

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

Relatore ESTERNI - GABRIELE NUZZO

Seduta del 22/01/2026

FATTO

1. Con ricorso del 10 settembre 2025, il Ricorrente riferisce che, in data 6 agosto 2025, intorno alle ore 15:30, riceveva una telefonata dal numero 350****37. L'interlocutore si qualificava quale operatore del servizio antifrode dell'Intermediario e lo avvertiva di un accesso anomalo al suo *account* da un paese estero.

Rappresenta che, nel corso della telefonata, riceveva sull'App dell'Intermediario una notifica *push* con la quale si chiedeva l'autorizzazione a un pagamento di Euro 700,00, che rifiutava, su indicazione del sedicente operatore.

Il Ricorrente riferisce che, a questo punto, cadeva la linea e, in seguito, veniva contattato dal numero di rete fissa 0966*****, apparentemente riconducibile alla filiale dell'Intermediario nel suo comune di residenza e già memorizzato sul telefono. Afferma che, durante tale seconda chiamata, altro soggetto qualificatosi come operatore dell'Intermediario lo invitava a verificare l'assenza di anomalie sull'App e a recarsi il prima possibile presso un ufficio dell'Intermediario per mettere in sicurezza il conto; allo stesso tempo lo esortava a trasferire immediatamente il saldo per evitare prelevamenti da parte di truffatori. In particolare, il sedicente operatore lo invitava ad autorizzare una richiesta di pagamento di Euro 4.940,00 (somma di poco inferiore al limite di operatività giornaliera di Euro 5.000,00), promettendogli che tale importo gli sarebbe stato riaccreditato non appena messo in sicurezza l'*account*.

Il Ricorrente riferisce di avere, in un primo momento, negato il pagamento, ma di averlo in seguito autorizzato, facendo affidamento sulla qualifica del sedicente operatore, anche in ragione della preoccupazione di subire una sottrazione di denaro.

A questo punto – secondo quanto riferito dal Ricorrente –, il sedicente operatore gli chiedeva di comunicargli le credenziali dell'*account*, con l'asserita finalità di modificarle per ragioni di sicurezza. Il Ricorrente ammette di avere quindi fornito al sedicente operatore le proprie credenziali (nome utente, *password* e numero del conto).

A tal punto, la chiamata si interrompeva e solo allora il Ricorrente si rendeva conto di essere stato truffato.

Afferma di aver richiamato il numero da cui era stato contattato senza ricevere risposta e di avere quindi contattato il numero verde dell'Intermediario, chiedendo il blocco della carta e dell'*account*.

Rappresenta altresì di avere sporto denuncia e di avere presentato formale reclamo, riscontrato negativamente dall'Intermediario.

Lamenta di essere stato vittima di una truffa con il metodo dello *spoofing* e di essere stato tratto in inganno per avere ricevuto una notifica *push* finalizzata ad autorizzare un pagamento non richiesto nel corso di una telefonata proveniente da un numero riconducibile all'Intermediario.

Chiede pertanto il rimborso dell'importo di Euro 4.940,00.

2. Nel presente procedimento, in luogo dell'Intermediario convenuto, si è costituito un IMEL che deduce di essere l'effettivo titolare del rapporto giuridico oggetto del presente procedimento.

L'IMEL rileva che il Ricorrente, titolare del conto corrente n. *133 collegato alla carta di debito n. ***734, richiede il rimborso della somma di Euro 4.940,00 relativa a un acquisto *e-commerce* effettuato il 6 agosto 2025.

Rileva che la truffa perpetrata a danno del Ricorrente appare riconducibile allo schema della manipolazione, nel quale il malcapitato dispone operazioni di pagamento a seguito di istruzioni ricevute da un terzo soggetto, asseritamente qualificatosi come operatore della sezione antifrode dell'intermediario, al fine di mettere in sicurezza i suoi risparmi. Evidenzia che, in tali casi, è il cliente stesso a disporre di propria volontà l'operazione di pagamento.

Fa presente, in ogni caso, che l'operazione contestata è stata correttamente autenticata, registrata e contabilizzata, senza che vi sia stato alcun malfunzionamento o compromissione dei sistemi.

Precisa poi che, ai fini dell'utilizzo della citata procedura di autenticazione forte, è necessario in via preventiva installare l'App dell'Intermediario sul proprio dispositivo, associare lo strumento di pagamento (carta di pagamento o conto corrente) e configurare il codice "*****ID", attraverso l'inserimento:

- (i) delle credenziali di accesso ai servizi di *internet banking* (*username* e *password*);
- (ii) dei dati dello strumento di pagamento utilizzato per effettuare i pagamenti *online* (nel caso della carta, ad es., PAN, CVV2 e data di scadenza);
- (iii) della *password* dinamica "usa e getta" (c.d. "OTP") inviata via SMS sul numero di cellulare certificato fornito dal cliente e associato allo strumento di pagamento in modo sicuro.

Osserva pertanto che l'operazione disconosciuta, tenuto conto della modalità con cui è stata autorizzata, poteva essere eseguita soltanto dal titolare dello strumento di pagamento, che è in possesso del dispositivo su cui è inviata la notifica per l'inserimento del codice di sicurezza "*****ID", ovvero da un terzo a cui potrebbero essere stati forniti (anche inconsapevolmente) i codici di sicurezza e la *password*.

Deduce che l'utenza telefonica collegata alla posizione del ricorrente non ha subito nel tempo alcuna modifica.

Osserva che il Ricorrente ha confermato di avere autorizzato personalmente l'operazione di pagamento, seppure nel contesto di una frode; di conseguenza, eccepisce l'inapplicabilità della disciplina speciale in materia di operazioni non autorizzate di cui agli art. 10 ss. del d.lgs. n. 11/2010. Evidenzia poi che il Ricorrente ha dichiarato di avere dato seguito alle indicazioni impartite da un sedicente operatore che lo ha contattato da un numero di telefono privato in alcun modo riconducibile all'Intermediario.

Precisa, in ultimo, di condurre da tempo campagne informative antifrode informando i propri clienti tramite il proprio sito *web*, trasmettendo avvisi relativi a possibili comportamenti anomali che l'intermediario non è solito tenere, svolgendo azioni di sensibilizzazione della clientela e che mette a disposizione dei clienti il servizio di SMS *alert*, che può essere attivato gratuitamente e offre la possibilità di mantenere sotto controllo i movimenti della carta.

Chiede pertanto il rigetto del ricorso.

3. In sede di repliche, il Ricorrente precisa che, mentre la prima telefonata ricevuta proveniva da un numero sconosciuto, la seconda proveniva da un numero fisso riconducibile all'Intermediario. Ribadisce dunque di essere stato vittima di *spoofing* e di aver autorizzato l'operazione disconosciuta solo perché convinto di parlare con un operatore alle dipendenze dell'Intermediario. Precisa, peraltro, di avere comunicato le credenziali dell'*account* solo dopo l'autorizzazione dell'operazione contestata. Osserva di avere bloccato la carta il giorno stesso, alle ore 16:30, dunque dopo meno di un'ora dalla frode subita, considerato che l'operazione fraudolenta avveniva alle ore 15:47 e la chiamata con il truffatore terminava alle 16:05.

Lamenta poi la mancata attivazione di un servizio di monitoraggio, rilevando la presenza di indici di frode nel caso di specie. In particolare, afferma che, dalla documentazione allegata dall'Intermediario alle controdeduzioni, emergerebbero due tentativi, non andati a buon fine, di eseguire pagamenti su siti di scommesse e con beneficiari ad alto rischio, che avrebbero dovuto allertare il sistema bloccando l'operatività del conto.

Insiste quindi per l'accoglimento del ricorso.

4. Nelle controrepliche, l'IMEL si riporta a quanto già eccepito in sede di controdeduzioni e insiste per il rigetto del ricorso.

DIRITTO

1. Preliminarmente, si rileva che il presente procedimento, attinente alla richiesta di rimborso di quanto indebitamente sottratto a seguito dell'esecuzione di un'operazione disconosciuta, è stato instaurato nei confronti dell'Intermediario, ma nella presente sede si è costituito l'IMEL emittente la carta prepagata su cui sono state addebitate le operazioni contestate e che ha dichiarato di essere l'effettivo titolare del rapporto giuridico oggetto del presente procedimento.

Al riguardo, il Collegio osserva che, in effetti, l'operazione disconosciuta risulta effettuata con addebito su una carta emessa dall'IMEL il quale, nel costituirsi nel presente procedimento, ha inoltre versato in atti le schermate relative all'operatività fraudolenta, difendendosi, dunque, anche nel merito della domanda avanzata dal ricorrente.

In casi simili, l'orientamento prevalente dei Collegi territoriali, pur riconoscendo la distinta soggettività giuridica dei due intermediari, è nel senso di evidenziare la "cointeressenza" di questi ultimi nella gestione del rapporto con il cliente, anche in considerazione delle modalità di presentazione dei reclami aventi ad oggetto disconoscimenti di operazioni di pagamento (cfr., tra le molte, Collegio di Bari, decisioni nn. 4008/2024 e 9480/2023; Collegio di Napoli, decisione n. 12911/2022).

2. Venendo al merito della controversia, il Collegio rileva che l'operazione contestata è stata eseguita sotto il vigore 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).

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)". Secondo il Collegio di Coordinamento, "[l]a ratio di tale scelta legislativa è fin troppo notoriamente quella [...] di allocare sul fornitore dei servizi di pagamento il rischio d'impresa, essendo quest'ultimo in grado di parcellizzare, distribuendolo sulla moltitudine dei clienti, il rischio dell'impiego fraudolento di carte di credito o di strumenti di pagamento" (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, ex 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. L'IMEL ritiene che l'operazione sia stata disposta e autorizzata personalmente e volontariamente dal Ricorrente, seppure a seguito di raggiri, contestando pertanto l'applicabilità della sopra illustrata disciplina speciale in materia di operazioni non autorizzate.

Ad avviso del Collegio, l'eccezione sollevata dall'IMEL non è fondata. Secondo la più recente posizione condivisa dai Collegi territoriali, infatti, un'operazione di pagamento deve considerarsi autorizzata e quindi non soggetta al regime di responsabilità sopra descritto quando è eseguita per intero dal pagatore (con inserimento della disposizione di pagamento e di tutti i fattori di autenticazione). Per contro, 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 disciplina sopra illustrata, 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 oggetto del presente procedimento, il Ricorrente ha dichiarato espressamente di non avere personalmente disposto l'operazione contestata, ma ha confermato di avere ricevuto durante la chiamata con il truffatore una notifica *push* per autorizzare un pagamento e di avere fornito al sedicente operatore le credenziali di accesso al suo *account* solo dopo l'autorizzazione dell'operazione. Da tali elementi, il Collegio può ricavare che il Ricorrente ha effettivamente ricevuto e validato sul proprio dispositivo la notifica *push* autorizzativa dell'operazione contestata, ma – sulla base della documentazione in atti e delle allegazioni del Ricorrente – è verosimile ritenere che l'inserimento e la predisposizione dell'ordine di pagamento siano stati eseguiti dai frodatori.

Ne deriva che, ad avviso del Collegio, trova applicazione al caso oggetto del presente procedimento la speciale disciplina sopra illustrata in tema di operazioni non autorizzate, non essendo stata l'operazione eseguita per intero dal Ricorrente.

4. Tanto premesso, in ossequio ai principi in tema di riparto dell'onere probatorio sopra enucleati, è necessario innanzitutto verificare la conformità dell'operazione disconosciuta alle prescrizioni normative in tema di SCA.

Al riguardo, l'IMEL ha dedotto e provato:

- (i) l'avvenuto *enrollment* della carta di pagamento del Ricorrente al sistema autorizzativo di tipo dinamico funzionante mediante invio con SMS della *password* dinamica;
 - (ii) la mancata modifica del dispositivo associato (identificato dallo stesso numero di cellulare indicato dal Ricorrente in sede di denuncia) nel contesto dell'operatività contestata;
 - (iii) l'utilizzo del codice "****ID" (fattore di conoscenza) per l'autorizzazione dell'operazione contestata.
- L'IMEL afferma che *"l'operazione disconosciuta, tenuto conto della modalità con cui è stata autorizzata, poteva essere eseguita soltanto dal titolare dello strumento di pagamento, che è in possesso del device su cui è inviata la notifica in APP per l'inserimento del codice di sicurezza ****ID", o, in ultima istanza, da un terzo a cui potrebbero essere state fornite, anche inconsapevolmente nell'ambito di uno schema fraudolento di phishing tradizionale, i codici di sicurezza e la password dinamica necessari per l'abilitazione di tale procedura di autenticazione"*. Non fornisce tuttavia evidenza che detta operazione sia stata autenticata tramite il dispositivo solitamente utilizzato dal cliente (non soccorrono al riguardo le risultanze dei *log* prodotti, che non recano evidenza dell'operatività pregressa, con conseguente impossibilità di confrontare l'identificativo del dispositivo utilizzato per autorizzare l'operazione con quello del Ricorrente).

Tale parziale carenza di prova può tuttavia, ad avviso del Collegio, essere colmata sulla base delle dichiarazioni del Ricorrente (aventi natura confessoria ex art. 2730 c.c.), il quale ha espressamente confermato di avere ricevuto *"una richiesta di pagamento di € 4940"* che *"inizialmente [avrebbe] negato"* e, in seguito, *"con la presunzione di star realmente parlando con un operatore [dell'Intermediario]"*, personalmente autorizzato (anche nella denuncia, il Ricorrente ha dichiarato che, *"CONSAPEVOLE CHE QUEL NUMERO FOSSE DELLA MIA FILIALE ..., AUTORIZZAVO UN PAGAMENTO DI CIRCA 4.940,00 EURO"*).

In ragione della compresenza di tali elementi, il Collegio ritiene pertanto raggiunta la prova della corretta autenticazione dell'operazione contestata tramite SCA.

5. 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 del 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 del Ricorrente appare connotata da grave negligenza. Dalla cronologia delle chiamate depositata in atti dal Ricorrente (e contrariamente a quanto dallo stesso dichiarato) risulta, infatti, che lo stesso ha ricevuto:

- alle ore 15:33, una chiamata (della durata massima di due minuti) da un numero salvato in rubrica con il nome dell'Intermediario e che sembra riconducibile a un ufficio dell'Intermediario vicino alla residenza del Ricorrente;
- alle 15:35, una seconda chiamata dal numero privato 350***, che il Ricorrente afferma essere terminata alle 16.05 (orario questo compatibile con la successiva chiamata effettuata dal Ricorrente alle ore 16.13).

Alla luce di quanto precede, tenuto conto che l'operazione contestata è stata inserita alle 15:45:25 e autorizzata alle 15:47:48, sulla base della documentazione in atti, risulta che il Ricorrente, su indicazione di un soggetto qualificatosi come dipendente dell'Intermediario, ha (per sua stessa ammissione) autorizzato personalmente un'operazione di pagamento espressamente qualificata nella notifica *push* quale "*Pagamento E-COMMERCE*" (e sebbene il sedicente operatore avesse giustificato la necessità di eseguire operazione quale misura di sicurezza per evitare prelievi non autorizzati), nella consapevolezza che la chiamata proveniva da un numero di cellulare non riconducibile all'Intermediario (350***).

Ad avviso del Collegio, pertanto, la perdita subita dal ricorrente è da imputare integralmente alla sua condotta negligente.

6. In sede di repliche, il Ricorrente ha lamentato la mancata attivazione, da parte dell'intermediario, di un servizio di monitoraggio della presenza di indici di frode. Secondo il Ricorrente, in particolare, i due tentativi, precedenti all'operazione contestata e non andati a buon fine, di eseguire pagamenti su siti di scommesse e con beneficiari ad alto rischio, che risultano dalla documentazione depositata dall'Intermediario con le controdeduzioni, avrebbero dovuto allertare il sistema bloccando l'operatività del conto.

Questo Collegio è solito dare rilievo alla disciplina dettata dall'art. 8 d.m. n. 112/2007 [che identifica i casi di frode da segnalare 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], al fine di valutare se, sulla base delle evidenze disponibili, emerga in concreto un apporto causale dell'Intermediario alla produzione del danno e al compimento della frode (così Collegio di Bari, decisione n. 9279/2024; Collegio di Bologna, decisione n. 9454/2024).

Detta disciplina, pur non avendo un valore precettivo diretto sulla materia delle operazioni non autorizzate, sulla base dell'orientamento condiviso dai Collegi, può fornire all'Intermediario 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.

Ad avviso dei Collegi, una volta accertata la colpa grave del cliente, può individuarsi una concorrente responsabilità del PSP qualora sussista uno dei seguenti indici di frode:

- 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;
- 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;
- 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.

Le operazioni che il Ricorrente pretende di ricondurre a detti indici di frode sono due richieste di pagamento non andate a buon fine: la prima, alle ore 15:32, di Euro 402,80; la seconda, alle ore 15:42, di Euro 4.940,00.

Nel caso, non ricorrono le ipotesi *sub (i)* e *sub (iii)*. La seconda delle due operazioni di cui sopra e quella andata a buon fine sono state fatte presso il medesimo punto vendita, ma trattandosi di due sole operazioni è da escludersi pure la rilevanza dell'ipotesi *sub (ii)*.

L'eccezione del Ricorrente, ad avviso del Collegio, non è pertanto fondata.

7. La mancata dimostrazione dell'esistenza di un servizio di SMS *alert ex post* da parte dell'IMEL (che si limita a riferirne l'attivazione di *default*) appare, ad avviso del Collegio, irrilevante perché, sulla base di quanto dichiarato dal Ricorrente, è presumibile che lo stesso abbia effettivamente ricevuto le notifiche relative alle due operazioni non andate a buon fine.

È lo stesso Ricorrente, infatti, a dare conto che:

- (i) nel corso della prima delle due telefonate ricevute (dalla schermata allegata dal Ricorrente risultano due chiamate in entrata dal numero 096***78, la seconda delle quali inizia alle 15.33), "*l'operatore [lo] invita[va] a rifiutare*" "*una richiesta di pagamento ... tramite notifica push sull'app*" (si tratta, presumibilmente, della prima delle due operazioni non andate a buon fine: ore 15:32:45);
- (ii) nel corso della seconda delle due telefonate ricevute (iniziata alle 15.35), "*inizialmente h[a] negato il pagamento*" "*di €4940 per impedire qualsiasi altro prelievo in giornata poiché potevano essere spesi massimo €5000 al giorno*" (si tratta, presumibilmente, della seconda delle due operazioni non andate a buon fine: ore 15:41:22). Successivamente, "*con la presunzione di star realmente parlando con un operatore [dell'Intermediario ed essendosi] fidato, ... autoriz[ava] il pagamento estorto con l'inganno*" (si tratta dell'operazione contestata, autorizzata dal Ricorrente alle 15.47:48).

In ogni caso, l'eventuale assenza di un sistema di *alert ex post* sarebbe irrilevante anche perché:

- (i) 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 del cliente;
- (ii) l'invio al cliente di notifiche "parlanti", che descrivono chiaramente la propria finalità, "*rende ininfluyente la circostanza che non sia state fornite indicazioni circa l'operatività di un sistema Sms-Alert ex post*" (cfr. Collegio di Bari, decisioni nn. 189/2025 e 9015/2024). Nel caso, l'IMEL ha provato di avere inviato al Ricorrente una notifica *push* autorizzativa dell'operazione contestata con testo "*Pagamento E-COMMERCE*".

8. In conclusione, alla luce di quanto sopra osservato in ordine (i) alla conformità della procedura di SCA e (ii) alla sussistenza di una condotta gravemente negligente del ricorrente, il Collegio ritiene che il ricorso non sia meritevole di accoglimento.

P.Q.M.

Il Collegio non accoglie il ricorso.

IL PRESIDENTE