BANCA D'ITALIA
EUROSISTEMA

UIF
Unità di Informazione Finanziaria
per l'Italia

UNITÀ DI INFORMAZIONE FINANZIARIA PER L'ITALIA

PREVENTION OF FINANCIAL CRIME PHENOMENA LINKED TO THE COVID-19 EMERGENCY

1. The current health emergency situation exposes the financial system to serious threats of illicit behaviours: frauds, corruption and speculative ploys are of particular concern, also at an international level; the economic weakening of families and enterprises increases the risks of usury and may facilitate the direct or indirect acquisition of firms by criminal organizations; public sector aids in favour of liquidity may be subject to misuse or embezzlement, also through collusive conducts; quick changes in social relationships increase the exposure of large sectors of the population to illegal actions, also carried out through the web.

In this context it is necessary to act in a coordinated manner so that public interventions be fulfilled, effectively supporting individuals and enterprises in difficulties, avoiding possible distortive effects and preserving the integrity of the legal economy. In order to address such concerns, which have already been expressed by national and international institutions[1], the comprehensive system in place for the prevention of money laundering may represent an effective tool, because it is able to act quickly, also on on-going operations, thanks to its ability to involve the entire economic structure of the Country, and not only in the crime-repression phase.

Financial intermediaries, professionals and other qualified operators as well as public administrations, which play an active role in prevention, are required today to carry out their relevant AML/CFT obligations in the most effective manner according to specific exigencies: it is necessary to facilitate the implementation of support measures, but also to detect and promptly communicate to the Unità di Informazione Finanziaria per l'Italia all suspicious behaviours in order to trigger the appropriate analysis and investigative actions, according to art. 10 and 35 of the Legislative Decree n. 231/2007.

In order to facilitate the active cooperation, some issues are indicated below to which obliged entities are requested to pay close attention.

2. Specific risky behavioural profiles may occur in the context of the health emergency management. This refers, most notably, to potential scams in the supply and services sectors most directly linked to the contrast of COVID-19.

The supply and marketing of products such as individual protective equipment, sanitizers, and electromedical devices that are either non-existent, counterfeit or below-standard are of particular concern; specific attention should be paid to the activities in this area by operators who do not appear to have had previous experience in the sector or in other comparable ones. Possible cases of speculative ploys regarding these products should also be taken into account, which might have criminal relevance, as well as public offerings of stocks of companies engaged in scientific research or the production of electromedical devices. For the purpose of preventing illegal practices, it shall be useful to assess all the

[1] See, in particular, the reports issued by Europol on March 27th, 2020 "*Pandemic profiteering: how criminals exploit the COVID-19 crisis*", FATF on April 1st, 2020, with the "*Statement by the FATF President: COVID-19 and measures to combat illicit financing*", as well as by Interpol on April, 6th 2020 on "*Preventing crime and protecting police: INTERPOL's COVID-19 global threat assessment*".

available elements and, in particular, the existence of any reasons for incompatibility or inconsistency between the observed operations and the profile of those involved or deficiencies in the documentation or information provided by the customer.

In view of the urgency associated with the management of the health emergency, the risk of corruption is not negligible, most notably in the awarding of contracts for supplies and services necessary in the activities of assistance and research. In order to mitigate this risk, particularly important are the enhanced due diligence measures required in the case of involvement of politically exposed persons (PEPs), as are the assessments associated with the receipt of public funds, especially when these are sizable and inconsistent with the client's activity.

There may also be fraudulent mechanisms associated with fundraising, including online crowdfunding platforms, in favour of fictitious non-profit organizations. Such initiatives, which appear to be intended for emergency-affected areas or research activities aimed at overcoming the pandemic, might actually be directed towards the diversion of funds. It is therefore necessary to monitor the accounts into which the raised funds flow, with regard to the customer's profile as assessed through customer due diligence and the use of said funds[2].

3. The prolonged lockdown has led to financial difficulties resulting in the risk of criminal infiltration by organizations which, thanks to their territorial penetration, the recruitment of affiliates from the weakest sections of the population and the wide availability of illicit capital, may find new opportunities to carry out usury and take over or infiltrate ailing companies for money laundering purposes. It is therefore necessary to pay close attention to situations that may be symptomatic of such criminal phenomena. Assessments should mainly focus on information relating to ownership structures and business and corporate operations (for example, the anomalous transfer of shares, guarantees issued or received, the disinvestment of company assets on non-market conditions are particularly noteworthy), the origin of funds and the actual economic and financial purposes underlying transactions[3].

It is also necessary for the obliged entities, most notably professionals, to assess the operations of client companies undergoing financial difficulties, in order to detect possible abuses of support measures introduced by provisions aiming at facilitating the continuation of their operations[4].

Public intervention aims to allocate new financial resources where the need is real[5]; the proper fulfilment of preventive measures – including in the area of customer due diligence[6] – and the assessment of all the information available on those who apply for funds may stem the risk of criminal abuses both in the phase of access to credit, guaranteed by the various forms of public intervention, as well as in the phase relating to the use of available resources.

In particular, in the first phase, there may arise suspicions of fraudulent conducts aimed at obtaining publicly guaranteed funds, lacking the requirements set out in the law or in breach thereof, by altering or falsifying the necessary documentation or in violation of the rules governing their disbursement. In this area, cases may come up of banking fraud and forgery as well as aggravated fraud for obtaining public disbursements and undue reception of funds to the detriment of the State.

With regard to the phase when grants are used, attention should be paid to the destination of financial flows, especially when they are earmarked, as there may arise suspicions of embezzlement against the State and diversion of funds possibly linked to corporate and bankruptcy crimes. In this context, procedures for controlling cash flows to high risk countries for money laundering should be

---

[2] Especially noteworthy is the reception of funds, usually through multiple payments, which can be traced back to suspected fraudulent activities against unwitting or particularly weak individuals, often elderly, who are requested contributions for fake activities related to the contrast of COVID-19 (e.g. sanitation or the administering of swabs) or for the financial support of distant family members.

[3] See in this regard UIF's Communique of 9 August 2011, containing abnormal behavioural patterns relating to usury and the previous Communique of 24 September 2009 for the part relating to ailing companies.

[4] See articles 5 to 11 of d.l. 8 April 2020, n. 23.

[5] See the aforementioned d.l. 8 April 2020, No. 23.

[6] Lastly, see the Bank of Italy's Recommendation of 10 April 2020 on measures relating to economic support measures arranged by the Government.

promoted.

4. Finally, it is necessary to focus on the relevance of monitoring remote activities, particularly *on line*[7].

Electronic payment instruments become relevant and their use – which is certainly positive to ensure the traceability of cash flows - will be more frequent in the next few months as a result of the measures of social distancing, which have led to the transition of many trading activities from the traditional channel to IT payment solutions.

In the current emergency there is a higher risk that such instruments could be used for online scams, through the system of trading non-existent or counterfeit goods, or selling at disproportionate prices. The use of such tools may also become recurrent in other illegal contexts, for example in retail drug trafficking.

Online transactions, including instantaneous or urgently requested transactions, should therefore be closely monitored through the procedures for automatic selection of anomalous transactions used by the obliged entities for prevention purposes, taking into account the type of customers and their activities.

The increased use of online services also enhances the risk of cybercrime against individual users or companies or entities. Reference is made to *phishing attacks*, *Business email compromise* or *CEO frauds*[8], or *ransomware attacks*[9], also linked to ransom demands in cryptocurrency. In this regard, information about the origin and destination of the funds have great relevance; any anomalies concerning the way the provision has been set up and the subsequent use of it could lead to suspicion of illegal activities[10].

5. The information elements in this Communique are purely illustrative. All the obliged entities pursuant to the articles 10 and 35 of d.lgs. 231/2007 must therefore carefully assess further behaviours and characteristics related to the risk of criminal infiltration associated with the epidemiological emergency from COVID-19.

In particular, it is necessary to carry out a concrete analysis and an overall assessment of the operations detected with the use of all the information available for the purpose of a timely detection of suspects. In case of activities involving multiple obliged entities, it is important to ensure information sharing, in line with the provisions of Article 39 of d.lgs. 231/2007.

Any suspicious transactions must be promptly brought to the attention of UIF, in order to enable the activation of internal and international cooperation and also the possible exercise of the postponement power provided for by Article 6, paragraph 4, lett. c), of d.lgs. 231/2007.

In order to facilitate the prompt identification of the contexts relating to the cases covered by this communique, it is worth expressly recalling the connection with the COVID – 19 in the descriptive fields of the report/communique.

The obliged entities are requested, within the framework of their own organizational autonomy and in the most appropriate manner, to bring this communique to the attention of staff and collaborators in charge of assessing operations and will take up the task to raise awareness through appropriate initiatives, by issuing instructions aimed at ensuring an effective application of the anti-money laundering discipline.

---

[7] See the UIF Communique of 27 March on the theme "Epidemiological Emergency fromCOVID-19. Temporary measures and warnings to mitigate the impact on the subjects obliged to transmit data and information to the UIF".

[8] Forms of business e-mail compromise against commercial, government and non-profit organizations, in order to obtain specific economic benefits; typically the attack is carried out through e-mails apparently sent by individuals with a specific role (employees, business managers or recurring customers) with instructions for making payments to fraudsters. See *Egmont Group Bulletin, Business Email Compromise Fraud*, July 2019.

[9] Ransomware are computer viruses that make the data of infected computers inaccessible; to restore them, the payment of a "ransom" is required, often in the form of virtual assets.

[10] In this respect, see the UIF Communique of 5 February 2010 with representative patterns of anomalous behaviour relating to cyber fraud and the UIF Communique of 28 May 2019 on the misuse of virtual currencies.