

## COLLEGIO DI MILANO

composto dai signori:

|                 |                                                           |
|-----------------|-----------------------------------------------------------|
| (MI) TINA       | Presidente                                                |
| (MI) MODICA     | Membro designato dalla Banca d'Italia                     |
| (MI) RIZZO      | Membro designato dalla Banca d'Italia                     |
| (MI) SANTARELLI | Membro di designazione rappresentativa degli intermediari |
| (MI) GILIBERTI  | Membro di designazione rappresentativa dei clienti        |

Relatore (MI) RIZZO

Seduta del 18/12/2025

## FATTO

Il cliente, nel ricorso, afferma quanto segue:

- il 25/07/2025 prenotava tramite noto provider alberghiero operante on line una struttura in Egitto;
- durante la prenotazione registrava i dati della carta esclusivamente a titolo di garanzia, essendo il pagamento previsto in loco;

- il 09/08/2025, dopo una comunicazione ufficiale del provider sul rifiuto della carta, il cliente veniva contattato via WhatsApp da un soggetto che, in possesso dei dati reali della prenotazione, si qualificava come operatore della struttura;
- ritenendo la comunicazione credibile, il cliente inseriva i dati della carta su un sito clone e autorizzava l'operazione tramite OTP;
- in data 10/08/2025, il ricorrente sporgeva denuncia ai Carabinieri e chiedeva il disconoscimento dell'operazione all'intermediario convenuto;
- l'intermediario rigettava la richiesta di disconoscimento in data 26/08/2025.

Il ricorrente domanda, quindi, il rimborso della somma di € 1.083,43, oltre agli interessi e alle spese.

Nelle controdeduzioni, l'intermediario convenuto, riportato il fatto, afferma quanto segue:

- il ricorso è inaccoglibile in quanto la truffa si è consumata al di fuori dell'ambito di controllo dell'intermediario e l'esecuzione del pagamento contestato è imputabile esclusivamente al ricorrente medesimo, perché disposto da questi sulla scorta di istruzioni ricevute tramite una chat di WhatsApp intrattenuta con un soggetto terzo e, comunque, evidentemente non riconducibile alla Banca;
- la rappresentazione dei fatti presentata dal cliente contiene la dichiarazione, di natura confessoria, per cui è stato lo stesso cliente ad effettuare le operazioni seguendo le istruzioni del frodatore;
- di conseguenza, 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, l'operazione è stata comunque correttamente contabilizzata, registrata e autenticata in quanto posta in essere con il corretto inserimento delle credenziali.

L'intermediario convenuto domanda, quindi, il rigetto del ricorso in quanto infondato in fatto e in diritto.

## **DIRITTO**

Oggetto della presente controversia è un'operazione contestata, per un importo di € 1.083,43, posta in essere il 09/08/2025.

È agli atti la denuncia del cliente presentata in data 10/08/2025.

La truffa di cui è controversia è stata realizzata tramite un sito clone di una piattaforma e-commerce del settore turistico, sul quale il ricorrente – che aveva in precedenza fatto una prenotazione sulla piattaforma genuina – ha inserito i dati della sua carta di credito, provvedendo poi ad autorizzare la transazione contestata. L'intermediario afferma che la disposizione di pagamento oggetto di disconoscimento sia stata autorizzata direttamente dal cliente e che, pertanto, non trovi applicazione la disciplina prevista dal D.lgs. 11/2010. Il cliente conferma di avere proceduto personalmente all'inserimento dei dati sul sito, ma ritiene non valido il suo consenso in quanto tratto in inganno dal sito clone di una piattaforma on line cui era stato indirizzato dal truffatore.

Secondo l'orientamento dei Collegi ABF, quando l'operazione è eseguita per intero dal pagatore (con l'inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), l'operazione stessa

deve considerarsi autorizzata; pertanto, non viene in rilievo il regime di responsabilità per le operazioni di pagamento non autorizzate di cui alla direttiva 2015/2366/EU ("PSD2") e al D.lgs. n. 11/2010.

In ogni caso, dall'esame dei log informatici prodotti agli atti dall'intermediario convenuto risulta che l'operazione contestata è stata, correttamente, autenticata attraverso i fattori del possesso (dello smartphone) a seguito di notifica push; e della conoscenza (del PIN).

Quanto alla condotta delle parti e ai profili rilevanti per la valutazione di sussistenza della colpa, rammenta il Collegio come il cliente nel ricorso affermi che il 25/07/2025 ha effettuato una prenotazione tramite Booking.com per una struttura in Egitto, inserendo i dati della propria carta esclusivamente a titolo di garanzia, con pagamento previsto in loco. In data 9/08/2025, dopo avere ricevuto una comunicazione ufficiale da Booking.com riguardo al rifiuto della carta, il cliente è stato contattato tramite WhatsApp da un soggetto che, in possesso dei dati reali della prenotazione, si è qualificato come operatore della struttura. Considerando la comunicazione come credibile, il cliente è stato indotto a inserire i dati della carta su un sito clone e a autorizzare l'operazione tramite OTP, cadendo vittima di un raggiro. In sede di denuncia emergono, tuttavia, alcune divergenze rispetto a quanto esposto nel ricorso, in particolare: nel ricorso il cliente sottolinea che le credenziali della carta erano state inserite su Booking esclusivamente a titolo di garanzia, mentre nella denuncia il cliente dichiara che in sede di prenotazione era previsto il pagamento di una caparra; la comunicazione avvenuta con il truffatore tramite Whatsapp è stata intrattenuta dalla fidanzata e non dal cliente stesso, come invece sembrava emergere dal ricorso.

Considerato tutto quanto premesso, questo Collegio ritiene raggiunta la prova dell'efficacia causale determinante, nella produzione dell'evento dannoso, della colpa grave del ricorrente.

### **PER QUESTI MOTIVI**

**Il Collegio non accoglie il ricorso.**

**IL PRESIDENTE**