

## COLLEGIO DI MILANO

composto dai signori:

|                         |                                                           |
|-------------------------|-----------------------------------------------------------|
| (MI) TINA               | Presidente                                                |
| (MI) BARTOLOMUCCI       | Membro designato dalla Banca d'Italia                     |
| (MI) DELL'ANNA MISURALE | Membro designato dalla Banca d'Italia                     |
| (MI) PERON              | Membro di designazione rappresentativa degli intermediari |
| (MI) SCARANO            | Membro di designazione rappresentativa dei clienti        |

Relatore (MI) SCARANO

Seduta del 20/01/2026

### FATTO

Il ricorrente rappresenta di essere stato vittima di una frode informatica su una piattaforma di vendita online e di aver subito, in data 28.07.2025, l'addebito di cinque operazioni di pagamento *online* non riconosciute, per un importo complessivo pari a € 2.489,03.

Riferisce che, accortosi dell'accaduto, provvedeva immediatamente al blocco dello strumento di pagamento, presentava denuncia presso l'Autorità competente e procedeva al disconoscimento delle operazioni attraverso i canali messi a disposizione dall'intermediario, il quale ha rigettato la richiesta di rimborso sostenendo che le operazioni fossero state regolarmente autorizzate mediante l'utilizzo dei codici dispositivi.

Afferma che, sebbene sia possibile che, in occasione della prima operazione, abbia inconsapevolmente autorizzato un pagamento dal suo dispositivo, ciò non toglie che subito dopo siano state eseguite altre quattro operazioni anomale verso lo stesso beneficiario. Secondo il ricorrente, tale sequenza avrebbe dovuto attivare i sistemi di prevenzione delle frodi e le misure di sicurezza previste dalla normativa di settore, mentre l'inerzia dell'intermediario avrebbe consentito il perfezionamento della truffa, integrando una violazione degli obblighi di diligenza e protezione del cliente.

L'intermediario, nelle proprie controdeduzioni, ha eccepito che la frode si è consumata integralmente al di fuori della propria sfera di controllo e che l'esecuzione delle operazioni è imputabile esclusivamente alla condotta del cliente, il quale avrebbe disposto i pagamenti sulla base di istruzioni ricevute tramite una *chat* intrattenuta con un soggetto terzo non riconducibile alla banca. Osserva che sia in sede di denuncia sia nei moduli di disconoscimento, il cliente ha dichiarato di aver eseguito personalmente le operazioni, circostanza che, secondo l'intermediario, ne comporta la qualificazione come operazioni regolarmente autorizzate ai sensi della normativa vigente. Sostiene che le transazioni sono state correttamente autenticate, registrate e contabilizzate, e che il danno lamentato è conseguenza dell'incauto affidamento del cliente in una richiesta manifestamente anomala proveniente da un mittente ignoto.

L'intermediario ha infine evidenziato che il cliente avrebbe ignorato sia gli avvisi di prudenza diffusi dalla piattaforma apparentemente coinvolta nella vicenda, sia il contenuto delle notifiche di autorizzazione ricevute sul proprio dispositivo, nelle quali erano chiaramente indicati importo, tipologia e beneficiario delle operazioni.

## DIRITTO

La parte ricorrente disconosce cinque operazioni dell'importo complessivo di € 2.489,03, consistenti in pagamenti *on line* eseguiti a favore di un medesimo beneficiario in data 28.07.2025 alle ore 15:56 per € 545,00, alle ore 15:59 per € 519,00, alle ore 16:04 per € 510,00, alle ore 16:06 per € 515,00 e alle ore 16:09 per € 400,03.

Dalla documentazione acquisita emerge che il cliente, dopo essersi registrato su una piattaforma di vendita online, è stato indotto, mediante una comunicazione di posta elettronica apparentemente riconducibile alla piattaforma stessa, a cliccare su un collegamento che lo reindirizzava a un sito web

contraffatto, graficamente identico a quello ufficiale. All'interno di tale sito era presente una chat attraverso la quale un sedicente operatore richiedeva l'inserimento dei dati della carta di pagamento e di ulteriori informazioni, prospettando la necessità di collegare tali dati all'account per proseguire nell'utilizzo del servizio.

A seguito di tali operazioni, il cliente iniziava a ricevere sul proprio dispositivo una serie di notifiche provenienti dalla banca, che il soggetto fraudolento lo invitava ad autorizzare, rassicurandolo circa il fatto che si trattasse di passaggi meramente tecnici e privi di effetti economici. In tale contesto si colloca la dichiarazione resa dal cliente nei moduli di disconoscimento, ove egli ha risposto affermativamente alla domanda circa l'avvenuta disposizione delle operazioni.

La dinamica descritta rientra nelle ipotesi di frode informatica in cui il cliente presta un contributo materiale all'esecuzione dei pagamenti, pur senza la consapevolezza di disporre effettive transazioni di pagamento, trattandosi di operazioni eseguite sulla base delle indicazioni del frodatore, comunemente qualificate come operazioni "sotto dettatura".

In tale prospettiva, occorre distinguere tra la prima operazione, integralmente disposta dal cliente mediante inserimento dei dati dello strumento di pagamento e completamento dell'iter autorizzativo, e le successive operazioni, attivate dal soggetto fraudolento una volta acquisiti i dati della carta, con un apporto del cliente limitato alla fase finale di autorizzazione tramite notifiche *push*. La prima operazione deve pertanto ritenersi autorizzata, con esclusione dell'applicazione del regime di responsabilità per le operazioni non autorizzate previsto dalla direttiva PSD2 e dal d.lgs. n. 11/2010, mentre per le operazioni successive viene in rilievo una fattispecie di concorso causale tra cliente e frodatore.

Nella fattispecie in esame, il Collegio in ogni caso procede alla verifica della corretta esecuzione e autenticazione delle operazioni ai sensi degli artt. 10 e seguenti del d.lgs. n. 11/2010, ritenendo assorbente la qualificazione delle condotte alla luce della dinamica complessiva dei fatti e delle risultanze documentali. Resta fermo che, in presenza di operazioni compiute direttamente dal cliente, l'intermediario è esonerato dall'onere di provare l'autenticazione e non è configurabile una responsabilità oggettiva a suo carico.

Sulla base delle evidenze in atti, risulta che le operazioni di pagamento sono state autorizzate da APP installata sul dispositivo del cliente identificato con codice univoco, attraverso la validazione della credenziale dinamica OTP utilizzando il fattore biometrico ("authType":TOUCH). Tutte le operazioni si sono perfezionate rispettando i requisiti di inerenza (il codice OTP è stato generato a seguito di

riconoscimento biometrico) e di possesso (il codice OTP è stato generato tramite l'APP installata sul telefono identificato dal codice univoco).

Riguardo il comportamento del cliente, risulta che egli sia stato vittima di "*phishing*", una forma di truffa attuata mediante richiesta via e-mail di inserire i propri dati personali attraverso un link a un sito clone del sito ufficiale di altro soggetto, che tuttavia in questo caso non è rappresentato dall'intermediario convenuto bensì da una piattaforma di vendita on line.

L'orientamento dei Collegi evidenzia da tempo che simili tipologie di truffa si svolgono secondo uno schema tipico e noto e che la diffusione del fenomeno è tale che in detti casi la condotta del cliente è generalmente connotata da colpa grave, in quanto l'impiego di una media diligenza sarebbe sufficiente a impedire la truffa.

Ciò nondimeno, anche in presenza di una colpa grave del cliente, il Collegio è chiamato a valutare anche la condotta dell'intermediario alla luce dell'operatività concretamente posta in essere e degli obblighi di controllo e monitoraggio gravanti sul prestatore dei servizi di pagamento.

Come noto, la necessità che gli intermediari operanti nel settore si dotino di sistemi di monitoraggio capaci di intercettare elementi sintomatici di un rischio di frode rispetto a operazioni c.dd. sospette si evince dalle indicazioni contenute nel D.M. 30 aprile 2007, n. 112, adottato in attuazione della legge 17 agosto 2005, n. 166 (recante "Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento").

In particolare, l'art. 8 del D.M. 112/2007 identifica i casi di frode che vanno segnalati all'Ufficio Centrale Antifrode dei Mezzi di Pagamento del Ministero dell'Economia e delle Finanze (UCAMP) per consentire un monitoraggio del mercato delle carte di pagamento. Sebbene detta normativa si riferisca alle operazioni effettuate con carta fisica, essa è stata ritenuta applicabile dalla giurisprudenza ABF anche alle operazioni eseguite con altri strumenti di pagamento (ad es. bonifici o ricariche online) in ragione dell'unicità della ratio. Per completezza, occorre ricordare che anche l'art. 2 del Regolamento Delegato (UE) n. 2018/389 impone agli intermediari di predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente, sebbene l'EBA abbia precisato che non è comunque richiesto un monitoraggio delle operazioni in tempo reale (si veda la Q&A EBA relativa alla *Question ID 2018\_4090*).

Nel caso di specie, sulla base delle evidenze in atti, risulta integrato l'indice di anomalia espressamente previsto dal D.M. 112/2007, art. 8, lett. a), punto 2, che individua quale fattispecie rilevante, ai fini del monitoraggio delle frodi, la presenza di tre o più richieste di autorizzazione sulla stessa carta, effettuate

nelle ventiquattro ore presso un medesimo punto vendita. Le operazioni contestate risultano infatti essere cinque, tutte eseguite nel medesimo giorno, in un arco temporale estremamente ristretto e in favore dello stesso beneficiario.

Secondo l'orientamento costante dei Collegi, le previsioni del D.M. n. 112/2007 non hanno valore precettivo diretto in materia di disconoscimento delle operazioni di pagamento, né determinano automaticamente l'obbligo di rimborso di un numero predeterminato di transazioni. Esse costituiscono tuttavia un parametro qualificato per la formulazione di un giudizio in concreto sulla diligenza tecnica dell'intermediario e sull'adeguatezza dei presidi di prevenzione delle frodi.

In presenza di un indice di anomalia come quello sopra descritto, anche laddove sia stata accertata la colpa grave dell'utilizzatore, la ripartizione della responsabilità tra le parti deve essere effettuata caso per caso, tenendo conto delle specifiche circostanze di fatto. In particolare, l'intermediario è tenuto a dimostrare di aver adottato misure idonee a intercettare tempestivamente un'operatività manifestamente anomala, quale quella caratterizzata da una pluralità di pagamenti ravvicinati, di importo significativo e diretti verso il medesimo beneficiario.

Nel caso di specie, l'assenza di qualsiasi intervento automatico di blocco o di segnalazione, a fronte di un rischio frode oggettivamente elevato e riconducibile a uno schema tipico di truffa, consente di ravvisare una carenza nei presidi di controllo dell'intermediario e, conseguentemente, un suo apporto causale nella produzione del danno, seppur in concorso con la condotta gravemente imprudente del cliente.

Quanto alla quantificazione del rimborso, l'orientamento dei Collegi è nel senso di ritenere che la valutazione della responsabilità del prestatore di servizi di pagamento debba essere formulata in un giudizio sintetico, che tenga conto della condotta complessiva delle parti e di tutti gli elementi desumibili dal caso concreto. In tale prospettiva, la base di calcolo per la liquidazione della somma oggetto di condanna è costituita dall'intero ammontare delle operazioni disconosciute, senza esclusioni automatiche, procedendo a una distribuzione in concreto del concorso di colpa tra cliente e intermediario.

Alla luce di tali criteri, il Collegio ritiene di determinare il rimborso nella misura di € 1.425,00, corrispondente al valore della terza, quarta e quinta operazione, importo che rappresenta la quota di danno ascrivibile alla mancata attivazione di adeguati presidi di monitoraggio e contenimento dell'operatività anomala.

### **PER QUESTI MOTIVI**

**Il Collegio accoglie parzialmente il ricorso e dispone che l'intermediario corrisponda alla parte ricorrente la somma di € 1.425,00.**

**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