BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria per l'Italia

UNITÀ DI INFORMAZIONE FINANZIARIA PER L'ITALIA

COMUNICAZIONE DELL'8 GIUGNO 2026

OPERATIVITÀ CONNESSA CON TRUFFE, FRODI AGEVOLATE DALLA TECNOLOGIA, *MONEY MULING* E ALTRI REATI INFORMATICI

1. Le attività svolte dalla UIF nell'ambito dell'analisi finanziaria delle segnalazioni di operazioni sospette, dei rapporti di collaborazione con autorità nazionali ed estere nonché dei controlli evidenziano, in linea con i *trend* registrati a livello internazionale[1], una crescita significativa di episodi di truffe, frodi informatiche e altri illeciti collegati, favoriti dalla crescente digitalizzazione di servizi e operazioni.

I casi osservati si basano sull'impiego di canali sia tradizionali sia innovativi; talvolta presuppongono la collaborazione delle stesse vittime, in genere soggetti vulnerabili e inconsapevoli, poco avvezzi all'uso delle nuove tecnologie, ma talora anche in possesso di adeguate competenze digitali e finanziarie.

Negli ultimi anni il numero di segnalazioni di operazioni sospette (SOS) riferibili a tali fenomeni è cresciuto in modo particolarmente rilevante; un incremento significativo ha riguardato anche le richieste di collaborazione che la UIF riceve dall'Autorità giudiziaria e dagli Organi investigativi delegati, con l'obiettivo di agevolare l'identificazione degli autori delle condotte illecite e, laddove possibile, forme di *asset recovery* soprattutto all'estero, attraverso la cooperazione delle omologhe *Financial Intelligence Unit* (FIU); queste ultime possono costituire un canale prioritario per assicurare interventi tempestivi, in particolare prima dell'attivazione delle procedure di assistenza giudiziaria[2].

I fenomeni in argomento si inseriscono in un contesto di profonda trasformazione tecnologica che interessa, con ritmo crescente, i servizi bancari, finanziari e i sistemi di pagamento. La digitalizzazione e l'innovazione stanno favorendo l'emergere di nuovi operatori, in particolare nel settore *Fintech*, e di modelli di *business* che frequentemente prescindono dal contatto diretto con la clientela. Ne derivano indubbi benefici in termini di efficienza, modernità e inclusione finanziaria; nel contempo, crescono la portata e la complessità dei rischi di frode, anche tramite schemi di ingegneria sociale sempre più complessi, che consentono alla criminalità, spesso organizzata, di operare in Italia e oltre i confini nazionali, sfruttando piattaforme digitali, sistemi di pagamento istantaneo, *Virtual Iban*[3] e cripto-attività.

---

[1] Da ultimo, cfr. in argomento il documento pubblicato dal Gruppo d'Azione Finanziaria Internazionale nel febbraio 2026 sul tema Cyber-Enabled Fraud. Il valore delle perdite finanziarie è stato stimato nel 2025 in oltre 400 miliardi di dollari a livello mondiale (cfr. Fonte Interpol). In Italia, la Polizia Postale e per la sicurezza cibernetica ha rilevato nello stesso anno volumi superiori a 269 milioni di euro (cfr. Rapporto annuale per il 2025).

[2] Dal 2021 al 2025, la UIF ha ricondotto più di 80.000 SOS a schemi o fenomenologie fraudolente, con una crescita marcata di anno in anno: le segnalazioni in argomento sono passate da poco più di 9.000 nel 2021 a più di 30.000 nel 2025, con un *trend* che si sta manifestando ulteriormente crescente anche per il 2026. Per quanto riguarda le collaborazioni della UIF con l'Autorità giudiziaria e gli Organi investigativi delegati su fenomenologie analoghe, nel 2025 si è registrata una crescita del numero di richieste di tracciamento e recupero di proventi illeciti all'estero per oltre il 50 per cento; anche le richieste inerenti alle medesime fattispecie rivolte alla UIF dalle FIU estere hanno mostrato un andamento analogo.

[3] Si tratta di "un identificativo che fa sì che i pagamenti siano reindirizzati verso un conto di pagamento identificato da un IBAN diverso da tale identificativo" (cfr. art. 2, par. 1, n. 26), del regolamento (UE) 2024/1624). Il v-IBAN è cioè un codice IBAN associato a un conto di pagamento principale (dotato di IBAN tradizionale, c.d. *master account*) e

Il ricorso a queste ultime è sempre più frequente: le vittime di frodi sono spesso allettate da presunti rendimenti elevati; i criminali le utilizzano per ostacolare l'identificazione dell'origine illecita delle proprie disponibilità. Sebbene molte cripto-attività possano essere tracciate grazie ai registri distribuiti, l'utilizzo di *wallet* non ospitati[4] e di sistemi caratterizzati da elevati livelli di anonimizzazione (come VASP *no KYC, mixer, bridge*, ecc.) rendono arduo il tracciamento dei flussi e l'individuazione dei responsabili delle condotte illecite. Analoghi ostacoli si incontrano nel caso di utilizzo di *Virtual Iban*, in particolare se risultano emessi da intermediari autorizzati in paesi dell'Unione europea in favore di prestatori di servizi di pagamento, specie se insediati in giurisdizioni non pienamente cooperative.

La UIF ha osservato articolati schemi fraudolenti a danno sia di persone fisiche (*romance scam, job scam, investment scam*) sia di istituzioni, enti e intermediari bancari e finanziari (campagne *ransomware* e frodi economico-finanziarie), spesso accompagnati dal ricorso al *money muling;* l'Unità ha inoltre riscontrato altre ipotesi di reato, commesse o agevolate dall'utilizzo di strumenti informatici, con un impatto particolarmente rilevante sotto il profilo sociale (sfruttamento dei minori, atti estorsivi o persecutori quali *cyberstalking* e *sextortion*). Sono emersi impieghi a fini illeciti dell'intelligenza artificiale (IA)[5] generativa, la crescente diffusione di contenuti artificiali realistici (c.d. *deepfake*), l'apertura e l'utilizzo di rapporti intestati a identità fittizie, sintetiche[6] o a soggetti reali inconsapevoli.

L'analisi delle SOS, le interlocuzioni con i soggetti obbligati (*infra* anche "destinatari") ai sensi del d.lgs. 231/2007 (c.d. decreto antiriciclaggio) e le collaborazioni con l'Autorità giudiziaria e gli Organi investigativi mettono in luce anche il ricorso a forme di pagamento istantaneo per vanificare le possibilità di intercettare le anomalie e, talvolta, la concentrazione di queste ultime nelle prime fasi di sviluppo commerciale dell'attività o dell'offerta di prodotti e servizi. Riflessi positivi sono derivati dalla definizione di limiti quantitativi o da richieste di autorizzazione preventiva all'esecuzione di operazioni concordati dal soggetto obbligato con il cliente in relazione al suo profilo, specie quando questi detiene rapporti con capienza elevata.

Risulta altresì migliorata la capacità segnaletica dei soggetti obbligati nei casi di collaborazione tra i presìdi antifrode e antiriciclaggio, in particolare per l'attitudine dei primi a prevenire perdite finanziarie immediate e a intercettare tempestivamente anomalie operative e tentativi di impersonificazione; è emerso che tali elementi, utilmente valutati anche a fini antiriciclaggio secondo una prospettiva integrata, consentono di ricostruire schemi ampi e strutturati nonché di cogliere la dimensione spesso transnazionale dei fenomeni.

L'Unità ritiene pertanto necessario richiamare l'importanza delle attività di prevenzione[7] e della collaborazione attiva antiriciclaggio, in linea con le istruzioni emanate dalla UIF il 18 dicembre 2025 e con le indicazioni contenute nella presente comunicazione.

---

generato per offrire alla clientela un servizio finalizzato alla gestione dei flussi finanziari; in argomento si vedano le Indicazioni per i soggetti obbligati sull'applicazione degli obblighi in materia antiriciclaggio nell'apertura e gestione di conti di pagamento dotati di IBAN virtuali pubblicate dalla Banca d'Italia e dalla UIF in data 12 dicembre 2024.

[4] Si tratta di *wallet* attivati in autonomia dagli utenti senza ricorrere ai servizi dei soggetti autorizzati. L'articolo 3, punto 20), del regolamento (UE) 2023/1113 definisce in particolare l'indirizzo auto-ospitato come l'indirizzo nel registro distribuito non collegato a nessuno dei soggetti seguenti: a) un prestatore di servizi per le cripto-attività; b) un soggetto non stabilito nell'Unione che presta servizi analoghi a quelli di un prestatore di servizi per le cripto-attività.

[5] Cfr. regolamento (UE) 2024/1689.

[6] Le identità fittizie sono create deliberatamente con dati inventati o alterati; quelle sintetiche combinando dati reali con altri inventati o alterati.

[7] Si richiamano in argomento le iniziative del Gruppo d'Azione Finanziaria Internazionale e, in particolare, l'aggiornamento della Raccomandazione 16, volto a migliorare la trasparenza dei pagamenti transfrontalieri al fine di rafforzare la capacità di individuare reati finanziari, e la recente *Ministerial Declaration* del 17 aprile 2026. Si veda altresì il rapporto della nuova Autorità antiriciclaggio europea che, nel c.d. AMLA Roadshow 2025 pubblicato l'11 maggio 2026, ha rilevato come il confine tra frodi informatiche e riciclaggio sia sempre più labile e ha evidenziato la necessità -

Al fine di agevolare la rilevazione e l'individuazione dei sospetti, già nel 2010 l'Unità ha pubblicato uno schema di comportamento anomalo in materia di frodi informatiche; più di recente, con il Provvedimento del 12 maggio 2023 sono stati elaborati indicatori e sub-indici riguardanti profili soggettivi e oggettivi ricorrenti anche in ipotesi di truffe, frodi agevolate dalla tecnologia e altri illeciti collegati.

Con la presente comunicazione si forniscono elementi di attenzione aggiornati, che i soggetti obbligati considerano alla luce dell'attività svolta e di quanto in ragione di quest'ultima può essere in concreto osservato, per individuare anomalie inerenti ai profili soggettivi[8] e oggettivi e valutare tempestivamente la ricorrenza di sospetti da segnalare alla UIF.

Si mettono, inoltre, a disposizione dei destinatari specifici fenomeni da valorizzare nelle segnalazioni di operazioni sospette, al fine di indirizzare al meglio le analisi finanziarie dell'Unità e le conseguenti attività dei competenti Organi investigativi.

2. Rispetto alle fattispecie osservate, la UIF richiama in particolare l'attenzione sulle fenomenologie di seguito descritte:

2.1 Truffe e frodi agevolate dalla tecnologia[9]

Dal punto di vista soggettivo, assumono rilievo fattori quali il rifiuto o la riluttanza a fornire le informazioni o i dati ordinariamente richiesti, la non veridicità o incoerenza dei medesimi nonché l'illogicità di taluni comportamenti[10].

Elementi di anomalia possono riguardare situazioni non giustificate di frequente variazione o di coincidenza fra diversi soggetti di dati quali gli indirizzi di residenza/domicilio e di posta elettronica, numeri di cellulare, identificativi dei dispositivi (smartphone e personal computer) e indirizzi di connessione alla rete (IP) rilevati rispetto ai clienti stessi.

La presenza di denunce presentate dalla clientela e la ricorrenza di soggetti già menzionati in segnalazioni di operazioni sospette o coinvolti in richieste di informazioni da parte dell'Autorità giudiziaria, specialmente nell'ambito di ipotesi di truffe o frodi informatiche, può supportare le valutazioni – comunque necessarie – delle anomalie riscontrate.

Ricorre spesso l'utilizzo distorto di strumenti tecnologici finalizzato a occultare l'identità reale dei relativi utilizzatori, a simulare l'utilizzo di dispositivi diversi da quelli effettivi mediante sistemi di

---

da parte del settore finanziario - di adottare un approccio intersettoriale (esteso ai sistemi di telecomunicazione/*social network*) e integrato tra le funzioni antifrode e antiriciclaggio.

[8] Rilevano tra l'altro in argomento gli Orientamenti dell'EBA sull'utilizzo di soluzioni di *onboarding* a distanza del cliente attuati con Nota della Banca d'Italia n. 32 del 13 giugno 2023.

[9] Tra le ipotesi ricorrenti possono essere annoverate le seguenti: *phishing* basato sull'acquisizione di dati identificativi o delle credenziali di accesso a servizi online; *job scam* o "truffa dei *like"* basate su false offerte di lavoro con richieste di pagamento; *impersonation scam*, in cui il truffatore si presenta come persona o ente affidabile per indurre a trasferire fondi o cripto-attività; *business e-mail compromise* (BEC), attraverso e-mail inviate in genere a imprese e società da soggetti che si presentano falsamente in uno specifico ruolo aziendale e che recano ordini e istruzioni per l'esecuzione di pagamenti a favore di conti dei truffatori; *romance scam*, in cui si realizzano raggiri a sfondo sentimentale che simulano rapporti affettivi per ottenere denaro o dati personali; *purchase scam* riguardanti beni o servizi mai consegnati; *rental scam* inerenti ad affitti inesistenti con richieste di anticipo; *fake charity scam* in relazione a richieste di donazioni per cause inesistenti; *investment scam* concernenti truffe o frodi connesse all'offerta di investimenti – anche in cripto-attività – da parte di soggetti non autorizzati.

[10] Si vedano in particolare gli indicatori n. 1, n. 2 e n. 3 del citato Provvedimento della UIF del 12 maggio 2023.

emulazione[11] o virtualizzazione[12] o manipolare i dati acquisiti a fini antiriciclaggio. In più occasioni soggetti dediti ad attività fraudolente hanno cercato di indurre le vittime all'installazione, sui propri computer o dispositivi personali, di *software* di accesso e controllo remoto.

Più in dettaglio, occorre prestare attenzione ad anomali comportamenti o configurazioni tecniche idonee a mascherare l'origine delle connessioni o a rendere più difficoltosa la riconducibilità delle operazioni a un soggetto reale. Si fa in particolare riferimento all'utilizzo di reti private virtuali (VPN), *proxy* o altri strumenti di anonimizzazione[13] inusuali, non coerenti con il profilo del cliente e in assenza di giustificazioni.

Assumono rilievo, in primo luogo, gli accessi ai servizi offerti dal destinatario che risultano temporalmente correlati e originati da indirizzi IP condivisi da parte di una pluralità di rapporti o soggetti, l'associazione reiterata dei medesimi indirizzi IP a conti formalmente intestati a soggetti non collegati tra loro, le connessioni e gli accessi ai servizi provenienti da dispositivi localizzati in aree geografiche distanti, specialmente se concentrate in un arco temporale ristretto, o incompatibili con la localizzazione del cliente (ad esempio in relazione alla residenza, domicilio o sede legale del medesimo).

Nei limiti di quanto consentito dalla normativa a tutela della privacy, ulteriori anomalie possono riguardare le caratteristiche e la geolocalizzazione dei dispositivi utilizzati dal cliente per accedere ai servizi e per autenticarsi, rivelando ipotesi di *device* simulati o virtualizzati (cfr. *supra*), incongruenze e frequenti modifiche dei *fingerprint*[14] o di altre caratteristiche dei dispositivi (ad esempio, sistema operativo, *browser*, risoluzione, lingua, configurazioni *hardware*), la riconducibilità di molteplici operazioni o rapporti agli stessi dispositivi.

Tali elementi, considerati specialmente in combinazione tra loro, possono essere sintomatici di tentativi di apertura e utilizzo di rapporti con identità rubate, fittizie o sintetiche, funzionali alla realizzazione di schemi fraudolenti.

Ulteriori profili di anomalia riguardano le incongruenze che è possibile individuare tra il nominativo del beneficiario indicato dal mittente del trasferimento e l'effettiva intestazione del rapporto di accredito, in particolare nel caso in cui si proceda comunque all'esecuzione dell'operazione, nonché la presenza di operazioni rifiutate, stornate, disconosciute o richiamate.

La presenza di transazioni ripetute e prive di giustificazione, spesso in un ristretto arco temporale e poco dopo l'apertura del rapporto, con caratteristiche analoghe, anche per importo e controparti ricorrenti, potrebbe essere sintomatica di un collegamento tra soggetti professionalmente organizzati in reti, anche transnazionali, allo scopo di tramitare fondi di possibile origine illecita verso rapporti appositamente aperti, talvolta in paesi diversi da quelli in cui è stato commesso il reato.

Sono altresì frequenti i casi di operatività della specie concentrata in periodi festivi o a ridosso dei fine settimana.

Ricorrono utilizzi della provvista di solito poco dopo l'accredito: lo stesso giorno o nei giorni di poco successivi le disponibilità sono in genere trasferite verso altri rapporti, anche esteri, impiegate

---

[11] Software che riproducono in maniera artificiale il comportamento di un altro dispositivo o sistema, consentendo l'esecuzione di applicazioni e l'accesso a servizi come se provenissero da un dispositivo diverso da quello fisicamente utilizzato.

[12] Sono inclusi, a titolo esemplificativo, le macchine virtuali che consentono di aggirare meccanismi di controllo basati sull'unicità del dispositivo e simulare l'operatività di utenti diversi a partire dalla stessa infrastruttura tecnica.

[13] Si tratta di strumenti informatici che consentono di instradare la connessione Internet attraverso server intermediari, mascherando l'indirizzo IP reale dell'utente e rendendo meno immediatamente identificabile l'origine geografica e tecnica delle connessioni.

[14] Insieme di informazioni tecniche che, considerate nel loro complesso, permettono di distinguere un dispositivo da un altro.

su molteplici canali, ad esempio per acquisto di cripto-attività, operazioni di gioco o acquisti di beni nonché prelevate presso ATM (anche *crypto*-ATM).

2.2 *Money muling*

L'attività di *money muling* è spesso connessa a truffe e frodi agevolate dalla tecnologia ed è volta a favorire il transito e, quindi, il riciclaggio di proventi illeciti mediante il coinvolgimento di soggetti che mettono a disposizione, consapevolmente o inconsapevolmente, propri rapporti o strumenti di pagamento. Le caratteristiche sintomatiche di detta attività possono venire in evidenza anche in casi in cui difettano elementi utili a corroborare ipotesi di sospetti connessi con specifiche condotte fraudolente.

Oltre alla possibile ricorrenza di situazioni connesse con i già citati utilizzi distorti di strumenti tecnologici o di rapporti con identità oggetto di furto, fittizie o sintetiche, il *money muling* si caratterizza a titolo esemplificativo per: l'utilizzo di rapporti (ad esempio conti, carte di pagamento o *wallet*) di recente attivazione, intestati a soggetti il cui profilo denota inesperienza o vulnerabilità (ad esempio giovani, disoccupati o pensionati); l'anomala presenza di dati di contatto (ad esempio gli indirizzi e-mail) comuni a più soggetti ovvero modifiche non giustificate dei medesimi dati successive all'apertura del rapporto; la ricorrenza di circostanze anomale che il destinatario rileva in occasione dell'accesso digitale ai servizi offerti alla clientela, in particolare sotto il profilo della geolocalizzazione e secondo quanto indicato nel precedente paragrafo 3.1; la rapidità delle operazioni in accredito e in addebito, spesso frazionate, di importo contenuto e con l'estero, con soggetti diversi e tra loro privi di relazioni note; la ricorrenza di causali generiche, incongruenti con la natura dei trasferimenti o non corrispondenti ad attività economiche; richieste di *recall* difficilmente soddisfatte; irreperibilità o scarsa collaborazione dell'intestatario del rapporto.

La semplice operatività finalizzata all'azzeramento del saldo del rapporto non è da considerarsi di per sé sintomo di *money muling* e va valutata alla luce delle ulteriori anomalie richiamate in precedenza.

2.3 *Cybercrime*

Ferma restando la disciplina vigente in materia di cybersicurezza e tutela dei dati personali[15], nel contesto della presente comunicazione, con la locuzione *cybercrime* si intende fare riferimento all'insieme delle condotte illecite presupposto di riciclaggio realizzate digitalmente e agevolate mediante tecniche e strumenti informatici particolarmente sofisticati ed evoluti, al fine di compromettere la riservatezza, l'integrità o la disponibilità di dati, credenziali, risorse o sistemi informatici[16].

Rilevano in tale ambito sospetti di riciclaggio connessi con ipotesi di intrusione, compromissione o manipolazione digitale finalizzate, tra l'altro, all'acquisizione illecita di informazioni, all'appropriazione di credenziali o chiavi crittografiche nonché al controllo non autorizzato di sistemi o *account*; a titolo esemplificativo, si richiamano fenomeni quali *Advanced Persistent Threat* (APT), *malware, ransomware,* attacchi di tipo *man-in-the-middle*, *Distributed Denial of Service* (D-DOS).

Assumono rilievo le eventuali notizie disponibili su attacchi *cyber* ostili, anche sulla base di fonti di informazione pubblicamente accessibili, in particolare per ipotesi di accesso abusivo a sistema informatico.

---

15 Si richiamano senza pretesa di esaustività il d.lgs. 138/2024, il d.lgs. 196/2003 e il regolamento (UE) 2016/679.

16 Vi rientrano a titolo esemplificativo le ipotesi di accesso abusivo a sistema informatico o telematico, di danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico, di danneggiamento di sistemi informatici o telematici di pubblico interesse.

3. La collaborazione attiva in materia di truffe e frodi agevolate dalla tecnologia, *money muling* e *cybercrime* richiede particolare attenzione ai profili della qualità delle informazioni e della tempestività delle segnalazioni[17].

Occorre evitare automatismi segnaletici e SOS caratterizzate da contenuti non adeguati, da cui traspare l'assenza di adeguate valutazioni[18].

I destinatari sono chiamati a valutare con attenzione i contesti meritevoli di segnalazione alla UIF, ad adottare criteri di selettività dei dati e delle informazioni rilevanti ai fini della SOS e a evitare approcci meramente difensivi.

Ai fini della selezione dei predetti contesti, assumono rilievo la complessità e la rilevanza del caso, elementi quali l'importo e la frequenza delle operazioni, la ricorrenza o meno di collegamenti con ulteriori soggetti o transazioni, tali da far ritenere possibile l'esistenza di reti criminali ampie o di fenomeni nuovi, la presenza di denunce o di richieste di informazioni da cui possa desumersi che l'operatività sia già nota alle Autorità competenti e, in questi casi, il potenziale valore aggiunto di una segnalazione, in termini di possibile sviluppo dell'analisi rispetto all'intervento dell'Autorità giudiziaria[19].

Occorre inoltre valorizzare il flusso di ritorno della UIF quale strumento a disposizione del destinatario per orientare la propria attività segnaletica e tendere alla migliore qualità possibile delle SOS.

Per quanto concerne la tempestività, è fondamentale procedere alla segnalazione prima possibile, in particolare prima dell'esecuzione delle operazioni[20], per consentire interventi immediati a tutela delle vittime, specie nei contesti che riguardano importi elevati, e agevolare le analisi finanziarie a supporto delle indagini.

Analoga tempestività è richiesta ai destinatari in occasione delle risposte da fornire alla UIF nell'ambito degli approfondimenti finanziari.

Si richiama l'importanza della corretta e completa indicazione dei dati e delle informazioni in forma strutturata[21], in relazione sia ai soggetti sia alle operazioni rilevanti ai fini della rappresentazione del sospetto.

Nella descrizione dei sospetti i destinatari forniscono una rappresentazione chiara e completa dei flussi finanziari e dei collegamenti tra soggetti, inclusi anche eventuali elementi tecnici rilevanti[22], che possono agevolare la rilevazione e la ricostruzione di network più ampi.

Si raccomanda infine di evitare l'inserimento nella SOS di testi generici e standardizzati, ripetuti in modo uniforme in più segnalazioni. La descrizione dell'operatività sospetta e dei motivi del sospetto deve essere calibrata sugli specifici elementi del caso concreto, assicurando coerenza tra i

---

17 Cfr. in proposito le Istruzioni per la rilevazione e la segnalazione delle operazioni sospette della UIF del 18 dicembre 2025.

18 Cfr. il citato Provvedimento della UIF del 18 dicembre 2025, Parte Prima, Sezione I.

19 In ogni caso, l'eventuale esistenza di denunce all'Autorità giudiziaria non è di per sé sufficiente per l'individuazione del sospetto di cui all'art. 35 del d.lgs. 231/2007, non essendo giustificati automatismi segnaletici anche alla luce delle Istruzioni per la rilevazione e la segnalazione delle operazioni sospette della UIF del 18 dicembre 2025 (cfr. in particolare Parte Prima, Sezione IX).

20 I destinatari hanno cura di strutturare correttamente il campo dello schema segnaletico relativo allo stato di esecuzione delle operazioni.

21 Cfr. Parte terza, Sezione II, par. 2, lett. B), delle istruzioni emanate con Provvedimento dell'Unità del 18 dicembre 2025.

22 Si fa riferimento, ad esempio, agli elementi citati nella presente comunicazione quali indirizzi IP, VPN, *fingerprint, device*, geolocalizzazione.

profili effettivamente riscontrati e la rappresentazione dei medesimi, anche al fine di favorire una più efficace classificazione delle segnalazioni[23].

4. Gli elementi informativi riportati nella presente comunicazione hanno natura esemplificativa e non esaustiva. I fenomeni in esame sono altamente dinamici, mutevoli e in costante evoluzione. Tutti i destinatari degli obblighi di segnalazione alla UIF devono valutare con la massima attenzione anche ulteriori anomalie di natura soggettiva e oggettiva eventualmente individuate con riguardo a truffe, frodi agevolate dalla tecnologia e altri illeciti collegati.

Occorre in particolare svolgere un'analisi in concreto e una **valutazione complessiva e adeguata** dell'operatività rilevata con l'utilizzo di tutte le informazioni a disposizione per la tempestiva individuazione dei sospetti[24].

In presenza di attività che interessino più destinatari degli obblighi di collaborazione attiva, è importante assicurare la **piena condivisione delle informazioni**, in linea con le previsioni dell'articolo 39 del d.lgs. 231/2007, utilizzando tutti gli spazi di collaborazione consentiti da tale norma.

Per agevolare la classificazione dei contesti attinenti alle fattispecie oggetto della presente comunicazione, la UIF mette a disposizione **tre nuovi codici dei "fenomeni**", che i destinatari valorizzano nella compilazione della segnalazione, selezionando quello o quelli più coerenti con le caratteristiche dell'operatività osservata:

- **I01 – Truffe e frodi agevolate dalla tecnologia** dovrà essere utilizzato in presenza di sospetto di condotte fraudolente e di connesso riciclaggio;
- **I04 – *Money muling*** dovrà essere utilizzato in presenza di sospetto relativo al reclutamento di soggetti, più o meno consapevoli, per trasferire denaro ottenuto illegalmente, sia in assenza di elementi che rendano configurabile un'operatività riconducibile al fenomeno I01 sia in abbinamento a tale fenomeno laddove ricorrano i presupposti per l'impiego di quest'ultimo;
- **I05 – *Cybercrime*** dovrà essere utilizzato in relazione ai sospetti di reati informatici non rientranti nelle ipotesi di cui al fenomeno I01 e caratterizzati dall'alterazione o dall'abuso di sistemi informatici e strumenti digitali e, più in generale, da sofisticate tecniche di compromissione finalizzate a ottenere vantaggi economici illeciti.

A partire dalla pubblicazione della presente comunicazione non trova ulteriore applicazione lo schema rappresentativo di comportamenti anomali inerenti alle frodi informatiche, emanato con comunicazione della UIF del 5 febbraio 2010, e non sarà disponibile il codice del fenomeno I02-Frodi informatiche.

I destinatari degli obblighi di collaborazione attiva, nell'ambito della propria autonomia organizzativa e con le modalità ritenute più idonee, porteranno la presente comunicazione a conoscenza del personale e dei collaboratori incaricati della valutazione delle operazioni anomale e avranno cura di sensibilizzarli con idonee iniziative, diffondendo istruzioni volte ad assicurare un'efficace applicazione della disciplina antiriciclaggio.

La UIF continua a monitorare l'evoluzione della materia in collaborazione con le Autorità competenti e il settore privato.

---

[23] Cfr. Parte terza, Sezione II, par. 2, lett. C), delle istruzioni emanate con Provvedimento dell'Unità del 18 dicembre 2025.

[24] In proposito, i destinatari tengono anche conto delle citate istruzioni emanate con Provvedimento dell'Unità del 18 dicembre 2025.