

COLLEGIO DI PALERMO

composto dai signori:

(PA) MAUGERI	Presidente
(PA) MELI	Membro designato dalla Banca d'Italia
(PA) FORGIONE	Membro designato dalla Banca d'Italia
(PA) IMBURGIA	Membro di designazione rappresentativa degli intermediari
(PA) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore ANTONIO FORGIONE

Seduta del 26/02/2026

FATTO

Parte ricorrente agisce per il disconoscimento di plurime operazioni di pagamento non autorizzate, eseguite a valere sulla propria carta di credito in concomitanza con l'associazione dello strumento a un *wallet* digitale. A seguito degli addebiti, la parte provvedeva tempestivamente al blocco delle carte, sporgeva formale denuncia-querela e inoltrava istanza di rimborso all'intermediario. Quest'ultimo, pur avendo inizialmente stornato gli importi contestati, procedeva a un successivo riaddebito, imputando al cliente una presunta colpa grave nella custodia delle credenziali. Il ricorrente contesta fermamente tale determinazione. A propria difesa, deduce di aver eseguito l'installazione dell'applicativo con il supporto di un operatore telefonico e imputa l'accaduto a un malfunzionamento dei presidi di sicurezza dell'intermediario, che avrebbe consentito a terzi l'illecita acquisizione dei dati sensibili delle carte. Ribadendo la propria assoluta diligenza e di non aver mai comunicato a terzi i propri codici personali, la parte insiste per l'accertamento dell'illegittimità del riaddebito e per la definitiva restituzione delle somme sottratte, segnalando altresì di aver già richiesto l'estinzione del rapporto di conto corrente. Costitutosi nel procedimento, l'intermediario chiede il rigetto della pretesa, eccependo la piena regolarità delle transazioni, eseguite nel rispetto dei protocolli di *Strong Customer Authentication* (SCA) di cui al D.Lgs. n. 11/10. Dalle evidenze dei *log* informatici prodotti in atti, la parte ricostruisce una dinamica incompatibile con il dedotto malfunzionamento, poiché le operazioni contestate risultano precedute dalla regolare attivazione dell'applicazione per la gestione del *remote banking* su un dispositivo terzo. Tale associazione si è perfezionata regolarmente, previo inserimento delle credenziali statiche e di un codice OTP recapitato sull'utenza mobile certificata del ricorrente, con

contestuale disattivazione del *token* precedentemente in uso sul dispositivo abituale del cliente. L'intermediario deduce, pertanto, la colpa grave della propria controparte, ravvisabile in una condotta reticente sia in sede di denuncia, ove è stato fatto un generico riferimento a una clonazione dell'utenza, sia in sede di ricorso. Nelle proprie memorie di controreplica, l'intermediario poi evidenzia come il ricorrente non abbia in alcun modo contestato la ricostruzione proposta nelle controdeduzioni di una cooperazione prestata, per effetto della truffa, ai malfattori. Insiste per il rigetto delle domande articolate nel ricorso.

DIRITTO

La decisione della presente controversia richiede in primo luogo di valutare l'assolvimento dell'onere probatorio posto a carico dell'intermediario dalla disciplina sui servizi di pagamento di cui al D.Lgs. 11/10 e successive modifiche. Dalla documentazione tecnica prodotta emerge che la parte ha compiutamente provato la corretta autenticazione, registrazione e contabilizzazione delle operazioni disconosciute, nonché l'assenza di malfunzionamenti dei propri sistemi. In particolare, l'intermediario ha fornito evidenza informatica circa la regolarità della fase di associazione dell'applicativo a un nuovo dispositivo, avvenuta nel pieno rispetto dei protocolli SCA. Tale procedura si è regolarmente perfezionata mediante l'impiego combinato di due distinti fattori di sicurezza quali sono il fattore di conoscenza (codice cliente, data di nascita e parte del codice PIN) e quello del possesso (corretta digitazione dell'OTP, regolarmente recapitata sull'utenza telefonica mobile certificata della parte ricorrente). Parimenti, dai *log* informatici prodotti risulta che anche le successive transazioni dispositive sono state eseguite nel rispetto degli standard di autenticazione forte richiesti dalla normativa europea PSD2.

Accertato l'assolvimento dell'onere probatorio gravante sull'intermediario, l'indagine del Collegio deve concentrarsi sulla condotta del ricorrente, al fine di verificare l'eventuale sussistenza della colpa grave, che costituisce causa di esclusione del rimborso. Nel caso di specie, alla luce degli elementi complessivamente acquisiti e delle deduzioni svolte, non è possibile ricostruire con sufficiente precisione la dinamica concreta della frode denunciata.

In proposito, il Collegio, in coerenza con i principi interpretativi accolti dal consolidato orientamento della giurisprudenza arbitrale, osserva che, quando risultino provati l'autenticazione tecnica delle operazioni, la conformità del sistema di pagamento ai requisiti di SCA e l'assenza di evidenti indici di anomalia o di ulteriori elementi oggettivi imputabili all'intermediario, l'insufficienza delle allegazioni del cliente assume rilievo sul piano giuridico. In particolare, la mancata indicazione puntuale delle circostanze di fatto in cui si sarebbe consumata la frode può integrare un significativo elemento presuntivo, che, valutato unitamente alle risultanze dei tracciati informatici, consente di desumere la sussistenza della colpa grave del cliente, ravvisabile nella negligente custodia ovvero nella incauta comunicazione a terzi delle credenziali personalizzate.

Applicando tali criteri al caso in esame, il ricorrente non ha fornito una ricostruzione idonea a spiegare in modo plausibile l'acquisizione fraudolenta, da parte di terzi, di molteplici e articolati fattori di sicurezza, se non postulando una cooperazione, quantomeno colposa, nella loro divulgazione o utilizzazione. Ne consegue che la pretesa restitutoria non può essere accolta, dovendosi ritenere legittimo il riaddebito operato dall'intermediario.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE