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) DI STEFANO	Membro di designazione rappresentativa dei clienti

Relatore SERGIO SCIBETTA

Seduta del 12/12/2024

FATTO

Con ricorso del 01/08/2024, proposto dopo l'esito negativo del reclamo inviato direttamente all'intermediario, il ricorrente riferisce di essere titolare di una carta di credito con cui sarebbe stata effettuata un'operazione di pagamento dell'importo di € 1.274,98 che non viene riconosciuta e di cui viene chiesto quindi il rimborso.

In particolare il ricorrente riferisce che, in data 26/7/2024, avrebbe ricevuto una chiamata proveniente dal numero intestato all'intermediario, nel corso della quale un sedicente operatore avrebbe segnalato l'esigenza di bloccare una operazione di acquisto criptovalute tramite carta di credito e, dopo aver inviato un *link* a mezzo sms, avrebbe comunicato lo storno della somma di € 1.274,98 invitando a ripetere l'operazione.

Il ricorrente si sarebbe accorto della truffa in atto contattando immediatamente il servizio clienti e benché dichiari di non aver né comunicato né utilizzato il proprio nome utente e la propria password, si è visto addebitare il costo dell'operazione, di cui chiede quindi il rimborso oltre alla refusione delle spese di assistenza sostenute e quantificate in € 638,00.

Con controdeduzioni del 14/10/2024 l'intermediario si è opposto all'accoglimento del ricorso in quanto dalle verifiche effettuate non sarebbero emerse anomalie e l'operazione contestata risulterebbe essere stata regolarmente autorizzata tramite inserimento del codice OTP conosciuto dal solo titolare dello strumento di pagamento.

L'intermediario riferisce che l'operatività della carta di credito del cliente sarebbe sottoposta al sistema di autorizzazione a doppio fattore sia per l'accesso all'*home banking* sia per l'esecuzione delle operazioni di pagamento e che proprio l'operazione contestata sarebbe stata autorizzata tramite inserimento del PIN e del codice OTP generato dal mobile token a disposizione del cliente.

Secondo l'intermediario resistente quanto accaduto sarebbe imputabile unicamente alla condotta del cliente il quale, nonostante i sistemi di sicurezza predisposti e le notifiche *push* ricevute all'operazione in corso, avrebbe consentito al truffatore di perfezionare l'operazione.

In ogni caso l'intermediario ritiene che alla luce di quanto emerge dalla denuncia presentata dal cliente alle forze dell'Ordine, l'operazione in argomento sarebbe stata da lui effettuata personalmente e che quindi la vicenda non sia sottoposta alla normativa PSD2 ed al sistema di tutele ivi previsto.

Con repliche del 24/10/2024 il ricorrente ha reiterato le proprie difese ed ha contestato quanto dedotto dall'intermediario resistente escludendo di aver personalmente eseguito l'operazione e di non aver fornito alcun codice al truffatore.

Con la medesima memoria il cliente ha contestato la ricostruzione dell'operatività della propria carta di pagamento per come descritta dall'intermediario ed ha contestato a quest'ultimo la mancata predisposizione di adeguati sistemi di sicurezza a tutela dell'operatività degli strumenti di pagamento.

DIRITTO

Il ricorso sottoposto al collegio verte in tema di esecuzione fraudolenta di operazioni di pagamento e consequenziale richiesta di rimborso delle somme addebitate al cliente.

In via preliminare appare necessario esaminare l'eccezione sollevata dall'intermediario in ordine alla normativa applicabile ed in particolare in ordine all'invocata esclusione dei criteri di valutazione conformi alla direttiva PSD2 in quanto l'operazione contestata sarebbe stata eseguita personalmente dal cliente.

In realtà dagli elementi acquisiti al fascicolo la circostanza invocata dall'intermediario non risulta provata in quanto né nella denuncia presentata dal cliente alle Forze dell'Ordine né nel ricorso introduttivo si rinvengono elementi che possano indurre a ritenere provata la personale esecuzione dell'operazione.

Nel merito l'operazione contestata è stata posta in essere nella vigenza del D.Lgs. 27/1/2010 n° 11 come modificato dal D.Lgs. 15/12/2017 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 13/1/2018, che ha modificato le direttive 2002/65/CE, 2009/110CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, ed abrogato la direttiva 2007/64/CE, ed ha provveduto all'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 S*trong Customer Authentication* (c.d. SCA) si rinvengono negli artt. 97 e 98 della PSD2, nell'art. 10 bis del D.Lgs. 10/2011, nelle norme tecniche di regolamentazione emanate dall'EBA e recepite con il Regolamento Delegato Ue 2018/389 della Commissione Europea, applicabile a far data dal 14/9/2019, nonché nei criteri interpretativi forniti dall'EBA, e tra questi in particolare il parere dell'EBA del 21/6/2019.

Sulla base della citata normativa, affinché l'intermediario possa andare esente da responsabilità deve fornire prova, oltre che dell'insussistenza di malfunzionamenti, dell'adozione di un sistema di sicurezza adeguato e della corretta registrazione, autenticazione e contabilizzazione delle operazioni contestate.

Inoltre, come precisato dal Collegio di Coordinamento con la decisione n. 22745/19 "*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".*

Dai tracciati telematici prodotti dall'intermediario emerge che nel giorno in cui è stata eseguita l'operazione contestata il cliente avrebbe effettuato un accesso alla propria App tramite inserimento del proprio ID utente e del PIN (costituito dal F**id) nonché del codice OTP generato dal *mobile token* nella sua disponibilità.

Successivamente risulta essere stata eseguita l'operazione tramite inserimento del PIN (F**Id) e di un nuovo codice OTP generato a sua volta dal *mobile token* integrato alla App operativa del sistema di pagamento.

Le superiori circostanze risultano provate tramite la produzione di tabulati elettronici e di una adeguata legenda da cui si ritiene di poter trarre conferma in ordine alla conformità del sistema approntato dall'intermediario alla SCA sia per l'accesso all'area personale del cliente che per l'autorizzazione delle operazioni di pagamento.

Non sembra superfluo evidenziare che il sistema operativo in esame è stato già riconosciuto conforme alla SCA da altri Collegi territoriali chiamati a decidere in ordine a fattispecie similari a quella dell'odierno ricorrente (*ex multis* si richiama Collegio di Torino dec. N° 669/24, Collegio di Bari dec. N° 9382/24 e Collegio di Roma dec. N° 9162/24).

A fronte del rispetto dei canoni di sicurezza SCA da parte dell'intermediario, nella vicenda oggetto del ricorso sembrano sussistere elementi idonei a ritenere provata la colpa grave del cliente il quale, per come emerge dagli atti del procedimento, avrebbe autorizzato l'operazione nella convinzione che si trattasse di uno storno e non ha prodotto l'sms contenente il *link* inviato dal truffatore, omissione che per costante orientamento dei Collegi Territoriali, rappresenta un elemento da cui il Collegio può trarre il proprio convincimento.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARIA ROSARIA MAUGERI