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

Relatore FILIPPO BOTTALICO

Seduta del 26/05/2025

FATTO

La ricorrente premette di essere titolare di un conto corrente presso l'intermediario A e di un "*conto/carta*" presso l'intermediario B.
Fa presente che la carta emessa dall'intermediario B era "*bloccata*", circostanza nota solo a lei stessa, e che il 14/11/2024, alle ore 13:30, riceveva una telefonata nel corso della quale l'interlocutore, qualificatosi come operatore dell'intermediario B, le comunicava di dovere procedere allo "*sblocco*" della carta.
Precisa che non forniva al sedicente operatore alcun dato personale o bancario e che durante la telefonata il suo smartphone "*andava in blocco*".
Aggiunge che, rilevata la citata anomalia, contattava immediatamente l'intermediario A, apprendendo che dal proprio conto corrente erano stati eseguiti dei bonifici sul conto/carta in essere presso l'intermediario B, e che da quest'ultimo erano state effettuate delle operazioni in favore di terzi, per un ammontare complessivo di € 5.505,00.
Rappresenta di avere segnalato immediatamente l'accaduto alle controparti richiedendo di "*bloccare*" i bonifici, inviando una prima email all'intermediario B alle ore 16:38, "*dopo meno di 10 minuti dall'operazione fraudolenta*" in cui disconosceva le operazioni in esame.
Afferma di avere continuato a segnalare l'accaduto con successive email il 14/11/2024, dalle ore 16:42 alle ore 20:09, mentre solo il mattino seguente controparte richiedeva la compilazione del "*modulo di contestazione*"; aggiunge di avere presentato formale reclamo agli intermediari resistenti il 29/11/2024.

Fa presente che l'intermediario B riscontrava negativamente il predetto reclamo in data 18/12/2024, riferendo che la cliente era stata vittima di *phishing* e aveva fornito i codici di autenticazione, comunicando altresì di avere rimborsato la somma di € 199,00 quale "*differenza tra la 2^ e la 3^ operazione*" e di avere attivato le procedure di *recall* "*non appena è stata informata della circostanza*".

Espone che in data 06/12/2024 anche l'intermediario A riscontrava il reclamo, dichiarandosi esente da ogni responsabilità in quanto i bonifici contestati erano stati eseguiti sulla carta dell'intermediario B intestata alla ricorrente.

Ciò premesso, lamenta la violazione del d.lgs. n. 11/2010 in relazione alle menzionate operazioni di pagamento, nonché l'onere di diligenza professionale richiesto dall'art. 1176, co. 2 c.c., considerato che in "*pochi minuti*" sono state effettuate diverse operazioni, tra cui l'acquisto di criptovalute, il loro immediato disinvestimento ed il successivo invio dei fondi a mezzo bonifico a soggetti terzi, senza che tali circostanze fossero rilevate dagli intermediari resistenti.

Lamenta, altresì, la violazione dell'art. 2050 c.c. e dell'art. 15 d.lgs. n. 196/2003 in relazione all'illecito trattamento dei propri dati personali.

Contesta la circostanza che entrambe le convenute non hanno posto limiti giornalieri per i bonifici (intermediario A) e per i pagamenti con carta (intermediario B), che le avrebbero consentito almeno di ridurre i danni.

Chiede, quindi, la condanna degli intermediari resistenti "*alla restituzione/ripetizione/rifusione delle somme indebitamente sottratte pari a €. 5.505,00*".

Costituitosi, l'intermediario A afferma che la ricorrente è titolare di un conto corrente acceso nel 2016 a valere sul quale, in data 14/11/2024, veniva eseguito un bonifico di € 5.500,00 mediante l'utilizzo dei "*codici personali*".

Fa presente di avere dato seguito all'ordine di pagamento, provvedendo ad inviare specifico SMS-*alert* al recapito telefonico censito, nonché notifica *push,* e che in pari data la cliente disconosceva la predetta disposizione, presentando il successivo 28/11/2024 formale reclamo, riscontrato negativamente il 06/12/2024.

Ciò premesso, precisa che alcuna evidenza documentale di quanto dichiarato dalla ricorrente in sede di denuncia e di ricorso risulta prodotto in atti, con particolare riguardo alla chiamata ricevuta, nonché alla "*serie di operazioni*" eseguite il giorno della frode.

Evidenzia che la ricorrente ha dato seguito alle istruzioni impartite da un soggetto che l'ha contattata presentandosi come operatore dell'intermediario B ed in relazione al blocco di una carta di pagamento detenuta sempre dalla ricorrente presso l'intermediario B: pertanto, nel "*disegno criminoso*" del frodatore non vi era alcun riferimento all'intermediario A.

Aggiunge che l'unica disposizione di bonifico eseguita dal conto corrente veniva effettuata verso altro conto avente pari intestazione, quindi in assenza di una "*vera e propria*" perdita patrimoniale, e che i bonifici verso tale IBAN erano frequenti (22 nell'ultimo anno); ritiene pertanto non fondata la contestazione in ordine al mancato monitoraggio dell'operazione.

Precisa inoltre, che a seguito del bonifico la ricorrente ha ricevuto sul proprio numero di telefono sia un SMS-*alert*, sia una notifica *push* dall'*app* con i dettagli dell'operazione appena eseguita.

Evidenzia, altresì, che, secondo la ricostruzione dei fatti, i malfattori avrebbero operato contestualmente su rapporti di conto detenuti su due intermediari diversi, ciò rappresentando un ulteriore elemento presuntivo della condotta gravemente colposa dell'utente.

In relazione all'asserita violazione dell'art. 2050 c.c. e dell'art. 82 GDPR, sostiene che la frode non è stata causata in alcun modo da un'illecita intromissione di terzi nei suoi

sistemi, ma dal comportamento gravemente negligente della ricorrente che ha comunicato al frodatore i propri codici personali.
Rinvia alla perizia tecnica di parte prodotta in atti per "*maggiori dettagli tecnici*" sul sistema di autenticazione delle operazioni adottato, da cui risulta estratto il procedimento di autorizzazione del bonifico in esame.
A sua volta costituitosi, l'intermediario B sostiene che, sulla base di quanto riferito dalla ricorrente in sede di denuncia, i danni lamentati sono riconducibili alle ormai note pratiche di "*phishing/vishing*".
Precisa che la ricorrente ha ottenuto il rimborso di una delle tre operazioni di bonifico disconosciute (€ 3.000,00) mediante l'immediata restituzione di € 2.801,01 e la successiva restituzione della differenza (pari ad € 199,00) in data 18/12/2024.
In relazione alle altre due operazioni di bonifico istantaneo rimanenti, per un ammontare complessivo di € 5.304,00, sostiene che le stesse sono state eseguite tramite SCA, sono state autenticate dal *device* in uso alla ricorrente e sullo stesso *device* sono giunte le notifiche *push* informative.
Sostiene inoltre che la cliente è incorsa con colpa grave nella violazione degli obblighi previsti dall'art. 7 d.lgs. n. 11/2010 per essersi fatta raggirare nonostante i presidi di sicurezza messi a disposizione dei clienti (richiama il "*bollino di sicurezza*" presente in *app* ogni volta che un suo operatore avvia un contatto con la clientela), nonché una campagna informativa di "*rafforzamento*" rivolta alla propria clientela al fine di sollecitare l'adozione di azioni tempestive di "*autotutela*".
Rileva che la ricorrente non ha prodotto alcuna evidenza della chiamata truffaldina ricevuta, richiamando il principio condiviso dai Collegi ABF secondo cui la mancata allegazione da parte del cliente di evidenze che consentono di ritenere attendibile il contatto ricevuto determina il rigetto della domanda di rimborso.
Evidenzia, altresì, la presenza di elementi discordanti nella ricostruzione dei fatti riportati dalla ricorrente, in quanto la telefonata sarebbe stata ricevuta alle ore 13:30, mentre le transazioni disconosciute sono state disposte dalle ore 12:13 alle ore 13:43; in particolare, le operazioni in uscita di € 3.000,00 e di € 2.500,00 sarebbero state disposte prima del contatto telefonico.
Precisa che le transazioni disconosciute, essendo bonifici istantanei, sono irrevocabili e che la ricorrente ha segnalato l'accaduto tramite un canale di comunicazione (email) che non ha caratteristiche di "*immediatezza e tempestività di riscontro*", mentre non ha provato di avere contattato telefonicamente il Servizio Assistenza Clienti.
Fa presente che la ricorrente non fornisce elementi utili a provare che le operazioni fossero realmente fraudolente, limitandosi a disconoscere le predette e contestando genericamente un illecito subito.
In relazione alla doglianza di controparte relativa all'illecito trattamento dei suoi dati personali, conferma la "*totale assenza*" di violazioni del suo sistema informatico.
Contesta altresì l'assunto di controparte relativo all'impostazione di un "*limite giornaliero*" alle operazioni di pagamento, in quanto "*tutti*" i suoi prodotti sono caratterizzati da un limite specifico, compreso le operazioni di bonifico istantaneo; precisa che l'operatività in contestazione, per numero e importo, si è svolta nei limiti fissati per la tipologia di prodotto utilizzata dalla ricorrente.
Da ultimo, evidenzia di aver attivato le procedure di *recall* dei bonifici, tuttavia senza esito.
Entrambi gli intermediari concludono per il rigetto del ricorso.
In sede di repliche, la ricorrente evidenzia che per mero "*errore materiale*" ha indicato in sede di denuncia un orario differente rispetto quello in cui ha ricevuto la telefonata dal sedicente operatore, confermando che la telefonata è pervenuta "*prima dell'operatività*" contestata.

Precisa che, "*cessata*" la telefonata, il suo *smartphone* si è spento ed alla sua riaccensione risultava "*completamente riformattato*" con conseguente perdita dei "*dati in entrata ed in uscita*", e che ha contattato gli intermediari utilizzando il telefono del suo compagno.
Richiama l'art. 10 d.lgs. n. 11/2010, sostenendo che è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento sia stata autenticata, correttamente registrata e contabilizzata, e che non si siano verificati malfunzionamenti delle procedure, nonché fornire la prova della frode, del dolo o della colpa grave dell'utente.
Ritiene che, seppur non sussista un "*dovere generale*" dell'istituto di credito di monitorare la regolarità delle operazioni disposte dal cliente, in applicazione del principio di buona fede nell'esecuzione del contratto sussiste un obbligo di protezione che gli impone di rifiutare l'esecuzione dell'operazione qualora appaia *ictu oculi* "*anomala*".
Precisa che, nel caso in esame, le operazioni disconosciute, eseguite "*in pochi secondi*", riguardavano l'acquisto di criptovalute, mentre l'operatività del conto è sempre stata "*di tipo ordinario*", con fondi utilizzati per le "*spese domestiche*" ed il pagamento delle "*bollette per utenza*".
All'atto delle controrepliche, l'intermediario A rileva che la ricorrente conferma di non essere in possesso di alcuna evidenza di quanto accaduto, con particolare riguardo alla chiamata ricevuta ed alla "*serie di operazioni*" eseguite su indicazione del sedicente operatore.
Ribadisce che nella ricostruzione dei fatti operata dalla ricorrente viene menzionato esclusivamente l'intermediario B e che l'unica operazione di bonifico è stata disposta verso un conto corrente intestato anch'esso alla ricorrente presso l'intermediario B e, pertanto, tale operazione non rappresenterebbe una "*vera e propria*" perdita patrimoniale ma rientra nella "*normale operatività*" della cliente effettuare bonifici verso il conto aperto presso l'intermediario B.
Conclude insistendo per l'accoglimento delle conclusioni formulate in sede di controdeduzioni.
Nelle proprie controrepliche l'intermediario B ribadisce che la ricorrente non ha fornito, nemmeno in sede di repliche, prove "*concrete*" di aver effettivamente ricevuto un contatto telefonico da parte di un presunto operatore.
Precisa che vi è "*netta*" discordanza tra le dichiarazioni rilasciate in sede di denuncia e gli orari di esecuzione delle operazioni disconosciute.
Fa presente che è onere della ricorrente fornire elementi idonei a circostanziare lo svolgimento dei fatti, ovvero allegare documentazione utile alla ricostruzione della vicenda, mentre nel caso in esame non risulta verificatasi.
Precisa che non è possibile accertare le reali modalità di "*attacco subito*" dalla ricorrente, poiché la stessa si limita ad argomentare i fatti senza fornire alcuna evidenza a supporto.
Sostiene di aver dimostrato che le operazioni in esame sono state correttamente contabilizzate, registrate ed autenticate mediante lo smartphone utilizzato dalla cliente (fattore di possesso) e l'inserimento della password (fattore di conoscenza), avendo prodotto i relativi *log*.
Evidenzia un ulteriore elemento di colpa grave della ricorrente consistente nel mancato tempestivo contatto del suo servizio clienti, avvenuto "*solamente 3 ore dopo i fatti*".
Conclude insistendo nell'accoglimento delle conclusioni formulate in sede di controdeduzioni.

DIRITTO

Premesso che le operazioni contestate erano state eseguite sotto il vigore del d.lgs. 27/01/2010, n. 11, come modificato dal d.lgs. 15/12/2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/01/2018, in sede di denuncia, presentata alle competenti autorità in data 15/11/2024, la ricorrente ricostruiva i fatti oggetto di controversia dichiarando che, il precedente 14/11/2024, alle ore 13:30 circa, veniva contattata telefonicamente dall'utenza n. 02*****977.

L'interlocutore si qualificava come operatore dell'intermediario B, riferendole che la sua carta di debito abbinata al conto era "*bloccata*", e che doveva eseguire una "*serie di operazioni per riattivarla*"; eseguiva "*quanto richiesto*" e, alle ore 14:30 circa, si accorgeva che il suo telefono cellulare era "*andato in blocco*"

Immediatamente contattava l'intermediario A, apprendendo in tale occasione che "*ignoti avevano svuotato*" il suo conto corrente, compiendo operazioni per un ammontare complessivo di € 5.505,00.

Più precisamente, la ricorrente disconosce sia l'operazione di bonifico di € 5.500,00 (oltre ad € 5,00 di commissioni) disposta il 14/11/2024, alle ore 12:12, dal conto corrente aperto presso l'intermediario A, sia le successive operazioni di bonifico disposte in pari data tramite la provvista costituita con tale somma dal conto aperto presso l'intermediario B di € 3.000,00 (ore 12:13), € 2.500,00 (ore 13:08) ed € 2.800,00 (ore 13:43).

Si precisa che è la stessa ricorrente in sede di denuncia a riconoscere un rimborso parziale di € 2.801,01 avvenuto il 14/11/2024, alle ore 13:41, e che l'intermediario B produce specifica evidenza contabile interna attestante l'ulteriore rimborso di € 199,00 il 18/12/2024, sostenendo che con tale ultimo rimborso la ricorrente "*nulla ha più da pretendere*" in relazione al primo bonifico di € 3.000,00.

Tali operazioni, ad eccezione dell'ulteriore rimborso di € 199,00, risultano altresì dalle liste movimenti prodotte in atti dalla ricorrente e relative ai menzionati conti, dal cui esame si evince altresì che i due bonifici di € 2.500,00 ed € 2.800,00 (oltre ad € 2,00 di commissione per ciascuna operazione) risultano essere istantanei e, pertanto, irrevocabili.

Sul punto, si richiama l'art. 17, co. 1 d.lgs. n. 11/2010, il quale prevede che "*una volta ricevuto dal prestatore di servizi di pagamento del pagatore l'ordine di pagamento non può essere revocato dall'utilizzatore*".

Alla luce delle predette movimentazioni, la pretesa della ricorrente ammonterebbe a € 5.304,00.

In ordine alla creazione della provvista tramite bonifico disposto a valere sul conto radicato presso l'intermediario A, si rammenta che il Collegio di Coordinamento ha statuito che: "*I pagamenti da e verso lo stesso utente titolare di diversi conti accesi presso lo stesso intermediario possono essere sottratti all'obbligo della SCA anche nell'ipotesi in cui essi abbiano costituito la provvista necessaria per la realizzazione di successive operazioni fraudolente*" (Collegio di Coordinamento, decisione n. 8671/2024)

Questo Collegio ha poi condivisibilmente applicato i medesimi principi anche quando le operazioni di costituzione della provvista sono avvenute tra rapporti dello stesso titolare intrattenuti presso due diversi intermediari in caso di cointeressenza tra gli stessi (così Collegio di Bari, decisione n. 4082/2025).

Per completezza, si rammenta che i Collegi di Palermo e Milano, a fronte di una fattispecie analoghe a quella appena descritta, hanno ritenuto necessaria l'adozione della SCA, ma al contempo hanno comunque ritenuto di non poter accogliere il ricorso perché il trasferimento mediante le operazioni disconosciute in favore di un rapporto di titolarità dello stesso ricorrente, pure intrattenuto presso un PSP terzo, non integra, isolatamente

considerato, un evento dannoso (Collegio di Palermo, decisione n. 3379/2025), ovvero poiché all'interno della catena causale generatrice del nocumento economico in danno del cliente rilevano soltanto le operazioni successive verso i terzi (Collegio di Milano, decisione n. 4494/2025).

Nel caso di specie, i conti sono radicati presso due PSP diversi non legati da cointeressenze, in quanto appartenenti a gruppi distinti che non collocano l'uno i prodotti dell'altro.

Pertanto, appare innanzitutto opportuno vagliare le modalità di autenticazione dell'operazione di bonifico di € 5.500,00, effettuata a valere sul conto radicato presso l'intermediario A e che ha costituito la provvista per l'esecuzione delle operazioni contestate.

L'intermediario A sostiene che il giorno della frode (14/11/2024) è stato eseguito l'accesso all'area riservata mediante *app* associata univocamente al *device* del cliente (elemento di possesso) inserendo il codice cliente ed il codice di accesso (elemento di conoscenza).

Precisa che, una volta all'interno dell'area personale, sono stati inseriti i dettagli del bonifico; successivamente è stata inviata una notifica in *app*, è stato inserito il PIN personale all'interno dell'*app* che ha generato un OTP dinamico "*usa e getta*" inviato per verifica ai sistemi della banca.

Si può dunque sostenere che l'intermediario A abbia fornito prova della conformità a SCA dell'operazione di creazione della provvista (in senso conforme, Collegio di Roma, decisione n. 1657/2025).

Per quanto concerne le operazioni contestate, preliminarmente l'intermediario B fa presente che in data 10/05/2024 la ricorrente ha associato un *device* al proprio *internet banking* e che da tale data utilizza il medesimo dispositivo mobile.

Sostiene che in data 14/11/2024 risultano eseguiti "*multipli accessi*" da tale *device* ID 14154** al proprio *internet banking* a partire dalle ore 11:40, e che tramite tale *device* (elemento di possesso) sono state autorizzate in pari data le due operazioni di bonifico istantaneo oggetto del presente ricorso alle successive ore 13:08 (€ 2.500,00) e 13:43 (€ 2.800,00), mediante inserimento della password (elemento di conoscenza).

A supporto di quanto affermato produce i relativi *log* corredati da legenda esplicativa.

L'intermediario fa presente che per la corretta disposizione delle operazioni è obbligatorio:

- utilizzare il dispositivo associato all'*account* (requisito di possesso);
- inserire la password (requisito di conoscenza) o il parametro biometrico (requisito di inerenza).

Precisa che nel caso di specie le operazioni sono state eseguite:

- dal *device* associato al codice IB della ricorrente (requisito di possesso);
- tramite l'inserimento della password (requisito di conoscenza).

Allega il *log* di autorizzazione delle due operazioni e della relativa verifica della password inserita.

Senonché, dalla disamina di tali *log* mentre risulta l'utilizzo del fattore di conoscenza (password), invece non si evince quello di possesso, in quanto manca un riferimento al *device* utilizzato.

E' pur vero che, secondo il più recente orientamento condiviso dai Collegi, ai fini 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; inoltre, anche eventuali dichiarazioni confessorie del cliente assumono valore di prova legale ai sensi dell'art. 2730 c.c.

Nel caso di specie, però, dai *log* – come appena evidenziato – non è possibile inferire la prova della conformità ai requisiti normativamente previsti in tema di SCA delle operazioni

contestate, né le difese dell'intermediario forniscono elementi documentali che possano colmare tale *deficit*; a ciò si aggiunga che la ricorrente nega non solo di aver utilizzato il proprio *device,* ma anche di aver comunicato al frodatore i propri codici personali.
Pertanto, si richiama in senso adesivo la giurisprudenza di questo Collegio che, in caso di difetto di prova in merito ad uno dei due fattori di autenticazione indicati e di ulteriori elementi a supporto, non ha ritenuto provata l'adozione della SCA (cfr. per tutte più di recente, Collegio di Bari, decisione n. 4082/2025).
Richiamata la normativa vigente in materia, il difetto della prova in ordine alla conformità a SCA delle operazioni contestate assorbe ogni altro motivo di ricorso, che pertanto è meritevole di accoglimento nei confronti dell'intermediario B.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario B corrisponda al ricorrente l'importo di € 5.304,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario B 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

Firmato digitalmente da
ANDREA TUCCI