COMMITTEE OF EXPERTS ON THE EVALUATION OF ANTI-MONEY LAUNDERING MEASURES AND THE FINANCING OF TERRORISM (MONEYVAL)

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 25 January 2022

AML/CFT SUPERVISION IN TIMES OF CRISIS AND CHALLENGING EXTERNAL FACTORS

TYPOLOGIES REPORT

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The Typologies Report on AML/CFT Supervision in times of crisis and challenging external factors was adopted by the MONEYVAL Committee at its 62nd Plenary Session (Strasbourg, 15-17 December 2021).

TABLE OF CONTENTS

I. INTRODUCTION

1. One of the MONEYVAL Polish Presidency's priorities was to revive the work on typologies projects. The present report was inspired and builds up on a previous analysis carried out by the MONEYVAL Committee on "Money laundering and terrorism financing trends in MONEYVAL jurisdictions during the COVID crisis". The project was approved by the 60th Plenary with the purpose of outlining best practices available in the MONEYVAL jurisdictions as well as in the broader Global Network on the AML/CFT supervision in the times of crisis and challenging external factors.

2. Under Polish leadership, the project team was established to lead the work on the report. The project team consisted of the project leader - Marek Kaplita (Poland) and project team members - Alisa Amirbekyan (Armenia), Dita Daukste (Latvia), Nick Herquin (Guernsey), Shana Krishnan (FATF Secretariat), Alexandr Kuryanov (Russian Federation), Kadri-Liis Raun (Estonia), Matej Santej (Slovenia), Nazerke Zhampeiis (EAG Secretariat), and supported by Irina Talianu, Laura Kravale and Lorena Ungureanu from MONEYVAL Secretariat.

3. This best practice paper provides an overview of business continuity measures that supervisors may wish to consider in the context of the COVID-19 pandemic and challenging external factors. The report takes account of examples and considerations provided by supervisors in response to a questionnaire sent by the Project Team to the MONEYVAL member states and beyond and on qualitative data obtained through subsequent interviews and additional written contributions.

4. The purpose of this document is to assist the authorities and SROs in the consideration of their own possible domestic measures to be applied in crisis situations. Although most supervisors will already have well-developed business continuity plans, these may need some adjustments, given the nature of the 2020-2021 crisis and wider government responses. This document does contain key findings but does not make specific recommendations as national circumstances and considerations may vary.

5. As highlighted by the FATF and MONEYVAL in their recent thematic reports[1], the COVID-19 pandemic generated new threats and vulnerabilities to the AML/CFT system. Supervisors have faced new challenges, mainly related to the proper assessment of emerging risks and communication with the obliged entities on appropriate mitigating measures to be taken.

6. In their effective response to the COVID-19 pandemic, supervisory authorities experienced limitations, mostly due to social distancing and physical movement restrictions ("lockdowns") applied in their jurisdictions which impeded the execution of on-site visits. Supervisors faced other difficulties such as limited human resources (due to sickness or people at risk from COVID-19 which needed to particularly protected) and technical shortcomings, including access to IT support for remote working, access to data bases and access to information of the reporting entities. The primary challenge for supervisory authorities, as for most of the other entities, was the transition to generalized remote working during the lockdown and the other extraordinary measures implemented by governments in order to prevent the pandemic from spreading.

7. The main sources of information of this paper were experiences and actions of authorities taken to overcome the difficulties caused by the COVID-19 pandemic. Nevertheless, some findings, in particular the ones relating to remote supervision, are relevant in case of other challenging circumstances, such as the supervision of entities having only limited or no physical presence in a given jurisdiction.

---

[1] FATF Guidance (2021), *Risk-Based Supervision*; Moneyval Report (2020), *Money laundering and terrorism financing trends in MONEYVAL jurisdictions during the COVID crisis;* https://eurasiangroup.org/files/uploads/files/%D0%9C%D0%B5%D1%80%D1%8B_%D0%B2_%D1%81%D0%B2%D1%8F%D0%B7%D0%B8_%D1%81_COVID-19/Information_note_on_COVID-19_measures_eng_rev4.pdf

Methodology

8. The findings for this study are based on:

- A review of existing literature and open-source material on this topic to further develop the scope and the findings of this report, including identifying specific challenges encountered by supervisors and best practices to focus on.
- A questionnaire to MONEYVAL delegations and to the international community sent in January 2021 covering the risk and challenges encountered by supervisory authorities due to the COVID-19 pandemic, solutions for ensuring business continuity and crisis management measures, digitalization and other regulatory adjustments, as well as supervisory tools, sanctions, outreach and international cooperation. In total, by the end of February 2021, input from 31 countries[2] was received. In June 2021 a preliminary version of the report was prepared, and the Project Team turned to some jurisdictions for additional information.
- Interviews conducted and written additional contributions were received from two jurisdictions in August 2021. The first draft was ready and distributed to the membership in September 2021.

II. Key findings identified throughout the report

9. Business Continuity Plans (BCP) proved to be a useful tool to helping countries swiftly overcome crisis situations. Among other things, the BCPs set out (i a risk assessment methodology, (ii) detailed governance arrangements, (iii) division of responsibilities and (iv) specific actions to be undertaken in relation to the crisis in order to ensure the continuity of business operations. It was proved to be beneficial to include AML/CFT supervision in such plans.

10. Due to the physical movement limitations, and the need to make use of the virtual meetings and other forms of communication, involving IT and internal security departments in the development of business continuity strategies and plans and in their implementation appeared to be a good practice.

11. BCPs may include protocols with the reporting entities to ensure their collaboration and active participation in the crisis management arrangements and allow access to data/information and documents under special circumstances.

12. When the AML/CFT supervision is dissipated amongst several supervisors, setting a coordination committee showed positive results.

13. The COVID-19 pandemic proved that in crisis situations where employees are unable to return to the office, technology is key, both software and hardware, in order to inter alia: (i) collate information/documentation from reporting entities on ML/TF risks and (ii) to be able to continue hybrid onsite and/or offsite supervision using video conferencing tools. Moreover, such can be used in case of other challenging circumstances, such as the supervision of entities having only limited or no physical presence in a given jurisdiction.

14. There are different approaches to remote working across various jurisdictions, but the following are the most common IT control measures implemented by authorities: (i) use of

[2] Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, China, Croatia, Cyprus, Czech Republic, Estonia, Germany, Guernsey, Hungary, Isle of Man, Israel, Latvia, Liechtenstein, Lithuania, Malta, Monaco, Mongolia, Nauru, New Zealand, Poland, Romania, Russian Federation, Serbia, Slovakia, Slovenia, Ukraine.

solutions for secure VPN connections or joining the call using special platforms, (ii) limiting and controlling remote access for users to the institution's server or internal network, (iii) use of restriction settings for downloading data from a remote computer to a personal device, (iv) encryption of locally stored data, (v) record user activity during remote sessions, (vi) multi-factor authentication and (vii) regular change of passwords.

15. Supervisors sought additional sources of data to allow the monitoring of ML/TF risks at reporting entities.

16. Shifting to remote or hybrid inspections to replace traditional on-site visits was the main solution found to continue the AML/CFT supervision during the crisis. Maintaining regular communication with the employees is key.

17. Supervisory focus has also been diverted to thematic supervision to enable an assessment of the vulnerabilities of internal systems and controls across a broad range of reporting entities.

18. Supervisors developed guidelines and/or regulations to permit the use of digital ID systems by reporting entities.

19. Supervisors explored the exceptional use of simplified CDD in low-risk scenarios, for reporting entities to on-board clients and facilitate the delivery of government benefits in response to the pandemic.

20. Clear and direct communication on the ML/TF risks in challenging circumstances is an effective tool in continuing AML/CFT compliance by the private sector. Supervisors used different channel of communication for example posted video clips or e-learning materials posted on their websites. Further outreach was carried out by organizing webinars, online trainings and workshops. Information on reports and studies published by international organizations such as FATF and MONEYVAL.

21. Cross-border cooperation between supervisors in times of crisis could be enhanced by simplifying existing regulations and procedures relating to cross-border cooperation and data exchange.

22. Existing MoUs, could include a specific provision on assistance in time of crisis and in case of *force majeure*. In the absence of a specific provision, the general MoU rules could allow and/or encourage communication and cooperation using electronic means when availed.

III. Solutions for ensuring business continuity/crisis management measures

23. The COVID-19 pandemic demonstrated the importance of effectively managing business continuity risks of public and private sectors alike. Many public sector entities provide essential services for a country's economic and financial stability, and failure to deliver these could have significant consequences. Even services which may not be essential can cause disruptions with significant economic costs.

24. In the event of a major operational disruption, supervisory authorities have broad public responsibilities for safeguarding and maintaining public confidence in the financial system. However, as the mandates of supervisory authorities vary (*e.g.* some prudential supervisors are responsible for systemic issues while others, such as AML/CFT supervisors, are not), the approach to business continuity management must be tailored depending on the circumstances, and a one-size-fits-all approach may not be always efficient.

25. For example, in one jurisdiction, different measures were implemented by different supervisors, all commensurate with the materiality, risk and context of their role within the country. The National Bank applied a complex business continuity/contingency plan due to its vital role as a central bank responsible for the payments systems and financial stability etc, while

the Financial Supervisory Authority identified and analysed the risks generated by the pandemic and implemented the necessary measures to protect the health of employees and maintaining its supervisory activity. A different picture was observed at the casino and gambling sector supervisor, given that the activity of the supervised entities was significantly reduced if not stopped in certain periods of time during the pandemic.

26. On the other hand, in smaller jurisdictions, an integrated approach, run at the national level for all the public administration, bore some advantages, such as increased security in remote communication.

27. When looking at the replies to the questionnaire, it results that most supervisors have managed in some way to overcome the challenges of COVID-19 pandemic. When comparing approaches, it is evident that those countries that had engaged in business continuity management earlier and developed a more formalised approach - be it by adopting a Crisis Management Plan (CMP), a Business Continuity Plan (BCP) or establishing a Crisis Committee - had ensured minimal disruption to their operations. A timely reaction in switching from regular business to CMPs or BCPs was proven to be effective and enabled those supervisory authorities to smoothly transition to other working modes, ensuring uninterrupted performance and maintaining high quality of service that they provide.

IV. Overview of existing Business Continuity and Crisis Management Plans

28. The majority of the responding supervisory authorities declared having BCPs already in place when the COVID-19 pandemic started, which included various kinds of possible crisis scenarios, such as natural disasters, state of war, terrorist attacks, outages, technical system failures or cyber-attacks. However, the pandemic/outbreak scenario was (rarely) mentioned and only one country had a specific pandemic scenario covered in their BCP.

29. Some jurisdictions had BCPs which were not finalised or not yet adopted, while one jurisdiction reported that their BCP would not cover AML/CFT supervision. Several jurisdictions indicated that following the COVID-19 pandemic, the BCP was subject to amendments to include remote working and other lessons learned during the experience of the confinement.

30. The majority of BCPs described in the responses to the questionnaire set out: (i) a risk assessment methodology, (ii) detailed governance arrangements, (iii) division of responsibilities and (iv) specific actions to be undertaken in relation to the crisis in order to ensure the continuity of business operations. Ideally, when designing a BCP, a business impact analysis should be conducted at the inception of the process. This undertaking should take into account all functions of the supervisory authority including elements of AML/CFT supervision.

31. In general, the relevant documents are confidential and therefore could not be disclosed in the context of the present analysis. However, the general structure of a BCP mainly consists of five parts pertaining to five phases of overall recovery process: (i) the background strategy; (ii) the preparation before a disruptive event; (iii) the reaction to a disruptive event; (iv) the restoration (the implementation of alternative solutions until full recovery) and (v) the recovery (the post-recovery tasks and the transition back to the normal functioning). BCPs are normally reviewed and modified once a year.

32. One supervisory authority has developed and included in its BCP a supervisory toolbox for emergency situations and defined sub-plans for various scenarios. Drawing from the COVID-19 pandemic experience other supervisors supplemented the existing protocols with additional checkboxes or quick reference tables, to minimise the response time and efficiently ensure business continuity. These checklists clearly delineate the chain of responsibility between different management levels/categories responsible for crisis mitigation.

33. As an example of crisis situation, the COVID-19 pandemic impacted the work conditions in supervisory authorities twofold: (i) limiting access to buildings and (ii) limiting the number of staff available to carry out daily tasks. This issue was addressed in some jurisdictions that implemented arrangements to ensure business continuity with limited physical presence of staff. One jurisdiction had alternative BCPs prepared to continue supervisory activity with 10%, 30% and 50% of employee capacity.

34. For safety reasons, the majority of staff were instructed to work remotely, with the exception of critical operational teams (*e.g.* IT operations, physical security, general services, etc.) who continued to work on premises with regular rotation of team members.

35. As an exception, in one jurisdiction, due to the impossibility to access certain documentation or IT systems outside of the organization's premises, a *"bubble policy"* was implemented, as described below.

Case Example – Malta

The supervisory authority implemented a social "bubbles" policy which aimed to keep a certain level of presence in the premises while minimizing the risk of infection spreading among employees. The staff were clustered in "bubbles" with the general rule of no physical interaction between people from different "bubbles", during and after working hours.

The "bubbles" policy was consistently implemented at different levels: shifts, breaks, quarantine, transport and canteen facilities.

The "bubbles" allowed to loosen some uncomfortable restrictions inside the office such as the obligation to wear a protective mask. While contact time between employees from different bubbles was exceptionally allowed for 10 minutes for work purposes only, within the "bubble" protection measures were not mandatory. The contingency plan in case of positive cases detection was applicable only to the relevant "bubble", without impacting the work of the whole organisation.

36. When supervisors were not able to freely move to accomplish their duties, it was proven that having available and sufficient standby remote working devices ready to use in case of emergency was a good practice. Implementing secured cloud-based virtual work environments in order to decrease the dependence on the availability of buildings and allow for enhanced data protection was another.

37. Reportedly, the inaccessibility of premises prompted some organisations to start preparing relocation plans where the supervisors would move to different premisses in order to allow social distancing. Relocation primarily posed a challenge to the IT service, whose availability is crucial for ensuring reconstruction of data and systems in an alternative premise.

38. Some supervisory authorities follow international standards requiring having business contingency plans in place, among which two ISO Standards were mostly reported: ISO27001 (Information Security Management) and ISO31000 (Risk Management). Other authorities from jurisdictions being part of European Monetary Union chose to follow the ECB Security Guidelines.

39. One important aspect that determined a successful business continuity management was the state of digitalization in the supervisory authority. Almost all respondents indicated that due to available IT solutions and digitalization of work process, limitation to physical presence did not create major operational disturbance. For this reason, in the majority of jurisdictions IT security and critical infrastructure departments were closely involved in the development of business continuity strategies and plans and in their implementation. Some jurisdictions combined the responsibility for ensuring business continuity within the supervisory authority with the IT

security departments. Section 3 of this report discusses in more detail the best practices in using IT solutions for ensuring uninterrupted supervisory work.

40. In order to effectively address crisis situations, several jurisdictions mentioned the creation of dedicated Crisis Management Committees, comprising at least one member of the senior level management. As a good practice, a manager responsible for AML/CFT supervision could be a member of this Committee to receive updates and contribute to the creation of the set of measures to be adopted in tackling the situation.

41. Other supervisory authorities had dedicated teams trained to ensure the business continuity in the event of an incident (e.g. a Strategic Management Team). In some other cases, an ad hoc crisis management task force has been formed and instructed to conduct the disaster risk assessment, keep it up to date, and set an appropriate budget for the crisis management activities. Key people can be trained prior to crisis to have transferable skills to cover various areas (including AML/CFT supervision).

Case Example - Cyprus

According to the crisis management plan, an Ad hoc Task Force was set up to address the issues related to the pandemic crisis. It consisted of a General Manager, a Head of administration and finance department and an IT officer. The overall responsibility of the business continuity lay with the General Manager, who reported directly to the Board of Directors.

The CMP indicated a clear division of primary responsibilities among persons in each department in crisis situations.

The duties of this Task Force were mainly to monitor all legal aspects arising from new legislation, to provide technical support to the staff, to issue internal guidelines and procedures and to report to the Board of Directors.

The IT Officer was responsible for the maintenance of all ICT systems, liaised with external providers and ensured technical support was available to staff in case of any connectivity problems, bandwidth and use of the software on their laptops.

The BCP also provided for the digitalisation of the processes and documentation. The operating environment was cloud-based, with strong cyber-security measures in place, coupled with cyber and data security insurance plans.

42. To ensure that the crisis management measures are fit for purpose and effective, one jurisdiction conducts periodic crisis simulation exercises. This approach is proven to be beneficial as such exercises identify the problematic elements of the implemented crisis management approach and prepare core personnel on their responsibilities.

43. Another issue that can impact effective crisis management is the integration of AML/CFT supervisors into a centralised governmental agency or the fragmentation of AML/CFT supervision between different supervisors (*e.g.* FIs and DNFBPs). AML/CFT supervisors are often part of bigger organizations (central banks, ministries of finance, tax administrations etc.), in which case their duties are very different to those of other departments in the organisation. For this reason, some organisations reported having tailored BCPs (and also CMPs) for departments responsible for AML/CFT supervision in addition to the general CMPs of the organization. One jurisdiction reported having several specialised BCPs for each department in the main organization in addition to the general BCP.

44. As for the fragmentation, in the majority of the responses, the AML/CFT supervision of various reporting entities is divided between many bodies which are each responsible for particular sectors. Most of these bodies have their own CMP. However, a good practice would be to develop

some coordination mechanisms available in case of a global crisis such as the COVID-19 pandemic. Such coordination was rarely identified in the replies to the questionnaire and could be provided, for instance, by a common crisis committee chaired by the main AML/CFT supervisor in the country, who will ensure that no organization is left behind and there is no gap in the whole system.

Case Example – Russian Federation

In the context of the spread of coronavirus infection, Rosfinmonitoring put into commercial operation the Personal Account of the supervisory authority, which is a channel for interagency information sharing. The supervisory authority's Personal Account was used as one of the tools for building a unified system of risk-based AML/CFT supervision for all oversight authorities. Information on the risks in the sectors and in the activities of specific organizations was communicated in a prompt manner.

To assess the compliance of supervised entities with the AML/CFT requirements, Rosfinmonitoring communicated to the supervisory authorities the risk indicator obtained through the aggregation of data on supervisory risk assessments, indicating the average values for each set of criteria.

The Personal Account of the supervisory authority was also used as a communication channel between Rosfinmonitoring and the oversight authority, which significantly reduced the cost of correspondence and increases the speed of reception and transfer of the necessary documents (registers of entities, information about carried out inspections, information on the identified typologies etc.).

V. Digitalization

Increasing the capacity of the available technological solutions

45. Limitations on physical presence in the offices as well as inability to physically inspect reporting entities has provided to be a serious operational disturbance to the supervisors during COVID-19 pandemic.

46. This prompted both the private and public sector to rapidly increase digitalization of their core functions in order to maintain operational continuity. Several jurisdictions referred to the need of strengthening the capacity of available technological solutions**,** through (i) use of protected data exchange channels and additional protected communication channels, (ii) performing real time information exchange, (iii) elaboration of specific supervision analytical tools with remote access, (iv) providing an independent and secure internet connection, (v) integration of automated solutions for remote supervision, (vi) implementing machine learning, big data analysis and graph analysis tools, (vii) improving the capacity of transaction monitoring and analysis and (viii) implementing proper back-up and logging tools for an on-line document management system.

47. Increase in use of widely known commercial video conferencing tools has been highlighted by many jurisdictions, including the possibility to use video conferencing for reviewing sensitive documents and client files. Some jurisdictions indicated that when conducting remote inspections, supervisory authorities requested to have directed access through secured channel to the client files and compliance data from reporting entities. Such direct access has made it easier to inspect reporting entities directly without the need to send confidential client information through other electronic means. However, such possibility is limited to reporting entities that have more sophisticated IT systems and store their client data and internal documentation in digital format.

48. It has been emphasized by several jurisdictions that as a result of COVID-19 pandemic, in order to ensure operational continuity, many supervisors had to improve their actual technical

equipment. Likewise, one jurisdiction highlighted that pandemic accelerated use of additional IT tools for AML/CFT supervision, for example, in sanctions screening, whereas others stated working on new system using the Blockchain technology.

Ensuring data security with limited physical presence of staff

49. Supervisors from different jurisdictions have found different solutions to ensure data security and specific IT security measures were implemented at institutional level. Considerable investments into additional personnel equipment, data security improvement and necessary IT tools had to be made during the outbreak of the pandemic. Only a few supervisors reported to have all of the necessary devices such as laptops and IT tools such as secure remote access solutions and data encryption utilities already in place to provide access to corporate data and applications for effective working of the remote users.

50. In addition to VPN (Virtual Private Network), which refers to a secure communication tunnel between two online locations, supervisors have used privileged user control and connection encryption service systems, that make it possible to establish secure, isolated remote sessions, log all access information and record all activity during that session. While using this system end users never directly connect to target systems and databases, reducing the risk of downloading malware. Session recordings are securely and centrally stored to make it easy for security, audit and compliance to increase accountability and compliance. Some jurisdictions noted that for ensuring security they had introduced firewall protocols and their proper functioning was regularly screed. Additionally, some supervisors have opted for engaging external vendors for performing reviews of data security through penetration testing on a regular basis in order to ensure that the security measures are up-to-date.

51. Multi-factor authentication was added as an extra security layer. Some supervisors opted for cybersecurity solutions that would allow access to the internal network and data only through work laptops, using security policy setting that determines which user can access the login screen of a remote device through a Remote Desktop Connection. A remote connection would only be established via a host server to the supervisor's laptop, equipped with the most up-to-date anti-virus software, applications and operating system (including all security patches). This should be ensured through running regular operation system updates and antivirus scans in the background. This solution is only possible if most of the personnel are working on laptops provided and controlled by the supervisory authority. In the case of personal mobile devices (which are not provided by the institution), some security container applications (virtual desktop, workspace capsules) that use containerization or encapsulation mechanisms were implemented and used. This solution allows to separate corporate and personal data and to secure corporate data inside corporate network, so that the protected information cannot be disseminated outside the work ecosystem.

52. To limit the risk of hacking, stealing or disclosing sensitive data, supervisors restricted settings for downloading data from remote computers to or printing on personal devices and also disabled USB's and CD drives from the work laptops. When processing data from the internal network special utilities were used for encrypting and storing sensitive information on the working device to prevent unauthorised access.

53. New protocols relating to remote working and data security had to be put in place. For example, one supervisor introduced a teleworking agreement for employees working from home, where the employees must ensure that the home office meets certain requirements included in the guidelines of the teleworking policy. Another supervisor introduced clear desk and clear screen policy to ensure certain level of privacy from other family members, while working remotely or participating in virtual meetings. Many supervisors have introduced or enhanced the use of digital signatures in order to authenticate official documents. Procedural changes stipulating use of digital documentation were needed in order to replace paperwork and avoid disruption of supervisory processes.

54. To ensure a successful introduction and application of these new policies some supervisors purchased IT services (sub-contracted IT professionals) and ensured that their employees were trained on cyber security and data protection issues in order to further prevent risk.

VI. Remote supervision and other measures and tools.

Assessment of Emerging ML/TF Risks

55. In a "business as usual" state, supervisors base their understanding of ML/TF risks on the analysis of all relevant and up-to-date qualitative and quantitative information. This may include: (i) prudential and conduct information already held by the supervisor, (ii) information gathered through surveys or periodic onsite or offsite inspections, (iii) AML/CFT supervisory returns and/or, (iv) information shared by other domestic or foreign competent authorities.

56. Major operational disturbances contributed significantly to the increase of AML/CFT and operational risks. In the case of COVID-19 pandemic, the resulting lockdown measures and change to on-line and non-face-to-face activities at entities level, contributed to an increase in predicate crimes such as cybercrime and various types of fraud[3]. In order to respond effectively to the emerging risks in the event of major operational disruptions, supervisors supplemented existing AML/CFT related data with a swift and desk-based assessment of emerging crisis-related ML/TF risks within each defined sector and the entities under its supervision.

Case Examples – Russian Federation

Following a risk assessment, Rosfinmonitoring and the Bank of Russia requested banks to consider the economic rationale of transactions involving funds allocated by the government to support entities operating in the most impacted industries – the so-called compensation payments. Many banks begun to create a database of untrustworthy entities which were not engaged in any real business activities, but claimed their eligibility for the resources allocated under the government-funded support programs.

Rosfinmonitoring developed and posted additional red flags and indicators of risks and customers' suspicious activities on its official website based on the analysis of STRs that reported suspicious transactions related to new risks, as well as considering the information published in the FATF Secretariat document entitled "COVID-related Money Laundering and Terrorist Financing Risks and Policy Responses". The reporting entities were also advised to pay enhanced attention to customers' activities related to production and distribution of medical goods and products.

57. When undertaking such targeted assessment of emerging risks, supervisors should take into account both the inherent ML/TF risks and the controls employed by entities to mitigate such crisis scenarios. In the case of the COVID-19 pandemic, many supervisors issued questionnaires and surveys to solicit information from reporting entities on their exposure to emerging ML/TF risks. For this purpose, some jurisdictions used existing AML/CFT public-private partnership mechanisms.

58. Other supervisors had previously invested in online submission portals whereby their reporting entities could submit electronically information on new risks and observed anomalies in the behavioural and transactional activity of certain clients. These tools were used in addition

[3] See "Money laundering and terrorism financing trends in MONEYVAL jurisdictions during the COVID crisis", https://rm.coe.int/moneyval-2020-18rev-covid19/16809f66c3

to STR and SAR reporting. Employing such mechanisms allowed competent authorities to identify new typologies of ML associated with the crisis specific risks such as embezzlement of government funds allocated for supporting businesses and citizens and overinflated pricing of the personal protective equipment and medicines.

Case Study – Guernsey

As a result of COVID-19 pandemic the Bailiwick of Guernsey instigated a lockdown in the second quarter of 2020. The Guernsey Financial Services Commission ("GFSC") sought to understand the impact of the lockdown and switch to homeworking was having on the application of AML/CFT internal controls at reporting entities, therefore it issued questionnaires electronically to those reporting entities considered systemically important to the Bailiwick's financial services sector. To further aid the GFSC's understanding of the impact of COVID-19 the GFSC held a number of video/telephone calls with representatives of the reporting entities to discuss their responses in greater detail. The following questions were posed to reporting entities about their experiences during the lockdown:

- How many internal SARs were received and externalised during the lockdown?
- How did the money laundering reporting officer reach out to staff during the period of home working to maintain awareness of the importance of reporting suspicion?
- Is the reporting entity able to maintain its AML/CFT compliance monitoring programme?
- Were there any changes to the reporting entity's compliance monitoring programme?
- Has there been an increase in the level of exception reports arising from transaction monitoring?
- Were any cases presented during lockdown where the reporting entity was unable to complete verification of customers?
- Did the reporting entity make exceptions to its AML/CFT policies and procedures?

The results of the questionnaire were analysed and feedback given to the industry at a GFSC hosted hybrid physical/virtual seminar.

Allocation of resources for core functions and adjustment of supervisory plan

59. It is recognised that a crisis scenario such as COVID-19 does impose stresses and strains on a supervisor. Firstly, it may lead to a temporary reduction in staffing due to illness, and secondly, resource may have to be devoted to other more pressing needs. It is a particular concern for those supervisors who have both a prudential and AML/CFT remit, as resources may have to be diverted to prudential supervision, if it considered that financial stability is at risk and entities could fail, which could ultimately lead to greater social harm to consumers.

60. Supervisors typically have a fixed cycle of onsite inspections driven by the ML/TF risks in the sectors and firms they supervise. During the COVID-19 pandemic this fixed cycle required revaluation due to the resource constraints. Most of the supervisory authorities indicated that their supervisory plan was re-evaluated on the basis of risk, to enable supervisors to focus on those entities which were considered to pose unacceptable ML/TF risks and require supervisory intervention.

61. The survey demonstrated that the scope of the supervision was not changed by the pandemic conditions, but for practical purposes, in order to adapt to remote supervisory arrangements, the number of samples required in the course of an "inspection" were decreased for medium and low risk entities.

62. The COVID-19 pandemic has contributed significantly to the increase of AML/CFT and operational risks connected with on-line and non-face-to-face activities at entities, particularly predicate crimes such as cybercrime and fraud, as criminals may exploit weaknesses in reporting entities policies, procedures and controls due to staff working from home. Therefore, supervisors focused foremost on ensuring that entities' internal systems and controls were operating effectively, particularly in known vulnerable areas such as the onboarding of new customers.

63. The European Banking Authority[4] also consider that mitigating the adverse effects of a crisis situation such as a pandemic may require temporary adjustments of supervisory priorities and plans to ensure that AML/CFT supervision remains effective. This in turn implies that prioritization is key in a crisis and the allocation of resources should be on the basis of risk.

Impact of crisis situation on the AML/CFT supervisory actions: the shift from on-site to off-site

64. At the beginning of the COVID-19 pandemic and resulting lockdowns the majority of supervisors suspended their onsite inspection programme for a few weeks and focussed on offsite monitoring. This short period of suspension did impact the number of traditional onsite inspections in 2020, but supervisors considered that this did not impact the overall effectiveness of AML/CFT supervision.

65. When it became clear that there would be further lockdowns or similar measures, it also became apparent that ordinary onsite inspections would not be possible in the near future and therefore new ways of conducting onsite inspections were introduced.

66. The adjustment time varied but some supervisors were able to shift to remote inspections within three weeks. Reportedly this was a result of existing CMPs, teleworking arrangements already in place before the crisis and a business continuity culture which made employees understand and accept that the work must keep going on regardless of the restrictions. For the latter, some supervisors pointed to the paramount role of pro-active internal communication with the employees during the pandemic restrictions. A need for clear procedural instructions on how much to communicate, to which level of detail, how often, on which tone, to whom and by whom, when etc., was expressed through the answers to the questionnaire. Apart from the motivational side, the communication is meant to lift as much burden from the employees as possible, giving all the necessary information on how to act or react in the face of the restrictions.

67. The majority of surveyed supervisors are now conducting hybrid on-site inspections where information/documentation is requested electronically and then meetings are held by commercially available video communication methods with representatives of reporting entities or if a physical on-site inspection is required that those inspections are undertaken in strict compliance with all anti-epidemic measures. Some larger entities provided virtual data rooms in order to share confidential business information with supervisors. Reporting entities unable to provide data rooms submitted information/documentation through online submissions portals (if made available by the supervisor) or by encrypted e-mail systems.

Case Example – Germany

In June 2020, BaFin conducted a special inspection on a supervised bank remotely. The inspection focused on the identification requirements of the contracting party or the person representing that party, the requirements for clarifying or, where appropriate, identifying the beneficial owner and clarifying whether they met the criteria of a politically exposed person. For this purpose, random samples of customer documents were inspected. The supervisors selected

[4] EBA statement. Available here

a sample from the total inventory of new business relations established by the bank since 1 February 2019. As with a regular on-site inspection, a data space was established that served the exchange of documents. Unlike with a regular inspection, the bank was informed of the sample selected shortly before the inspection started. The bank then uploaded the data sets specified onto the data space provided. A three-day period was set for the inspection itself. The samples were assessed and a number of interviews with responsible individuals in the bank were conducted, notably with the money laundering officer, his/her deputy and the responsible board member. The inspection opened with an introductory conversation explaining the broader context and planned schedule for the inspection; it ended with a closing conversation. Conversations were conducted via conference calls.

68. Particular situations have been flagged where reporting entities (amongst DNFBPs) refused or were unable to facilitate remote supervisory arrangements (such as sending the documentation electronically). In such cases, exceptionally, the supervisor conducted a physical on-site inspection and scanned or took copies of the relevant documentation and undertook the detailed analysis remotely. This demonstrates that in challenging times, a high degree of flexibility in applying supervisory actions, proves to be beneficial.

69. The pandemic has highlighted the importance of supervisors investing in technology in order that they: (i) can securely receive information from entities (ii) store that information centrally and electronically; (iii) retrieve stored information securely and remotely; (iv) analyze data to ascertain ML/TF risk and (v) communicate verbally both internally and externally.

70. Supervisors and reporting entities are becoming more accustomed to working from home, but supervisors highlighted that remote inspections are considered less effective compared to traditional physical onsite inspections for the following reasons: (i) arranging the submission of information electronically is time consuming for both reporting entities and supervisors; (ii) remote meetings may be interrupted due to the internet connection issues and (iii) documents may not be fully accessible as some customer records may be partially paper based. In addition, whilst supervisors have invested in video communication tools, communication is not as free flowing as a face-to-face conversation. Moreover, it has required revised managerial oversight arrangements as supervisors are working from home.

Case Examples – Liechtenstein

At the beginning of the pandemic the FMA tried to maintain the onsite inspection plan and postponed already planned inspections for a few weeks. Due to further lockdowns, further postponements had to be made. When it became clear that there will be further lockdowns or similar measures, and that ordinary onsite inspections would not be possible, the FMA decided to conduct the AML/CFT inspections on a remote/offsite basis.

71. In some jurisdictions supervisors have remote direct access to the intranet or the core internal systems of reporting entities. This is only possible where the internal IT systems of these entities allow such remote access for outside users. Such remote access allowed supervisors to verify the compliance of reporting entities during remote inspections and allow to double-check directly the information provided by the reporting entity.

72. One year into the COVID-19 pandemic has shown that not all supervisors have switched back to conducting on-site meetings. One supervisor noted that conducting remote onsite inspections would carry on for the foreseeable future for all lower risk reporting entities as they appear to be more efficient and faster. However, it was considered for higher risk reporting entities reverting to

physical on-site inspections is a must. Reportedly, the negative side of not carrying out on-sites, is that a part of the input is lost, especially intuitive type of information, such as feelings, moods, attitudes or any type of informal communication which is easily perceived during physical meetings.

73. It has been shown that thematic reviews may be particularly beneficial in lengthy or lasting crisis situation as supervisory resources are stretched and a thematic review enables supervisors to review a number of entities and assess a known vulnerability in depth. Thematic reviews provide flexibility as these inspections are conducted onsite or offsite or can be a mixture of both. Thematic inspections have been used as a tool to swiftly respond to crisis situation and establish communication with reporting entities at risk.

Case Example - Guernsey

Due to COVID pandemic and the resulting lockdown the Guernsey Financial Services Commission ("GFSC") temporarily suspended its onsite inspection program in the 2nd quarter of 2020 and focused on prudential supervision. However, it was recognised that the lockdown resulting from COVID-19 made entities vulnerable to financial crime as criminals may exploit weaknesses in entities policies, procedures and controls. In view of the increased vulnerability to financial crime the GFSC undertook a thematic review on entities ability to make suspicious activity reports ("SARs") to the Guernsey FIU, which encapsulated an assessment of an entity's governance, policies, procedures and controls in relation to suspicious activity reports and the capability and capacity of the money laundering reporting officer. The review consisted of four phases: Phase 1: analysis of the information on the number of SARS reported in the GFSC's annual financial crime risk return; Phase 2: analysis of board minutes; policies and procedures; compliance arrangements and registers in respect of SARs from a sample of firms; Phase 3: conduct interviews with Board members and MLROs and MLCOs with a sample of firms, either remotely by video conference or in person if it is safe to do so and Phase 4: publication of an external report on the findings of the thematic review [published in July 2021 on www.gfsc.gg].

74. It is common for entities which form part of international groups to operate globally, and therefore be subject to AML/CFT supervision in multiple jurisdictions. ML/TF risks are often cross-border in nature, and systems and control failings in one part of the group can be replicated elsewhere, accordingly it is key that good lines of communication are maintained between supervisors.

75. COVID-19 has presented a challenge to international cooperation as supervisors were unable to travel and attend face-to-face meetings with other supervisors. However, the pandemic has not restricted international cooperation as supervisors have switched to video communication methods. Several supervisors stated that the levels of co-operation have increased, possibly because it is so much quicker to set up a video call rather than attend a meeting in person. However, some replies to the questionnaire revealed that face-to-face meetings present an opportunity to provide more information in an informal setting.

Use of simplified measures in the time of crisis/ challenges with remote onboarding (digital ID)

76. As a result of the lockdown following COVID-19, individuals were unable to attend an entity in person to open an account or use a suitable trusted third party to confirm a positive link between his/her identity and identification data and certify as a true copy identification documentation such as an identity card or passport. Supervisors played a key role in ensuring that an appropriate risk-based AML/CFT regulatory framework was in place to enable entities to continue onboarding

customers and that citizens were not disadvantaged, particularly those who needed bank accounts to receive government benefit payments.

77. When establishing a business relationship, banks were allowed in a jurisdiction to ascertain and verify the customer's identity within one month after the inception of the business relationship, or within one month after the revocation of the pandemic related restrictions. Other supervisory authorities allowed reporting entities not to update customer information as it pertains to details of ID documents whose validity had expired during the state of alert or other exceptional status imposed in the country. The later would be consistent with some other measures taken by the national Governments to limit the spread of the virus, mainly through the "automatic" prolongation of expired ID documents until the end of the crisis or deferred deadlines for filing documents or other endeavours. The exceptions never concerned the STR obligations. Due to the lock-down, the number of cash transactions dramatically decreased in many jurisdictions.

Case Example – Slovenia

The exemption provided by the Intervention Act was not applicable in case of increased risk of money laundering and terrorist financing. With the Act Determining the Intervention Measures to Contain the COVID Epidemic and Mitigate its Consequences for Citizens and the Economy, the exception to the regular CDD requirements were extended also to some other obliged entities defined in the Act (financial institutions, insurance agency services and insurance intermediaries).

78. The survey shows that the COVID-19 pandemic accelerated the introduction of digital identification ("digital ID") of customers by financial institutions. Whilst the majority of supervisors permitted digital ID pre-COVID, several supervisors amended their AML/CFT legislation to permit digital ID as a result of the pandemic. In permissive regimes, supervisors highlighted that banks in particular had taken advantage of the use of digital ID as part of the customer on boarding experience.

79. In March 2020 the FATF released its new Guidance on Digital ID[5], which among other things highlights the potential benefits of trustworthy digital identity for improving the security, privacy and convenience of identifying individuals remotely while also mitigating money laundering and terrorist financing risks. The FATF, while acknowledging the risks inherent in digital ID, suggested that such systems, together with improving customer experience and originating cost savings, can even ensure higher levels of security and lower risks than traditional paper-based CDD, since they are more accurate, reliable and independent and do not have the weaknesses of the traditional paper-based CDD procedures which also require human verification and control systems.

Case Example – Estonia

In Estonia it is common to use digital ID. ID-cards are the primary identification document. They are compulsory for all citizens and residents and are the most widely used digital ID option. The ID-card has a photograph and a chip that securely stores personal identity data and digital signature certificates, using public key infrastructure. A customer can be on-boarded face-to-face, via information technology means (video on-boarding) and by using two different sources of identity verification. Estonian digital ID solutions are used for customer identification/verification at on-boarding, as well as for strong customer authentication.

[5] Documents - Financial Action Task Force (FATF) (fatf-gafi.org)

80. Nevertheless, a large proportion of entities still rely on traditional paper-based identification methods and do not have access to digital ID systems. Therefore, in the wake of COVID-19, a number of supervisors issued guidance advising for remote identification options and methods, such as the use of video calls in circumstances where the individual cannot arrange for certification of their identity documents but can or has provided an uncertified copy; or where the individual cannot provide the identity documents physically or copies thereof in paper or electronic form. However, it should be recognised that whilst video calls may be used, they do not contain the type of inbuilt security controls that a fully-fledged digital ID system employs and therefore entities should apply a risk-based approach when considering the use of a video call to verify the identity of an individual.

81. The COVID-19 lockdowns have disproportionately impacted lower income populations. To mitigate this impact, governments across the globe have launched disbursement programmes, but these programmes can face challenges as many lower income people are unbanked.

82. The FATF recommendations do permit simplified due diligence when entities identify lower ML/TF risks. The FATF has encouraged both countries and entities to explore the appropriate use of simplified measures to facilitate the delivery of government benefits in response to the pandemic.[6]

83. To a large extent COVID-19 has helped to blur the distinction between measures to be taken in a crisis and "business as usual". The ability for supervisory staff to work remotely, use of hybrid on-sites, need for good IT/data collection, use of analytical tools with remote access, use of digital ID for remote on-boarding, and use of webinars are likely to become part of a new digitalized way of supervision.

VII. Sanctions and outreach

Ensuring continued industry outreach and support during major operational disruption

84. The COVID-19 pandemic has underlined the importance of ensuring sustainable and constant private sector communication channels. Supervisors in many countries actively used their official websites to provide guidance and recommendations, information on compliance with mandatory requirements, new risks associated with COVID including FATF and MONEYVAL reports on this topic. As a follow-up to FATF's and MONEYVAL's publications, some jurisdictions conducted national research on the specific risks amid the pandemic and communicated the results to the reporting entities.

85. Most of the support to reporting entities was related to providing additional clarifications, including on developing business continuity or crisis management plans and reporting mechanisms, alerting the private sector to the impacts of COVID-19 associated ML/TF risks, and ensuring the usage of risk assessment approaches to support financial services and transactions.

Case Example – Israel

The Supervision Department of the Bank of Israel raised the banking sector's awareness of local and international publications in the field of anti-money laundering and terrorist financing, and sent the following supervisory letters to the banking corporations:

[6] Documents - Financial Action Task Force (FATF) (fatf-gafi.org)

- A letter containing key recommendations concerning monitoring money laundering and terrorist financing risks in the context of the COVID crisis - including a requirement to ensure that the current monitoring and control measures applied to identify exceptional financial activities are adequately adjusted to changes in business patterns.
- A letter containing an emphasis on risk management and the use of technological and innovative tools in the field of AML/CFT - including a requirement to examine the adequacy and effectiveness of the use of risk management and technological tools, in accordance with a risk-based approach and act to ensure proper risk management.

86. Most countries have produced specific guidance and organized webinars for the private sector, online trainings and workshops, including ones with the participation of professional syndicates or associations. The topics of these events were mainly related to the implementation of mandatory AML/CFT requirements in the context of the lockdown measures imposed by the governments and the specific ML/TF risks that started to emerge during the pandemic.

Case Example – Germany

As a very quick reaction of the Public Private Partnership "AFCA" (BaFin, FIU, Federal Police and numerous private sector participants) produced four specific papers (called "White Papers") targeting AML/CFT in COVID times providing a valuable guideline for the entire financial sector and the supervisors. The whitepapers included information on: the position of the FATF on COVID; factors driving changes in financial crime**;** AML information on misuse of financial support and abuse of unemployment benefits**;** Further indications for the filing of suspicious transaction reports (STRs)**;** Effects of the COVID pandemic on the manifestations of crime; Integration of illegal cash flows into the financial cycle and crimes related to vaccines.

87. Some supervisors have opted for other innovative solutions for direct communication with the private sector by posting video clips on the websites of competent authorities in order to communicate risk information and changes in AML/CFT rules and regulations, as well as to post e-learning materials.

Case Example – Russian Federation

Soon after the outburst of the pandemic and the introduction of restrictions, Rosfinmonitoring prepared and posted on their website an information letter containing the guidelines on coronavirus infection-related risks for the obliged entities, requesting them to promptly report the relevant suspicious behavior of customers with a special reference (COVID) for further reviewing. Subsequently, based on the STRs received with the new reference, Rosfinmonitoring developed and posted additional red flags and risk indicators on its official website. The reporting entities were advised to pay enhanced attention to customers' activities related to the production and distribution of medical goods and products. These communications had a clear impact on RE reporting behavior.

88. Some supervisors eased the reporting requirements for reporting entities, due to the impact of the crisis on private sector's resources. This included the imposition of a moratorium on prosecution for non-compliance with some AML/CFT obligations and extension of deadlines for fulfilling mandatory AML/CFT requirements, such as deadlines and frequency of reporting, updating of internal rules and procedures, the deadlines for updating documents, including identity documents which expired during the first wave of the pandemic.

89. Equally, some jurisdictions extended deadlines for remediation of AML/CFT deficiencies identified as a result of off-site and on-site inspections and had in view resource limitations when drawing up corrective action plans. In rare cases, supervisors accepted requests to postpone a scheduled inspection.

Prioritization of different types of remedial actions and sanctioning

90. The majority of respondents stated that due to the negative impact of the crisis on workplaces and the changing risks, supervisory authorities played a greater role in reaching out to entities to understand their challenges and providing advice and appropriate leeway, rather than resorting to punitive measures in cases of non-compliance due to COVID-19 factors.

91. Some jurisdictions have prioritized non-financial measures that allow to promptly eliminate the identified deficiencies over the monetary sanctioning. Applied measures were aimed at preserving business continuity of the challenged financial sector rather than sanctions that would inhibit further operation of the reporting entities.

92. When violations were not of a serious nature in some jurisdictions it was deemed sufficient to issue warnings, prescribe specific measures and deadlines for their implementation. When monetary sanctions were applied, consideration was given to the proportionality of sanctions in the context of the global disruption of the reporting entities' regular activities and the impact on their financial situation, and seriousness of the breach.

93. Most respondents applied a moratorium on the liability of reporting entities for minor violations of the law as long as the crisis continued. All such measures were considered taking into account the entity-specific risk, the gravity of violation and specific circumstances of the crisis. For example, during the COVID pandemic supervisory authorities applied a risk-based approach and paid particular attention to breaches of AML/CFT obligations in relation to identification of natural and legal persons. They monitored the entities with the most significant deficiencies. In case of continued non-compliance, stricter measures were taken.

94. When jurisdictions have chosen a stricter approach and did not make any concessions regarding the AML/CFT obligations and post-inspection requirements (remedial measures), extensions were granted exceptionally on a case-by-case basis taking into account e. g. shortages of manpower due to illness, lockdown etc.

95. This approach could have merit where the private sector entities are not able to meet some of their obligations to prevent ML/TF due to government-imposed restrictions, such as limitation on physical presence and movement of individuals. However, national authorities should make a case-by-case assessment when choosing to shift enforcement measures to remedial actions and possible risks such approach might have.

VIII. International cooperation

Enhancing cross border cooperation between supervisors during the time of crisis

96. It is important that the competent authorities are able to exchange information on new risks and emerging circumstances that impact the overall ability of reporting entities to comply with AML/CFT requirements. The majority of the respondents to the survey indicated that the COVID pandemic has not affected cross border communication between supervisors. In some cases, the international cooperation was even enhanced in that time (e.g., one country reported 43.18% increase in the international cooperation in 2020 due to the use of digital means of communication). Nevertheless, the crisis reshaped the format of communication from face-to-face to virtual and necessitated the use of alternative means of communication via the Internet.

97. No particular problems regarding IT tools for communication have been reported. Jurisdictions that were more used to virtual communication were less affected by the pandemic crisis and did not face major changes in their domestic and international cooperation.

98. One of the lessons learned by the responding jurisdictions from the COVID-19 pandemic experience was to favour the virtual meetings, which even in the usual times simplify the communication (e.g., the participants do not need to travel for meetings).

99. Another good practice identified by the supervisors in the course of the COVID-19 pandemic was to more carefully consider the communication by sending and requesting acknowledgements of receipt (to ensure receipt and to mitigate the risks of "lost" correspondence due to technical issues) and providing more comprehensive and clear answers and questions to avoid multiple back and forth messages.

100. Some respondents stressed the importance of having tools to prioritize international cooperation and information exchange in situations when facing major operational disturbance. Especially, in cases of consolidated group supervision both home and host supervisors should enhance the exchange of opinions on ways to understand and to assess AML/CFT risks, increase the frequency of meetings between regulators, and maintain a secured correspondence. Cross-border cooperation can only be enhanced with the real and effective commitment of all supervisors in a given country.

101. Some jurisdictions have noted that in the times of crisis such as the COVID-19 pandemic, international cooperation may sometimes be too slow due to practical limitations which may include restrictions in data access, decrease in human resources due to sickness or physical unavailability, IT issues and other. Therefore, it is important to include specific processes in the BCP that would help maintaining satisfactory levels of executed international cooperation requests.

102. Respondents noted that during the crisis, the international departments in supervisory authorities have been overburdened with the amount of incoming mutual assistance requests. A solution to address this challenge can be work in shifts to cover more time zones and increase number of responses to international requests. For this purpose, a good practice would be to create a crisis contact list that would be regularly updated.

103. The respondents underlined threats to security of sensitive information exchanged posed by cyberattacks, whose number increased during the COVID-19 pandemic. Only secured channels should be chosen to share information between authorities.

104. International organizations and other supranational bodies inform jurisdictions about good practices and potential policy responses to new threats arising from the health crisis scenario, including those related to transnational cooperation and exchange of information[7]. Also, by this indirect way supervisors shared their experience and information on specific risks identified.

Case Example - Guideline published by European Banking Authority (EBA)

EBA published guidelines on setting up EU international supervisory colleges and enhanced cooperation between authorities monitoring AML/CFT compliance of cross-border financial groups. Where the conditions are met, the lead supervisor, in cooperation with the competent authorities from host countries should establish and maintain an AML/CFT college. After first colleges have been started the EBA published a report on best practices in this area. According to

[7] Money laundering and terrorism financing trends in MONEYVAL jurisdictions during the COVID crisis (2020), Opportunities and Challenges of New Technologies for AML/CFT (FATF, 2021), COVID-related Money Laundering and Terrorist Financing Risks and Policy Responses (FATF, 2020); EAG organised International Compliance Council, with the main goals to exchange experience and best practices on the issues concerning application of AML/CFT preventive measures, and information interaction, including on the identification of new risks and the study of ML/TF typologies in the COVID times.

the MNB colleges constitute a progress in identification and management of cross-border ML/TF risks and enable enhanced communication between the authorities of the EU and of third countries.

Legal gateways for supervisory cooperation

105. Information exchange on an international level is governed by international conventions, reciprocity and on the basis of Memoranda of Understanding (MoU), that set out the mechanisms for cooperation. Most of the respondents concluded that a special clause on cooperation and assistance in the times of crisis is desirable and would enable more efficient response to queries (e.g. introducing simplified cooperation mechanisms, allowing alternative communication channels while being mindful to security).

106. Armenia considered that a clause on assistance between supervisory authorities in the time of crisis can ensure stability and permanency of cooperation. Another authority proposed to include a clause in the MoU that would forbid one party to unilaterally terminate communication during a crisis. For consolidated group-wide supervision MoU could allow for co-inspections and possibility to delegate supervisory activities. One jurisdiction has a reference to emergency/crisis situations in their MoU template, encouraging international cooperation.

Case Example – Germany

One key purpose of the emergency/crisis MoU is to establish a structured basis for co-operation in relation to AML/ CFT, including the exchange of confidential Information and assistance in conducting inquiries or e, to facilitate timely and effective AML/ CFT supervision, to provide mutual assistance in identifying risks to the integrity of the financial systems of our countries, and, where necessary, to address Emergency/ Crisis Situations, especially in instances where Emergency/Crisis Situations involve Financial Groups.

107. Some respondents questioned the need of special clause on assistance in times of crisis in MoUs, as it could result in over-regulation and in effect limit flexibility of international cooperation. It was pointed out that exchange of information and best practices and policies in such circumstances would likely be done without the need for additional agreements. Nevertheless, even in the absence of specific procedures to ease the cooperation in challenging times, a good practice might be for MoUs to provide for the possibility to cooperate using electronic means (videoconferencing) as well as remote information sharing necessary for consolidated group supervision.

www.coe.int/MONEYVAL

December 2021

MONEYVAL

Typologies Report

This report analyses AML/CFT supervision in times of crisis and challenging external factors