

COLLEGIO DI ROMA

composto dai signori:

(RM) SIRENA	Presidente
(RM) MARINARO	Membro designato dalla Banca d'Italia
(RM) PICARO	Membro designato dalla Banca d'Italia
(RM) BILOTTI	Membro di designazione rappresentativa degli intermediari
(RM) NOTARO	Membro di designazione rappresentativa dei clienti

Relatore MARCO MARINARO

Seduta del 13/02/2026

FATTO

Il ricorrente espone quanto segue:

- era intestatario di una carta di credito emessa dal resistente;
- in data 04.09.2024 si avvedeva, a seguito di un normale controllo del proprio conto, della contabilizzazione di due operazioni sconosciute eseguite da terzi ignoti il giorno 31.07.2024, la prima dell'importo di € 1.358,83, la seconda dell'importo di € 705,43, per totali € 2.064,26;
- il ricorrente ha provveduto al blocco cautelativo della carta e del conto;
- la carta di credito era sempre rimasta nella sua piena ed esclusiva disponibilità e non ha effettuato, né autorizzato le transazioni di cui sopra, né ha mai rivelato a terzi il codice PIN della carta stessa;
- né è mai stato in Indonesia, luogo ove sembrerebbero essere state effettuate le operazioni fraudolente.

Chiede il rimborso della somma di € 2.064,26 nonché interessi legali e rivalutazione monetaria.

Nelle controdeduzioni, l'Intermediario eccepisce quanto segue:

- il ricorrente non ha allegato alcun documento a sostegno dei fatti, fatta eccezione per la denuncia sporta presso la Stazione dei Carabinieri di Ascoli Piceno, in data 05.09.2024, ossia dopo oltre un mese dall'esecuzione delle transazioni nella quale dichiara che ha fatto accesso in app e ha preso atto dell'esecuzione delle transazioni fraudolente;
- non vi è dunque alcuna prova della asserita frode/falsificazione al di là delle mere dichiarazioni del ricorrente nel modulo di ricorso ed in denuncia, prive anch'esse di allegazioni e di indicazione di come, dove e quando la truffa sarebbe avvenuta;
- ha rigettato il reclamo in quanto le transazioni sono state effettuate dallo stesso ricorrente con autenticazione forte sia nella fase di enrollment dell'APP sul dispositivo (avvenuta due anni prima) sia

relativamente alle operazioni di pagamento mediante fattore di possesso (il dispositivo) e fattore biometrico (FingerPrint/FaceID) il tutto come dimostrato dai LOG;

- pertanto, senza la cooperazione del ricorrente, non sarebbe stato possibile portare a termine le transazioni (e presunta frode);
- le transazioni disconosciute sono due, avvenute in data 31.07.2024 alle ore 17:22 e 17:26 rispettivamente di 24.100.001,00 e 12.200.001,00 IDR (Rupie Indonesiane), pari rispettivamente a € 1.358,83 e € 705,43, con la carta di credito n. ****0855 emessa dal resistente;
- la carta è stata bloccata alle ore 20:31 del 05.09.2024 e quindi molto dopo le transazioni contestate. Chiede il rigetto del ricorso.

Nelle repliche, parte ricorrente deduce che:

- quanto al preteso ritardo nel disconoscimento delle operazioni, fa presente che esso è dovuto al fatto che non è pervenuto al cellulare del ricorrente nessun avviso e nessuna notifica sms o push;
- non ha mai attivato e utilizzato attraverso il proprio cellulare l'impronta digitale o riconoscimento facciale né tantomeno per autorizzare transazioni specifiche;
- l'intermediario nel rigettare il reclamo proposto dal ricorrente - ha fatto riferimento ad autorizzazione mediante otp ricevuto tramite sms e non ad altri sistemi (il riconoscimento facciale o l'impronta digitale) evocati tra l'altro solo nella memoria di costituzione;
- infatti, dal tabulato del traffico telefonico relativo agli SMS in entrata il giorno della frode non risulta alcun SMS recante codici OTP;
- l'intermediario avrebbe dovuto bloccare tempestivamente le operazioni contestate alla luce degli indici di anomalia quali: il limitato utilizzo che il ricorrente faceva della carta di pagamento e per operazioni di modico valore; le operazioni fraudolente sono state ravvicinate, a distanza di pochi minuti l'una dall'altra, per somme rilevanti e con destinazione inconsueta;

Insiste per l'accoglimento del ricorso.

Nelle controrepliche, l'intermediario eccepisce che:

- la parte ricorrente ha interpretato erroneamente i LOG depositati dalla resistente, confondendo le modalità di installazione dell'APP (SMS+OTP) con le modalità di autenticazione delle transazioni (device+fattore biometrico);
- dunque, per autenticare le due transazioni contestate, contrariamente a quanto erroneamente interpretato e riferito da controparte, non vi sono stati né SMS né OTP, ma autenticazioni con device e fattore biometrico, pertanto, egli ha ricevuto le notifiche di autorizzazione delle transazioni inviate in modalità push;
- il ricorrente ha sostenuto l'anomalia delle due transazioni perché ravvicinate e non corrispondente al suo normale utilizzo della carta, tuttavia le transazioni sono avvenute alle ore 17:22 e 17:26 e quindi a distanza di quattro minuti, in secondo luogo hanno avuto importi diversi e non hanno esaurito il plafond; pertanto, non vi era alcuna anomalia da rilevare;
- quanto al normale utilizzo della carta, ancorché questione irrilevante, il ricorrente ha prodotto uno stralcio dell'estratto conto trimestrale, relativo solo al mese di settembre (ha tagliato gli altri due mesi di cui l'estratto era composto), il che non prova alcuna abitudine di spesa (trattandosi di un solo mese) e comunque dallo stesso si evincono decine di transazioni.

Insiste per il rigetto del ricorso.

DIRITTO

1.- Le operazioni di pagamento online disconosciute dalla parte ricorrente sono state eseguite il 31 luglio 2024. Risultano pertanto effettuate dopo l'emanazione della direttiva 2015/2366/UE del Parlamento europeo e del Consiglio del 25 novembre 2015, (c.d. PSD 2 - Payment Services Directive 2), recepita con il d.lgs. n. 218 del 15.12.2017, entrato in vigore in data 13.01.2018, che modifica in più punti il d.lgs. n. 11 del 2010. Si rileva che tali operazioni sono altresì successive alla data di entrata in vigore del Regolamento Delegato (UE) n. 2018/389 della Commissione.

Sulla base di quanto previsto dalla direttiva (art. 115, par. 4), l'art. 5, comma 6, d.lgs. n. 218/2017 prevede tuttavia che "le misure di sicurezza di cui agli articoli 5-bis, commi 1, 2 e 3, 5-ter, 5-quater e 10-bis del decreto legislativo 27 gennaio 2010, n. 11, si applicano decorsi diciotto mesi dalla data di entrata in vigore delle norme tecniche di regolamentazione di cui all'articolo 98 della direttiva (UE) n. 2015/2366". In particolare, la Commissione – delegata ad adottare tali norme tecniche di regolamentazione, ai sensi dell'art. 98, par. 4, della direttiva – ha emanato il 27.11.2017 il regolamento delegato (UE) n. 2018/389 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri. Il regolamento, ai sensi dell'art. 38, par. 2, si applica a decorrere dal 14.09.2019 e cioè diciotto mesi dopo la pubblicazione sulla Gazzetta Ufficiale dell'Unione Europea, avvenuta in data 13.03.2018. Ne consegue che anche le norme del d.lgs. n. 11/2010 riferite alle misure di sicurezza, così come modificate dal d.lgs. n. 218/2017, hanno efficacia a partire dal 14.09.2019.

Esse risultano dunque applicabili alla vicenda oggetto del ricorso in esame.

2.- In estrema sintesi, la nuova normativa fa ricadere sull'intermediario la responsabilità delle operazioni disconosciute laddove quest'ultimo non abbia predisposto un c.d. "sistema di autenticazione forte" (in inglese *strong customer authentication* o SCA). Un simile sistema deve essere applicato, stando alla previsione dell'art. 10-bis, dai prestatori di servizi di pagamento anche quando l'utente dispone un'operazione di pagamento elettronico ovvero effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi. Quanto alla responsabilità del pagatore, ai sensi del comma 2-bis dell'art. 12 d.lgs. n. 11/2010, come inserito dal d.lgs. n. 218/2017, "salvo il caso in cui abbia agito in modo fraudolento, il pagatore non sopporta alcuna perdita se il prestatore di servizi di pagamento non esige un'autenticazione forte del cliente. Il beneficiario o il prestatore di servizi di pagamento del beneficiario rimborsano il danno finanziario causato al prestatore di servizi di pagamento del pagatore se non accettano l'autenticazione forte del cliente".

3.- Orbene, il concetto di "autenticazione forte" trova la propria definizione all'art. 1, comma 1, lett. q-bis), d.lgs. n. 11/2010 (lettera introdotta dal d.lgs. n. 218/2017): "un'autenticazione basata sull'uso di due o più elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilità degli altri, e che è concepita in modo tale da tutelare la riservatezza dei dati di autenticazione".

Il concetto è oggi ribadito e precisato, specie per quanto concerne la conformità di singole fattispecie concrete alle suddette categorie dell'autenticazione forte, dall'*Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2* del 21 giugno 2019.

L'EBA ha chiarito, per esempio, che, mentre l'OTP ricevuta tramite sms integra un elemento di possesso idoneo ai fini della strong customer authentication, i dati riportati sulla carta (numero, scadenza e CVV), non costituiscono né un valido elemento di possesso (par. 28), né un valido elemento di conoscenza (par. 33). Al par. 43 di tale documento si legge, in particolare, che "*a number of existing approaches within e-commerce, for card payments in particular, would not be compliant with SCA. This includes approaches in which card details printed in full on the card are used as stand-alone elements or used in combination with a communication protocol such as EMV® 3-D Secure or with only one compliant SCA element (such as SMS OTP)*".

4.- La parte ricorrente disconosce due operazioni di pagamento eseguite in data 31.7.2024 con la carta emessa dall'intermediario resistente.

Si tratta di un pagamento di € 1.358,83 e di un pagamento di € 705,43 entrambi su un sito indonesiano; per complessivi € 2.064,26.

La parte ricorrente non descrive le modalità della frode né nel ricorso né nella denuncia.

Invero, il ricorrente si limita ad affermare che in data 4.9.2024, ad un mese circa di distanza dalla frode, ha aperto l'app bancaria e ha constatato l'esecuzione di due operazioni fraudolente. Lo stesso ha

bloccato la carta in data 5.9.2024, quasi un mese dopo l'esecuzione delle operazioni fraudolente del 31.7.2024.

4.1.- La parte ricorrente sostiene di non aver ricevuto SMS alert e che per tale ragione avrebbe disconosciuto tardivamente le operazioni fraudolente.

Sul punto si rileva che l'intermediario ha prodotto le notifiche push che sono state ricevute sul device id del ricorrente.

4.2.- Il ricorrente poi invoca gli indici di anomalia delle operazioni fraudolente.

Tuttavia, non vengono in rilievo gli indici di anomalia di cui al D.M. 30 aprile 2007, n. 112, di attuazione della legge n. 166/2005, né alcun altro indice.

5.- D'altro canto, l'intermediario ha prodotto il LOG relativi all'enrollment dell'app sul device del ricorrente e alle operazioni dispositive.

L'intermediario ha fatto presente che l'app è stata installata sul dispositivo del ricorrente due anni prima della frode in data 31.10.2022 ed è così stato attribuito il DeviceId= E227257****.

L'installazione è avvenuta mediante doppio fattore di autenticazione ossia Password + userid (fattore di conoscenza) e mediante OTP pervenuto tramite SMS (fattore di possesso).

L'intermediario fa presente che non sono intervenute modifiche del device id.

L'intermediario precisa poi che non vi è stata alcuna installazione (enrollement) dell'APP su altri device, ma le transazioni sono state eseguite tramite autenticazione dal device del ricorrente (E227257***).

Dai LOG si evince come il ricorrente ha ricevuto la richiesta di autorizzazione delle transazioni oggetto di contestazione tramite push notification sul suo device (fattore di possesso).

Le transazioni sono state autenticate mediante fattore biometrico (FingerPrint/FaceID ovvero impronta digitale o riconoscimento facciale) (fattore di inerenza) cfr. la colonna "Tipo di Autorizzazione" che riporta la voce "FINGERPRINT_FACEID".

L'operazione è stata quindi autorizzata dal device del cliente. Infatti, come detto, l'app non risulta mai installata su altri device.

Secondo l'orientamento condiviso dai Collegi ABF, "quando l'operazione è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione), deve considerarsi autorizzata e non è quindi soggetta al regime di responsabilità previsto dalla PSD2. Rientrano in questa fattispecie le operazioni eseguite dal pagatore seguendo le indicazioni del frodatore, senza la consapevolezza di disporre una transazione (ad esempio, le c.d. operazioni "sotto dettatura").

In questi casi, non è configurabile una responsabilità oggettiva del PSP. Il Collegio potrà comunque rilevare una responsabilità concorrente del PSP, sulla base delle evidenze disponibili e secondo le norme di diritto comune, quando emerge in concreto dalla documentazione in atti un apporto causale dell'intermediario alla frode come, ad esempio, nei casi di:

a) mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore;

b) mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, cui il pagatore si sia rivolto esponendo le richieste del frodatore;

c) mancato rilievo di indici di frode nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere".

Laddove quindi emerga che è lo stesso ricorrente ad aver materialmente disposto l'operazione contestata, i Collegi ABF ritengono inapplicabile la disciplina prevista dal d.lgs. n. 11/2010, rigettando la domanda di restituzione dell'importo dell'operazione involontariamente disposta (Collegio di Roma, decisione n. 1314/2024).

6.- Peraltro, ferma restando l'allocazione dell'onere della prova a carico dell'intermediario, questo Collegio ritiene che sussista in capo al ricorrente un onere di allegazione delle circostanze che possano, al minimo, offrire una attendibile ipotesi alternativa rispetto a quella, altrimenti residuale (ed

anzi unica), dell'utilizzo imputabile (direttamente o per colpa grave) al titolare (Coll. Roma, dec. n. 10723/19).

Non si ravvisano, d'altro canto, elementi idonei ad imputare una qualche responsabilità in capo all'intermediario resistente.

7.- Alla luce di quanto esposto, il Collegio ritiene che la domanda non possa trovare accoglimento.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE