

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) MAIMERI	Membro designato dalla Banca d'Italia
(RM) BONACCORSI DI PATTI	Membro di designazione rappresentativa degli intermediari
(RM) FULCHERI	Membro di designazione rappresentativa dei clienti

Relatore FABRIZIO MAIMERI

Seduta del 06/02/2026

FATTO

Con ricorso del 20.8.2025, parte attrice espone di essere stato contattato, il 10.3.2025, via telefono, da un sedicente operatore dell'intermediario, tramite un numero riconducibile all'intermediario; costui ha informato il ricorrente di presunti pagamenti sospetti a valere sulla sua carta prepagata, chiedendo al ricorrente stesso di "bloccare" queste operazioni cliccando sulla notifica *push* di volta in volta ricevuta sul proprio *smartphone* e utilizzando l'autenticazione biometrica. In realtà, seguendo queste istruzioni, il ricorrente ha autorizzato inconsapevolmente operazioni di pagamento *online* per un valore complessivo di € 8.900,00, avviate dal truffatore. La provvista per le operazioni fraudolente era stata inconsapevolmente costituita dallo stesso ricorrente, che, sempre su indicazione del truffatore, aveva effettuato alcune ricariche dal suo conto bancario detenuto presso altro intermediario verso la sua carta prepagata oggetto della frode. Tanto premesso, si chiede la retrocessione dell'importo relativo alle operazioni contestate.

In sede di controdeduzioni, l'intermediario afferma che le operazioni disconosciute sono state effettuate in prima persona dal ricorrente. Pertanto, al caso di specie non può trovare applicazione la disciplina di cui al d.lgs. n. 11/2010 relativa alle operazioni "non autorizzate". Quanto all'autenticazione, le operazioni di pagamento sono state autorizzate tramite l'utilizzo di elemento biometrico (fattore di ineranza) nella *token app* dell'intermediario installata sullo *smartphone* del ricorrente (fattore di possesso), a seguito della ricezione di una notifica *push*; fa eccezione solo la prima operazione da € 22,90, già rimborsata al ricorrente, che rientrava nelle operazioni di modesta entità per le quali, ai sensi dell'art. 16 del Regolamento UE 2018/389, non è previsto l'obbligo di autenticazione forte del cliente. Il ricorrente ha agito con colpa grave, dando seguito pedissequamente alle richieste telefoniche del truffatore, senza insospettirsi; in ogni caso, quanto al fatto che le operazioni non sono state bloccare preventivamente, l'ABF ha già chiarito che «l'obbligo di protezione che grava sull'intermediario si debba estendere sino al punto di procedere *ex ante* a blocchi automatici al superamento di un certo numero di operazioni o di determinati ammontari in assenza di precisi indici di frode» (cfr. Collegio di Milano, decisione n. 6732 del 9.7.2025). Tanto premesso, l'intermediario chiede il rigetto del ricorso.

In sede di repliche, parte ricorrente sostiene che egli non ha agito affatto con colpa grave, bensì si è accertato del fatto che la telefonata provenisse dall'intermediario resistente. Il ricorrente ha addirittura effettuato una chiamata al *call center* dell'intermediario per accertare l'identità del chiamante e, pur riuscendo a interagire solo con una registrata, ha ottenuto la conferma del fatto che il numero appartenesse effettivamente alla banca; inoltre, la telefonata fraudolenta è stata accompagnata da *sms* che confermavano le prospettazioni del truffatore.

In sede di controrepliche, parte resistente osserva che il numero di telefono da cui apparentemente proveniva la telefonata fraudolenta non consente di parlare con un operatore umano, ma solo con una voce registrata. Pertanto, secondo l'intermediario, non era credibile che un operatore umano chiamasse da quel numero e il ricorrente avrebbe dovuto avvedersi di questa anomalia.

In relazione alle rispettive argomentazioni, il ricorrente chiede all'Arbitro «di analizzare dettagliatamente il ricorso che ho presentato nei confronti [dell'intermediario] per un riconoscimento di un rimborso totale delle somme economiche perdute a seguito di una truffa telematica (approfonditamente descritta nei documenti che trasmetto in allegato)». Dal canto suo, l'intermediario chiede il rigetto del ricorso.

DIRITTO

1. In base alla denuncia in atti, il 10.3.2025 il ricorrente è stato contattato telefonicamente da un sedicente operatore dell'intermediario, tramite un numero riconducibile all'intermediario. È versato in atti lo *screenshot* del registro chiamate, da cui risulta l'utilizzo di un numero telefonico utilizzato dall'intermediario sul suo sito *internet* e la provenienza della telefonata dalla Lituania, dove ha sede legale l'intermediario resistente. Il truffatore ha rappresentato al ricorrente la presunta esecuzione di pagamenti fraudolenti a valere sulla sua carta prepagata; lo ha poi guidato nello spostamento di fondi da un suo conto detenuto presso altra banca sulla carta prepagata, per costituire la provvista ai fini della frode. A questo punto, il truffatore ha chiesto al ricorrente di cliccare sulle notifiche *push* ricevute sul suo *smartphone* ed effettuare l'autenticazione tramite elemento biometrico. Il ricorrente ha eseguito la richiesta, autenticando inconsapevolmente n. 17 operazioni di pagamento *online*, nella convinzione di bloccare, invece, le operazioni fraudolente già eseguite. Nel corso della telefonata, il ricorrente riceveva *sms* volti a confermare le ricariche effettuate e il presunto blocco dei pagamenti truffaldini.

In primo luogo, l'intermediario eccepisce l'inapplicabilità del regime di responsabilità previsto dalla PSD2, in quanto le operazioni contestate sarebbero state eseguite in prima persona del ricorrente. In

realtà, secondo l'orientamento condiviso tra i Collegi, l'operazione disconosciuta non è soggetta al regime di responsabilità previsto dalla PSD2 solo quando è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione). Nel caso in questione, invece, le operazioni sono pagamenti *online* avviati dal frodatore via *browser* tramite i dati della carta del ricorrente e inconsapevolmente completate dal ricorrente cliccando sulla notifica *push* e autenticandosi con il fattore biometrico. In caso di frodi simili a quella odierna, che parrebbe riconducibile alla tipologia del *caller ID spoofing*, il Collegio di Roma è solito ritenere applicabile l'orientamento condiviso dei Collegi elaborato in materia di *sms spoofing*. In particolare, tende a ravvisare un concorso di colpa tra le parti in relazione, da un lato, alla negligenza grave dell'utente che agevola il compimento della truffa – similmente a quanto avviene negli episodi di *phishing* – e, dall'altro lato, alle criticità organizzative del servizio di pagamento offerto dall'intermediario (Collegio di Roma, decisione n. 4547 del 12.5.2025). Le operazioni contestate sono n. 17 pagamenti *online* eseguiti il 10.3.2025 a valere sulla carta prepagata del ricorrente, per un importo complessivo di € 8.907,89.

2. Si osserva che tutti i pagamenti 18 pagamenti (compreso quello rimborsato) sono avvenuti tra le 14:04 e le 16:43 del 10/03/2025, sicché è stata superata la soglia di 7 richieste di autorizzazione in 24 ore individuata come indice di un rischio di frode dall'art. 8, d.m. 30.4.2007, n. 112. Infatti, l'art. 8, del d.m. dispone: «Si configura il rischio di frode di cui all'art. 3, comma 1 della legge, quando viene raggiunto uno dei seguenti parametri: (...) b) riguardo alle carte di pagamento sottoposte a monitoraggio di cui all'art. 7, lett. c): 1) sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento; 2) una ovvero più richieste di autorizzazione che nelle 24 ore esauriscano l'importo totale del *plafond* della carta di pagamento; 3) due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta». Secondo l'orientamento condiviso tra i Collegi, le previsioni di cui all'art. 8 del d.m. n. 112/2007 non hanno un valore precettivo diretto sulla materia in esame, ma rappresentano utili indicatori per identificare anomalie e scenari di frode anche ai sensi dell'art. 2 del Regolamento EBA n. 2018/389, in base al quale gli intermediari sono tenuti a predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente (in tal senso cfr. Collegio di Roma, decisioni n. 14333 del 7.11.2022, n. 7426 dell'11.5.2022, n. 22127 del 25.10.2021). Conseguentemente, sempre in base all'orientamento condiviso, una volta accertata la colpa grave del cliente, qualora sussista uno dei riferiti indici di frode, la ripartizione della responsabilità con il prestatore dei servizi di pagamento (PSP) debba essere determinata caso per caso, in relazione alle circostanze di fatto, in quanto le previsioni del d.m. rappresentano un parametro per la formulazione di un giudizio in concreto della negligenza tecnica dell'intermediario (così Collegio di Roma, decisione n. 14333 del 7.11.2022). Per quanto concerne infine la quantificazione del rimborso da riconoscere all'utente in questi casi, in base all'orientamento condiviso dei Collegi, la valutazione della responsabilità del PSP deve essere formulata in un giudizio sintetico che tenga conto della sua condotta complessiva e di tutti gli altri elementi desumibili dal caso concreto: la base di calcolo per la liquidazione della somma oggetto di condanna è costituita dall'intero ammontare degli importi disconosciuti, senza esclusioni, procedendo a una distribuzione in concreto del concorso di colpa tra le parti. Infatti, il d.m. non ha un valore precettivo in materia di disconoscimento delle operazioni non autorizzate e non è ravvisabile una diretta correlazione tra l'integrazione dell'indice di frode e il numero di operazioni da rimborsare. Accanto a questo criterio di quantificazione del danno in concorso tra le parti, vi è poi anche l'altro elemento, costituito dalla circostanza che la telefonata "esca" proveniva da un numero telefonico riconducibile dalla banca, elemento che ha colpevolmente rafforzato la fiducia del ricorrente nel soggetto frodatore.

3. Circa l'autenticazione delle operazioni, l'intermediario dichiara che per ciascun pagamento è stato utilizzato l'elemento di autenticazione biometrica (fattore di inerenza) all'interno della *token app* installata sullo *smartphone* del ricorrente (fattore di possesso), a seguito della ricezione di una notifica

push. Questa ricostruzione è riconosciuta dallo stesso ricorrente, che dichiara di aver cliccato sulle notifiche *push* e utilizzato l'elemento biometrico nell'*app* dell'intermediario, autenticando inconsapevolmente i pagamenti. Ha prodotto, altresì, *log* analoghi al seguente, che attestano l'invio della notifica *push* ("*push_message_state = SENT*") allo smartphone del ricorrente (cfr. "*device_id*").

Portando a conclusione gli elementi sopra indicati, ne segue che sussiste un concorso di colpa fra l'intermediario e il ricorrente, quantificabile, in misura equitativa, in € 4.500,00.

PER QUESTI MOTIVI

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda alla parte ricorrente la somma di euro 4.500,00, determinata in via equitativa.

Dispone, inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di euro 200,00 (duecento/00) quale contributo alle spese della procedura e alla parte ricorrente quella di euro 20,00 (venti/00) quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE