

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) DEPLANO	Membro designato dalla Banca d'Italia
(RM) SICA	Membro di designazione rappresentativa degli intermediari
(RM) MASTROROSA	Membro di designazione rappresentativa dei clienti

Relatore STEFANO DEPLANO

Seduta del 18/02/2026

FATTO

Parte ricorrente rappresenta che: i.) in data 5 marzo 2025 ha ricevuto sul proprio cellulare alcuni SMS apparentemente provenienti dall'Intermediario terzo, emittente la carta di pagamento collegata a un conto in essere presso la Banca convenuta; ii.) gli SMS, ignorati, la avvertivano dell'esistenza di "problemi tecnici" e la invitavano a cliccare su un *link* allegato; iii.) tempo dopo, precisamente il 27 marzo, ha ricevuto una telefonata da parte di un sedicente operatore della convenuta che l'ha convinta a porre in essere alcune operazioni al fine di risolvere i "problemi tecnici" indicati nell'SMS; iv.) dando seguito a tali richieste, ha seguito le istruzioni impartite dal sedicente operatore; v.) ha quindi disattivato l'APP presente sullo *smartphone*; vi.) insospettita, ha contattato il numero verde della Banca per apprendere che ignoti avevano effettuato un bonifico di importo pari a 11.700,00 (undicimilasettecento/zero) euro dapprima per spostare la somma sulla carta e, successivamente, per trasferirla ad un terzo; vii.) i dati relativi alle disposizioni sono stati interamente inseriti dai frodatori; viii.) l'Intermediario terzo, emittente la carta di pagamento, ha già rimborsato un importo pari alla metà dell'ammanco subito.

Parte resistente riferisce che: i.) le operazioni dispositive sono state eseguite dopo essere state autenticate, correttamente registrate e contabilizzate, come comprovato dall'estratto delle registrazioni elettroniche versato in atti; ii.) le transazioni sono state ordinate dal *device* normalmente utilizzato dal ricorrente; iii.) dalle evidenze informatiche emerge che, alle ore 18:20 del giorno 27 marzo 2025, è stato eseguito un accesso tramite APP correttamente validato dall'OTP generato dal citato *device* previa autenticazione con fattore biometrico; iv.) in pari data, alle ore 18:28, è stato effettuato

l'inserimento di un bonifico istantaneo, confermato previa autenticazione con fattore biometrico e validazione del codice OTP; v.) l'operazione è stata resa possibile soltanto a seguito della condotta gravemente colposa della ricorrente che ha disposto il pagamento sotto la guida del truffatore; vi.) non sono versati in atti elementi probatori utili a verificare il numero dal quale proveniva la telefonata né altri elementi utili.

In sede di repliche, ribadito di non aver effettuato in autonomia il bonifico oggetto di controversia, parte ricorrente evidenzia di essere rimasta vittima di *spoofing* e rappresenta un possibile *enrollment* dell'APP su un nuovo dispositivo.

In sede di controrepliche, evidenziato che dai *log* emerge con certezza che l'operazione controversa è avvenuta dall'APP installata sul *device* della ricorrente, si esclude l'*enrollment* su un altro dispositivo. Parte ricorrente chiede la restituzione della somma di 5.850,00 (cinquemilaottocentocinquanta/zero) euro, pari alla metà dell'importo di altro bonifico, già disconosciuto e rimborsato al 50% da altro Intermediario.

Parte resistente insiste per il rigetto del ricorso.

DIRITTO

1. – La controversia ha ad oggetto il disconoscimento di un bonifico dell'importo di 11.700,00 euro eseguito a favore di un altro rapporto da lei stessa intrattenuto presso un Intermediario terzo. Da tale ultimo rapporto è stato poi disposto un nuovo bonifico istantaneo a favore di un conto intestato a beneficiario sconosciuto.

1.1. – Mette conto evidenziare che metà dell'importo movimentato è già stato restituito dal destinatario del primo bonifico.

2. – La ricorrente nega di aver eseguito l'operazione controversa e afferma che i frodatori avrebbero, dapprima, scaricato l'APP su un proprio dispositivo e poi, attraverso quest'ultimo, disposto sia il primo bonifico (quello oggi in contestazione) sia la seconda transazione (mediante la quale è stata trasferita a terzi la somma in contestazione).

3. – L'operazione contestata è stata effettuata sotto la vigenza del d.lgs. n. 11 del 2010, così come modificato dal d.lgs. n. 218 del 2017, che ha recepito la nuova Direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015 (c.d. PSD 2). In base a tali disposizioni, come applicate da questo Arbitro (cfr. Coll. Coord., dec. n. 22745 del 2019), occorre volgere l'attenzione a due dirimenti profili disciplinari. In primo luogo, è l'Intermediario a dover provare, oltre all'insussistenza di malfunzionamenti, l'autenticazione, la corretta registrazione e la contabilizzazione dell'operazione, dovendo in particolare fornire evidenza che l'operazione disconosciuta sia stata autenticata con un c.d. "Sistema di autenticazione forte" (SCA), posto che ai sensi del comma 2 *bis*, art. 12, d.lgs. n. 11 del 2010, come inserito dal d.lgs. n. 218 del 2017 «salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accertano l'autenticazione forte del cliente». In secondo luogo, è sempre l'Intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.

4. – Con riferimento al primo profilo, l'Intermediario versa in atti puntuale documentazione. Da questa si evince che l'accesso in APP è avvenuto alle ore 18:20 attraverso la validazione con fattore biometrico e inserimento dell'OTP dal *device* della ricorrente. Si ricava, in secondo luogo, che alle 18:28 è stato disposto il bonifico oggetto del ricorso confermato con il codice OTP dal *device* del ricorrente, previa validazione con fattore biometrico.

4.1. – A fronte di similari evidenze documentali, prodotte dallo stesso Intermediario in controversie analoghe a quella odierna, l'ABF ha ritenuto provata l'autenticazione della operazione contestata e *compliant* con la SCA il sistema di pagamento adottato dal PSP (Coll. Torino, dec. n. 92 del 2023).

4.2. – L'Intermediario ha quindi dato prova di essersi dotato di un sistema di autenticazione forte in linea con la normativa di settore.

5. – Con riferimento al secondo profilo innanzi richiamato assume rilievo assorbente la circostanza che il bonifico disconosciuto è stato eseguito a beneficio di un altro rapporto, anch'esso intestato alla ricorrente e acceso presso un Intermediario estraneo al presente giudizio. Il bonifico istantaneo mediante il quale si è effettivamente realizzato un ammanco nel patrimonio della ricorrente è stato disposto, a ben vedere, da tale ultimo rapporto.

5.1. – Secondo un costante indirizzo interpretativo fatto proprio dai Collegi, se il bonifico è disposto a favore di un conto intrattenuto dallo stesso ricorrente presso un Intermediario terzo, l'operazione di costituzione della provvista non concretizza un danno patrimoniale (Coll. coord., dec. n. 8671 del 2024; Coll. Milano, dec. n. 2190 del 2025; Coll. Roma, dec. n. 10242 del 2025). Si tratta di un orientamento che merita di essere confermato anche in relazione al presente giudizio in quanto l'operazione oggi disconosciuta non ha cagionato alcun detrimento patrimoniale nel patrimonio del ricorrente il quale, invece, è stato danneggiato unicamente dal secondo bonifico (peraltro già parzialmente rimborsato) realizzato tramite i sistemi di un PSP estraneo alla presente controversia.

6. – Per completezza si evidenzia che lo *smishing* misto a *vishing* asseritamente subito dal ricorrente non risulta in alcun modo documentato.

7. – Tanto posto, il ricorso non è fondato e non può essere accolto.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE