COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) BARTOLINI	Membro designato dalla Banca d'Italia
(BA) NUZZO	Membro designato dalla Banca d'Italia
(BA) BUSSOLI	Membro di designazione rappresentativa degli intermediari
(BA) QUARTA	Membro di designazione rappresentativa dei clienti

Relatore FRANCESCA BARTOLINI

Seduta del 07/04/2025

FATTO

La ricorrente è correntista dell'intermediario A: al conto corrente sono associate due carte – una di credito e una di debito – emesse dall'intermediario B. Esaurita senza esito la fase del reclamo, la ricorrente si rivolge all'Arbitro chiedendo l'accertamento del proprio diritto alla restituzione dell'importo di 95.579,40 euro, corrispondente al valore di una serie di operazioni di pagamento che disconosce perché effettuate da terzi ignoti a seguito di una frode.
Nel ricorso afferma di aver ricevuto, il 27.6.2024, un SMS da un'utenza riconducibile all'intermediario B, che la informava di un "pagamento anomalo" e la invitava a contattare l'assistenza clienti a un numero di cellulare indicato nello stesso SMS. Riferisce di aver parlato telefonicamente con un sedicente funzionario antifrode, che la invitava a cliccare su un link contenuto in un SMS che avrebbe ricevuto dopo pochi istanti; ciò che poi faceva, con la convinzione di aver così bloccato un pagamento fraudolento; riceveva poi un messaggio tramite un'app di messaggistica istantanea, che la invitava a rimuovere le app riconducibili a entrambi gli intermediari convenuti, poiché compromesse; veniva poi contattata telefonicamente da una diversa utenza mobile, quel giorno e nei giorni successivi; il 9.7.2024 il sedicente operatore la informava che era stata eseguita un'operazione dispositiva dal conto corrente e la invitava ad attivarsi presso la filiale per sbloccare il conto;

lo stesso invito riceveva il 12.7.2024, per autorizzare, in filiale, un ulteriore bonifico dell'importo di 10.000,00 euro. Afferma di essersi accorta della frode solo il 21.7.2024, nonostante la natura anomala delle operazioni che risultavano disposte a valere sul suo conto corrente. Lamenta che le operazioni disconosciute superassero i limiti dispositivi giornalieri e mensili previsti contrattualmente, e di non aver ricevuto alcuna telefonata o comunicazioni di sorta da parte degli intermediari convenuti. Chiede, oltre al rimborso dell'ammontare complessivo delle operazioni disconosciute, il rimborso delle spese di assistenza professionale, che quantifica in 4.000,00 euro.

L'intermediario A, costituitosi, eccepisce che: il 9.7.2024 era la ricorrente a contattare, tramite un'app di messaggistica istantanea, il proprio gestore di fiducia, chiedendogli espressamente lo sblocco del bonifico di 4.990,00 euro che era stato bloccato dal sistema antifrode; il gestore, verificata la movimentazione anomala del conto corrente, chiedeva espressamente alla ricorrente se fosse a conoscenza anche degli altri bonifici effettuati dal conto, ricevendo risposta affermativa; il 12.7.2024 la ricorrente si recava personalmente in filiale per effettuare il bonifico dell'importo di 10.000,00 euro con causale "acquisto automobile"; l'operatore di sportello in quell'occasione le chiedeva conto dell'operatività anomala dei giorni precedenti, che veniva tuttavia confermata. Eccepisce che è la stessa ricorrente ad ammettere, nella denuncia, di aver rimosso le app degli intermediari dal proprio dispositivo mobile e di aver consentito le numerose operazioni di bonifico e prelevamento "grazie alle credenziali incautamente fornite" al frodatore; eccepisce l'individuazione delle operazioni disconosciute e la relativa quantificazione, che ritiene invece correttamente individuata per l'importo complessivo di 80.585,20 euro; eccepisce che le operazioni disconosciute sono state eseguite in parte mediante bonifico, in parte tramite c.d. pagamento "plick" (un servizio che permette il trasferimento di una somma di denaro a un beneficiario individuato esclusivamente tramite numero di telefono o indirizzo e-mail), in parte con prelevamenti cc.dd. "Smartcash" che non sono soggetti ai medesimi limiti previsti per quelli eseguiti con carta bancomat. Eccepisce la conformità dei propri sistemi di autenticazione e autorizzazione ai parametri SCA, in quanto basati su tre fattori (codice utente, password e PIN). Inoltre sottolinea come sia sempre necessario che il cliente registri un device sul quale poi possa ricevere le notifiche push per autorizzare le operazioni (c.d. enrollment, elemento di possesso); le singole autorizzazioni vengono poi rilasciate mediante codice PIN (elemento di conoscenza). Quanto al caso di specie eccepisce che dalle allegazioni tecniche prodotte, unitamente al tenore di quanto dichiarato dalla stessa ricorrente, si evince l'installazione di un nuovo dispositivo con il quale sono state eseguite tutte le operazioni contestate, mediante corretto funzionamento dell'autenticazione forte del cliente. Eccepisce dunque la colpa grave della ricorrente per negligente custodia delle credenziali personali. Chiede il rigetto anche della domanda di rimborso per le spese di assistenza professionale. In subordine, chiede di valutare il comportamento colposo della ricorrente ex art. 1227 c.c.

L'intermediario B, costituitosi, eccepisce la carenza di legittimazione passiva, perché il rapporto nel contesto del quale risultano addebitate le somme di cui è chiesta la restituzione è riferibile esclusivamente all'intermediario A e i prelevamenti disconosciuti non erano stati disposti tramite le proprie carte di pagamento, ma attraverso un'apposita funzionalità dell'app rilasciata dall'intermediario A; inoltre, il link contenuto nell'SMS civetta non sarebbe in alcun modo a sé riconducibile.

In fase di replica la ricorrente contesta la tempestività delle controdeduzioni presentate dall'intermediario A.

In controreplica l'intermediario A sostiene di aver rispettato il termine di 45 giorni di cui alle Disposizioni ABF per la presentazione delle proprie controdeduzioni.

DIRITTO

1. Il Collegio è chiamato a esprimersi sul diritto della ricorrente di vedersi rimborsato dagli intermediari resistenti l'importo di 95.579,40 euro, corrispondente al valore di varie operazioni di pagamento effettuate da terzi ignoti a seguito di una frode.
2. Il ricorso merita accoglimento nei termini e per le ragioni che seguono.
3. Va vagliata anzitutto l'eccezione preliminare di carenza di legittimazione passiva avanzata in controdeduzione dall'intermediario B, emittente delle carte di pagamento, il quale eccepisce che le operazioni disconosciute risultano addebitate sul conto intrattenuto presso l'intermediario A, e non eseguite con le carte di pagamento. L'esame dei documenti prodotti agli atti mostra che tutte le operazioni disconosciute sono state in effetti disposte attraverso il servizio di Internet Banking dell'intermediario A, senza utilizzo fisico o tokenizzazione fraudolenta delle carte. Del resto, la stessa ricorrente afferma che dal proprio smartphone è possibile visualizzare le operazioni effettuate tramite le carte emesse dall'intermediario B e collegate al conto radicato presso l'intermediario A e che non si riscontrano quelle relative ai prelevamenti disconosciuti. L'eccezione va dunque accolta, e la posizione dell'intermediario B stralciata.
4. Occorre, prima di passare alla valutazione nel merito, analizzare l'eccezione di tardivo deposito delle controdeduzioni avanzata dalla ricorrente, che è infondata perché, secondo le Disposizioni ABF – sez. VI, par. 1 – qualora l'intermediario aderisca a un'associazione degli intermediari, le controdeduzioni sono trasmesse entro il termine perentorio di 30 giorni alla predetta associazione, che entro il termine perentorio di 15 giorni dalla ricezione delle stesse provvede a inoltrarle alla Segreteria Tecnica; nel caso in esame il ricorso è stato inviato all'intermediario il 3.12.2024 a seguito di una richiesta di integrazione documentale inoltrata al ricorrente; le controdeduzioni risultano depositate il 31.1.2025, entro il termine di 45 giorni applicabile tenuto conto della sospensione dei termini della procedura – dal 23 dicembre al 6 gennaio – (Disp. ABF, sez. VII, par. 4).
5. Venendo al merito, tutte le operazioni disconosciute sono state disposte nella vigenza del d.lgs. n. 11/2010, così come modificato dal d.lgs. n. 218/2017, che ha recepito la nuova Direttiva sui servizi di pagamento nel mercato interno – 2015/2366/UE (c.d. PSD 2) – e del Regolamento Delegato (UE) n. 2018/389, nonché successivamente all'emanazione dell'*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019 in tema di autenticazione forte, appunto, *Strong Customer Authentication*, o SCA.
6. Si impone dunque, anzitutto, la verifica sul sistema di autenticazione predisposto dall'intermediario resistente e sul rispetto dei requisiti di cui alla predetta disciplina, la quale pone proprio sull'intermediario l'onere di 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» e che il sistema di autenticazione e autorizzazione delle operazioni di pagamento è conforme alla *Strong Customer Authentication* – SCA –, secondo cui è necessaria un'autenticazione c.d. a doppio fattore (un fattore "di possesso" e uno "di conoscenza").
7. Nel caso di specie le operazioni sono eterogenee nel tipo e consistono in: 10 bonifici (eseguiti tra il 27.6.2024 e il 12.7.2024 per un controvalore complessivo di 40.445,00 euro), 18 prelevamenti (eseguiti tra il 1°.7.2024 e il 5.7.2024 per un controvalore complessivo di 25.000,00 euro), 5 pagamenti c.d. plick, ossia operazioni di trasferimento di una somma di denaro in favore di un beneficiario individuabile attraverso il numero di telefono o l'indirizzo e-mail (eseguiti tra il 2.7.2024 e l'8.7.2024 per un controvalore complessivo di 40.083,00 euro) e 15 addebiti commissionali, relativi a bonifici e pagamenti "plick", per un controvalore

complessivo di 50,40 euro. L'importo contestato ammonta complessivamente a 105.578,40 euro. Vanno stralciate però due operazioni: (*i*) il bonifico da 10.000,00 euro – con la relativa commissione di 4,10 euro –, autorizzato in filiale personalmente dalla ricorrente, seppure a seguito dei raggiri perpetrati dal frodatore, per il quale non è applicabile la sopra richiamata disciplina sulla responsabilità dei PSP nei casi di operazioni non autorizzate e (*ii*) il pagamento "plick" del 5.7.2024, che risulta dai documenti prodotti agli atti stornato il 10.7.2024. L'ammontare oggetto del vaglio del Collegio risulta allora di 85.576,30 euro. Le operazioni vanno vagliate "per tipo" e per ciascun tipo va verificata la compatibilità ai parametri SCA del sistema di autenticazione del cliente e autorizzazione delle operazioni approntato dall'intermediario resistente.

8. Per quanto riguarda le operazioni online, l'intermediario sostiene la piena compatibilità ai requisiti SCA di tutte le fasi nelle quali si sono articolate le operazioni disconosciute. Afferma che sia la fase di accesso, sia quella di disposizione, siano state autorizzate tramite il token software installato precedentemente sul device del frodatore, a causa dell'incauto comportamento della ricorrente che avrebbe divulgato le proprie credenziali riservate, dopo aver cliccato il link contenuto nel messaggio civetta e disinstallato le app, sempre su indicazione dei truffatori. Quanto all'enrollment del nuovo device, afferma che risulta nel caso di specie l'installazione di un nuovo Token Software tramite l'invio di un codice di attivazione via SMS all'utenza mobile di titolarità della ricorrente (elemento di possesso) e la finalizzazione del login con il corretto inserimento di un codice user ID e della password (elemento di conoscenza). A supporto di quanto descritto produce copia delle schermate tratte dal proprio sistema informatico dalle quali risulta come, a seguito della rimozione delle app a opera della stessa ricorrente su indicazione del truffatore, sia stato in effetti eseguito l'enrollment del nuovo device il 27.6.2024; il sistema, rilevando un nuovo dispositivo, non ha consentito l'accesso ma ha richiesto un secondo fattore di autenticazione, mediante invio di una OTP via SMS e subito dopo il truffatore ha inserito il codice pervenuto sull'utenza mobile intestata alla ricorrente; l'operazione risulta quindi andata a buon fine. Dalla copia del contratto relativo al servizio di internet banking si evince che il numero di telefono al quale è stata inviata la OTP coincide con quello indicato dalla ricorrente.

9. Con particolare riferimento ai bonifici, i primi sei "urgenti", gli altri tre "istantanei", e dunque preceduti, secondo quanto segnalato dall'intermediario, dall'attivazione del relativo servizio, la sessione di login risulta effettuata con il nuovo device (elemento di possesso) e con l'inserimento di una password (elemento di conoscenza). I documenti prodotti agli atti mostrano l'accesso tramite il device del frodatore configurato secondo le descritte modalità (elemento di possesso) e mediante uso della password (elemento di conoscenza). Le stesse modalità di autenticazione del cliente e autorizzazione delle operazioni caratterizzano i bonifici istantanei e, prima ancora, l'attivazione del servizio necessario a disporli. In questo caso, dunque, il sistema approntato dall'intermediario appare al Collegio conforme ai requisiti SCA.

10. Venendo ai prelevamenti c.d. Smartcash, le copie dei log prodotti dall'intermediario mostrano l'uso del device del frodatore installato secondo le già descritte modalità e l'inserimento di una password (elemento di conoscenza) per eseguire l'accesso. Per l'attivazione del servizio risulta inviata una password OTP al numero di cellulare intestato alla ricorrente. Tuttavia, le evidenze prodotte non consentono al Collegio di ricavare riferimenti ai fattori di autenticazione adottati per la fase dell'esecuzione dei prelevamenti disconosciuti, di talché il Collegio non ritiene assolto l'onere probatorio descritto in apertura in relazione ai prelevamenti c.d. Smartcash, per i quali, in conformità con quanto affermato dal Collegio di Coordinamento (n. 22745/2019), il profilo della colpa grave della ricorrente, eccepita in controdeduzione dall'intermediario, è assorbito dalla carenza di prova sul rispetto dei requisiti SCA: la prova di autenticazione rappresenta infatti, in aderenza al dato

normativo, un prius logico rispetto alla prova della colpa grave dell'utente. La domanda, *in parte qua*, va accolta.

11. Venendo infine ai pagamenti "plick", l'intermediario afferma che ogni transazione risulta preceduta da un'autonoma sessione di accesso. I log di cui produce copia mostrano l'utilizzo del device del truffatore registrato secondo le modalità già descritte (fattore di possesso) e l'inserimento della password (fattore di conoscenza). Nell'ambito della stessa sessione (riutilizzo dell'elemento di possesso), il pagamento risulta autorizzato con un nuovo inserimento della password, (elemento di conoscenza). In questo caso il Collegio ritiene provata la compatibilità SCA del sistema adottato dall'intermediario.

12. Per quanto riguarda i bonifici e i pagamenti "plick", tipo di operazioni per le quali il Collegio ha ritenuto il sistema dell'intermediario conforme a SCA, è necessario a questo punto vagliare l'eccezione di colpa grave della ricorrente avanzata dall'intermediario in controdeduzione. Va rammentato a tal proposito il principio espresso dal Collegio di Coordinamento con la già menzionata decisione n. 22745/2019, per cui «[…] 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». La colpa grave dell'utente può dunque ritenersi provata anche attraverso il combinarsi di più elementi indiziari, e anche, quindi, in via presuntiva, sulla base delle risultanze agli atti del procedimento in relazione alle modalità con le quali l'operazione truffaldina è stata posta in essere.

Nel caso di specie la ricorrente, nella denuncia, ha dichiarato che il primo messaggio civetta proveniva da un'utenza riconducibile all'intermediario B. È agli atti la copia dell'SMS, che non appare inserirsi in una chat contenente messaggi genuini; il messaggio contiene l'invito a telefonare un numero di cellulare non riconducibile all'intermediario, e si riscontrano diversi errori grammaticali. Mancano supporti probatori in relazione alle telefonate intercorse, ed è pacifico che la ricorrente abbia seguito l'indicazione del frodatore, in una chat di messaggistica istantanea – della quale sono agli atti le copie delle schermate –, di disinstallare le app degli intermediari. Risulta, inoltre, che la OTP inviata via SMS all'utenza mobile della ricorrente informasse espressamente dello scopo relativo all'attivazione di un token software. Sono poi agli atti le schermate dell'app di messaggistica istantanea e dell'interlocuzione con il servizio clienti dell'intermediario dai quali emerge come quest'ultimo avesse bloccato l'ordine del primo bonifico fraudolento, che è proprio la ricorrente ad aver chiesto di sbloccare.

13. Alla luce delle circostanze sopra descritte, il Collegio ritiene provata la colpa grave della ricorrente, la quale ha negligentemente cooperato con i frodatori consentendo il buon esito della frode.

14. Quanto alla mancata attivazione di sistemi di alert, l'interlocuzione sopra menzionata mostra che la ricorrente era a conoscenza degli addebiti (ritenuti erroneamente genuini) a valere sul proprio conto corrente. In ogni caso, l'invio sull'utenza telefonica della ricorrente del messaggio contenente la OTP autorizzativa dell'enrollment dell'app sul device del truffatore rende […] ininfluente la circostanza che non siano state fornite indicazioni circa l'operatività di un sistema Sms-Alert *ex post* (fra le molte, in tal senso, questo Collegio, n. 6971/23).

15. La condotta dell'intermediario resistente non merita censura con riferimento alla mancata attivazione in presenza di indici di frode: è provato che, dal 9.7.2024, ravvisata in effetti un'anomalia nella movimentazione del conto, l'intermediario resistente ha bloccato il

primo bonifico istantaneo, tuttavia disposto ugualmente a seguito della richiesta di sblocco pervenuta dalla stessa ricorrente.
16. Infine la contestazione sul superamento dei limiti dispositivi contrattualmente pattuiti: poiché nel caso di specie l'operatività fraudolenta è stata caratterizzata dall'attivazione e dall'utilizzo di apposite funzionalità dell'app, senza utilizzo delle carte fisiche, i limiti operativi rilevanti nel caso di specie sono quelli previsti per le disposizioni impartite tramite internet banking, che non risultano superati.
17. Infine non merita accoglimento la domanda di rifusione delle spese di assistenza professionale, presentata solo nel ricorso, e non nel prodromico reclamo e, in ogni caso, priva di alcuna documentazione probatoria di supporto.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario A corrisponda al ricorrente l'importo di € 25.000,00.
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

Firmato digitalmente da
ANDREA TUCCI