stesse.

Nel caso specifico, l'entità delle operazioni ha superato i limiti previsti, fatto che avrebbe dovuto allertare la banca.

L'intermediario, riportandosi a quanto dichiarato in sede di controdeduzioni, insiste per il rigetto del ricorso.

Nelle controrepliche specifica che il ricorrente, se da un lato riconosce come proprio il bonifico di € 10,00, effettuato in data 5/02/2025, dall'altro pretende di disconoscere i successivi bonifici eseguiti il 26/02/2025, pur essendo stati eseguiti tutti secondo le medesime modalità operative.

Ribadisce che tutte le operazioni che il ricorrente tenta di disconoscere risultano essere state autorizzate mediante accesso all'area personale dell'*internet banking* della Banca, avvenuto con l'inserimento delle credenziali statiche e la validazione del dispositivo previsti dal sistema. Non rileva, pertanto, alcuna discontinuità procedurale né alcuna anomalia tecnica tra il bonifico che il ricorrente riconosce come legittimo e quelli che intende disconoscere, compreso lo svincolo del deposito.

Ritiene poi imprescindibile evidenziare che le operazioni oggetto di contestazione sono state eseguite dal ricorrente nell'ambito di una precisa attività di investimento che egli stesso aveva volontariamente intrapreso. Il ricorrente aveva avviato tali investimenti e li seguiva attivamente, mantenendo un rapporto di fiducia con il proprio interlocutore e intrattenendo con lui frequenti conversazioni telefoniche volte a verificare l'andamento delle operazioni.

Ne deriva quindi che le movimentazioni contestate non possono essere considerate come operazioni isolate o sconosciute al ricorrente, ma al contrario appaiono coerenti con la volontà di investimento da lui stesso perseguita e confermata.

Eccepisce inoltre di aver avvisato il ricorrente in tempo reale delle operazioni.

Infine, la Banca contesta sia il riferimento allo *spoofing*, che risulta ultroneo, che il richiamo della decisione n. 11117/24 del Collegio ABF di Milano, che si fonda su presupposti fattuali e giuridici estranei al caso in esame.

DIRITTO

Il ricorso non va accolto.

Il ricorrente disconosce n. 3 bonifici istantanei eseguiti il 26/02/2025 per un importo complessivo pari a 31.700 euro e documenta di aver presentato denuncia all'Autorità di Pubblica Sicurezza, dalla quale si desumono le modalità della frode e, in particolare, il suo investimento su una piattaforma di criptovalute. Vi si legge che, invitato ad utilizzare altro conto sul quale riversare la liquidità del fondo che lui aveva chiesto di sbloccare, effettuava un bonifico di € 10,00 richiesto dall'interlocutore per verificare l'esistenza di un secondo conto.

Qualche giorno dopo, al fine di accelerare l'effettuazione dei bonifici in suo favore derivanti dallo sblocco dei fondi, era invitato "*a condividere le informazioni tramite applicativo ...desk*".

Dopo di che, gli veniva comunicato che i bonifici erano andati a buon fine, sicché il giorno seguente avrebbe potuto controllare i movimenti di accredito. Senonché il giorno successivo aveva la sgradevole sorpresa di constatare che non vi erano accrediti, ma addebiti dovuti a tre bonifici per l'ammontare complessivo richiesto.

Non vi è concordia delle parti in ordine alla ricostruzione della vicenda.

Mentre l'intermediario afferma che le operazioni sarebbero state autorizzate personalmente dall'utente, costui riferisce di aver autorizzato unicamente un bonifico di 10,00 euro il 5/2/2025 (ovvero circa 20

giorni prima della frode), precisando di non aver mai fornito l'autorizzazione, né con riferimento ai n. 3 bonifici oggetto di contestazione (del 26/02/2025), né per l'operazione di costituzione della provvista. I Collegi ABF distinguono tra operazioni autorizzate con l'intervento parziale del pagatore (quando il pagatore autorizza l'operazione precedentemente inserita dal frodatore) e operazioni eseguite per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione).

Secondo l'orientamento condiviso, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa non è completo (come in caso di inserimento di uno dei fattori di autenticazione), la transazione non può essere qualificata come autorizzata, atteso che la normativa speciale (PSD2 e disposizioni di recepimento) prescinde dalla nozione civilistica di "consenso", disponendo che esso può configurarsi soltanto se prestato nella forma convenuta tra il pagatore stesso e il PSP.

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, con la conseguenza che non può ritenersi assoggettata al regime di responsabilità previsto dalla PSD2.

I Collegi ABF hanno così escluso l'applicazione del regime di protezione previsto dal D. Lgs. 11/2010 e, di conseguenza, ritenuta irrilevante l'eventuale prova fornita dall'intermediario in ordine all'autenticazione, nel caso di operazioni disposte ed autorizzate personalmente dal titolare dello strumento di pagamento, sebbene sulla base di un consenso viziato dagli artifici e raggiri posti in essere da un truffatore anche per mezzo di sms o chiamate "civetta" apparentemente provenienti dall'intermediario resistente (*ex multis* Collegio di Bologna, n. 2290/2023)

Ora, nel caso di specie, entrambe le parti riferiscono che il truffatore, spacciandosi per esperto in criptovalute, tanto da aver determinato l'investimento di discrete somme di danaro in tale settore finanziario, ha acquisito il controllo da remoto del pc del ricorrente tramite l'applicazione .."desk".

Alla fattispecie in esame devono dunque considerarsi applicabili le disposizioni del D.lgs.n. 11/2010 nella versione oggi vigente che prevede nel suo articolo 10, in caso di disconoscimento di operazioni da parte del cliente, uno specifico regime di ripartizione dell'onere probatorio.

Sulla base di esso, il prestatore di servizi di pagamento ha anzitutto l'onere di dimostrare che l'operazione è stata autenticata, correttamente registrata e contabilizzata, senza aver subito le conseguenze del malfunzionamento delle procedure indispensabili per la sua esecuzione o di altri inconvenienti (primo comma).

Assolto con esito positivo questo primo onere, di per sé necessario ma ancora insufficiente, incombe su di lui anche l'ulteriore onere di provare (secondo comma) che l'uso indebito del dispositivo è da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto.

Ebbene, per quanto attiene al primo profilo, l'intermediario resistente ha fornito piena prova della corretta autenticazione dell'operazione disconosciuta dal ricorrente, conformemente ai criteri SCA.

Più in particolare vi è prova sia del valido accesso all'area riservata di *internet banking* che della correttezza della disposizione, autenticate tramite inserimento di username, password e del codice pin dispositivo (elemento della conoscenza) con digitazione personale del ricorrente in seguito alla notifica PUSH che riceveva sul suo dispositivo certificato (elemento del possesso).

I fattori di autenticazione utilizzati per l'accesso all'*internet banking* sono dunque una password ed un pin dispositivo (elementi di conoscenza) e notifica PUSH sul dispositivo del cliente (elemento di possesso). L'accesso all'area riservata risulta eseguito tramite inserimento della password e della push generata sul dispositivo mobile del ricorrente.

L'intermediario offre anche una legenda dalla quale si desume la conferma di quanto precedentemente evidenziato circa i fattori utilizzati ai fini dell'autenticazione.

Come noto, i Collegi si sono espressi in merito alla valenza da attribuire alle informazioni presenti nei log prodotti dagli intermediari per provare l'autenticazione forte del cliente nelle operazioni di

pagamento disconosciute (artt. 10, comma 1 e 10-bis del D.lgs. 11/2010), nei casi in cui dalla tracciatura informatica non risulti in modo esplicito uno dei fattori di autenticazione inseriti (conoscenza, possesso o inerenza).

Tenuto conto che la PSD2 è tecnologicamente neutrale e non prevede un sistema informatico standard per l'inserimento e la tracciatura dei fattori di autenticazione forte, i Collegi ritengono che, per valutare l'assolvimento dell'onere della prova della SCA, possono essere valutati (oltre ai log) anche ulteriori elementi esplicativi, quali la legenda e/o quanto rappresentato dal PSP nelle proprie difese in relazione al caso concreto, purché consentano di verificare i singoli passaggi registrati dal sistema informatico come prova di autenticazione.

Assolto da parte dell'intermediario il primo onere probatorio, occorre ora verificare se l'uso indebito del dispositivo sia da ricondursi al comportamento fraudolento, doloso o gravemente colposo dell'utilizzatore, rispetto agli obblighi di condotta imposti a quest'ultimo dall'art. 7 dell'anzidetto decreto. La dinamica della truffa, come precisato sopra, è descritta nella denuncia, nella quale il ricorrente ha dichiarato che, previa registrazione su una piattaforma di criptovalute ed esecuzione di un investimento, seguendo le indicazioni e le richieste di un sedicente consulente, con cui intratteneva contatti telefonici, eseguiva alcuni bonifici, onde ottenere lo sblocco e il trasferimento dei fondi. In particolare, precisa che, autorizzato un bonifico di 10 euro il 5/02/2025, il 26/02/2025 è stato richiesto sempre dallo stesso interlocutore di condividere l'accesso tramite l'applicativo **desk, che sarebbe stato asseritamente necessario per accelerare l'esecuzione dei bonifici.

Ricevuta la notizia che i trasferimenti in suo favore erano stati effettuati, il ricorrente, a seguito di un controllo dei movimenti, si avvedeva che era stati effettuati trasferimenti in uscita.

Agli atti non vi è evidenza dell'interlocuzione telefonica, che in ogni caso il ricorrente riferisce essere avvenuta con un consulente della piattaforma di criptovalute e non con un operatore della convenuta. Appurato che il ricorrente, come si desume esplicitamente dalla sua stessa denuncia, ha condiviso con un soggetto presentatosi come consulente relativo all'investimento in criptovalute le informazioni relative all'applicativo ..desk, consentendogli così di controllare da remoto il suo dispositivo e dunque di compiere bonifici, occorre tenere presente che, secondo l'orientamento dei Collegi, richieste come quella accolta dal ricorrente, data la loro evidente anomalia, devono indurre il cliente a non seguire le indicazioni del falso operatore (cfr. , *ex plurimis*, Collegio di Roma, decisione n. 7659/2023; Collegio di Roma, decisione n. 17334/2021). Il ricorrente, non essendosi attenuto a questa prescrizione, ha dato credito ad un interlocutore (della cui identità peraltro non aveva certezza, come dimostra l'indicazione generica relativa al suo ruolo ed alle sue qualità professionali), colpevolmente seguendone le istruzioni. Sicché, omettendo con grave leggerezza di ponderare le conseguenze derivanti dal comunicare informazioni rilevanti, ha in tal modo contribuito, con un apporto causale decisamente significativo a far sì che la frode fosse realizzata. (v. *ex multis* Collegio di Milano, decisione n. 10639 del 10 ottobre 2024; Collegio di Roma, decisione n. 7151 del 19 giugno 2024).

Per ciascuna operazione disconosciuta, peraltro, risulta una notifica via mail (oltre che la *push* autorizzativa per l'esecuzione delle transazioni).

Né vale invocare la responsabilità dell'intermediario per non essersi dotato di un sistema di monitoraggio delle frodi.

Infatti i Collegi territoriali ABF hanno più volte affermato l'assenza di un obbligo generale di monitoraggio *ex ante* in capo all'intermediario e del connesso obbligo di bloccare l'operatività degli strumenti di pagamento (cfr. in tal senso la sentenza del Tribunale di Milano n. 1596/2023 nonché Coll. Torino, decisione N. 9093/2024, Coll. Milano, decisione n. 8338 del 16 luglio 2024, Coll. Roma, decisione n. 4805 del 24 aprile 2024).

Sul piano civilistico la giurisprudenza di legittimità (Cass. 30588/2023) conferma l'inesistenza per la banca di alcun dovere generale di monitorare la regolarità delle operazioni ordinate dal cliente.

Da ultimo deve rilevarsi che dagli atti emerge che il tentativo di recall, posto in essere dalla resistente,

non ha sortito alcun effetto positivo.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE