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 SERGIO SCIBETTA

Seduta del 26/06/2025

FATTO

Con ricorso del 14/03/2025, promosso dopo l'esito negativo del reclamo indirizzato direttamente all'intermediario, la ricorrente ha riferito di essere titolare di tre conti correnti da cui, nella notte del 22/1/2025, sarebbero state eseguiti n° 6 bonifici istantanei, per un importo di € 4.380,00, a favore di soggetti a lei sconosciuti e di cui pertanto chiede il rimborso.

La ricorrente ha dichiarato di essersi accorta dell'accaduto in virtù della ricezione delle notifiche con cui veniva comunicato il perfezionamento delle singole operazioni ed ha escluso di aver mai ricevuto sms o link fraudolenti con collegamenti a pagine web né di aver mai memorizzato le proprie credenziali per l'operatività sui propri conti correnti.

In conclusione la ricorrente, poiché dagli elementi disponibili - anche in virtù del riscontro al reclamo – gli accessi ai conti correnti non sarebbero a lei imputabili quanto piuttosto alla insufficiente protezione garantita dal sistema operativo approntato dall'intermediario, chiede il rimborso integrale della somma sottratta.

Con le proprie controdeduzioni l'intermediario si oppone alla richiesta formulata dalla ricorrente in quanto le operazioni contestate sarebbero state regolarmente validate nel rispetto della SCA e dei sistemi di sicurezza richiesti dalla normativa vigente.

In particolare l'intermediario specifica che nessuna delle operazioni contestate presenterebbe alcuna anomalia e conferma che le operazioni sono state confermate a mezzo di notifica *push* su due distinti dispositivi precedentemente configurati.

A detta dell'intermediario quanto accaduto sarebbe imputabile esclusivamente alla responsabilità della cliente che non avrebbe diligentemente custodito le proprie credenziali e che avrebbe dato credito ad un sms, da lei stessa prodotto, che presentava evidenti segni di anomalia che dovevano indurre ad escluderne l'autenticità.

Per tutti i superiori motivi l'intermediario ha chiesto il rigetto integrale del ricorso.

Con repliche del 13/5/2025 la ricorrente ha contestato le difese spiegate dall'intermediario e la conducenza della documentazione prodotta; ha negato che le operazioni siano state perfezionate secondo le modalità riferite dall'intermediario nonché di aver mai ricevuto messaggi con link fraudolenti.

La ricorrente in particolare nega di essere a conoscenza dell'intervenuta registrazione di un ulteriore dispositivo giacchè l'OTP sms ricevuto in data 16/1/2025, utilizzato per perfezionare la detta registrazione, non avrebbe avuto alcun elemento da cui poter ricavare indizi della truffa in corso di esecuzione.

Con le proprie controrepliche l'intermediario ha riaffermato la genuinità e conducenza dei file prodotti, ha evidenziato come la cliente abbia regolarmente ricevuto la notifica *push* con cui è stato poi configurato il nuovo dispositivo ed ha evidenziato come l'OTP sms inviato per perfezionare la procedura recasse espressamente l'indicazione di essere destinato a consentire la configurazione di un nuovo dispositivo.

DIRITTO

Il ricorso sottoposto al Collegio verte in tema di esecuzione fraudolenta di n° 6 bonifici istantanei, dell'importo complessivo di € 4.380,00, eseguiti in data 22/1/2025 e della consequenziale richiesta di rimborso delle somme addebitate ala cliente.

In particolare le operazioni oggetto del ricorso sono le seguenti:

1. Bonifico € 950,00 – C/C ***6884
2. Bonifico € 940,00 – C/C ***6884
3. Bonifico € 330,00 – C/C ***6884
4. Bonifico € 940 – C/C ***1738
5. Bonifico € 500,00 – C/C ***1738
6. Bonifico € 750,00 - C/C ***7328

Le operazioni contestate sono state poste 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".*

L'intermediario con le proprie memorie riferisce che in data 16/1/2025 è stato registrato un nuovo dispositivo per consentire di operare nell'home banking della cliente e dimostra che tale operazione è stata effettuata in conformità alla normativa vigente ed alla SCA tramite l'inserimento del codice cliente, del codice segreto di esclusiva conoscenza della cliente, di un secondo codice segreto e di un codice OTP notificato al *device* della cliente.

Il detto procedimento risulta comprovato dalla produzione di alcune schermate informatiche che, benché non corredate da una apposita legenda, risultano di facile intellegibilità e comunque compatibili con la ricostruzione dell'operazione fornita dall'intermediario.

Anche l'accesso alla pagina personale della cliente risulta effettuata nel rispetto della SCA tramite inserimento del codice cliente, di un codice segreto con fattore biometrico precedentemente attivato e poi l'inserimento di un secondo codice segreto generato automaticamente da un silent token,

Infine l'intermediario fornisce prova del fatto che le singole operazioni dispositive sono state anch'esse autorizzate con un sistema compatibile alla SCA ossia tramite digitazione di un secondo codice segreto con fattore biometrico ed inserimento del codice generato dal mobile token.

Ogni singola operazione risulta altresì essere stata accompagnata dall'invio di una notifica *push* che risulta essere stata trasmessa ad entrambi i dispositivi collegati con l'utenza.

A fronte della prova fornita dall'intermediario in ordine alla predisposizione di un sistema operativo conforme alla vigente normativa di sicurezza, dalla documentazione acquisita al fascicolo si rileva che nella vicenda oggetto del ricorso sussistono degli elementi di colpa grave imputabili alla ricorrente.

Difatti, contrariamente a quanto sostenuto nel ricorso introduttivo, dalla produzione allegata al ricorso stesso emerge che la cliente in data 16/1/2025 ha effettivamente ricevuto un messaggio apparentemente proveniente dall'intermediario, con cui veniva avvisata del fatto che si stava procedendo alla certificazione del nuovo dispositivo.

Ebbene tale messaggio, pur non contenendo particolari errore o anomalie grammaticali, è caratterizzato da vistosi errori di punteggiatura che avrebbero dovuto indurre la cliente ad escludere che provenisse dall'intermediario.

Al suddetto elemento si aggiunge anche il colpevole silenzio della ricorrente sulle modalità con cui si sarebbero svolti i fatti e su come si sarebbe perfezionata la truffa in suo danno, e tale atteggiamento, per costante orientamento dei Collegi territoriali, non consentendo la ricostruzione degli accadimenti può costituire oggetto di valutazione in sede di decisione.

Appare provato che l'intermediario avesse predisposto un sistema di alert idoneo ad avvisare la cliente delle operazioni effettuate e, considerando che la stessa ricorrente afferma di aver avuto conoscenza delle operazioni effettuate attraverso la ricezione dei

relativi messaggi di conferma, appare provato che il sistema abbia correttamente funzionato.

Non sembra infine potersi invocare l'applicazione degli indici di anomalia delle operazioni, sovente forieri dell'individuazione di un concorso di colpa tra intermediario e cliente, poiché le operazioni contestate, seppur numerose e molto ravvicinate tra loro, sono state effettuate su tre distinti conti correnti.

PER QUESTI MOTIVI

Il Collegio non accoglie il ricorso.

IL PRESIDENTE

Firmato digitalmente da
MARIA ROSARIA MAUGERI