

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 DANIELA CONCETTA NOTARO

Seduta del 13/02/2026

FATTO

Con ricorso del giorno 1 agosto 2025 (preceduto da rituale reclamo negativamente riscontrato dall'intermediario) l'istante si è rivolto a codesto Collegio rappresentando che in data 15.01.2025 ha ricevuto l'estratto conto della carta di credito ed ha appurato che a sua insaputa erano state eseguite 58 operazioni non autorizzate su un sito per adulti, dal 17.11.2024 al 14.01.2025, per complessivi euro 2.223.67.

Ha, pertanto, prontamente contattato il numero verde al fine di bloccare la carta di credito, compilando anche il modulo per il disconoscimento.

Tuttavia, l'Istituto di credito riconosceva soltanto il rimborso della somma di euro 65,08.

Pertanto, con l'odierno ricorso l'istante deduce una asserita clonazione della carta e la mancata attivazione dell'sms alert, chiedendo il rimborso della residua somma di euro 2.158,61.

Nel costituirsi con apposite controdeduzioni, l'intermediario ha affermato che le transazioni sono state autenticate con SCA dal device del ricorrente.

Tutte le 54 transazioni risultano autenticate dallo stesso ricorrente, mediante dispositivo (elemento di possesso) e fattore biometrico "FINGERPRINT_FACEID" (elemento di inerenza), come dimostrato dai LOG riportati nei doc.ti allegati, nei quali è indicato solo uno stralcio di alcune operazioni - ma che su richiesta del Collegio potranno esser depositati per intero.

Ha chiarito che non vi è stata alcuna installazione (enrollement) dell'APP su altri device.

Tra le transazioni contestate ve ne sono ben 33, nello stesso periodo, che il ricorrente non ha disconosciuto, anche presso lo stesso sito internet per adulti ed anche mediante l'uso materiale della carta.

Tale circostanza, unitamente alla mancata contestualizzazione della frode, esclude l'ipotesi della clonazione.

Il servizio SMS Alert era attivo ed ha perfettamente funzionato inviando al cellulare registrato un messaggio per ogni transazione superiore ad euro 100,00 (limite impostato dallo stesso ricorrente come si evince dal campo "Servizio sms").

I due SMS Alert del 15.12.2025 lo hanno puntualmente avvisato delle transazioni eseguite.

Ne consegue che il ricorrente ha omesso di controllare l'home banking e la sua movimentazione.

In sede di repliche il ricorrente ha dichiarato che nel periodo in cui si sono verificate le operazioni sconosciute era a Tokyo e pertanto aveva inserito nel cellulare una SIM giapponese.

Nelle controrepliche – ed in via preliminare - la banca deduce che il cambio di SIM, contrariamente a quanto sostenuto dalla difesa avversaria, consente proprio di avere la connessione dati anche nel paese estero: pertanto il sito dell'intermediario era perfettamente consultabile e così anche l'APP.

In secondo luogo, il ricorrente poteva comunque connettersi al sito della propria banca ed all'APP indipendentemente dalla SIM, tramite PC.

Dalla copia del passaporto allegata alle repliche si evince che il 21.12.2024 il ricorrente ha fatto rientro in Italia.

Ha, quindi, insistito per il rigetto del ricorso.

DIRITTO

Come noto, l'utilizzo fraudolento è disciplinato dal d.lgs. 27 gennaio 2010, n. 11, modificato a seguito dell'entrata in vigore (il 13/01/2018) del D.lgs. 15 dicembre 2017, n. 218, di recepimento della direttiva (UE) 2015/2366 (c.d. PSD2) relativa ai servizi di pagamento nel mercato interno, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta.

In tale contesto normativo, secondo la posizione consolidata dell'ABF, la disciplina sopra citata prevede un regime probatorio di favore per l'utente di strumenti e servizi di pagamento, essendo *"ispirata al principio del "rischio d'impresa", e cioè all'idea secondo la quale è razionale far gravare i rischi statisticamente prevedibili legati ad attività oggettivamente "pericolose", che interessano un'ampia moltitudine di consumatori o utenti, sull'impresa, in quanto quest'ultima è in grado, attraverso la determinazione dei prezzi di vendita dei beni o di fornitura del servizio, di ribaltare sulla massa dei consumatori e degli utenti il costo dell'assicurazione di detti rischi"* (così – ex multis - Collegio di Coordinamento, decisione n. 3498/2012).

In particolare, l'art. 10 del d.lgs. 11/2010 prevede, in merito all'onere della prova gravante sul prestatore dei servizi di pagamento (PSP), una precisa e graduata sequenza, in base alla quale il PSP è tenuto a dimostrare:

1. l'autenticazione, la corretta registrazione e contabilizzazione della o delle operazioni contestate e l'assenza di malfunzionamenti delle procedure necessarie per la sua esecuzione o di altri inconvenienti che si configura come antecedente logico rispetto alla prova della colpa grave (o dolo) dell'utente;
2. il comportamento gravemente colposo (o fraudolento o doloso) dell'utilizzatore (anche per presunzioni).

Nel merito, si rileva che il ricorrente ha contestato 58 transazioni (quasi interamente avvenute su un sito per adulti) nel periodo compreso fra il 17.11.2024 e il 15.01.2025, per un importo complessivo di euro 2.158,61, al netto del parziale rimborso della somma di euro 65,08.

L'intermediario evidenzia che l'app non ha subito enrollment su altri dispositivi: è stato infatti lo stesso Titolare tramite l'APP installata sul proprio dispositivo con Deviceld, sin dal giorno 14/07/2022 e già utilizzata per autorizzare accessi e operazioni, ad aver utilizzato la medesima APP ed il medesimo device per autorizzare ed autenticare la transazione contestata.

Orbene, 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. Tale circostanza, tuttavia, non esclude che la condotta dell'intermediario debba essere scrutinata in base alle regole generali del diritto delle obbligazioni, sotto il profilo del corretto adempimento delle obbligazioni contrattuali, eventualmente integrate dal principio di buona fede (Collegio di Roma, decisione n. 361/25; Collegio di Napoli, decisione n. 6488/23, Collegio di Milano, decisione n. 8435/23, Collegio di Torino n. 15116/2022), potendosi dunque fondare la decisione sugli artt. 1375, 1176, co. 2, e 1218 c.c. (Collegio di Roma, decisione n. 2531/24).

Ciò al fine di verificare se sussistono elementi che possono essere presi in considerazione sotto il profilo del diligente adempimento alle obbligazioni contrattuali da parte del prestatore di servizi di pagamento (art. 1218 c.c.) e, quindi, di un concorso di colpa ex art. 1227 c.c.

Il Collegio, infatti, potrebbe 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 indizi 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.

Ad ogni modo, l'intermediario versa in atti i log relativi alla sua autenticazione, dai quali si evince l'utilizzo dell'app della ricorrente (push autorizzativa come fattore di possesso) installata sul device e del fattore biometrico (fattore di inerenza), come da legenda allegata in atti.

In ordine agli elementi rilevanti del fatto, si evidenzia che in data 15.01.2025 il ricorrente ha ricevuto l'estratto conto della carta di credito ed ha appurato che a sua insaputa erano state eseguite 58 operazioni non autorizzate su un sito per adulti, dal 17.11.2024 al 14.01.2025, per complessivi euro 2.223,67.

Al riguardo si osserva che, secondo l'orientamento condiviso dei Collegi, le mancate allegazioni del cliente sulle circostanze di fatto della frode rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo, qualora l'intermediario abbia offerto la prova dell'autenticazione delle transazioni disconosciute.

In dettaglio, con riferimento agli utilizzi fraudolenti on line, i Collegi hanno ritenuto che si debba distinguere l'ipotesi in cui la mancata autorizzazione dell'operazione di pagamento sarebbe legalmente presunta (ciò si verifica nei casi di furto o smarrimento dello strumento di pagamento) da quella in cui, in assenza della predetta presunzione, il ricorrente debba allegare i fatti che rendano plausibile che l'operazione di pagamento è stata disposta da un terzo non autorizzato. Conseguentemente, hanno convenuto che, nelle contestazioni di utilizzi fraudolenti on line di strumenti di pagamento in cui: i.) l'intermediario ha offerto la prova dell'autenticazione delle transazioni sconosciute; ii.) il sistema di pagamento risulta conforme alla Strong Customer Authentication (SCA); iii.) non risultano indizi di anomalia delle operazioni e/o ulteriori elementi, le mancate allegazioni del cliente sulle circostanze di fatto della frode, che afferma di aver patito, rappresentano un elemento da cui il Collegio può trarre il proprio convincimento, insieme ad altre circostanze, circa la colpa grave del ricorrente medesimo.

Ma vi è di più.

In caso di operazioni sconosciute intervallate da operazioni autorizzate, deve rilevarsi come la prospettazione del ricorrente, che impugni selettivamente solo alcune operazioni – implicitamente riconoscendo la legittimità delle altre – fornisca un quadro presuntivo, incerto e contraddittorio incompatibile con l'ipotesi di clonazione dello strumento.

Oltretutto, come emerge dalla copiosa documentazione in atti, a parere di questo Collegio appare evidente che il ricorrente abbia tenuto un comportamento negligente nel mancato controllo del conto di appoggio della carta. Infatti, il ricorrente solo a distanza di diverso tempo dal preteso utilizzo fraudolento della carta rilevava l'esistenza di movimentazioni anomale e procedeva al blocco della carta. A ciò consegue che il ricorso non merita accoglimento.

PER QUESTI MOTIVI

Il Collegio respinge il ricorso.

IL PRESIDENTE