

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) CIPRIANI	Membro di designazione rappresentativa degli intermediari
(BA) BOTTALICO	Membro di designazione rappresentativa dei clienti

Relatore FILIPPO BOTTALICO

Seduta del 13/04/2026

FATTO

La ricorrente afferma che, in data 10/08/2025, veniva contattata per un articolo che aveva messo in vendita su un sito di *marketplace*.

Riporta che la finta acquirente, tramite un sito apparentemente riconducibile a quello reale, le forniva indicazioni su come ottenere il pagamento e, a tal fine, la sollecitava a fornire i dati della sua carta.

Ammette di aver inserito i dati della carta, da cui successivamente venivano effettuati gli addebiti contestati.

Rappresenta che le veniva inoltre richiesto di aprire un conto presso un terzo intermediario e riferisce di essersi avveduta della truffa *“dopo l’ennesima richiesta di denaro”*.

Dichiara di aver contattato il servizio clienti dell’intermediario odierno convenuto, che le riferiva che *“erano state rilevate alcune anomalie relative alla [...] carta di credito e che le autorizzazioni alle operazioni erano state bloccate automaticamente”*.

Nonostante l’iniziale accredito degli importi sconosciuti, ne contesta il riaddebito e il riscontro fornito dall’intermediario secondo cui venivano rilevate *“criticità nella custodia delle [...] credenziali usate per l’autorizzazione delle operazioni dispositive”*.

Chiede *“che il reclamo inoltrato [...] venga riesaminato e accolto”*

Costitutosi, l’intermediario premette che la ricorrente, a seguito di una truffa *online* perpetrata ai suoi danni, ha chiesto il rimborso di due operazioni di pagamento tramite carta di credito pari rispettivamente ad € 428,16 ed € 721,96.

Afferma che la ricorrente, in sede di denuncia e nel modulo di disconoscimento, riferiva di essere stata contattata per la vendita di un prodotto su un sito di *marketplace* e di *“aver seguito le indicazioni del sedicente compratore, comunicando le credenziali e i codici della propria carta”*.

Ciò posto, afferma che le operazioni contestate venivano effettuate in vigenza del d.lgs. 27/01/2010, n. 11; al riguardo, evidenzia di adottare un sistema di autenticazione forte sia per l'accesso all'area riservata sia per l'autorizzazione delle operazioni di pagamento.

Riferisce che la ricorrente attivava il servizio *token* in data 03/07/2025 e che, in generale, per accedere all'area riservata sul sito il cliente deve inserire i propri dati in due diverse sessioni:

- nella prima, il codice cliente (codice di sette cifre, assegnato dalla banca al cliente in fase di stipula del contratto) e la data di nascita;
- nella seconda il codice PIN (codice personale e segreto consegnato dalla banca al cliente e da lui modificabile).

Per completare l'accesso è richiesta l'autorizzazione sul *device* del cliente mediante *token*, un codice monouso generato tramite l'utilizzo dello *smart code* (codice di sei cifre impostato dal cliente, in fase di attivazione del *token*, con l'utilizzo dell'impronta digitale o dei suoi dati biometrici).

Per autorizzare il pagamento, è richiesto di fare “tap” su “autorizza” e, conseguentemente, inserire il codice *smart code* ovvero il codice biometrico.

Nel caso di specie descrive che *“la Cliente, titolare della Carta, accede al portale on-line e predispone l'acquisto; all'atto del pagamento digita numero di carta, mese e anno di scadenza, nome e cognome del Titolare, codice di sicurezza (CVV) e conferma l'operazione”*.

Nello specifico, il sistema di autenticazione forte predisposto per l'autorizzazione delle operazioni di pagamento prevede dunque la ricezione della notifica *push* sul *device* ove risulta attivo il *token* (fattore di possesso), validata mediante digitazione dello *smartcode* o, in alternativa, mediante riconoscimento di impronta digitale/*face-id* (fattore di conoscenza o inerenza).

Da ultimo, ritiene gravemente colposa la condotta della ricorrente, poiché le operazioni contestate sono state eseguite dietro indicazioni del sedicente acquirente.

Fa presente, inoltre, che la ricorrente nella truffa in esame ricopriva il ruolo di venditrice e non di acquirente, con evidente anomalia della richiesta dei dati della carta.

Pertanto, chiede il rigetto della richiesta di rimborso.

In sede di repliche la ricorrente evidenzia che la prima transazione €721,96 è stata *“immediatamente bloccata”* e per tale ragione non comprende le motivazioni a fondamento del mancato blocco della seconda transazione *“ugualmente e puntualmente contestata”*.

Al riguardo, precisa di aver inizialmente ricevuto comunicazione di blocco della transazione perché sospetta *“e poi senza giustificato motivo la predetta transazione veniva evasa in favore del presunto truffatore”*.

Pertanto, insiste per l'accoglimento del ricorso *“con conseguente obbligo [per la convenuta] di liquidare la somma di € 428,16, oltre interessi maturati”*.

All'atto delle controrepliche l'intermediario richiama integralmente quanto sollevato in sede di controdeduzioni e richiede il rigetto del ricorso.

DIRITTO

In via preliminare, si segnala che la ricorrente, nell'ambito della stessa truffa, ha presentato il ricorso n. 1845004/2025 nei confronti di diverso intermediario, accolto dal Collegio per mancato assolvimento dell'onere probatorio relativo alla SCA, con pronuncia n. 543/2026.

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, in sede della denuncia versata in atti la ricorrente ricostruiva i fatti oggetto della presente controversia in termini

analoghi a quelli esposti nel ricorso, in particolare ammettendo di aver fornito i dati della carta da cui venivano effettuati i due pagamenti poi contestati, che consistono in due pagamenti *online* rispettivamente di € 428,16 e di € 721,96 eseguiti in data 10/08/2025.

Si precisa che in sede di repliche la ricorrente ha affermato che la transazione di € 721,96 è stata *“immediatamente bloccata”* e ha lamentato il mancato blocco anche della seconda.

Ha insistito nella richiesta di accoglimento del ricorso (in cui chiedeva il *“riesame”* del reclamo) con conseguente *“obbligo della convenuta di liquidare [...] la somma di 428,16 oltre interessi maturati”*.

A fronte di tale precisazione della domanda da parte della ricorrente e in assenza di deduzioni sul punto da parte dell'intermediario resistente, la disamina del ricorso proseguirà con riguardo alla sola operazione di € 428,16.

In ordine alla modalità di autenticazione ed esecuzione di tale operazione, l'intermediario innanzitutto evidenzia che il *token* risulta associato al profilo della ricorrente dal 03/07/2025, con codice univoco dell'*app* *“98483****233e”*.

Il successivo 10/08/2025, alle ore 11:59, la ricorrente autorizzava tramite *app* la transazione di € 428,16 con carta di credito n. **27.

La resistente rappresenta, in generale, che il sistema di autenticazione forte per l'esecuzione dei pagamenti *online* prevede che:

1. il titolare della carta accede al portale *online*;
2. all'atto del pagamento viene digitato il numero della carta, il mese e l'anno di scadenza, oltre che il nome e cognome del titolare della carta e il codice di sicurezza (CVV), confermando l'operazione;
3. l'intermediario riceve i dati della transazione, li elabora e prepara la notifica *push*, inviandola al *device* registrato ovvero allo *smartphone* su cui il cliente ha attivato il *token*;
4. viene autorizzata l'operazione tramite *smart code*/impronta digitale/riconoscimento facciale;
5. l'*app* comunica all'intermediario l'avvenuta autorizzazione da parte del cliente.

Dunque afferma che l'autenticazione forte del cliente si articola in:

- fattore di possesso: il cliente riceve una notifica *push* sul *device* registrato;
- fattore di conoscenza o inerenza: *smart code* o impronta digitale/riconoscimento facciale.

A supporto produce le relative evidenze, dalle quali risulta che alle ore 11:59 iniziava la fase di autorizzazione della transazione *online*, tramite *token/push*.

Alle ore 11:59:24 l'intermediario inviava al *provider* la risposta del servizio *StartAuth* con *authenticationType* *“OOB”* (per notificare al *provider* che il pagamento sarebbe stato autorizzato tramite *token/push*) in attesa dell'autorizzazione della ricorrente.

Successivamente, l'intermediario riferisce che dalla pagina *web* del *merchant* il cliente viene poi rimandato all'*app* ove gli viene mostrata la notifica *push*; a sostegno, produce la schermata relativa al caso di specie.

L'operazione, pertanto, è stata effettuata tramite:

- fattore di possesso: notifica *push* sul *device* registrato o su cui il cliente ha attivato il *token* (cfr., *mobileApplId*, valore *“98****33e”* che risulta coincidere con quello riportato nella prima schermata relativa all'attivazione del *token* avvenuta già il 03/07/2025);
- fattore di inerenza: *“il cliente autorizza l'operazione dalla APP attraverso il riconoscimento del volto (FACE ID)”*.

Sulla scorta di tali evidenze documentali, si richiama in senso adesivo la giurisprudenza arbitrale che ritiene la documentazione prodotta idonea ad attestare la conformità ai requisiti normativamente previsti in tema di SCA delle operazioni contestate (*ex multis*, Collegio di Milano, decisioni nn. 11448/2024 e 11130/2024; Collegio di Roma, decisioni nn. 7140/2024 e 8658/2024; Collegio di Torino, decisioni nn. 11216/2024 e 7763/2024).

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.

Nel caso di specie, la ricorrente ha affermato di essere stata contattata su un sito astrattamente riconducibile al sito reale del *marketplace* e di aver fornito al falso acquirente i dati della carta.

Peraltro, dalla disamina degli *screenshot* relativi all'interlocazione avvenuta con il frodatore non solo non si evince alcuna comunicazione truffaldina proveniente da mittenti riconducibili all'intermediario convenuto, ma soprattutto il tenore dei messaggi evidenzia una colpevole e inescusabile negligenza della ricorrente.

La ricorrente lamenta, inoltre, il perfezionamento dell'operazione, *"pur essendo stata ritenuta sospetta"* nonostante l'immediato blocco dell'altra.

Non vi sono però elementi da cui poter riscontrare il carattere sospetto di tale pagamento, e in ogni caso si rammenta che *"mentre l'art. 2 del Regolamento Delegato n. 2018/389 prescrive un monitoraggio ex post sulle operazioni di pagamento, non è previsto un obbligo di monitoraggio delle operazioni in tempo reale"* (Q&A dell'EBA n. 4090/2018; in senso conforme, Collegio di Bari, decisione n. 1912/2026; Collegio di Roma, decisione n. 707/2022).

In tema di sistemi di allerta, si rammenta che, secondo l'autorevole insegnamento del Collegio di Coordinamento, *"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).

Il medesimo Collegio di Coordinamento ha precisato che *"la mancata attivazione del servizio sms – alert costituisce in ogni caso una carenza organizzativa imputabile all'intermediario che, oltre a produrre l'effetto giustificativo solo a fronte della specifica dichiarazione liberatoria di rifiuto del cliente ad avvalersene (già affermata dal precedente "coordinamento"), non può non essere rilevata anche d'ufficio"* (Collegio di Coordinamento, decisione n. 8672/2024).

Nel caso di specie, si evidenzia che l'intermediario ha versato in atti le notifiche *alert* inviate tramite *email* alla ricorrente.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE