COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) PIRAINO	Membro designato dalla Banca d'Italia
(PA) SCIBETTA	Membro di designazione rappresentativa degli intermediari
(PA) CLEMENTE RUIZ	Membro di designazione rappresentativa dei clienti

Relatore FABRIZIO PIRAINO

Seduta del 26/06/2025

FATTO

Il ricorrente riferisce che, in data 26/02/2025, riceveva una telefonata da parte di un operatore della Banca, il quale comunicava che, per motivi di sicurezza l'*account* era stato bloccato, poiché risultava una transazione sospetta effettuata verso un sito di compravendita di criptovalute. Durante la conversazione telefonica cercava di accedere al proprio *account* per verificare la veridicità di quanto riferitogli, ma non riusciva a effettuare l'accesso in quanto l'*account* era bloccato. Non riuscendo ad accedere all'*account* e fidandosi dell'interlocutore, seguiva quanto lo stesso gli riferiva al fine di bloccare la transazione e, pertanto, procedeva a comunicargli i codici che riceveva via via tramite SMS. Una volta comunicati tali codici, la telefonata si concludeva e nel frattempo riceveva la notifica di avvenuta esecuzione di una transazione di € 753,75. Decorse ventiquattro ore e constatando che non riceveva il rimborso atteso, il ricorrente realizzava di essere caduto vittima di frode. Egli presentava, quindi, denuncia ai Carabinieri e disconosceva l'operazione, ma l'Intermediario rigettava la richiesta di rimborso. Con il ricorso, l'istante domanda il rimborso della somma di € 753,75.
In sede di controdeduzioni, l'intermediario eccepisce che l'operazione disconosciuta dal cliente (eseguita alle 17:11 e non alle 16:11 così come da lui sostenuto) è stata correttamente autorizzata mediante l'utilizzo delle credenziali statiche e dinamiche in possesso del Cliente stesso con autenticazione forte a due fattori. La vicenda ha visto la

colpevole collaborazione del ricorrente, che, come ammesso anche nel ricorso, ha condiviso tutti i codici OTP ricevuti sul proprio numero di cellulare, senza i quali il truffatore non avrebbe potuto eseguire l'operazione. Il ricorrente sostiene, inoltre, di aver ricevuto sul proprio numero di cellulare una telefonata da un numero apparentemente proveniente dalla Banca, ma non ha fornito alcuna prova in merito. Su tali basi di fatto e di diritto, l'intermediario chiede il rigetto della domanda.

DIRITTO

Le operazioni contestate sono state poste in essere sotto il vigore del 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, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, e di adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta. In particolare, le fonti normative che regolano la *strong customer authentication* (cd. SCA) sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 *bis* d.lgs. 10/2011, 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).
Il ricorrente disconosce un'operazione di pagamento di € 753,75, eseguita in data 26/02/2025 alle ore 17:11.
Dalle deduzioni dell'intermediario resistente e dei log allegati emerge che: a) l'accesso prodromico all'operazione dispositiva è avvenuto mediante doppio fattore ovvero: password (elemento di conoscenza) e OTP (elemento di possesso); b) il reset della *password* è avvenuto unicamente mediante inserimento del fattore di conoscenza (due cifre del PIN della carta). Si potrebbe considerare come secondo fattore di autenticazione il riutilizzo di un sms OTP adoperato in precedenza, ma l'intermediario non ne fa menzione nelle controdeduzioni; c) l'operazione dispositiva è avvenuta mediante doppio fattore costituito dal CVV dinamico (che l'intermediario qualifica come elemento di conoscenza giacché nel processo di generazione del medesimo CVV si è adoperato un fattore di conoscenza) e OTP (elemento di possesso); d) il ricorrente ammette di aver comunicato tutti i codici ricevuti tramite sms durante la conversazione col finto operatore.
Nel caso di specie è necessario stabilire la valenza attribuibile al codice CVV dinamico, che l'intermediario qualifica come elemento di "conoscenza". Alla luce delle indicazioni fornite dall'EBA nell'Opinion del 21 giugno 2019, il CVV dinamico parrebbe essere qualificabile come elemento di possesso. In alcuni precedenti dell'Arbitro, in cui veniva in rilievo l'autenticazione mediante CVV dinamico, quest'ultimo è stato qualificato come elemento di possesso (in questo senso, Collegio di Bari, decisione n. 9345 del 27 settembre 2023; Collegio di Roma, decisioni n. 2840 del 22 marzo 2023 e n. 10679 del 6 novembre 2023; da ultimo, Collegio di Milano, decisione n. 8153 del 13 luglio 2024). Com'è noto, un doppio fattore di possesso non risulta conforme alla SCA in quanto, in base alla citata Opinion dell'EBA, l'autenticazione forte presuppone il ricorso a due fattori di autenticazione appartenenti a categorie diverse. Per di più, in procedimenti originati da ricorsi nei confronti del medesimo intermediario qui convenuto, caratterizzati da analoghe modalità di autenticazione tramite CVV dinamico, il Collegio di Milano ha ritenuto non provata l'autenticazione a doppio fattore (Collegio di Milano, decisione n. 3554 del 20/03/2024; Collegio di Milano, decisione n. 8153 del 13 luglio 2024). E, nello stesso

senso, si è pronunciato il Collegio di Torino, decisione n. 7207 del 19/06/2024 e, da ultimo, anche il Collegio di Palermo, che, con la decisione n. 2775 del 13/03/202,5 ha ritenuto non provata l'autenticazione a doppio fattore.
E tuttavia vanno anche considerate le modalità con cui si genera il CVV dinamico. Il CVV dinamico viene generato con inserimento di un OTP sms dall'interno dell'area personale del cliente. Poiché l'accesso all'area personale richiede l'uso di password + OTP sms (accesso web), la generazione del CVV dinamico prevede in concreto l'uso di almeno due diversi fattori, uno di conoscenza e l'altro di possesso. La procedura di autenticazione delle operazioni, nel prevedere l'utilizzo del CVV dinamico (generato all'interno dell'area riservata), recupera un fattore dal processo di generazione di tale codice (conoscenza) e vi aggiunge l'elemento di possesso rappresentato da un OTP sms inviato al numero certificato del cliente. In tale senso si è orientato il Collegio di Napoli, con decisione n. 3006/2025, nella quale si è ritenuto di qualificare il CVV dinamico come fattore di conoscenza, valorizzando il riutilizzo di un fattore di autenticazione in fase di generazione.
Alla luce di tali rilievi, possono considerarsi operanti due fattori di autenticazione aventi diversa natura per quanto concerne l'operazione dispositiva. Manca invece una specifica deduzione e la connessa evidenza dell'operare di un secondo fattore di autenticazione nell'operazione di reset della *password.* Non può, quindi, essere ritenuta raggiunta la prova della SCA.
Alla luce di tali ragioni, la domanda del ricorrente va accolta.

PER QUESTI MOTIVI

In accoglimento del ricorso, il Collegio dichiara l'intermediario tenuto alla restituzione dell'importo complessivo di € 753,75.
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
MARIA ROSARIA MAUGERI