Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI NAPOLI

composto dai signori:

(NA) CARRIERO	Presidente
(NA) BENEDETTI	Membro designato dalla Banca d'Italia
(NA) MARIANELLO	Membro designato dalla Banca d'Italia
(NA) NERVI	Membro di designazione rappresentativa degli intermediari
(NA) SORRENTINO	Membro di designazione rappresentativa dei clienti

Relatore ESTERNI - GIUSEPPE SORRENTINO

Seduta del 24/02/2026

FATTO

Il ricorrente afferma che: *(i)* in data 26/01/24 la banca lo avvisava dell'arrivo di una nuova carta di debito; *(ii)* tra febbraio e marzo, dopo aver contattato la banca per avere notizie sulla mancata consegna della carta, apprendeva che la spedizione non era andata a buon fine e che sarebbe stata riemessa una nuova carta; *(iii)* in data 06/03/24 riceveva una chiamata dal numero della banca ed il presunto operatore (che possedeva i dati della carta spedita il 26/01/24) gli spiegava che per riemettere una nuova carta bisognava attivare una nuova procedura, per tale ragione accedeva ad un link inviatogli via sms e poi trasmetteva al presunto operatore l'OTP generato; *(iv)* durante la telefonata riceveva notifica sul cellulare dell'avvenuta effettuazione di un bonifico istantaneo di € 4.900,00; *(v)* segnalata la cosa all'operatore questi sosteneva che era un errore e che avrebbe annullato l'operazione; *(vi)* da successiva verifica si avvedeva che non vi era stato alcuno storno, risultando l'ammanco di € 4900,00, per tare ragione avvisava subito la banca e si recava dai Carabinieri. Insoddisfatto dell'interlocuzione con l'intermediario, che ha rifiutato il rimborso dell'operazione contestata, ricorre all'Arbitro. L'intermediario, nel costituirsi, precisa che: *(a)* adotta un sistema di autenticazione forte di accesso all'Area Riservata e di autorizzazione delle disposizioni di pagamento; *(b)* il cliente ha attivato il Servizio Token in data 15 Dicembre 2022 su uno smartphone Apple_iPhone, al quale vengono inviate tutte le PUSH; *(c)* i fattori di autenticazione impiegati per l'accesso all'area riservata sono la notifica PUSH inviata sul dispositivo registrato del cliente (elemento di possesso) e il riconoscimento del volto (elemento di inerenza); *(d)* l'operazione è stata autenticata nella pagina web della banca tramite inserimento del codice Token generato nell'App della banca (si tratta di "procedura offline", alternativa

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

all'invio della notifica PUSH, dove il codice Token generato parrebbe assimilabile all'SMS OTP e quindi configurabile come elemento di possesso, mentre il secondo fattore può essere rinvenuto nel riconoscimento facciale, fattore di inerenza inserito nella fase di accesso al conto). Tanto osservato, l'intermediario insiste per il rigetto del ricorso.

DIRITTO

Il ricorrente disconosce un bonifico istantaneo eseguito on line con l'utilizzo di credenziali a lui riferibili e per l'importo di € 4.900,00. Per la risoluzione della questione le coordinate ermeneutiche vanno ricavate dal D. Lgs. 27 gennaio 2010 n. 11, come modificato dal D. Lgs. 15 dicembre 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 particolare, le fonti normative che regolano la strong customer authentication (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PSD2, nell'articolo 10 bis del D. Lgs. n. 11/2010, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14 settembre 2019, nonché nei criteri interpretativi forniti dall'EBA (v. in particolare il parere dell'EBA del 21 giugno 2019). Nel caso in esame, come precisato dall'intermediario, l'autorizzazione dell'operazione, resa possibile dopo che il cliente è entrato in autonomia (seppur indotto dal truffatore) nella sua area personale è avvenuta con la generazione di un "Codice di operazione temporaneo" che, inserito nell'APP (in esclusivo possesso del ricorrente), ha generato il codice Token trasmesso dall'ultimo al frodatore; tanto ha reso possibile la consumazione della truffa. Da tali dati, confermati dai tracciati informatici, si ricava la piena conformità delle procedure autorizzative alla Strong Customer Authentication. Per completezza di analisi si osserva che sulla medesima procedura l'Arbitro ha avuto modo di esprimersi, argomentando come esegue: *"risulta che il codice OTP necessario per l'autenticazione dell'operazione è stato inserito nella medesima sessione autorizzata con il precedente inserimento di password e OTP. Ragion per cui si può da ritenere che l'elemento di conoscenza (password) precedentemente inserito possa costituire il primo fattore di autenticazione anche per tale operazione, secondo quanto chiarito dall'EBA (v. Opinion EBA 2018_4141)." (Collegio di Milano, decisione n.1212 del 04.02.2025).* Accertato il rispetto da parte dell'intermediario della normativa tecnica sulle procedure di autorizzazione e registrazione delle operazioni, occorre ora indagare sulle condotte delle parti al fine di ripartire correttamente le responsabilità a seconda del grado di negligenza addebitabile a ciascuna di esse. Analizzando il comportamento tenuto nella circostanza dalla parte ricorrente, pare che esso non si mostri esente da censura in quanto, nonostante la procedura suggerita dal truffatore per la riemissione della carta fossa anomala, ha incautamente *(i)* digitato i codici che hanno consentito (al truffatore) l'accesso alla pagina web della banca e *(ii)* trasmesso (al truffatore) il codice token reso solo a lui visibile sull'APP installata su device in suo esclusivo possesso. Al pari, però, non può non tenersi in adeguata considerazione che nessuna truffa si sarebbe concretizzata qualora il nuovo strumento di pagamento fosse giunto al legittimo destinatario e, quindi, qualora non fosse stato intercettato dal truffatore. Infatti, considerando che *(a)* a causa dell'impossessamento della carta il truffatore si è reso credibile agli occhi del ricorrente (dimostrandogli di essere in possesso dei suoi dati personali) e che *(b)* il cliente è stato contattato da numero identico a quello dell'intermediario, la truffa contiene elementi di sofisticazione tali da giustificare parzialmente la condotta del ricorrente. A tanto va aggiunto che secondo l'articolo 8 del D.lgs 11/2010 *"I rischi derivanti dalla spedizione di uno strumento di pagamento o delle relative credenziali di sicurezza personalizzate sono a carico del prestatore di servizi di pagamento.* Nel caso in esame, come già rilevato in altre circostanze da questo Collegio, emerge la mancata adozione da parte dell'intermediario di presidi di sicurezza idonei a evitare l'ingerenza di terzi nella sfera patrimoniale del cliente**.** (Collegio di Napoli – decisione n. 5196/24)**.** Alla luce delle suesposte considerazione pare giusto concludere che ciascuna parte sia responsabile nella

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

misura del 50%, ragion per cui l'intermediario sarà tenuto a risarcire il danno per la sua quota parte e per un importo pari ad € 2450,00.

P.Q.M.

In parziale accoglimento del ricorso, il Collegio accerta il diritto del ricorrente alla restituzione dell'importo di € 2.450,00 oltre interessi legali dalla data del reclamo.
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