Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

COLLEGIO DI BARI

composto dai signori:

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

Relatore ESTERNI - GABRIELE NUZZO

Seduta del 16/03/2026

FATTO

1. Con ricorso del 4 novembre 2025, presentato per il tramite di un rappresentante volontario, la Ricorrente espone di essere titolare di un conto di moneta elettronica acceso presso l'Intermediario.
Riferisce di avere subito, in data 7 novembre 2024, una truffa informatica a seguito della ricezione di una telefonata da parte di un soggetto qualificatosi come operatore di un terzo intermediario, il quale le segnalava la presenza di operazioni sospette sul conto acceso presso l'Intermediario convenuto.
La Ricorrente deduce che, nel corso della telefonata, il presunto operatore le chiedeva di confermare quattro operazioni di pagamento – ciascuna di importo pari a Euro 1.490,00, per un totale di Euro 5.960,00 – ai fini del loro annullamento. Precisa di avere ricevuto, durante la procedura, messaggi di disconoscimento delle operazioni con impegno di riaccredito delle somme.
Lamenta che l'Intermediario non avrebbe adottato misure di sicurezza adeguate, non avendo rilevato l'anomalia di quattro operazioni di rilevante e identico importo, eseguite in rapida sequenza presso un medesimo punto vendita. Contesta, altresì, che la mera messa a disposizione di campagne informative antitruffa non possa esonerare l'Intermediario da responsabilità.
Chiede, pertanto, la restituzione della somma di Euro 5.960,00, oltre alla rifusione delle spese di assistenza difensiva.
2. Costituitosi nel presente procedimento, l'Intermediario rileva che, in data 7 novembre 2024, la Ricorrente ha subito l'appropriazione indebita di Euro 5.960,00 mediante quattro transazioni non autorizzate sul proprio saldo di moneta elettronica.

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

Precisa che il sistema di autenticazione adottato prevede, quali fattori di sicurezza, la notifica *push* sul telefono del cliente (fattore di possesso) e, alternativamente, il parametro biometrico (fattore di inerenza) o la *password* dell'APP (fattore di conoscenza).
Nel caso di specie, riferisce che ciascuna delle quattro operazioni contestate veniva autenticata tramite *Strong Customer Authentication* (SCA), in quanto la Ricorrente:

(i) riceveva una notifica *push* sul dispositivo mobile associato al conto, con titolo «autorizza pagamento» (requisito di possesso);
(ii) proseguiva con la conferma dell'operazione;
(iii) completava l'autorizzazione tramite parametro biometrico (requisito di inerenza).

L'Intermediario sostiene, pertanto, che le operazioni contestate sarebbero state autorizzate personalmente dalla Ricorrente e che non troverebbe applicazione la disciplina di cui al d.lgs. n. 11/2010.
Sottolinea, inoltre, che la semplice lettura del contenuto delle notifiche push avrebbe impedito la prosecuzione dei pagamenti e che la Ricorrente non ha prodotto evidenza documentale della telefonata asseritamente ricevuta.
Afferma, infine, di avere fornito il servizio di *alert* mediante l'invio di una notifica *push* istantanea per ogni operazione eseguita e di avere predisposto campagne informative antitruffa.
Chiede, pertanto, il rigetto del ricorso.
3. In sede di repliche, la Ricorrente si riporta a quanto già dedotto e alle conclusioni formulate con il ricorso. Afferma di avere fornito evidenza dello *screenshot* della chiamata ricevuta dal truffatore (che, invero, non risulta allegato né al ricorso, né alle repliche) e nega di avere comunicato credenziali o codici di alcun tipo.
Insiste per l'accoglimento del ricorso.
4. Nelle controrepliche, l'Intermediario si riporta a quanto già dedotto e alle conclusioni formulate.

DIRITTO

1. Oggetto del presente procedimento sono quattro operazioni di pagamento *online*, di Euro 1.490,00 ciascuna, effettuate in data 7 novembre 2024.
Al riguardo, l'Intermediario ha eccepito che le operazioni disconosciute sono state in realtà poste in essere personalmente dalla Ricorrente e che, pertanto, esse non sarebbero soggette al regime previsto dall'art. 10 d.lgs. 11/2010.
Al riguardo, il Collegio intende dare continuità al suo precedente orientamento secondo cui, se il concorso causale dell'utente in fase dispositiva e/o autorizzativa è parziale (ad es. con l'inserimento di uno dei fattori di autenticazione), la transazione non deve intendersi, per ciò solo, autorizzata, poiché la normativa speciale (PSD2 e disposizioni di recepimento), prescindendo dalla nozione civilistica di "consenso", dispone che quest'ultimo dev'essere prestato nella forma convenuta tra il pagatore stesso e il PSP.
Nel caso di specie la ricorrente nega di avere eseguito personalmente le operazioni, avendo fatto solo riferimento ad una richiesta (del truffatore) di conferma di operazioni da annullare, trovando quindi nel caso applicazione la disciplina del d.lgs. 27 gennaio 2010, n. 11, come modificato dal d.lgs. 15 dicembre 2017, n. 218 (entrato in vigore il 13 gennaio 2018), che ha recepito la direttiva (UE) n. 2015/2366, relativa ai servizi di pagamento nel mercato interno (c.d. PSD 2).
2. Con riguardo a detta disciplina, il Collegio rammenta che, ai sensi dell'art. 10 d.lgs. n. 11/2010, «[q]ualora l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento già eseguita o sostenga che questa non sia stata correttamente eseguita, è onere del prestatore di servizi di pagamento provare che l'operazione di pagamento è stata autenticata, correttamente registrata e contabilizzata e che non ha subito le conseguenze del malfunzionamento delle procedure necessarie per la sua esecuzione o di altri inconvenienti».

Il secondo comma del medesimo art. 10 precisa, inoltre, che, ove l'utilizzatore neghi di avere autorizzato un'operazione di pagamento eseguita, «l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7» (: obblighi di custodia e di corretta utilizzazione dello strumento di pagamento).
Sempre il secondo comma stabilisce che «è onere del prestatore di servizi di pagamento, compreso, se del caso, il prestatore di servizi di disposizione di ordine di pagamento, fornire la prova della frode, del dolo o della colpa grave dell'utente».
La disciplina relativa all'autenticazione e alle misure di sicurezza da adottare nel caso di operazioni elettroniche di pagamento a distanza è contenuta nell'art. 10-*bis* d.lgs. n. 11/2010, secondo il quale:

(i) «i prestatori di servizi di pagamento applicano l'autenticazione forte del cliente quando l'utente:
   a) accede al suo conto di pagamento on-line;
   b) dispone un'operazione di pagamento elettronico;
   c) effettua qualsiasi azione, tramite un canale a distanza, che può comportare un rischio di frode nei pagamenti o altri abusi» (1° comma);

(ii) «[n]el caso dell'avvio di un'operazione di pagamento elettronico di cui al paragrafo 1, lettera b), per le operazioni di pagamento elettronico a distanza, l'autenticazione forte del cliente applicata dai prestatori di servizi di pagamento comprende elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e a un beneficiario specifico» (2° comma).

Ai sensi dell'art. 1, 1° comma, lett. q-*bis*), d.lgs. n. 11/2010, per "autenticazione forte del cliente" (di seguito, "SCA") si intende «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 Collegio di Coordinamento ha, in più occasioni, precisato che la disciplina in esame istituisce "*un regime di speciale protezione e di altrettanto speciale favor probatorio a beneficio degli utilizzatori, i quali sono, dunque, tenuti al semplice disconoscimento delle operazioni di pagamento contestate, mentre è onere del prestatore dei servizi di pagamento provare che l'operazione disconosciuta sia stata autenticata, correttamente registrata e contabilizzata e che la sua patologia non sia dovuta a malfunzionamenti delle procedure esecutive o ad altri inconvenienti del sistema*". Il Collegio di Coordinamento ha, peraltro, precisato che "*l'apparentemente corretta autenticazione dell'operazione* [non] *è necessariamente sufficiente a dimostrarne la riconducibilità all'utilizzatore che la abbia disconosciuta, cosicché la responsabilità dell'utilizzatore resta circoscritta ai casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato. Laddove una simile responsabilità non possa essere dimostrata dall'intermediario prestatore del servizio, pertanto, l'utilizzatore non sarà tenuto a sopportare le conseguenze dell'uso fraudolento, o comunque non autorizzato, dello strumento di pagamento (se non nei limiti, eventualmente stabiliti dall'intermediario, di una franchigia non superiore a 50 euro)*" (così Collegio di Coordinamento, decisione n. 3947/2014; in senso conforme, Collegio di Coordinamento, decisioni nn. 3498/2012, 991/2014; cfr. anche Collegio di Coordinamento, decisione n. 22745/2019, con particolare riguardo all'insufficienza della prova della regolarità formale dell'operazione contestata, ai fini dell'assolvimento dell'onere della prova gravante sull'intermediario, *e x* art. 10, 2° comma, d. lgs. n. 11/2010).
Il menzionato orientamento ha trovato riscontro nella giurisprudenza di legittimità (Cass. 3 febbraio 2017, n. 2950), secondo cui la disciplina speciale relativa agli strumenti di pagamento ha esplicitato un principio generale applicabile in tema di onere probatorio a carico del debitore professionale nelle

azioni di risoluzione contrattuale, risarcimento del danno o adempimento, "*in quanto si è ritenuto che non può essere omessa la verifica dell'adozione da parte dell'istituto bancario delle misure idonee a garantire la sicurezza del servizio* [...]; *infatti la diligenza posta a carico del professionista ha natura tecnica e deve essere valutata tenendo conto dei rischi tipici della sfera professionale di riferimento ed assumendo quindi come parametro la figura dell'accorto banchiere*" [in senso conforme, cfr. Cass., 12 aprile 2018, n. 9158; Cass. 12 febbraio 2024, n. 3780; v. anche Cass., 26 novembre 2020, n. 26916, anche per l'importante statuizione, secondo cui "*al fine di garantire la fiducia degli utenti nella sicurezza del sistema (il che rappresenta interesse degli stessi operatori), è del tutto ragionevole ricondurre nell'area del rischio professionale del prestatore dei servizi di pagamento – prevedibile ed evitabile con appropriate misure destinate a verificare la riconducibilità delle operazioni alla volontà del cliente – la possibilità di un'utilizzazione dei codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o a comportamenti talmente incauti da non poter essere fronteggiati in anticipo*"].

3. Tanto premesso, in ossequio ai principi in tema di riparto dell'onere probatorio sopra enucleati, è necessario innanzitutto verificare la conformità delle operazioni disconosciute alle prescrizioni normative in tema di SCA.

Al riguardo, il Collegio osserva che l'Intermediario ha prodotto evidenza documentale dalla quale risulta che le quattro operazioni contestate sono state eseguite dal dispositivo mobile identificato dal *device* ID n. a91cb**********, associato all'utenza della Ricorrente dal 23 maggio 2024.

In particolare, dall'esame dei *log* forniti dall'Intermediario – corredati dalla relativa legenda esplicativa – risulta che ciascuna operazione è stata autenticata mediante:

(i) la notifica *push* autorizzativa inviata sul dispositivo mobile della Ricorrente, recante espressamente la menzione "*Autorizza pagamento*" (fattore di possesso);
(ii) la validazione tramite parametro biometrico (fattore di inerenza), come attestato dal valore "*OOB* " nella colonna "*Pay_auth_type*" dei *log*.

Sulla base di tali evidenze, il Collegio – in conformità con il proprio precedente orientamento (cfr. Collegio di Bari, decisioni nn. 4080/2025, 10521/2025 e 5596/2023) – ritiene raggiunta la prova della conformità delle operazioni disconosciute ai requisiti della SCA.

4. Sulla base dei principi elaborati dal Collegio di Coordinamento (v. sopra, n. 2), l'accertamento della conformità della procedura di autenticazione alla definizione di SCA contenuta nel d.lgs. n. 11/2010 non è di per sé dirimente per escludere la responsabilità della cliente, che sussiste, invece, nei «casi di comportamento fraudolento del medesimo ovvero al suo doloso o gravemente colposo inadempimento degli obblighi previsti dall'art. 7 del decreto sopra menzionato» (Collegio di Coordinamento, decisione n. 3947/2014, cit.).

Più di recente, il medesimo Collegio di Coordinamento ha chiarito che «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» (decisione n. 22745/2019).

Nel caso in esame, sulla base di quanto emerge dagli atti del procedimento, la condotta della Ricorrente appare connotata da grave negligenza. In particolare, il Collegio rileva i seguenti elementi:

(i) la Ricorrente ha dichiarato di avere ricevuto una telefonata da un soggetto qualificatosi come operatore di un terzo intermediario, diverso da quello convenuto, e di avere confermato le operazioni su richiesta di quest'ultimo;
(ii) nel modulo di disconoscimento compilato in data 8 novembre 2024, la Ricorrente ha riconosciuto di avere ceduto a terzi le proprie credenziali;
(iii) la Ricorrente, pur avendo affermato di avere versato in atti evidenze relative alla telefonata e ai messaggi ricevuti, non ha prodotto documentazione idonea a dimostrare le circostanze della

frode: in particolare, non risulta allegato il registro delle chiamate né lo screenshot della telefonata ricevuta;

(iv) le notifiche *push* autorizzative recavano espressamente la menzione "*Autorizza pagamento*", sicché la semplice lettura del messaggio comparso sul dispositivo avrebbe impedito la prosecuzione dei pagamenti.

La mancata allegazione del registro delle chiamate (che, come detto, non risulta – al contrario di quanto dedotto dalla Ricorrente – allegato al ricorso o alle repliche) non consente al Collegio di accertare se risultino o meno integrati gli estremi di un legittimo affidamento della Ricorrente circa la genuinità dell'interlocuzione con l'Intermediario (cfr. Collegio di Milano, decisioni nn. 24/2025 e 12970/2024; Collegio di Bari, decisioni nn. 2663/2023 e 3157/2022). È peraltro la stessa ricorrente a dichiarare di avere "*ricevuto una telefonata a mezzo … da persona qualificata come operatore*" di altro intermediario).

Ad avviso del Collegio, pertanto, la condotta della Ricorrente è connotata da colpa grave ai sensi dell'art. 12, 4° comma, d.lgs. n. 11/2010.

5. Accertata la colpa grave della Ricorrente, il Collegio deve valutare se la condotta dell'intermediario abbia in qualche modo contribuito alla produzione del danno.

Con riguardo ai sistemi di *alert*, la verifica della cui attivazione è rilevabile d'ufficio, il Collegio di Coordinamento ha affermato il principio per cui, "*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*" (decisione n. 24366/2019).

Nel caso, anche volendo prescindere dal fatto che le operazioni sono state eseguite in rapida sequenza nell'arco di soli quattro minuti (il che renderebbe irrilevante la fornitura del servizio di *alert*), l'Intermediario ha comunque dato evidenza di avere inviato alla Ricorrente un SMS "parlante" per ogni operazione eseguita al numero di telefono dalla stessa indicato, che coincide con quello riportato nel modulo di presentazione del ricorso.

È peraltro da osservare che, per ciascuna delle operazioni contestate, l'Intermediario ha anche inviato alla Ricorrente una notifica *push*, che descrive chiaramente la propria finalità ("*Transazione di 1490,00€ a favore di …*") e contiene il testo "*Autorizza pagamento*".

6. Fermo quanto precede, ad avviso del Collegio, della complessiva vicenda oggetto del presente procedimento, emergono elementi che inducono a ritenere sussistente sotto altro profilo un concorso di colpa dell'Intermediario nella produzione del danno, ai sensi dell'art. 1227, 1° comma, c.c.

In proposito, il Collegio osserva che, dalla documentazione versata in atti, risulta che le quattro operazioni contestate – ciascuna di importo pari a Euro 1.490,00, per un totale di Euro 5.960,00 – sono state eseguite nell'arco di soli quattro minuti, presso un medesimo punto vendita e per importi identici e di rilevante entità. Si tratta, quindi, di un'operatività che, per la sua concentrazione temporale, per la ripetitività e per l'ammontare complessivo delle transazioni, presentava caratteristiche anomale, tali da dovere essere intercettate dai sistemi di monitoraggio di un intermediario diligente.

Al riguardo, il Collegio rammenta che gli Orientamenti finali sulla sicurezza dei pagamenti via internet – adottati il 19 dicembre 2014 dall'EBA e recepiti in Italia, nel maggio 2016, con il 16° aggiornamento alla Circolare n. 285/2013, Parte Prima.IV.4.24 – raccomandano l'adozione di sistemi efficaci di monitoraggio delle operazioni in grado di rilevare modelli di comportamento anomalo del cliente o del dispositivo di accesso del cliente (cfr. anche l'art. 2 del Regolamento delegato (UE) n. 2018/389). In particolare, al punto 10 degli Orientamenti si prevede che "*i meccanismi per il monitoraggio delle operazioni volti a prevenire, rilevare e bloccare il traffico dei pagamenti fraudolenti dovrebbero essere attivati prima dell'autorizzazione finale del prestatore di servizi di pagamento*" e che "*le operazioni sospette o ad alto rischio dovrebbero essere oggetto di una specifica analisi e procedura di valutazione*". Al punto 10.1 si precisa, inoltre, che "*i prestatori di servizi di pagamento dovrebbero utilizzare sistemi*

Arbitro Bancario Finanziario
Risoluzione Stragiudiziale Controversie

di rilevamento e prevenzione delle frodi per individuare operazioni sospette prima che il prestatore di servizi di pagamento autorizzi da ultimo le operazioni o i mandati elettronici".
Nel caso di specie, l'esecuzione di quattro pagamenti *online* di importo identico e rilevante (Euro 1.490,00 ciascuno) nell'arco di soli quattro minuti, presso il medesimo esercente, costituisce un'anomalia oggettivamente rilevabile dai sistemi automatici di monitoraggio di cui un prestatore di servizi di pagamento diligente sarebbe tenuto a dotarsi ai sensi della normativa sopra richiamata. Tale rapida sequenza di operazioni avrebbe dovuto indurre l'Intermediario a sospettare che fosse in corso un'operatività fraudolenta e a bloccarla tempestivamente, al fine di effettuare le opportune verifiche con la titolare dello strumento di pagamento.
La mancata attivazione dell'Intermediario dinanzi a un'operatività così palesemente anomala configura un difetto organizzativo che integra gli estremi del fatto colposo del creditore che ha concorso a cagionare il danno, ai sensi dell'art. 1227, 1° comma, c.c. (cfr., in termini, Collegio di Bari, decisione n. 10175/2023; Collegio di Roma, decisione n. 8843/2023; Collegio di Bologna, decisione n. 5884/2024).
Tale conclusione, peraltro, è ulteriormente avvalorata dalla circostanza che le operazioni oggetto del presente procedimento sono state effettuate presso un medesimo punto vendita nell'arco della stessa giornata, integrando l'indice di frode di cui all'art. 8, comma 1, lett. a), n. 2), d.m. 30 aprile 2007, n. 112, che configura il rischio di frode in presenza di "tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita". Come noto, sebbene il d.m. n. 112/2007 faccia riferimento alla prevenzione delle frodi sulle carte di pagamento, gli indici di frode ivi disciplinati possono costituire un ulteriore parametro di valutazione del comportamento del PSP anche con riguardo ad operazioni eseguite con altri strumenti di pagamento, in ragione dell'unicità della *ratio* sottesa a tale normativa (cfr. Collegio di Bologna, decisione n. 8394/2024; Collegio di Palermo, decisione n. 7019/2024).
7. Fatta questa premessa, tenendo conto, da un lato, della gravità della condotta negligente della Ricorrente – la quale ha confermato quattro operazioni di pagamento su richiesta di un soggetto qualificatosi come operatore di un intermediario diverso dal proprio, omettendo di leggere il contenuto delle notifiche *push* autorizzative – e, dall'altro, del significativo difetto organizzativo dell'Intermediario – che non ha predisposto meccanismi di monitoraggio idonei a rilevare e bloccare un'operatività macroscopicamente anomala, caratterizzata da quattro operazioni di identico e rilevante importo eseguite nell'arco di soli quattro minuti – il Collegio ritiene equo liquidare alla Ricorrente un danno pari a Euro 3.000,00.
8. Non meritevole di accoglimento è la domanda di rimborso delle spese di assistenza professionale, in conformità con i principi enunciati dal Collegio di Coordinamento nella decisione n. 4580/2025, non risultando, peraltro, in alcun modo documentata o quantificata.

P.Q.M.

Il Collegio, in parziale accoglimento del ricorso, dispone che l'intermediario corrisponda al ricorrente la somma di € 3.000,00.
Il Collegio dispone inoltre, ai sensi della vigente normativa, che l'intermediario corrisponda alla Banca d'Italia la somma di € 200,00 quale contributo alle spese della procedura e al ricorrente la somma di € 20,00 quale rimborso della somma versata alla presentazione del ricorso.

IL PRESIDENTE