DR Diritto del Risparmio

LA RICERCA DELL'ANOMALIA NELLE OPERAZIONI FRAUDOLENTE

di Federico CORALLO*

This paper examines the role of anomaly indicators in identifying potentially fraudulent banking transactions and in assessing the conduct and liability of payment service providers. Starting from the current regulatory framework, with particular reference to Ministerial Decree No. 112/2007 and to the European provisions governing strong customer authentication and transaction monitoring, the study highlights the shortcomings arising from the lack of updated and uniformly applicable criteria across different payment instruments and channels. Particular attention is devoted to the debate surrounding the function of transaction monitoring, considered from the dual perspective of preventive detection of suspicious transactions and ex post analysis of fraudulent events. Within this framework, the paper reviews the different, and at times conflicting, judicial approaches—particularly those developed by the Italian Banking and Financial Ombudsman (Arbitro Bancario Finanziario)—regarding the existence and scope of a duty to monitor transactions and to intervene preventively when anomalous patterns emerge. The analysis shows that, although Ministerial Decree No. 112/2007 continues to serve as an important evidentiary benchmark in assessing the technical diligence of financial intermediaries, it was adopted in a technological and fraud-risk environment substantially different from the present one. The paper therefore advocates a renewal of the regulatory framework through the introduction of new and updated risk criteria capable of taking into account the individual customer's transactional profile, technological developments, and the evolution of contemporary fraud schemes. The proposed approach aims to promote transparent, graduated, and uniform parameters, subject to periodic updating, in order to strike an appropriate balance between effective fraud prevention and the need to preserve the freedom and efficiency of payment transactions.

Settembre
fascicolo 3/2026

ISSN 2785-3004

*Addetto reclami e contenzioso stragiudiziale presso primario Gruppo Bancario. La presente opera viene redatta a titolo puramente personale e passionale, non riguarda e/o fa riferimento a casi trattati in ambito professionale.

Rivista di Diritto del Risparmio – Fascicolo n. 3/2026
ISSN 2785-3004

Rivista di Diritto del Risparmio

La ricerca dell'anomalia nelle operazioni fraudolente[*]

di Federico CORALLO[**]

Settembre
fascicolo 3/2026

[*] Contributo approvato dai *referee*.

[**] Addetto reclami e contenzioso stragiudiziale presso primario Gruppo Bancario. La presente opera viene redatta a titolo puramente personale e passionale, non riguarda e/o fa riferimento a casi trattati in ambito professionale.

Abstract

This paper examines the role of anomaly indicators in identifying potentially fraudulent banking transactions and in assessing the conduct and liability of payment service providers. Starting from the current regulatory framework, with particular reference to Ministerial Decree No. 112/2007 and to the European provisions governing strong customer authentication and transaction monitoring, the study highlights the shortcomings arising from the lack of updated and uniformly applicable criteria across different payment instruments and channels. Particular attention is devoted to the debate surrounding the function of transaction monitoring, considered from the dual perspective of preventive detection of suspicious transactions and ex post analysis of fraudulent events. Within this framework, the paper reviews the different, and at times conflicting, judicial approaches—particularly those developed by the Italian Banking and Financial Ombudsman (Arbitro Bancario Finanziario)—regarding the existence and scope of a duty to monitor transactions and to intervene preventively when anomalous patterns emerge. The analysis shows that, although Ministerial Decree No. 112/2007 continues to serve as an important evidentiary benchmark in assessing the technical diligence of financial intermediaries, it was adopted in a technological and fraud-risk environment substantially different from the present one. The paper therefore advocates a renewal of the regulatory framework through the introduction of new and updated risk criteria capable of taking into account the individual customer's transactional profile, technological developments, and the evolution of contemporary fraud schemes. The proposed approach aims to promote transparent, graduated, and uniform parameters, subject to periodic updating, in order to strike an appropriate balance between effective fraud prevention and the need to preserve the freedom and efficiency of payment transactions.

****

Il contributo analizza il ruolo degli indici di anomalia nella qualificazione delle operazioni bancarie come potenzialmente fraudolente e nella conseguente valutazione della condotta degli intermediari. Muovendo dall'attuale quadro normativo e, in particolare, dal D.M. n. 112/2007, nonché dalle disposizioni europee in materia di autenticazione forte e monitoraggio delle operazioni di pagamento, lo studio evidenzia le criticità derivanti dall'assenza di criteri normativi aggiornati e uniformemente applicabili ai diversi strumenti e canali di pagamento. Particolare attenzione è dedicata al dibattito relativo alla funzione del monitoraggio, analizzato nella duplice prospettiva dell'individuazione preventiva delle operazioni sospette e dell'analisi ex post delle dinamiche fraudolente. In tale contesto, vengono esaminati i differenti e talvolta contraddittori orientamenti giurisprudenziali, soprattutto in sede di Arbitro Bancario Finanziario, circa l'esistenza e l'estensione di un obbligo di monitoraggio e di intervento preventivo in presenza di operazioni anomale. Il lavoro evidenzia come il D.M. n. 112/2007, pur continuando a rappresentare un importante parametro indiziario nella valutazione della diligenza tecnica dell'intermediario, sia stato elaborato in un contesto tecnologico di fraud scenario profondamente diverso da quello attuale. Si propone pertanto un rinnovamento del quadro normativo attraverso l'introduzione di nuovi e più aggiornati criteri di rischio, capaci di considerare le caratteristiche dell'operatività del singolo cliente, le innovazioni tecnologiche e l'evoluzione delle moderne tecniche di frode. L'obiettivo è favorire l'adozione di parametri trasparenti, graduati e uniformi, periodicamente aggiornati, idonei a conciliare l'esigenza di prevenzione delle frodi con la libertà e la celerità dell'esecuzione dei pagamenti.

La ricerca dell'anomalia nelle operazioni fraudolente

A cura di Federico CORALLO.

SOMMARIO: 1. Premessa. Un fattore umano. – 2. L'attuale suolo normativo. – 3. Gli indici di frode secondo il D.M. 112/2007. – 4. Orientamenti giurisprudenziali sull'obbligo di monitoraggio. – 5. Un funerale per rinascere.

1. Premessa. Un fattore umano.

Chi scrive inizialmente aveva l'idea di un *incipit* ad effetto, giusto per accattivarsi l'attenzione del lettore virtuale dinanzi ad un titolo apparentemente noioso e – sempre *apparentemente* – dedicato principalmente agli addetti di settore.

Nulla di tutto ciò.

La necessità di riportare le considerazioni che si andranno leggendo – condivisibili o meno – nasce da un'assenza normativa che si ripercuote nelle aule di giudizio e, prima ancora, nelle politiche degli intermediari e dei relativi uffici.

Il problema che si cercherà di affrontare è un tema andato alla ribalta negli ultimi anni soprattutto in sede di giudizio davanti all'Arbitro Bancario Finanziario (ABF) e riguarda l'eventuale sussistenza degli indici di anomalia durante l'esecuzione di operazioni bancarie fraudolente.

La questione è interessante già dal punto di vista della sua diffusione. L'applicazione degli indici di anomalia, infatti, concerne sia eventi di frode in materia di operazioni "*non autorizzate*", tecnicamente inserite e/o autorizzate da soggetti terzi diversi dal titolare del rapporto coinvolto, nonché eventi di truffa, operazioni ove quindi sia l'inserimento che l'autorizzazione sono stati gestiti interamente dal titolare del rapporto, ma il consenso è stato carpito con l'inganno.

Inoltre, l'applicazione degli indici non fa distinzione tra operazioni eseguite da remoto (*home banking*), all'ATM, al POS oppure allo sportello. Pertanto, è valevole per tutti i canali di pagamento.

Come anticipato, lo scritto si propone di affrontare un vuoto normativo poiché una vera e propria scala moderna di indici a cui fare riferimento non esiste. Spesso, infatti, si fa accenno – in maniera quasi desolante – ad un testo normativo che ha quasi ormai compiuto vent'anni

e concepito secondo gli schemi fraudolenti dell'epoca. Un'epoca in cui gli *smartphone* non erano ancora un elemento imprescindibile nel quotidiano e l'autenticazione forte neanche lontanamente immaginata dal legislatore europeo.

Anni in cui chi scrive era alla fine del proprio ciclo scolastico e non aveva la minima idea del lavoro che avrebbe intrapreso. E che quindi, un po' controvoglia e un po' per diletto, si ritrova ad affrontare un tema diventato contraddittorio negli orientamenti giurisprudenziali.

Contraddizione emotiva che ha un fondo di tristezza poiché gli indici di anomalia riguardano frodi e le frodi attaccano i risparmi delle persone. Pertanto, e purtroppo, più di qualcuno ci ha rimesso e queste sono le storie che non emergono, ma si percepiscono (o debbono essere percepite).

Proprio su tale aspetto vorrei catturare una prima attenzione e che non è riportata nei vari *report* e/o statistiche di settore bancario. Parlo dei cosiddetti traumi *post* frode che la vittima spesso è costretta ad affrontare.

Un approfondito e recente studio di aprile 2026 - *Mental health and psychosocial sequelae of fraud victimization: a systematic review*[1] - analizza i principali sintomi che possono comparire a seguito di una frode finanziaria. Tra i più comuni, senza pretesa di esaustività, vi sono: ansia; vergogna; isolamento sociale; perdita di fiducia; tensioni nelle relazioni; disturbi del sonno e difficoltà di concentrazione; depressione; "*suicide risk*" (non serve tradurre).

Aspetti che spesso all'interno di un fascicolo, a sua volta dentro una mole di pratiche da gestire, si disperdono in quella che è l'ormai obbligata velocità di un processo decisionale.

Ed è questa impronta di umanità che si intende recuperare, tramite un essenziale bisogno di regole certe e criteri applicabili in maniera uniforme da parte di tutti gli attori, onde evitare incertezze da parte di chi giudica ed illusioni per chi spera in un facile recupero delle somme tramite vie legali.

L'articolo è dunque un vero e proprio articolo '*triste*'.

Ma è un po' come quando chiesero a Luigi Tenco perché scrivesse solo canzoni tristi. E la risposta fu: "*Perché quando sono felice, esco*".

[1] Bai J, Ho M-H, Sung H-T, Hung C-S and Tsai J-H (2026) Mental health and psychosocial sequelae of fraud victimization: a systematic review. Front. Psychol. 17:1805536. doi: 10.3389/fpsyg.2026.1805536

2. L'attuale suolo normativo.

Prima di passare alle logiche giurisprudenziali, è necessario un breve inquadramento delle norme chiave.

Una trattazione a parte verrà riservata al D.M. 112/2007, spesso utilizzato quale *deus ex machina* a tutela del consumatore, una volta vinte dall'intermediario coinvolto l'eventuale prova dell'autenticazione forte (*strong customer authentication* – "SCA") e della colpa grave a carico dell'utente, secondo quanto disposto dall'art. 10 D.lgs. 11/2010[2].

Ed è proprio da quest'ultimo decreto – identificabile quale normativa italiana che recepisce la c.d. PSD2 (*Payment Services Directive* – Direttiva EU 2015/2366) che incomincerei la ricerca delle anomalie nelle operazioni bancarie oggetto di frode.

Il paragrafo 1 dell'art. 10, infatti, prevede testualmente che "*Qualora 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*".

In realtà, questo primo cenno presuppone una prova negativa da parte dell'intermediario, ossia l'assenza di anomalie puramente "*tecniche*" (es., *bug*) e che può essere soddisfatta tramite la produzione di tracciature (c.d., *log* informatici) a dimostrazione dell'intervenuta applicazione della SCA nelle operazioni contestate dal cliente.

Venendo a contenuti più di merito, l'art. 2 ("*Obblighi generali di autenticazione*") del Regolamento Delegato (UE) 2018/389 del 27/11/2017 stabilisce i requisiti tecnici della SCA a supporto ed integrazione della PSD2.

Sebbene il regolamento non parli espressamente di anomalie, tuttavia impone dei criteri volti ad analizzarle onde instaurare un controllo costante. In particolare, è previsto che:

"*1. I prestatori di servizi di pagamento dispongono di meccanismi di monitoraggio delle operazioni che consentono loro di rilevare le operazioni di pagamento non autorizzate o fraudolente ai fini dell'attuazione delle misure di sicurezza di cui all'articolo 1, lettere a) e b)*[3].

[2] Così come modificato dal D.lgs. 15/12/2017, n. 218 (in G.U. 13/01/2018, n.10).

[3] Che, rispettivamente, impongono la SCA nelle operazioni ovvero la sua esenzione a condizioni specifiche disciplinate all'interno della medesima normativa.

Detti meccanismi si basano sull'analisi delle operazioni di pagamento, tenendo conto di elementi che sono tipici dell'utente dei servizi di pagamento in condizioni di normale utilizzo delle credenziali di sicurezza personalizzate.

2. I prestatori di servizi di pagamento provvedono affinché i meccanismi di monitoraggio delle operazioni tengano conto, come minimo, dei seguenti fattori di rischio:

a) gli elenchi degli elementi di autenticazione compromessi o rubati;

b) l'importo di ciascuna operazione di pagamento;

c) gli scenari di frode noti nella prestazione dei servizi di pagamento;

d) i segnali di presenza di malware in qualsiasi delle sessioni della procedura di autenticazione;

e) se il dispositivo o il software di accesso sono forniti dal prestatore di servizi di pagamento, un registro dell'utilizzo del dispositivo o del software di accesso forniti all'utente del servizio di pagamento e l'utilizzo anomalo degli stessi".

Cercando di riassumere il dettato, una prima lettura altamente testuale, siccome il riferimento concerne gli "*elementi che sono tipici dell'utente*", impone che la Banca sia tenuta ad adattare il monitoraggio alle caratteristiche proprie del singolo cliente, la cui operatività può essere sporadica, di modesta entità ovvero frequente e/o con importi significativi.

Ma un'altra interpretazione, ad avviso di chi scrive più corretta nella sua *ratio*, vede un'interpretazione '*impersonale*' dell'utente dei servizi di pagamenti, ossia rivolta ad una massa indistinta di clienti. Ciò perché il periodo successivo descrive criteri altrettanto generici e non commisurati alla singola esperienza del cliente.

Tuttavia, è anche corretto affermare che i criteri di cui alle lett. b), d) ed e) necessariamente devono adeguarsi in qualche modo al comportamento abituale del cliente, poiché: l'importo registrato può risultare manifestamente anomalo per quel tipo di cliente; la rilevazione di un *malware* durante una sessione è per forza rimandata all'analisi di "*quella*" sessione propria del singolo cliente; infine, la lettera e) instaura una sorta di registro che tenga conto di quanto e come viene usato il *token* (fisico) consegnato al cliente ovvero l'app mobile (*token app*) installata sul dispositivo smartphone associato all'utenza di *home banking*.

Anche qui, alcuni elementi contraddittori che però ben si amalgamano nell'impasto legislativo.

Frase che può far storcere il naso a prima vista, tuttavia, già poco dopo l'entrata in vigore del regolamento tecnico, l'EBA (*European Banking Authority*) si è trovata costretta a chiarire

l'applicazione dell'art. 2 a fronte della domanda posta da un istituto di credito e riguardante l'eventuale sussistenza di un obbligo di monitoraggio delle transazioni in tempo reale.

Sul punto, l'EBA, con la Q&A 2018_4090[4] ha espressamente escluso a carico dell'intermediario bancario l'obbligo di un monitoraggio in tempo reale delle transazioni fraudolente. Infatti, come specificato, il rischio di frode nei pagamenti deve essere affrontato applicando la SCA del cliente, supportata dal monitoraggio delle transazioni. Il monitoraggio, tuttavia, "*non deve necessariamente essere in tempo reale, poiché la SCA offre già una solida protezione*".

In conclusione, il meccanismo di monitoraggio generale previsto dall'art. 2 non richiede l'attivazione del "*monitoraggio del rischio in tempo reale*" e viene solitamente effettuato "*dopo*" l'esecuzione della transazione di pagamento.

Per chi ha un debole per gli anni '80 (vissuti o meno), a parer di chi scrive, le conclusioni dell'EBA sono una sorta di *masterpiece* che però vedono anche una "*camminata con la grazia di un elefante*"[5], in quanto un monitoraggio *ex post* – cioè, a frode subita – non è sicuramente il miglior conforto per il cliente.

Un monitoraggio, infatti, dovrebbe essere tale che, a fronte dell'analisi (*ex post*) dei criteri sopra citati, si arrivi a sistemi di blocco (*ex ante*) periodicamente aggiornati in base ai nuovi schemi di frode.

In altre parole, così come avviene in campo scientifico, nel momento in cui si presenta una malattia fino a quel momento sconosciuta, a fronte dell'analisi dei pazienti coinvolti, si arrivi un domani all'ottenimento di una cura, così da prevenire l'insorgere della stessa in altri soggetti.

Ma non è tutto da buttare. Infatti, come riportato anche nella stessa Q&A, il regolamento tecnico prevede in talune casistiche un monitoraggio *real time* delle transazioni.

Tale prospettiva è presente nell'art. 18 ("*Analisi dei rischi connessi alle operazioni*"), il quale autorizza i prestatori di servizi di pagamento a non applicare la SCA qualora l'operazione disposta dal cliente a distanza presenti un basso rischio secondo i meccanismi di monitoraggio di cui al citato art. 2, nonché di quelli di cui al par. 2 lett. c). Quest'ultima espressione stabilisce per l'appunto che le operazioni di pagamento elettronico sono considerate come aventi un basso livello di rischio se sono soddisfatte tutte le seguenti condizioni:

[4] 2018_4090 Does transaction monitoring need to be real time? | European Banking Authority.
[5] *Masterpiece* - Gazebo, singolo di debutto (1982).

"*(…)*
c) i prestatori di servizi di pagamento non hanno rilevato uno dei seguenti elementi a seguito di un'analisi dei rischi eseguita in tempo reale:
i) uno schema di spesa o di comportamento anomalo del pagatore;
ii) informazioni insolite sull'utilizzo del dispositivo o del software del pagatore a fini di accesso;
iii) la presenza di malware in una qualsiasi delle sessioni della procedura di autenticazione;
iv) uno scenario di frode noto nella prestazione di servizi di pagamento;
v) localizzazione anomala del pagatore;
vi) localizzazione ad alto rischio del beneficiario".

Criteri che indubbiamente aumentato la "*personalizzazione*" del monitoraggio che deve adeguarsi all'esperienza di spesa del singolo cliente. Concetto che, infatti, è accentuato nel paragrafo immediatamente successivo poiché:

"*3. I prestatori di servizi di pagamento che intendono esentare le operazioni di pagamento elettronico a distanza dall'autenticazione forte del cliente a motivo del fatto che presentano un basso rischio tengono conto almeno dei seguenti fattori di rischio:*
a) i precedenti schemi di spesa del singolo utente di servizi di pagamento;
b) la cronologia delle operazioni di pagamento di ciascun utente dei servizi di pagamento del prestatore di servizi di pagamento;
c) la localizzazione del pagatore e del beneficiario al momento dell'operazione di pagamento nei casi in cui il dispositivo o il software di accesso è fornito dal prestatore di servizi di pagamento;
d) il rilevamento di schemi di pagamento anormali dell'utente dei servizi di pagamento rispetto alla sua cronologia delle operazioni di pagamento".
Come si vedrà anche nel prosieguo, per quanto sia ravvisabile un coraggioso intento di proteggere il cliente "*nell'immediato*" durante le operazioni a basso rischio (che, di fatto, concernono operazioni di modesta entità), il problema è stabilire quando e come un'operazione o una serie di operazioni sono da ritenersi "*anormali*".
O meglio. Guardando la questione da un'altra angolazione, chi e come stabilisce la normalità dell'operazione per quel tipo di cliente?
Il rischio è una deriva puramente arbitraria rimessa a qualche insindacabile giudizio, poiché, così come capita nella vita quotidiana, la normalità esiste finché decidiamo di crederci.

3. Gli indici di frode secondo il D.M. 112/2007.

Passiamo ora all'analisi del D.M. 30/04/2007 n. 112, quale Regolamento di attuazione della legge 17/08/2005, n. 166, recante «*Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento*», in vigore dal 14/08/2007.

È bene premettere come la materia dei pagamenti, sia a livello unionale che nazionale, nel 2007 fosse in una fase di assoluta transizione. Infatti, i rischi di frode che si andranno esaminando, sono stati pubblicati prima ancora che la Comunità Europea si dotasse della prima direttiva unitaria in materia di pagamenti (PSD1[6]), in un'epoca ove, senza ombra di dubbio, il volume transazioni a mezzo carte era inferiore rispetto ai parametri attuali, così come lo erano le frodi e le relative tecniche attuative meno sofisticate.

Per i meno giovani come lo scrivente, basti pensare come allora, per alcune transazioni a mezzo POS, in alternativa alla digitazione del codice PIN fosse sufficiente l'apposizione della propria firma sulla ricevuta di pagamento[7].

Ad ogni modo, il cuore del D.M., concepito per limitare il fenomeno delle frodi in modalità "*card present*", ancora oggi, è rappresentato dall'art. 8 rubricato "*Rischio di frode*" e dispone che questo si configura ogni qualvolta venga raggiunto uno dei seguenti parametri:

a) con riferimento ai punti vendita (esercizi commerciali[8]):

1. cinque o più richieste di autorizzazione con carte diverse, rifiutate nelle 24 ore, presso un medesimo punto vendita;
2. tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita;
3. richiesta di autorizzazione, approvata o rifiutata, che superi del 150% l'importo medio delle operazioni effettuate con carte di pagamento, nei tre mesi precedenti, presso il medesimo punto vendita;

b) riguardo alle carte di pagamento[9]:

[6] Datata 13/11/2007, entrata in vigore il 25/12/2007 e, infine, recepita in Italia solamente con il D.lgs. 11/2010, entrato in vigore il 01/10/2010.

[7] Firma che, teoricamente, doveva essere controllata dall'esercente coinvolto.

[8] Quindi, per quanto riguarda le operazioni a mezzo carta su POS fisico.

[9] In questo caso, la portata è più estesa, siccome scompare il riferimento esclusivo dei punti vendita di cui alla lettera precedente. Pertanto, visto anche il riferimento agli ATM all'interno dell'art. 6 del medesimo decreto, tali parametri sono stati concepiti indifferentemente sia per le operazioni a mezzo POS che di prelievo presso sportelli ATM.

1. sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento;

2. una ovvero più richieste di autorizzazione che nelle 24 ore esauriscano l'importo totale del plafond della carta di pagamento;

3. due o più richieste di autorizzazione provenienti da Stati diversi, effettuate, con la stessa carta, nell'arco di 60 minuti.

Dei sei parametri sopra riportati, è possibile affermare come i più utilizzati in giurisprudenza – anche per l'estensione ad altre forme di pagamento – sono sostanzialmente la metà, ossia il criterio di cui alla lett. a), n. 2 e quelli di cui alla lett. b), nn. 1-2.

Infine, prima di vagliare i diversi orientamenti giurisprudenziali che si sono susseguiti nel tempo, si precisa come il D.M., al ricorrere di almeno uno dei citati parametri, l'intermediario aveva un mero onere di segnalazione all'UCAMP (Ufficio Centrale Antifrode Mezzi di Pagamento) facente parte del MEF, la cui struttura, a seguito delle novità normative *medio tempore* intervenute, è stata riorganizzata all'interno del Dipartimento del Tesoro.

4. Orientamenti giurisprudenziali sull'obbligo di monitoraggio.

Di seguito si illustreranno i principali orientamenti emersi in contenzioso, in particolar modo in sede di giudizio dinanzi all'Arbitro Bancario Finanziario (ABF) ove si concentra la maggior parte dei ricorsi aventi per oggetto il tema delle frodi.

La portata del fenomeno ha però assunto posizioni spesso diverse e contradditorie all'interno dei Collegi territoriali, stante l'assenza di un vero e proprio obbligo normativo di controllo preventivo delle operazioni e, soprattutto, l'assenza di parametri ben delineati a cui fare riferimento.

Un primo orientamento restrittivo, assunto dal Collegio di Milano con decisione del 13/01/2025 n. 323, riconosce a carico dell'intermediario un dovere di protezione *ex ante*, stabilendo che gli indici di frode di cui all'art. 8 del D.M. n. 112/2007 possono costituire un parametro di valutazione del comportamento dell'intermediario bancario anche con riguardo ad operazioni effettuate con altri strumenti di pagamento, quali bonifici, ricariche online o presso ATM, in funzione dell'unicità della *ratio* sottesa a tale normativa. Proprio per tale motivo, i principi in parola non hanno un valore precettivo diretto in materia di disconoscimento di operazioni non autorizzate, bensì sono espressione di un generale

obbligo di monitoraggio delle transazioni, da valorizzare per valutare la condotta dell'intermediario.

Il Collegio può quindi valorizzare anche indici di frode ulteriori a quelli del D.M. 112/2007 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. In presenza di taluni di questi elementi, e segue una responsabilità concorrente dell'intermediario in relazione agli obblighi di protezione gravanti sull'intermediario ai sensi dell'art. 1375 c.c., che impongono l'adozione di misure idonee a monitorare l'utilizzo degli strumenti di pagamento dei clienti e a prevenire truffe a danno di questi ultimi. In particolare, il Collegio ritiene che rientri tra i doveri dell'intermediario l'adozione di adeguati presidi automatici di sicurezza, che "*consentano il blocco delle operazioni non in linea con una normale operatività*". Al riguardo, i Collegi sono unanimi nel ritenere che la ripartizione della responsabilità con il prestatore dei servizi di pagamento debba 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.

Negligenza tecnica che, però, nasce a monte da una valutazione di merito da parte dell'intermediario, il quale, nell'alimentazione del proprio algoritmo di sicurezza, ha valutato se rendere o meno quel tipo di parametro sospetto in base ad un punteggio di rischio.

Di segno contrario, però, all'interno della medesima sezione lombarda, una decisione di poco successiva, adottata in data 09/07/2025 ove è stata invece sancita l'impossibilità di un intervento preventivo da parte dell'intermediario. Infatti, "*il fatto che dette operazioni nel loro complesso non rientrassero nella normale operatività sia per importi che per destinatari non è di per sé significativo sia perché non si può escludere che vi siano occasioni in cui un cliente debba effettuare operazioni diverse dalle sue abitudini in relazione a esigenze specifiche (cosa, peraltro, riscontrata nella specie, come emerge dall'estratto conto del mese di giugno 2024 prodotto dall'intermediario) né che debba bonificare per la prima volta soggetti a cui favore non ha mai effettuato in precedenza operazioni di pagamento sia, infine, perché non è dato comprendere quali siano gli elementi che possano determinare il momento e il contesto in cui l'intermediario avrebbe dovuto bloccare l'operatività del conto, se si considera che ogni bonifico aveva un*

destinatario ed un importo diverso. In conclusione, non ritiene il Collegio che l'obbligo di protezione che grava sull'intermediario si debba estendere sino al punto di procedere ex ante *a blocchi automatici al superamento di un certo numero di operazioni o di determinati ammontari in assenza di precisi indici di frode*".

Tipo di pensiero che era già stato ricalcato un mese prima da parte del Collegio di Torino, con la decisione n. 5576 dell'11/06/2025. In merito, si è stabilito che allo stato non è rinvenibile un obbligo di monitoraggio delle operazioni in capo all'intermediario, il quale non può evitare che i propri clienti dispongano liberamente delle somme di cui hanno la disponibilità sul presupposto – indimostrato ed indimostrabile – che ogni operazione anomala sarebbe di per sé truffaldina (cfr. Collegio di Torino, decisione n. 1787/2025). L'ipotesi di un obbligo in capo al PSP di intervenire ogniqualvolta il proprio utente pagatore disponga uno o più bonifici di importo anomale "*non è supportata da adeguata base giuridica*" e, a normativa vigente, confligge con l'obiettivo di garantire certezza e celerità dei pagamenti, anche nell'interesse dei consumatori stessi, e con il delicato bilanciamento normativo di riparto delle reciproche responsabilità, secondo le rispettive sfere di influenza (Tribunale di Milano, sentenza n. 1596/2023)[10].

Pertanto, anche in questo caso, la sezione territoriale ha – giustamente, tra le righe – invocato la necessità di un appiglio giuridico onde poter effettuare una valutazione in merito alla sussistenza o meno di indici di anomalia.

Ad ogni modo, precursore di questo indirizzo, è stato sicuramente il Tribunale di Ancona, con la sentenza n. 338 del 16/02/2024 che, nell'aderire a quanto già sostenuto dal Tribunale di Milano nelle sentenze nn. 4995/2022 e 1596/2022, ha statuito che "*L'obbligo di monitoraggio e sospensione dei pagamenti in caso di anomalia degli stessi non è sancito esplicitamente né dall'art. 8 d.lgs. 11/2010 né dall'art. 70 dir. 2366/2015 UE di cui il predetto articolo 8 costituisce attuazione. Se il legislatore europeo avesse voluto introdurre un obbligo di monitoraggio preordinato a un obbligo di sospensione dell'esecuzione del contratto, lo avrebbe inevitabilmente sancito, avendo predisposto una dettagliata disciplina di riparto di responsabilità ed obblighi. E invece, laddove ha previsto un obbligo di monitoraggio, non l'ha mai correlato a un dovere di intervento preventivo, evidentemente per evitare prevedibili, frequenti e*

[10] Vd. Anche Collegio di Torino, decisione n. 2684 del 13/03/2025.

potenzialmente pregiudizievoli intoppi al mercato dei servizi di pagamento. In difetto di parametri di riferimento, non può nemmeno invocarsi il principio di buona fede integrativa. I prestatori di servizi di pagamento gestiscono cospicui traffici di pagamento; imporre ai medesimi di intervenire ogni qualvolta un'operazione superi, per importo o frequenza, uno schema di comportamento storico comporterebbe una discrezionalità difficilmente compatibile con la ratio del sistema normativo".

Quello a cui si fa cenno, infatti, è che un blocco preventivo delle operazioni apparentemente anomale sfocerebbe inevitabilmente in un aumento considerevoli dei casi "*falsi positivi*", ossia di casi genuini, ma bloccati perché valutati come sospetti dall'algoritmo antifrode, in attesa di una loro giustificazione da parte dell'ordinante. Logicamente, una simile mole, paralizzerebbe il circuito dei pagamenti con relativi danni collaterali.

Venendo a casi più recenti, però, il Collegio di Milano, con decisione n. 4700 del 26/05/2026, ha nuovamente ritenuto astrattamente applicabili gli indici di anomalia, tuttavia non rinvenibili nella fattispecie riguardante un caso di truffa con bonifico eseguito allo sportello ("*Non risulta la sussistenza di indici di anomalia e/o di rischio frode, che avrebbe invero potuto riscontrarsi in presenza di più operazioni ex D.M. 112/2007*").

Nella medesima seduta, ancora, ne ha ammesso l'astratta applicazione anche in presenza di operazioni *e-commerce* a mezzo carta (Collegio di Milano, decisione n. 4690/2026).

Pertanto, sembrerebbe ormai assodata l'estensione degli indici *ex* D.M. 112/2007 a tutti i mezzi e canali di pagamento[11].

Meritevole di lettura è sicuramente la decisione n. 4584 del 21/05/2026 sempre del medesimo Collegio. Infatti, "*secondo l'orientamento costante dei Collegi, le previsioni del D.M. n. 112/2007 non hanno valore precettivo diretto in materia di responsabilità civile, ma costituiscono un parametro indiziario per valutare la diligenza dell'intermediario. I Collegi possono altresì valorizzare indici di frode ulteriori a quelli del D.M. n. 112/2007 in presenza di operatività anomala rispetto alle movimentazioni storiche del ricorrente, con riguardo al numero, alla tipologia, all'importo, al tempo di esecuzione e alla riconducibilità delle operazioni al medesimo beneficiario. Dalle evidenze in atti risultano effettuate dieci operazioni di bonifico nell'arco di circa tre giorni, per un importo complessivo di € 20.898,00. Si tratta di un numero e di un importo significativi, peraltro concentrati in un ristretto arco temporale. Tuttavia, non si dispone di estratti conto del cliente che consentano di valutare se l'operatività contestata fosse in linea o meno con la sua normale operatività bancaria: tale mancanza documentale impedisce di stabilire se*

[11] Vd., anche Collegio di Milano, decisioni nn. 4590 e 4592 del 21/05/2026.

le operazioni presentassero caratteri di oggettiva anomalia rispetto al profilo storico del rapporto, parametro necessario per identificare indici di frode concreti a carico del prestatore".

In altre parole, il Collegio è anche disponibile all'applicazione degli indici di cui al D.M. nonché valutarne ulteriori non codificati, tuttavia, è essenziale che tali "*anomalie*" risultino dalle evidenze prodotte, banalmente tramite la produzione di estratti conto pregressi a dimostrazione di un'operatività storica completamente diversa da parte del cliente.

La necessità di uno '*sguardo al passato*', era già presente nella decisione n. 4172 dell'08/05/2026, secondo cui "*I Collegi possono altresì valorizzare indici di frode ulteriori rispetto a quelli del D.M. 112/2007, in presenza di un'operatività anomala rispetto alle movimentazioni storiche del ricorrente (cfr. Collegio di Milano, decisione n. 12409/2023). Una volta accertata la colpa grave del cliente, in presenza di tali indici di frode, la ripartizione della responsabilità con il prestatore dei servizi di pagamento 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 sulla negligenza tecnica dell'intermediario. La base di calcolo per la liquidazione della somma oggetto di eventuale condanna è costituita dall'intero ammontare degli importi disconosciuti, senza esclusioni, procedendo a una distribuzione in concreto del concorso di colpa tra le parti*".

Analizzando altri Collegi territoriali, *in primis*, quello emiliano, è da scorgere un'applicazione più fedele proprio degli indici *ex* D.M. 112/2007. Infatti, con la decisione n. 3859 del 04/05/2026, in un caso riguardante quattro operazioni di bonifico, nelle 24 ore, a favore di uno stesso beneficiario, intervallate da diverse operazioni di giroconto, ha ritenuto sussistere l'indicatore di cui alla lett. a, punto n. 2 (tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita), dal che deve trarsi la conclusione che l'intermediario abbia colposamente omesso di attivarsi per impedire il rischio di frode normativamente tipizzato, nonostante la negligenza grave già individuata a carico del cliente. Nella fattispecie, ne è scaturita una responsabilità a carico dell'intermediario nella misura del 60% del *petitum*.

Sempre nella medesima seduta, lo stesso Collegio, in un caso avente ad oggetto tredici operazioni in tredici minuti, di cui solo cinque prelievi presso ATM andati a buon fine, ha ritenuto equo stabilire una ripartizione di responsabilità nella misura del 50% tra le parti (Collegio di Bologna, decisione n. 3853/2026)[12].

[12] Vd., anche Collegio di Bologna, decisione n. 2654 del 23/03/2026.

Di più difficile interpretazione, invece, la decisione n. 3527 del 22/04/2026 da parte del Collegio di Bari. Infatti, è stato chiarito che "*i Collegi hanno ritenuto possibile valorizzare anche ulteriori indici di frode, diversi da quelli previsti dal D.M. 112/2007, quando l'operatività risulti anomala rispetto alle movimentazioni storiche del ricorrente (ad esempio quanto a numero, tipologia, importo, tempistica di esecuzione e riconducibilità delle operazioni al medesimo beneficiario), purché tali anomalie emergano con sufficiente evidenza. Nel caso in esame, il ricorrente individua l'anomalia dell'operazione nella* "causale generica e anomala" *e, nelle repliche, segnala ulteriori profili, quali la natura di bonifico istantaneo e la novità del beneficiario. Si osserva, tuttavia, che il Collegio di Bari, con decisione n. 9567/25, ha escluso l'esistenza di* "un «dovere generale di monitorare la regolarità delle operazioni ordinate dal cliente» *in mancanza delle ipotesi di rischio di frode tipizzate dall'art. 8 del D.M. n. 112/2007 (così anche ABF Torino, nn. 10071/24 e 794/25)*".

Sembrerebbe, infatti, ammessa una sola e stretta applicazione degli indici di cui al decreto e, per quanto riguarda gli altri criteri non oggetto di espressa previsione normativa, solamente una loro valutazione qualora sia inevitabile, ossia nel momento in cui l'anomalia sia *ictu oculi*.

Degno di menzione è anche l'orientamento del Collegio di Napoli che, con decisione n. 3375 del 16/04/2026, ha precisato che "*nella specie sussistono gli indici di frode identificati dall'art. 8 del D.M. 112/2007 che, come noto, pur non avendo un valore precettivo diretto, rappresentano utili indicatori per identificare anomalie e scenari di raggiri anche ai sensi dell'art. 2 del Regolamento 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*", attribuendo quindi una funzione di monitoraggio *ex ante* ai principi di cui al già commentato art. 2 del regolamento tecnico.

Di tale avviso, alla fine, anche il Collegio di Torino che, nonostante le decisioni contrarie sopra citate, con la decisione n. 3061 del 09/04/2026, in un caso riguardante l'uso improprio di carta su ATM e POS, ha ritenuto valevole l'utilizzo degli indici di cui al decreto, onde individuare un concorso di colpa tra le parti[13].

L'obbligo di monitoraggio preventivo, poi, è stato riconosciuto anche dal Collegio capitale, poiché, in un ricorso avente ad oggetto il disconoscimento di ben sei bonifici, tutti istantanei, disposti nel medesimo giorno in rapida successione e caratterizzati da importi in gran parte coincidenti o prossimi, non può negarsi che una siffatta movimentazione costituisca un evidente indice di anomalia, che avrebbe dovuto insospettire e allertare i sistemi di

[13] Vd., anche Collegio di Torino, decisione n. 1792 del 18/02/2026.

monitoraggio automatizzati dell'intermediario resistente, inducendolo a porre in essere presidi di sicurezza idonei a salvaguardare la ricorrente dalle conseguenze di una frode palesatasi come estremamente probabile (Collegio di Roma, decisione n. 2486 del 18/03/2026).

Una responsabilità del 20% a carico dell'intermediario, invece, è stata riconosciuta da parte del Collegio di Palermo, con le decisioni nn. 2241 del 12/03/2026 e 617 del 23/01/2026 in casi aventi ad oggetto cinque operazioni disconosciute, a prescindere dal tipo di strumento e/o canale utilizzato[14].

Ad ogni modo, l'estensione degli indici di anomalia a tutti i tipi di pagamento non deve essere applicata in maniera cieca. Infatti, esistono alcuni tipi di pagamento, quali PagoPA e/o CBill, per i quali bisogna effettuare un diverso tipo di ragionamento. Sul punto, i Collegi hanno espresso posizioni contrastanti in merito all'utilizzabilità degli indici di frode a tali pagamenti. Da una parte, si è esclusa l'applicabilità degli indicatori di anomalia, in quanto gli indici sarebbero "*tipici di transazioni fraudolente verso esercenti privati*" (Collegio di Milano, decisione n. 2757 e 6965 del 2025 per i pagamenti CBill; decisione n. 8707/2025 per i PagoPA).

In senso opposto, si sono invece reputati applicabili gli indici anche a tale tipo di pagamenti (Collegio di Roma, decisione n. 1588/2025 per i CBill; Collegio di Bologna, decisione n. 6595/2025, nonché Collegio di Milano, decisione n. 10427/2024 per i PagoPA).

Ad ogni modo, ricordiamo come trattasi di operazioni per le quali la qualità dei beneficiari (Pubblica Amministrazione) e la tipologia delle causali (pagamenti di tributi e bollettini) comporta la mancanza dei caratteri tipici delle transazioni fraudolente verso esercenti privati, non consentendo di formulare un giudizio di responsabilità a carico dell'intermediario, il cui obbligo di monitoraggio non può spingersi ad intervenire su operazioni di tale natura[15].

Infine, un cenno merita anche il Collegio di coordinamento, sebbene sia necessario andare un po' più a ritroso nel tempo. Da quanto si evince nella decisione n. 27252 del 20/12/2018, gli elementi probatori devono essere valutati nell'ottica del rischio di frode di cui al D.M. 112/2007, evidenziando che "*un efficiente sistema di monitoraggio avrebbe potuto intercettare e valutare gli elementi stessi al fine di un eventuale blocco dell'operatività dello strumento di pagamento*".

Necessità di un controllo preventivo una volta superati gli indici già presente anche nella decisione n. 16237 del 26/07/2018. Tuttavia, è bene precisare come in entrambe le pronunce

[14] Ma cfr. anche Collegio di Palermo, decisione n. 502 del 21/01/2026 avente ad oggetto solo tre operazioni.
[15] Vd. anche Collegio di Milano, decisione n. 8707 del 01/10/2025.

si faccia riferimento ad un superamento dei massimali previsti dal *plafond* e, pertanto, sono stati correttamente valutati anche aspetti di inosservanza contrattuale tra le parti.

5. Un funerale per rinascere.

Non servono troppo giri di parole per affermare che l'attuale impianto normativo ha causato una serie di orientamenti ondivaghi in sede di contenzioso, prima riconoscendo un dovere di monitoraggio preventivo, che però talvolta è da escludersi a seconda della fattispecie.
Per quanto non specificato, il giudizio si è spesso incentrato sull'esistenza o meno di un consenso da parte del cliente, ossia se trattavasi di: operazioni non autorizzate; autorizzate, ma dietro raggiro; infine, autorizzate solo a fini di profitto (es., falsi investimenti).
Decisioni che, da un punto di vista di valutazione del comportamento del cliente, sono più che condivisibili, ma non eliminano il problema a monte, ossia dell'analisi del rischio e conseguente dovere di blocco delle operazioni ritenute sospette, alla luce anche di quanto chiarito da Autorità europee (EBA) in contraddizione con quanto poi effettivamente deciso talvolta dai Collegi.
Anche perché, al momento dell'esecuzione dell'operazione, allo stato attuale difficilmente un algoritmo può essere in grado di riconoscere se le operazioni possono essere classificate come frode (cioè, non inserite e/o autorizzate dal cliente), truffa (eseguite dal cliente dietro raggiri) o, infine, eseguite dal cliente per il perseguimento, p.e., di fini di investimento rilevatisi successivamente inesistenti.
È necessario, quindi, che vi siano parametri *ab origine* adattabili ad ogni tipo di situazione, per quanto il *pattern* di frode successivo possa ravvisare diversi gradi di colpa a carico del cliente.
Infine, ulteriore elemento a destare incertezza nel panorama dei pagamenti, è dato dal fatto che, vista l'assenza di chiari criteri normativi, ogni intermediario applica gli indici in base alle proprie esperienze. Pertanto, un tipo o una serie di operazioni possono essere ritenuti sospette presso l'intermediario A, ma non, invece, presso l'intermediario B.
Pertanto – e da qui il titolo apparentemente bizzarro del paragrafo finale – c'è bisogno di un funerale (*normativo*) per poter ridotarsi di nuove ed aggiornate regole antifrode, secondo quelli che sono gli attuali *trend* fraudolenti e, in particolar modo, criteri che siano uniformemente applicabili da parte di tutti gli intermediari.

La speranza è che quindi, quantomeno a livello nazionale, si giunga ad un nuovo ed unico riferimento normativo, che abroghi l'ormai D.M. 112/2007, ma ne conservi ovviamente alcuni precetti (almeno i tre criteri già visti e considerati più diffusi).
Di seguito, si tenterà di elencare una serie di parametri meritevoli di attenzione e valutabili quali fattori di rischio in presenza di una dinamica fraudolenta. Fattori che, ovviamente, non sono attualmente oggetto di recepimenti normativi, ma suggeriti dallo scrivente a mero titolo di speranza ("*Fuori le foglie morte giacciono sul prato. Prima che morissero, avevano alberi a cui appendere le loro speranze*"[16]).

Senza pretesa di esaustività, pertanto, si elencano una serie di elementi tecnici che possono essere valutati quali fattori di rischio durante l'esecuzione di un'operazione fraudolenta:

1. natura istantanea del pagamento;
2. primo utilizzo del metodo istantaneo;
3. importo anomalo, secondo diversi archi temporali, in quanto l'abitudine di spesa può aumentare o diminuire significativamente anche per scelte personali del singolo cliente;
4. nuovo beneficiario;
5. indirizzo IP mai registrato;
6. rete internet mai utilizzata;
7. geolocalizzazione anomala;
8. anomalie di sessione (es., rilevazione *malware* o di applicativi di controllo da remoto);
9. rilevazione telefonata durante la sessione;
10. utilizzo canale insolito (es., PC per un cliente che usa sempre solo app);
11. nuovo device, da valutare comunque nell'intervallo che decorre dall'ultimo *enrollment*;
12. età commerciale del dispositivo oggetto di nuovo *enrollment*[17];
13. cambio credenziali;
14. aumento massimali;

[16] *The Funeral* – Band of Horses (2007).
[17] Solitamente, un nuovo *enrollment* genuino da parte dell'utente presuppone l'associazione di un modello tecnologicamente più avanzato rispetto al precedente. Tuttavia, nei casi di *account takeover* da parte dei frodatori, si è soliti imbattersi nell'associazione di modelli commercialmente "più vecchi" rispetto a quelli dei clienti. Ad ogni modo, sarebbe più corretto che l'algoritmo di sicurezza valutasse il sistema operativo del nuovo modello associato, se più recente rispetto a quello precedentemente registrato.

15. orario insolito rispetto alle abitudini cliente secondo gli archi temporali di cui al punto 3;
16. pagamenti a ridosso del *weekend* ovvero di festività[18];
17. *login* tentati o ripetuti anche su diversi canali contemporaneamente;
18. bonifici tentati, falliti o ripetuti;
19. sequenza temporale ristretta tra le operazioni;
20. indisponibilità tecnica controllo VOP (*Verification of payee*).

All'interno di ogni voce, poi, andrebbe inserita una scala di valori tale da rendere più incisivo quel parametro.

Esempio: se la natura istantanea del pagamento è da considerarsi abituale, poco frequente, rara oppure primo utilizzo; se l'operatività in uscita aumenta lievemente oppure vede un cambio radicale del comportamento e quindi molto superiore allo storico; se la rete internet è abituale, poco utilizzata o di prima registrazione, così come l'indirizzo IP; se l'orario di esecuzione è lievemente insolito oppure completamente fuori dalle abitudini; se il cliente abitualmente effettua operazioni durante una telefonata oppure è la prima rilevazione; etc.

Tutti parametri, insomma, che a loro volta sono suscettibili di diversi gradi di rischio.

Tra i fattori di mitigazione del rischio, invece, oltre i casi diametralmente opposti a quelli sopra citati, bisognerebbe tenere conto degli accrediti straordinari (es. tredicesime o donazioni), per cui è mediamente lecito aspettarsi, in quel determinato periodo temporale, un maggiore volume di operazioni e/o di importi.

Diversamente, una serie eccessiva di accrediti potrebbe però mascherare un'attività altrettanto fraudolenta, poiché il cliente coinvolto, anche inconsciamente, potrebbe essere utilizzato quale "*money mule*", ossia quale mero transito di somme già oggetto di frode.

Tirando le somme, ad ogni parametro andrebbe quindi assegnato un punteggio di rischio, secondo una scala predefinita e in base alle diverse gradazioni che possono registrarsi all'interno della singola voce. Il punteggio ottenuto andrebbe poi mitigato con i fattori opposti, ossia quelli che tendono ad eliminare il sospetto in quanto coerenti per quel tipo di operatività.

[18] Studiati appositamente dai malfattori onde cercare di ritardare le segnalazioni di frode dei clienti alle proprie banche e/o autorità.

Infine, il punteggio ottenuto andrebbe studiato secondo diversi archi temporali predefiniti, siccome, come detto, le abitudini di spesa possono anche cambiare radicalmente nel corso del rapporto. Si pensi ad un improvviso cambio di lavoro e aumento di stipendio, tale da consentire al cliente maggiori volumi in uscita, logicamente non in linea con il pregresso recente, ma del tutto lecito.

Scala di fattori che, in conclusione, dovrebbe essere periodicamente aggiornata secondo i nuovi *trend* di frode ravvisati nei report condivisi tra gli intermediari e diffusi dalle Autorità di settore.