## COLLEGIO DI MILANO

composto dai signori:

| | |
|---|---|
| (MI) TINA | Presidente |
| (MI) BARTOLOMUCCI | Membro designato dalla Banca d'Italia |
| (MI) BALDINELLI | Membro designato dalla Banca d'Italia |
| (MI) SANTARELLI | Membro di designazione rappresentativa degli intermediari |
| (MI) GRIPPO | Membro di designazione rappresentativa dei clienti |

Relatore BARTOLOMEO GRIPPO

Seduta del 03/12/2024

## FATTO

Parte ricorrente afferma che: in data 10/01/2024 cadeva vittima di una truffa tramite un social network; a fronte di una coercizione psicologica effettuata dai truffatori, infatti, venivano effettuati due prelievi da € 250,00 ciascuno dalla sua carta di credito; presentava denuncia alle competenti Autorità e presentava reclamo all'intermediario, che tuttavia respingeva la richiesta di rimborso relativamente al secondo prelievo di € 250,00, affermando che esso sarebbe avvenuto con la sua collaborazione attiva.
Parte ricorrente – esperita senza successo la fase del reclamo – chiede il rimborso della somma complessiva di € 200,00.
L'intermediario, con le controdeduzioni, precisa che: dalle dichiarazioni rese dal ricorrente in sede di denuncia, si evince che egli avrebbe cliccato su un LINK reperito su un social network e avrebbe poi scaricato un'applicazione seguendo le istruzioni di un operatore presentatosi come consulente della società ****finance*; il cliente avrebbe quindi fornito a un sedicente operatore di detta società i dati della propria carta di credito, e successivamente si sarebbe accorto del compimento di due operazioni della somma di € 250,00 ciascuna; la vicenda è assimilabile alla c.d. "truffa degli investimenti" ("fake trading") ed essendo stato lo stesso cliente ad effettuare le operazioni seguendo le istruzioni del frodatore, non è applicabile la disciplina di cui alla PSD2 e al D. Lgs n. 11 del

27/01/2010; ferma restando l'inapplicabilità della predetta disciplina, le operazioni sono state comunque correttamente contabilizzate, registrate e autenticate in quanto poste in essere con il corretto inserimento delle credenziali; ha già rimborsato al ricorrente l'importo di una delle due operazioni (pari ad € 250,00) perché, nonostante fosse stata effettuata regolarmente, è stata stornata dall'esercente; nella denegata ipotesi in cui si ritenesse applicabile la disciplina di cui all'art 12 del D.lgs. 27 gennaio 2010, n. 11, sussistono in ogni caso evidenti indici di colpa grave dell'utilizzatore; è infatti pacifico che il cliente ha cliccato su un LINK reperito su un social network e ha seguito le indicazioni di sedicenti operatori di una presunta società di investimenti, senza alcuna cautela o approfondimento, comunicando tutti i suoi dati personali e i dati della carta.
L'intermediario chiede, pertanto, di rigettare il ricorso perché infondato.

## DIRITTO

La controversia sottoposta all'esame del Collegio verte sulla ormai nota questione del furto di strumenti di pagamento e sul rimborso di somme indebitamente sottratte a seguito di disposizioni fraudolentemente impartite.
L'operazione contestata da parte ricorrente (un'operazione di pagamento con carta del 11/01/2024 dell'importo di € 250,00) rientra nell'ambito di applicazione della disciplina del D. Lgs. 27/1/2010, n. 11 di recepimento della Direttiva sui servizi di pagamento come modificato dal D. Lgs. n. 218/17 di attuazione della direttiva 2015/2366/EU (PSD 2).
Dalle dichiarazioni rese nella denuncia dal ricorrente, infatti, quest'ultimo afferma di aver comunicato ai presunti truffatori i dati della propria carta, ma non dichiara di aver personalmente eseguito i pagamenti (che, anzi, disconosce e sostiene di non averli volontariamente effettuati).
La normativa richiamata ha provveduto a ripartire una serie di obblighi tra il prestatore di servizi di pagamento e l'utilizzatore di detti servizi.
L'utilizzatore, in particolare, ha il dovere di utilizzare lo strumento di pagamento in conformità con i termini contrattuali, di denunciarne lo smarrimento, il furto o l'utilizzo non autorizzato appena ne viene a conoscenza e deve adottare le misure idonee a garantire la sicurezza dei dispositivi personalizzati che ne consentono l'utilizzo (ad esempio conservare adeguatamente i codici PIN).
Per quanto riguarda l'intermediario, la normativa ricordata prevede, tra gli altri, l'obbligo di assicurare che i dispositivi personalizzati che consentono l'utilizzo di uno strumento di pagamento non siano accessibili a soggetti terzi.
Si richiede, pertanto, da ambedue le parti, la necessaria diligenza per evitare che lo strumento di pagamento possa essere utilizzato senza la necessaria autorizzazione o in maniera fraudolenta.
La normativa mostra un chiaro *favor* probatorio nei confronti dell'utilizzatore, in quanto l'intermediario, per liberarsi da ogni responsabilità in caso di utilizzo fraudolento dello strumento, dovrà dimostrare che l'operazione è stata autorizzata dall'utilizzatore medesimo oppure che questi abbia agito in modo fraudolento ovvero con dolo o colpa grave.
Alla luce di tali disposizioni, pertanto, due sono i passaggi ineludibili in materia. In primo luogo è l'intermediario a dover provare l'autenticazione, la corretta registrazione e contabilizzazione delle operazioni contestate, prova che comunque di per sé non è sufficiente a dimostrare il dolo o la colpa grave dell'utilizzatore. In secondo luogo, è sempre l'intermediario a dover provare tutti i fatti idonei ad integrare la colpa grave

dell'utilizzatore, unica ipotesi in cui, oltre al dolo, lo stesso può patire le conseguenze dell'utilizzo fraudolento dello strumento di pagamento.
Con riferimento alla *strong customer authentication* (c.d. SCA) le fonti normative sono rinvenibili negli artt. 97 e 98 della PDS2, nell'articolo 10 bis del 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). Nello specifico, l'autenticazione forte (SCA) è richiesta quando il cliente 1) accede al suo conto di pagamento online; 2) dispone un'operazione di pagamento elettronico; 3) effettua una qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi.
La SCA si realizza con il ricorso ad almeno due dei seguenti tre fattori: conoscenza; inerenza; possesso.
Gli elementi devono essere reciprocamente indipendenti e appartenere a categorie diverse.
Nel caso di specie, sotto il primo profilo, l'intermediario non ha prodotto una completa documentazione relativa alla registrazione, contabilizzazione e autenticazione dell'operazione disconosciuta.
Ad avviso dell'intermediario, tale operazione sarebbe stata eseguita mediante un elemento di conoscenza, rappresentato dai dati identificativi della carta di credito che è il ricorrente stesso ad ammettere di aver riferito al malfattore ed un elemento di possesso, rappresentato dall'OTP.
L'intermediario ha prodotto evidenza dell'SMS OTP inviato al numero di telefono del ricorrente, ma non vi è evidenza di un ulteriore valido fattore di autenticazione, oltre all'OTP, avendo in aggiunta solo un riferimento rispetto allo stato attivo del codice K**6 senza alcuna ulteriore indicazione se non ai dati identificativi della carta (i LOG prodotti dall'intermediario, peraltro, non sono corredati da legenda esplicativa).
In base alla regolamentazione vigente, l'inserimento dei dati statici stampati sulla carta, ivi incluso il CVV, non costituisce un elemento riconducibile alla categoria della conoscenza o del possesso, e quindi utile per l'autenticazione forte, come puntualizzato dall'EBA nella "*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*".
Pertanto, secondo gli orientamenti consolidati dei Collegi, l'autenticazione avvenuta con i dati statici della carta, pure incautamente forniti dall'utilizzatore al truffatore, non può essere considerata una procedura sicura di autorizzazione dell'operazione, in mancanza di ulteriori elementi di carattere dinamico
Il Collegio ricorda che è onere dell'intermediario provare che l'operazione contestata sia stata autenticata, correttamente registrata e contabilizzata (art. 10, D. Lgs. 11/2010).
In mancanza della suddetta prova l'intermediario sopporta - in ogni caso - integralmente le conseguenze delle operazioni disconosciute (cfr. Collegio di Coordinamento, decisione n. 22745 del 10 ottobre 2019).
Secondo gli orientamenti condivisi dei Collegi, infatti, la prova della corretta autenticazione/contabilizzazione/registrazione delle operazioni, in aderenza al dato normativo, rappresenta un antecedente logico rispetto alla prova della colpa grave dell'utente.
Per quanto esposto, questo Collegio dispone a favore di parte ricorrente il rimborso della somma pari all'ammontare dell'operazione disconosciuta; stante il principio di corrispondenza tra il chiesto e il pronunciato, posto dall'art. 112 c.p.c., la domanda può essere tuttavia accolta nei soli limiti del *petitum* pari ad € 200,00.

**PER QUESTI MOTIVI**

**Il Collegio accoglie il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 200,00.**
**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 alla parte ricorrente la somma di € 20,00, quale rimborso della somma versata alla presentazione del ricorso.**

IL PRESIDENTE

Firmato digitalmente da
ANDREA TINA