

COLLEGIO DI BARI

composto dai signori:

(BA) TUCCI	Presidente
(BA) PORTA	Membro designato dalla Banca d'Italia
(BA) BARTOLINI	Membro designato dalla Banca d'Italia
(BA) VESSIA	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore FILIPPO BOTTALICO

Seduta del 23/04/2026

FATTO

La ricorrente riferisce di aver ricevuto, in data 26/11/2025, un SMS che le segnalava un presunto pagamento e la invitava a contattare un numero di cellulare per il disconoscimento.

Sostiene di aver eseguito l'accesso in *app*, senza riscontrare alcuna anomalia, ma che ciò nonostante "*dopo pochi minuti*", riceveva notifiche in *app* e comunicazioni via *email* relative ad accessi non autorizzati, al cambio del dispositivo associato e alla modifica del numero collegato al conto.

Afferma che "*nel medesimo frangente*" venivano disposte due operazioni fraudolente per € 5,00 ed € 239,00 a valere sulla carta attivata presso l'intermediario odierno resistente.

Dichiara di essere stata vittima di una frode informatica realizzata mediante artifici e raggiri e invoca il riparto dell'onere probatorio di cui al d.lgs 11/2010.

Chiede il rimborso del complessivo importo sottratto, pari ad € 244,00, "*oltre agli eventuali oneri accessori*".

Costituitosi, l'intermediario afferma che le operazioni di pagamento sono state eseguite tramite SCA. In particolare, dichiara di allegare evidenze relative alle OTP-SMS inviate all'utenza certificata della ricorrente con i codici necessari per effettuare il cambio del dispositivo associato al profilo, di cui veniva inoltre inviata un'*email*, nonché una notifica *push* al *device* precedentemente in uso.

Illustra, altresì, il dettaglio delle notifiche *push* relative alle singole transazioni e riportanti il testo con l'importo dell'operazione che si stava per autorizzare.

Ritiene integrato il requisito della colpa grave posto che, dalla trascrizione della telefonata intercorsa con il servizio clienti, emerge la risposta "sì" della ricorrente al quesito esplicito dell'operatore volto ad accertare se l'interlocutore telefonico avesse richiesto i codici di accesso al conto.

Osserva, pertanto, che nonostante non ne sia fatta menzione in sede di ricorso e in sede di denuncia, la ricorrente ha dato credito ad un ignoto interlocutore e ad un SMS contenente un numero di cellulare per il disconoscimento di un presunto pagamento.

In ogni caso, rammenta che è onere del cliente fornire elementi idonei a circostanziare lo svolgimento dei fatti, cosa che nel caso di specie non è stata fatta.

Fa presente che l'allegato contenente il messaggio non conferma l'effettiva ricezione poiché è un'immagine parziale.

Rappresenta di aver introdotto un ulteriore presidio di tutela consistente in un "bollino di sicurezza" che appare nella prima schermata di accesso tutte le volte in cui un reale operatore della banca avvia un contatto con il cliente.

Sul punto, precisa di aver inviato alla ricorrente *email* informative di tale specifico servizio, nonché varie comunicazioni contenenti informazioni sull'argomento delle truffe online.

Ritiene che non ricorrano gli indici di frode di cui al d.m. n. 112/2007 e che, in ogni caso, non sarebbe tenuto ad intervenire ogniqualvolta si registrino pagamenti di importo anomalo, in quanto ciò comporterebbe un'indebita ingerenza nell'autonomia dispositiva dell'utente.

Chiede, pertanto, il rigetto del ricorso.

La ricorrente ha rinunciato alle repliche.

DIRITTO

Premesso che le operazioni contestate sono state eseguite sotto il vigore del d.lgs. 27/01/2010, n. 11, come modificato dal d.lgs. 15/12/2017, n. 218 di recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2), entrato in vigore il 13/01/2018, nella denuncia in atti la ricorrente non circostanzia la frode di cui asserisce essere stata vittima.

In sede di modulo di disconoscimento, nega di essere stata contattata da terze persone tramite SMS, chiamate o *email* e di aver fornito credenziali o codici autorizzativi.

Oggetto di disconoscimento sono dunque due operazioni di pagamento *online*, effettuate in data 26/11/2025.

Risulta un'ulteriore operazione disconosciuta del 27/11/2025, già rimborsata dall'intermediario e pertanto non oggetto di ricorso.

In ordine all'autenticazione e all'esecuzione delle operazioni oggetto della presente controversia, l'intermediario innanzitutto precisa che il 26/11/2025, giorno della truffa, è stato effettuato un accesso con *password* e che, *"rilevando il sistema un dispositivo mobile differente da quello utilizzato in precedenza dalla ricorrente"*, è stato richiesto un ulteriore *step* di autenticazione basato su una OTP SMS.

Precisa di aver introdotto una procedura di sicurezza rafforzata, al fine di garantire elevati standard di tutela, basata sull'invio di una seconda OTP SMS volta a convalidare l'associazione del nuovo dispositivo all'*account*.

A sostegno di quanto affermato, versa in atti la relativa documentazione tecnica, corredata di legenda esplicativa.

Riporta, inoltre, le evidenze dei due SMS contenenti le OTP e riportanti il tipo di operazione che la ricorrente si accingeva ad autorizzare (accesso e associazione di nuovo dispositivo).

Si evidenzia che il numero di cellulare destinatario dei messaggi coincide con quello indicato dalla ricorrente in sede di denuncia e nel modulo di presentazione dell'odierno ricorso.

Pertanto, ai fini dell'associazione all'*home banking* della ricorrente del dispositivo con cui sono state eseguite le operazioni, il sistema ha richiesto:

- la *password* di accesso (fattore di conoscenza);
- la OTP SMS inviata all'utenza della cliente (fattore di possesso).

Il nuovo device è contraddistinto dal codice alfanumerico 5c***f50 (cfr. valorizzazione colonna “ID_Device”).

L’intermediario afferma che le operazioni sono state autenticate mediante *tap* dell’apposita notifica *push* autorizzativa inviata sul *device* registrato secondo le modalità sopra descritte (fattore di possesso) e validazione tramite *password* (fattore di conoscenza); allega i relativi *log*, corredati da legenda esplicativa, nonché evidenza relativa all’esecuzione del *tap* sulla notifica *push* in questione.

Dall’esame di tali *log* si evince l’utilizzo della *password* (cfr. valorizzazione colonna “authorization Type”: fattore di conoscenza) per convalidare la notifica *push* ricevuta sul dispositivo 5c***f50 registrato secondo le modalità sopra descritte (cfr. riquadro rosso: fattore di possesso).

Alla luce di tale documentazione, si deve ritenere raggiunta la prova della conformità ai requisiti normativamente previsti in tema di SCA delle operazioni disconosciute (in senso conforme, Collegio di Bari decisioni nn. 4080/2025, 10521/2025 e 5596/2023; Collegio di Palermo, decisione n. 8844/2025; Collegio di Milano, decisione n. 7520/2025; Collegio di Roma, decisione n. 877/2024; Collegio di Torino, decisioni nn. 9708/2025, 2063/2024 e 3956/2023; Collegio di Bologna, decisione n. 10865/2025).

Senonché *“la previsione di cui all’art. 10, comma 2, del d. lgs. n.11/2010 in ordine all’onere posto a carico del PSP della prova della frode, del dolo o della colpa grave dell’utilizzatore, va interpretato nel senso che la produzione documentale volta a provare l’ ‘autenticazione’ e la formale regolarità dell’operazione contestata non soddisfa, di per sé, l’onere probatorio, essendo necessario che l’intermediario provveda specificamente a indicare una serie di elementi di fatto che caratterizzano le modalità esecutive dell’operazione dai quali possa trarsi la prova, in via presuntiva, della colpa grave dell’utente”* (Collegio di Coordinamento, decisione n. 22745/2019).

Difatti, la mancanza della prova di autenticazione è risolutiva e dirimente rispetto alla valutazione di eventuali profili di colpa ascrivibili al cliente, in quanto la prova di autenticazione rappresenta, in aderenza al dato normativo, un *prius* logico rispetto alla prova della colpa grave dell’utente.

Sul punto, la ricorrente sostiene di aver ricevuto un SMS che la informava di un presunto pagamento, invitandola a contattare un numero di cellulare per il disconoscimento.

Sia in sede di denuncia, sia in sede di ricorso, ha affermato di non aver chiamato tale numero, ma di aver controllato tramite *app* l’esistenza del pagamento.

Ha aggiunto di aver ricevuto notifiche relative all’accesso da un altro dispositivo e al cambio di utenza telefonica, prima di essersi avveduta dei pagamenti oggetto di ricorso.

Tuttavia, l’intermediario ha prodotto la trascrizione della telefonata intercorsa con l’autentico servizio clienti, in cui la ricorrente sembra alludere ad una chiamata con un presunto operatore della banca che la informava *“che il conto era bloccato”*.

L’intermediario, al riguardo, ha inoltre precisato che l’operatore reale [della convenuta] *“ha rivolto alla ricorrente un quesito esplicito volto ad accertare se l’interlocutore telefonico avesse richiesto i codici di accesso al conto, formulando testualmente la seguente domanda: ‘le ha richiesto dei codici di accesso al conto, immagino quindi dei codici che le arrivano via SMS o via mail’. Alla medesima ora, la ricorrente ha fornito risposta affermativa, dichiarando: ‘sì’*.

La ricorrente, che ha ricevuto le controdeduzioni con la relativa documentazione allegata, ha rinunciato alle repliche.

In ogni caso, si deve evidenziare che:

- la ricorrente versa in atti solo evidenza di un SMS, affermando di non avervi dato seguito ma che, ciò nonostante, si avvedeva dei pagamenti fraudolenti;
- per quanto il mittente pare riconducibile alla convenuta, il messaggio non si colloca all’interno di una *chat* contenente altri messaggi genuini;
- il numero di cellulare indicato per il disconoscimento non è in alcun modo riconducibile alla resistente.

A ciò si aggiunga che, come già osservato, sono in atti evidenze relative ai messaggi ricevuti dalla ricorrente sulla propria utenza telefonica, contenenti le OTP per eseguire l'accesso e per associare un nuovo dispositivo all'*account*; si tratta, dunque, di messaggi "parlanti" che sollecitavano l'attenzione della cliente sull'operazione che stava per autorizzare (cfr. Collegio di Bologna, decisione n. 2224/2024).

Pertanto, si richiama in senso adesivo l'orientamento di questo Collegio secondo il quale *"è indice di colpa grave la prova che sia pervenuta al cliente una comunicazione ulteriore rispetto alla procedura di autenticazione forte, tale da sollecitare la sua attenzione sull'operazione che sta per autorizzare (ad es. OTS) e il cui contenuto informativo non sia messo in dubbio da indicazioni di segno contrario (ad es. messaggi di storno)"* (Collegio di Bari, decisioni nn. 3171/2026 e 3128/2024; adde Collegio di Palermo, decisione n. 953/2024).

In ordine all'attivazione e al funzionamento di sistemi di allerta, il Collegio di Coordinamento ha affermato che *"fra i doveri di protezione dell'utente gravanti sull'intermediario rientra l'onere di fornire il servizio di sms alert o assimilabili da cui l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene. Gli effetti della mancata adozione del servizio di alert dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto"* (Collegio di Coordinamento, decisione n. 24366/2019).

Secondo la giurisprudenza arbitrale, la mancata attivazione ovvero il mancato funzionamento di tale servizio (o di servizio assimilabile) sono ritenuti irrilevanti nelle ipotesi di esecuzione di una sola operazione di pagamento fraudolenta ovvero di più transazioni ma a distanza di pochi minuti l'una dall'altra, e complessivamente in un arco di tempo limitato, in quanto la ricezione dell'alert non potrebbe in concreto limitare il pregiudizio dell'utente.

Nel caso in esame le operazioni sono state eseguite alle ore 18:44 e 18:45, dunque a distanza di un minuto l'una dall'altra.

A ciò si aggiunga che deve ritenersi comunque irrilevante un sistema di *alert ex post* in caso di invio – come nell'odierna vicenda – di SMS cc.dd. parlanti (*ex multis*, Collegio di Bari, decisioni nn. 2664/2023, 12866/2022 e 14020/2022).

Da ultimo, si rammenta che l'art. 8 d.m. n. 112/2007 identifica i casi di frode che, ai fini della normativa stessa, 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.

Secondo l'orientamento condiviso dei Collegi, le relative previsioni 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.

Conseguentemente, una volta accertata la colpa grave del cliente, qualora sussista uno dei seguenti indici di frode:

- i. sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento, prevista al punto 1 della lett. b) del menzionato art. 8;
 - ii. tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita, di cui al punto 2 della lett. a) del citato art. 8;
 - iii. due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di sessanta minuti, di cui al punto 3 della lett. b) del medesimo art. 8,
- la ripartizione della responsabilità con il prestatore dei servizi di pagamento (PSP) deve 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 (*ex multis*, Collegio di Bari, decisione n. 7126/2024; Collegio di Bologna, decisione n. 5884/2024).

Secondo la giurisprudenza arbitrale, inoltre, sebbene il d.m. n. 112/2007 faccia riferimento alla prevenzione delle frodi sulle carte di pagamento, gli indici di frode ivi disciplinati all'art. 8 possono costituire un parametro di valutazione del comportamento del PSP, ove possibile, anche con riguardo ad operazioni eseguite con altri strumenti di pagamento (ad es. bonifici o pagamenti online) in ragione dell'unicità della *ratio* sottesa a tale normativa (così Collegio di Bari, decisione n. 10175/2023; Collegio di Bologna, decisioni nn. 8394/2024 e 12960/2022; Collegio di Roma, decisione n. 8843/2023; Collegio di Milano, decisione n. 13092/2022; Collegio di Torino, decisione n. 3964/2022).

È inoltre possibile valorizzare indici di frode ulteriori a quelli del decreto ministeriale in presenza di un'operatività anomala rispetto alle movimentazioni storiche del ricorrente (ad esempio con riguardo al numero, alla tipologia, all'importo, al tempo di esecuzione e alla riconducibilità delle operazioni al medesimo beneficiario), ove vi sia un'evidenza delle stesse (così Collegio di Bari, decisione n. 4110/2024; Collegio di Roma, decisione n. 9732/2024; Collegio di Milano, decisione n. 6758/2024).

Tanto precisato, si ribadisce che, secondo l'orientamento più recente condiviso dai Collegi, i principi del d.m. n. 112/2007 non hanno un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate ma sono espressione di un generale obbligo di monitoraggio delle operazioni, da valorizzare per valutare la condotta dell'intermediario (*ex multis*, Collegio di Bari decisione n. 7228/2025).

Venendo al caso di specie, si osserva che, sebbene formalmente l'operatività contestata parrebbe ricondursi all'indice di frode *sub iii*), tuttavia la strettissima connessione temporale fra le due operazioni ma soprattutto la circostanza che una di queste (consistente in una ricarica *online* di € 5,00 in favore di un'azienda di telecomunicazioni italiana) risultava coerente con un'operatività normale inducono a ritenere l'insussistenza dell'insorgenza di indici che avrebbero dovuto indurre l'intermediario resistente ad attività presidi per contrastare una potenziale frode.

Ne consegue che il ricorso non è meritevole di accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE