BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria
per l'Italia

UNITÀ DI INFORMAZIONE FINANZIARIA PER L'ITALIA

PREVENZIONE DI FENOMENI DI CRIMINALITÀ FINANZIARIA CONNESSI CON L'EMERGENZA DA COVID-19

1. L'attuale situazione di emergenza sanitaria espone il sistema economico-finanziario a rilevanti rischi di comportamenti illeciti: sussiste il pericolo di truffe, di fenomeni corruttivi e di possibili manovre speculative anche a carattere internazionale; l'indebolimento economico di famiglie e imprese accresce i rischi di usura e può facilitare l'acquisizione diretta o indiretta delle aziende da parte delle organizzazioni criminali; gli interventi pubblici a sostegno della liquidità possono determinare tentativi di sviamento e appropriazione, anche mediante condotte collusive; il mutamento improvviso delle coordinate di relazione sociale aumenta l'esposizione di larghe fasce della popolazione al rischio di azioni illegali realizzate anche *on line*.

In questo contesto è necessario operare in maniera coesa perché gli interventi pubblici raggiungano gli obiettivi prefissati, sostenendo effettivamente persone e imprese in difficoltà, prevenendo possibili effetti distorsivi e preservando l'integrità dell'economia legale. Si tratta di preoccupazioni già espresse da istituzioni nazionali e internazionali[1], rispetto alle quali l'apparato di prevenzione del riciclaggio può rappresentare uno strumento efficace perché, grazie alla sua capacità di coinvolgere l'intera struttura economica del Paese, è in grado di intervenire tempestivamente sulle operazioni in corso e non solo ad ausilio della fase di repressione dei reati.

Agli intermediari, ai professionisti, agli altri operatori qualificati e alle Pubbliche amministrazioni, che sono parte attiva del sistema di prevenzione, è richiesto oggi un impegno particolare per calibrare i propri presidi antiriciclaggio nella maniera più efficace; occorre supportare adeguatamente il dispiegarsi dell'intervento di sostegno, ma anche intercettare e comunicare tempestivamente all'Unità di Informazione Finanziaria per l'Italia, ai sensi degli artt. 10 e 35 del d.lgs. 231/2007, tutte le situazioni sospette per consentire l'attivazione dei meccanismi di approfondimento e indagine.

Al fine di agevolare la collaborazione attiva si indicano di seguito alcuni aspetti su cui i soggetti obbligati sono chiamati a prestare attenzione.

2. Specifici profili comportamentali a rischio possono ricorrere nell'ambito della gestione dell'emergenza sanitaria. Si fa in particolare riferimento a possibili truffe nei settori delle forniture e dei servizi più direttamente collegati al contrasto del COVID-19.

Vengono in rilievo l'offerta e la commercializzazione di prodotti quali dispositivi di protezione individuale, igienizzanti, apparecchi elettromedicali in realtà non esistenti, contraffatti o di qualità inferiore agli standard richiesti; particolare attenzione dovrà essere dedicata all'attività svolta in tale ambito da operatori che non risultano avere precedente esperienza nel settore o in altri analoghi. Andranno considerate anche ipotesi di manovre speculative su detti prodotti che potrebbero rivelarsi

[1] Si vedano in particolare le posizioni espresse da Europol nel *report* del 27 marzo 2020 "*Pandemic profiteering: how criminals exploit the COVID-19 crisis*", dal GAFI il 1° aprile 2020, in occasione dello "*Statement by the FATF President: COVID-19 and measures to combat illicit financing*", nonché da Interpol lo scorso 6 aprile sul tema "*Preventing crime and protecting police: INTERPOL's COVID-19 global threat assessment*".

penalmente rilevanti nonché le proposte di sottoscrizione/vendita di titoli di aziende impegnate nella ricerca scientifica o nella produzione di *device* elettromedicali. A fini di prevenzione delle pratiche illecite è utile valutare tutti gli elementi a disposizione e, in particolare, la sussistenza di eventuali motivi di incompatibilità o incoerenza tra operatività osservata e profilo dei soggetti coinvolti ovvero di carenze nella documentazione o nelle informazioni fornite dal cliente.

Tenuto conto dell'urgenza connessa con la gestione dell'emergenza sanitaria non è poi trascurabile il rischio di ipotesi corruttive specie negli affidamenti per l'approvvigionamento delle forniture e dei servizi necessari all'attività di assistenza e ricerca. Al fine di mitigare questo rischio sono particolarmente importanti gli approfondimenti rafforzati richiesti nel caso di coinvolgimento di persone politicamente esposte (PEP), come anche le valutazioni connesse con la ricezione di fondi pubblici, specie se di importo rilevante e non coerente con l'attività svolta dal cliente.

Possono inoltre verificarsi meccanismi fraudolenti connessi con la raccolta di fondi, anche *on line* mediante piattaforme di *crowdfunding*, a favore di fittizie organizzazioni *non profit*; tali iniziative, apparentemente destinate alle aree colpite dall'emergenza ovvero alle attività di ricerca per il superamento della pandemia, potrebbero invece rispondere a intenti distrattivi. Occorre quindi monitorare i rapporti sui quali confluiscono dette raccolte di fondi, in relazione al profilo del cliente accertato in sede di adeguata verifica e all'utilizzo dei fondi stessi[2].

3. Il prolungato periodo di *lockdown* determina situazioni di difficoltà finanziaria rispetto alle quali è elevato il rischio di infiltrazione criminale da parte di organizzazioni che, attraverso il radicamento sul territorio, il reclutamento di affiliati presso le fasce più deboli della popolazione e l'ampia disponibilità di capitali illeciti, possono trovare nuove occasioni per svolgere attività usurarie e per rilevare o infiltrare imprese in crisi con finalità di riciclaggio. Occorre quindi prestare massima attenzione alle situazioni che possono essere sintomatiche di tali fenomeni criminali. Nelle valutazioni assumono centralità le informazioni sugli assetti proprietari e sulle operazioni aziendali e societarie (rilevano, ad esempio, gli anomali trasferimenti di partecipazioni, le garanzie rilasciate o ricevute, lo smobilizzo di beni aziendali a condizioni non di mercato), sull'origine dei fondi e sulle effettive finalità economico-finanziarie sottostanti alle transazioni[3].

È inoltre necessario che i soggetti obbligati, in particolare i professionisti, valutino l'operatività delle imprese clienti che si trovano in condizione di difficoltà finanziaria, al fine di intercettare ipotesi di abusi delle possibilità offerte dalle disposizioni dirette ad agevolarne la continuità operativa[4].

L'intervento pubblico mira ad allocare nuove risorse finanziarie dove il bisogno è effettivo[5]; il corretto adempimento degli obblighi di prevenzione – anche in materia di adeguata verifica[6] – e la valutazione di tutti gli elementi informativi disponibili sui richiedenti i finanziamenti potrà arginare il rischio che si verifichino abusi penalmente rilevanti tanto nella fase di accesso al credito garantito dalle diverse forme di intervento pubblico quanto in quella di utilizzo delle risorse disponibili.

In particolare, nella prima fase potrebbero emergere sospetti di condotte fraudolente tese a ottenere il finanziamento con garanzia pubblica in mancanza o in violazione dei presupposti stabiliti dalla normativa, mediante l'alterazione o la falsificazione della documentazione necessaria ovvero in violazione delle norme che ne disciplinano l'erogazione; in tale ambito possono venire in rilievo ipotesi di mendacio

---

2 Merita particolare attenzione anche la ricezione di fondi, in genere frazionati, che possono essere ricondotti a sospette attività fraudolente poste in essere nei confronti di soggetti inconsapevoli o particolarmente deboli, spesso anziani, ai quali vengono richiesti contributi per finte attività legate al contrasto del COVID-19 (es. di sanificazione o di somministrazione di tamponi) o per il sostegno economico di familiari lontani.

3 Si vedano in proposito la Comunicazione della UIF del 9 agosto 2011 recante schemi di comportamenti anomali riconducibili all'usura e la precedente Comunicazione del 24 settembre 2009 per la parte inerente alle imprese in crisi.

4 Si vedano gli articoli da 5 a 11 del d.l. 8 aprile 2020, n. 23.

5 In proposito si veda il citato d.l. 8 aprile 2020, n. 23.

6 Si veda, da ultimo, la Raccomandazione della Banca d'Italia del 10 aprile 2020 su tematiche afferenti alle misure di sostegno economico predisposte dal Governo.

bancario e reati di falso nonché fenomeni di truffa aggravata per il conseguimento di erogazioni pubbliche e di indebite percezioni a danno dello Stato.

Con riferimento alla fase di utilizzo delle sovvenzioni occorre prestare attenzione alla destinazione dei flussi finanziari, specie se accompagnati da un vincolo di scopo, poiché potrebbero rintracciarsi sospetti di malversazioni a danno dello Stato e attività distrattive collegate anche a reati societari e fallimentari. In tale ambito, vanno valorizzate le procedure per il controllo dei flussi finanziari verso Paesi che presentano elevati rischi di riciclaggio.

4. Infine, si richiama l'importanza del monitoraggio delle attività a distanza, in particolare *on line*[7].

Assumono rilievo gli strumenti di pagamento elettronici, il cui impiego – senz'altro positivo per assicurare la tracciabilità dei flussi finanziari – è destinato ad aumentare ulteriormente nei prossimi mesi, in conseguenza delle misure di distanziamento sociale, che hanno determinato il passaggio di molte attività di compravendita dal canale tradizionale a quello telematico.

Nell'attuale situazione emergenziale aumenta il rischio che tali strumenti possano essere impiegati per le truffe *on line*, mediante il sistema della compravendita di beni inesistenti o contraffatti, ovvero a prezzi sproporzionati. Il ricorso a detti strumenti può divenire più frequente anche in altri contesti illegali, ad esempio nello spaccio al dettaglio di sostanze stupefacenti.

Vanno perciò attentamente monitorate le transazioni *on line*, anche quelle istantanee o richieste con urgenza, attraverso le procedure di selezione automatica delle operazioni anomale di cui i soggetti obbligati si avvalgono per finalità di prevenzione, tenuto conto della tipologia di clienti e della loro attività.

Il maggior utilizzo di servizi *on line* accresce, inoltre, l'esposizione al rischio di reati informatici in danno di singoli utenti ovvero di imprese o enti. Si fa riferimento ai fenomeni di *phishing*, di cd. *Business email compromise* o *CEO frauds*[8] ovvero agli attacchi *ransomware*[9], anche collegati a richieste di riscatto in valuta virtuale. Al riguardo, assumono centralità le informazioni inerenti all'origine e alla destinazione dei fondi; eventuali anomalie relative alla modalità di costituzione della provvista e al successivo utilizzo della stessa potrebbero indurre il sospetto di attività illegali[10].

Ugualmente importante è il controllo dei flussi finanziari connessi con il gioco *on line*, i quali sono destinati ad aumentare in coincidenza della temporanea sospensione dell'attività di gioco su rete fisica.

5. Gli elementi informativi riportati nella presente Comunicazione hanno natura esemplificativa. Tutti i destinatari degli obblighi di comunicazione o segnalazione alla UIF ai sensi degli artt. 10 e 35 del d.lgs. 231/2007 devono pertanto valutare con la massima attenzione anche ulteriori comportamenti e caratteristiche delle operatività sintomatiche di rischi di infiltrazione criminale connessi con l'emergenza epidemiologica da COVID-19.

---

7 Si veda il Comunicato della UIF del 27 marzo scorso sul tema "Emergenza epidemiologica da COVID-19. Misure temporanee e avvertenze per mitigare l'impatto sui soggetti tenuti alla trasmissione di dati e informazioni nei confronti della UIF".

8 Forme di compromissione della posta elettronica aziendale per attaccare organizzazioni commerciali, governative e senza fini di lucro, ottenendo vantaggi economici specifici; in genere l'attacco si realizza con e-mail apparentemente provenienti da soggetti con uno specifico ruolo (dipendenti, esponenti dell'impresa o clienti ricorrenti) recanti istruzioni per l'esecuzione di pagamenti a favore dei truffatori. In argomento si veda *Egmont Group Bulletin*, *Business Email Compromise Fraud*, luglio 2019.

9 I *ransomware* sono virus informatici che rendono inaccessibili i dati dei computer infettati; per ripristinarli è chiesto il pagamento di un "riscatto", spesso sotto forma di *virtual asset*.

10 In argomento si vedano la Comunicazione della UIF del 5 febbraio 2010 recante schemi rappresentativi di comportamenti anomali relativi a frodi informatiche e la Comunicazione della UIF del 28 maggio 2019 sull'utilizzo anomalo di valute virtuali.

Occorre in particolare svolgere un'analisi in concreto e una valutazione complessiva dell'operatività rilevata con l'utilizzo di tutte le informazioni disponibili per la tempestiva individuazione dei sospetti. In presenza di attività che interessino più soggetti obbligati, è importante assicurare la condivisione delle informazioni, in linea con le previsioni dell'articolo 39 del d.lgs. 231/2007.

Eventuali operazioni sospette devono essere portate all'attenzione dell'UIF con la massima tempestività, al fine di consentire l'attivazione della collaborazione interna e internazionale e anche dell'eventuale esercizio del potere di sospensione previsto dall'articolo 6, comma 4, lett. c), del d.lgs. 231/2007.

Per agevolare una pronta individuazione dei contesti attinenti alle casistiche oggetto della presente comunicazione è opportuno che nei campi descrittivi della segnalazione/comunicazione sia espressamente richiamata la connessione con l'emergenza COVID-19.

I soggetti 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 e avranno cura di sensibilizzarli con idonee iniziative, diffondendo istruzioni volte ad assicurare un'efficace applicazione della disciplina antiriciclaggio.