Regulatory update

KPMG Lithuania

Forensic/AML Services

—

Issue 2021/04

This quarterly Regulatory update newsletter presents recent changes in the applicable EU-wide and local regulations in terms of prevention of money laundering and terrorist financing, risk management, internal controls and related topics that may be relevant to the financial market participants operating in Lithuania.

The publication can assist you in staying up to date with evolving application guidance and new regulatory developments concerning abovementioned topics.

Foreword

The second edition of the *Regulatory update* newsletter kicks off with an overview of the newly revised EBA Guidelines on ML&TF risk factors, which were published on 1st of March 2021.

This is followed by the EBA's biennial Opinion on risks of money laundering and terrorist financing (ML/TF) affecting the European Union's financial sector. The Opinion of EBA was published on 3rd of March 2021.

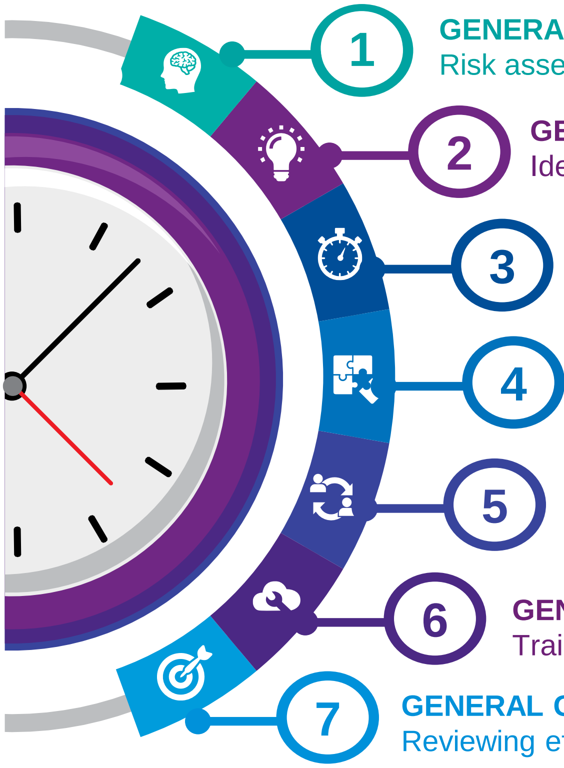
Next we have provided a brief review of ESAs Joint Warning on Crypto-Assets that was issued in March 2021, which brought to the attention of consumers the high risks of buying and/or holding so-called virtual currencies.

We have also shortly discussed the upcoming EU AML Package which is highly anticipated by financial market participants.

We finish this edition with the most important outcomes of the FATF Plenary that was held in February 2021.

We hope this publication serves its intended purpose of assisting you to staying up to date with evolving application guidance and new regulatory developments.

EBA GUIDELINES ON ML&TF RISK FACTORS



GENERAL GUIDELINE 1
Risk assessments: key principles for all firms

GENERAL GUIDELINE 2
Identifying ML/TF risk factors

GENERAL GUIDELINE 3
Assessing ML/TF risk

GENERAL GUIDELINE 4
CDD measures to be applied by all firms

GENERAL GUIDELINE 5
Record-keeping

GENERAL GUIDELINE 6
Training

GENERAL GUIDELINE 7
Reviewing effectiveness

The Guidelines include new sectoral guidelines for crowdfunding platforms, corporate finance, account information service providers and payment initiation services providers, as well as firms providing activities of currency exchanges offices.

The Guidelines help financial institutions to achieve the balance between the need for financial inclusion with the need to mitigate and manage ML/TF risk.

Competent authorities shall use these Guidelines when assessing the adequacy of firms' risk assessments and AML/CFT policies and procedures.

The Guidelines were published on 1st of March 2021 and will apply three months after publication in all EU official languages.

SECTORAL GUIDELINES ON ML&TF RISK FACTORS

Life insurance undertakings

Most life insurance products are designed for the long term and some will only pay out on a verifiable event, such as death or retirement. This means that many life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers. However, as with other financial services products, there is a risk that the funds used to purchase life insurance may be the proceeds of crime.

If the firm knows that the life insurance has been assigned to a third party, who will receive the value of the policy, they must identify the beneficial owner at the time of the assignment.

Trade finance providers

Banks that are party to trade finance transactions often have access only to partial information about the transaction and the parties to it. Trade documentation can be diverse, and banks may not have expert knowledge of the different types of trade documentation they receive. This can make the identification and assessment of ML/TF risk challenging.

Banks shall, nevertheless, use common sense and professional judgement to assess the extent to which the information and documentation they have could give rise to concern or suspicion of ML/TF.

Regulated Crowdfunding platforms

Crowdfunding Service Providers (CSPs) shall recognize the risks arising from the borderless nature of crowdfunding platforms where the CSP's customers can be located anywhere in the world, including high-risk jurisdictions. CSPs shall know their customers to prevent their crowdfunding platforms from being used to fund fictitious investment projects with illicit funds or being misused for TF purposes where a fictitious reason is given for a crowdfunding project, which never materializes and the funds obtained from crowdfunding are then used to finance a terror attack.

PISPs and AISPs

Even though Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) shall take adequate measures to identify and assess the ML/TF risks associated with their business, the inherent ML/TF risk associated with them is limited due to the fact that:

a) PISPs, although being involved in the payment chain, do not execute themselves the payment transactions and do not hold payment service users' (PSUs') funds;

b) AISPs are not involved in the payment chain and do not hold payment service user's funds.

Corporate finance

Firms providing corporate finance services should take into account the inherent ML/TF risks linked with these activities and be mindful that such activity is based on close advisory relationships in particular with corporate clients and other parties such as potential strategic investors.

Providers of corporate finance will, by the nature of the business, be gathering substantial due diligence information as a matter of course; firms should draw upon this information for AML/CFT purposes.

Investment firms

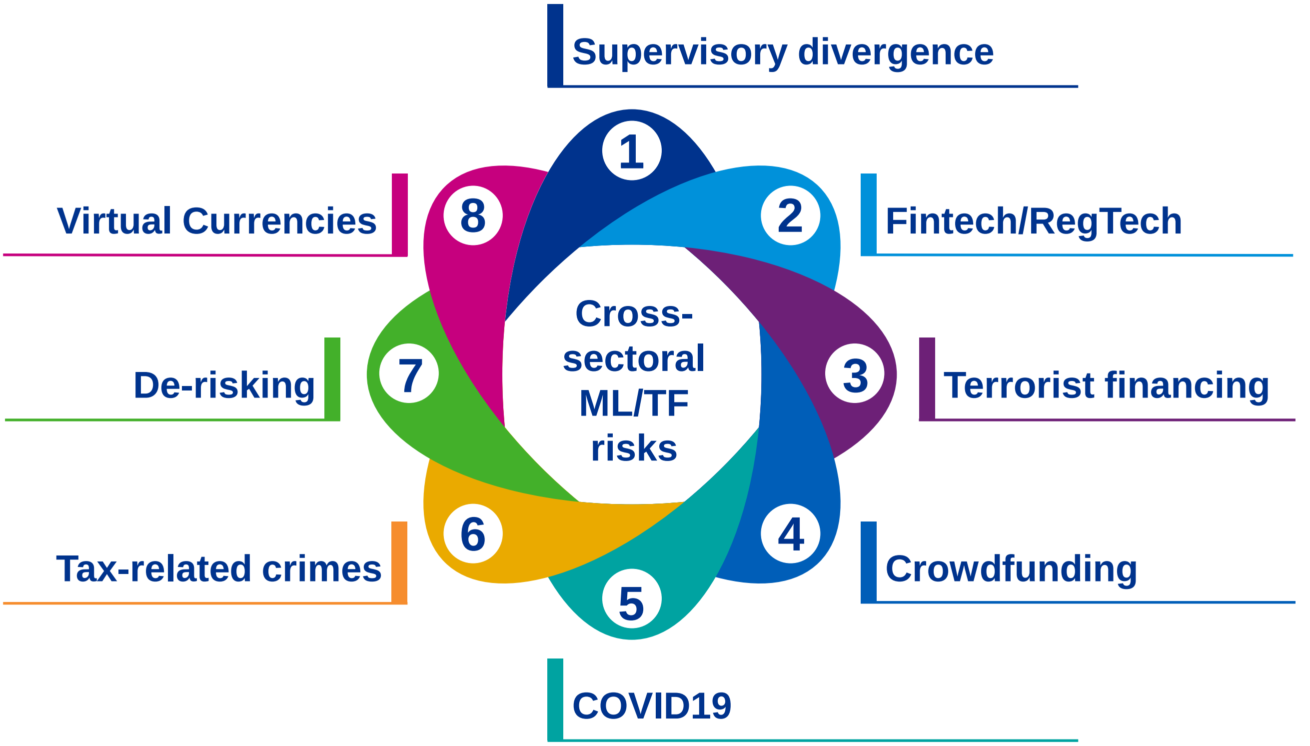
Investment firms shall consider that ML/TF risk in this sector is driven primarily by the risk associated with the clients whom investment firms serve and the nature of the activities which investment firms undertake means that they may be exposed to predicate offences such as market abuse, which may lead to ML/TF.

When developing their AML/CFT policies and procedures investment firms shall consider the extent to which information obtained for MiFID II and EMIR compliance purposes can be used also to meet their CDD obligations in standard situations.

Currency exchange offices

Firms shall have regard to the inherent risks of the currency exchange services which may expose them to significant ML/TF risks. Thus, firms shall be aware that these risks stem from the simplicity of transactions, their speed and their often cash-based character. Additionally, firms shall also have regard to the fact that their understanding of the ML/TF risk associated with the customer may be limited due to the fact that they usually carry out occasional transactions rather than establish a business relationship.

EBA's OPINION ON THE RISKS of ML & TF 2021



What you need to know

1. The European Banking Authority (EBA) on 3rd March 2021 published its biennial Opinion on risks of money laundering and terrorist financing (ML/TF) affecting the European Union's financial sector.

2. The ML/TF risks identified by the EBA include those that are applicable to the entire financial system, for instance the use of innovative financial services, while others affect specific sectors, such as de-risking.

3. The Opinion includes ML/TF risks that emerge from wider developments such as the COVID-19 pandemic that has an impact on both firms' AML/CFT compliance and competent authorities' supervision.

4. Risks associated with differences in the treatment by competent authorities of financial institutions' involvement in facilitating or handling tax-related crimes ('cum-ex/cum-cum') are included in the Opinion for the first time.

CROSS-SECTORAL ML & TF RISK FACTORS

Virtual Currencies

The European financial sector is exposed to the risks arising from VCs mainly in circumstances where customers of regulated credit and financial institutions deal in VCs or where they are virtual asset service providers (VASPs).

The main factors contributing to the increased exposure to the ML/TF risks is the limited transparency of VC transactions and the identities of the individuals involved in these transactions. Credit institutions, investment firms, electronic money issuers and payment institutions appear to be the sectors that are most exposed to these risks.

Several competent authorities identified in addition particular concerns related to the use of virtual currencies and crowdfunding platforms for terrorist financing purposes.

Crowdfunding

The absence of harmonized legal frameworks across the EU setting our clear AML/CTF obligations to crowdfunding service providers significantly increases the exposure of crowdfunding services to ML/TF risks. This is in addition to the existing exposure to inherent ML/TF risks associated with crowdfunding platforms.

Fintech/RegTech

An increased number of competent authorities expressed particular concerns about the provision of financial products and services through Fintech firms that do not fall within the scope of the AML/CTF legislation. Competent authorities indicated they were concerned about Fintech firms lack of understanding of their AML/CTF obligations. They also highlighted risks arising from the use of RegTech solutions by obliged entities, including remote onboarding.

In particular competent authorities perceived an over-reliance by those obliged entities on outsourcing their AML/CTF compliance to RegTech providers, without putting in place adequate safeguards to ensure that the use of RegTech solutions does not affect their ability to comply with their AML/CTF obligations.

Terrorist financing

Competent authorities continue to be concerned about the weaknesses in firms’ CTF systems and controls. Credit institutions, payment institutions, bureau de change, e-money institutions and credit providers are the sectors that appear to be most vulnerable to this risk.

De-risking

Practice of de-risking continues to pose ML/TF risks, in particular because customers affected by de-risking may resort to alternative payment channels in the EU and elsewhere to meet their financial needs. As a result, transactions may no longer be monitored, making the detection and reporting of suspicious transactions and, ultimately, the prevention of ML/TF more difficult.

COVID19

Several COVID-19 associated risks are relevant from an AML/CFT perspective. The reduction in some firms’ revenues as a result of the pandemic may for instance have had a negative impact on the firms’ AML/CFT compliance. Furthermore, an increased on-boarding of customers remotely due to restrictions on movement by firms, which may not be accustomed to remote on-boarding otherwise, may expose the financial sector to additional ML/TF risks. Since the start of COVID-19 pandemic, firms had to adapt quickly and there are concerns that some might not be sufficiently well equipped to mitigate resulting ML/TF risks effectively. The current pandemic also gave rise to new crime typologies, such as misuse of government funds.

Tax-related crimes

The EBA has observed significant divergence across the EU in terms of what practices are considered tax crimes under national laws. Furthermore, while cooperation with tax authorities seems to take place in some cases, a formal protocol for cooperation is still lacking in some Member States to ensure a sound exchange of information between AML/CFT supervisors and their counterparts in tax authorities.

Supervisory divergence

The EBA notes that competent authorities’ approaches to assessing ML/TF risk in the sectors under their supervision remain inconsistent across the EU and many competent authorities appear to find it difficult to supervise their sectors in line with a risk-based approach. There is risk that, in absence of adequate risk assessments, CAs may fail to identify, and act upon, ML/TF risks to which their sector is exposed.

JOINT ESAs WARNING ON VIRTUAL CURRENCIES

On 17 March 2021 three ESAs issued a joint warning to remind consumers that virtual currencies (VCs) can be extremely risky and are usually highly speculative. When buying VCs, or financial products giving consumers direct exposure to VCs, consumers are exposed to a number of risks, including those identified above and described below.

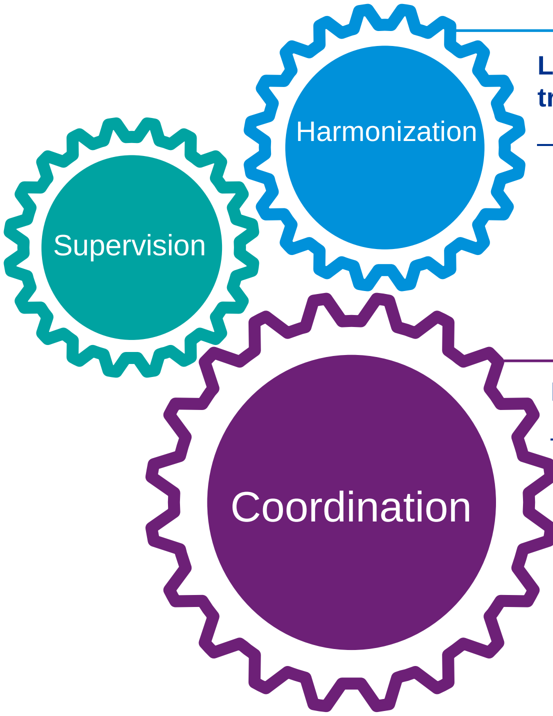
Why is it risky for consumers to buy VCs?

Operational disruptions – Some VC exchanges have suffered severe operational problems, such as trading disruptions. During these disruptions, consumers have been unable to buy and sell VCs at the moment they intended to and have suffered losses due to the price fluctuation of VCs held during the period of disruption.

Unsuitability of VCs for most purposes, including investment or retirement planning – The high volatility of VCs, the uncertainty about their future and the unreliability of the VC exchange platforms and wallet providers makes VCs unsuitable for most consumers, including those with a short-term investment horizon, and especially those pursuing long-term goals like saving for retirement. the training be executed / held, and when shall the training occur.

If consumers decide to buy VCs or financial products giving direct exposure to VCs, they should be aware that buying VCs from a firm regulated for financial services does not mitigate the above risks.

UPCOMING EU AML PACKAGE 2021



Less fragmentation in transposition at national level.

— This calls for greater harmonization in the application of certain rules by gatekeepers.

Enhanced supervision at EU level while not replacing national supervision.

Better coordination of FIUs.

— Cooperation between national FIUs could be supported at EU level, e.g. in helping them carry out joint analysis, through the development of standards for reporting suspicious transactions, or by providing information technology (IT) assistance and support for exchanging financial information.

In March 2021, European Parliamentary Research Service (EPRS) published the briefing, which presents the forthcoming Commission proposal as well as the opinions of relevant EU Institutions and stakeholders.

What is expected from the AML Package?

- A single EU rulebook to define the customer due diligence requirements to be applied by obliged entities throughout the internal market.
- EU-level supervision consisting of a hub and spoke model – i.e. supervisor at the EU level competent for direct supervision of certain financial institutions (FIs), indirect supervision/coordination of the other FIs, and a coordination role for supervising the non-financial sector as a first step.
- A coordination and support mechanism for Member State FIUs.

OUTCOMES OF THE FATF PLENARY 2021

February 2021
New jurisdictions subject to increased monitoring: Burkina Faso, the Cayman Islands, Morocco and Senegal.

March 2021
Public consultation launched on FATF draft guidance on a risk-based approach to virtual assets and virtual asset service providers.

March 2021
Public Consultation launched on FATF Guidance on Proliferation Financing Risk Assessment and Mitigation.

March 2021
FATF published Guidance on Risk-Based Supervision.

April 2021
FATF's mutual evaluation report of New Zealand.

June 2021
An update to the FATF Guidance for virtual Assets and VASPs.

June 2021
New guidance on proliferation of weapons of mass destruction.

The second Plenary of the FATF under the German Presidency of Dr Marcus Pleyer took place on 22, 24 and 25 February.2021.

The FATF approved new guidance to help improve effective, risk-based supervision. Effective supervisors ensure that regulated entities comply with their AML/CFT obligations and take appropriate action if those entities fail to do so.

The FATF has agreed to release an update to the FATF guidance for virtual assets and VASPs for public consultation. Feedback from the consultation will inform the final guidance which the FATF expects to approve in June 2021.

The FATF released the guidance for public consultation on proliferation financing risk assessment and mitigation in March before finalizing and approving it in June 2021.

How KPMG can help?

Our AML/CTF Services

AML Gap Analysis: We conduct a comprehensive review against national and/or international regulatory requirements and common practice noted in the industry. Recommendations are made for any deficiencies and gaps identified.

Enterprise-Wide Risk Assessment: We establish a detailed money laundering risks assessment framework, including but not limited to the allocation of risk weights used, and the determination of the applicable risk indicators.

AML system development and/or enhancement: Based on the findings of regulatory inspections, we can help you to develop rectification plan(s) and action items to enhance the effectiveness of the AML controls and processes.

AML/CTF Training: We are ready to design and deliver tailored and focused AML/CTF training programs aimed at various level of the staff complement within the organization.

Thematic reviews: We conduct a targeted, detailed deep-dive review of a specific components within your AML/CTF Framework, e.g. CDD standards and customer risk assessment framework and similar.

Transaction Monitoring: We are ready to conduct a full review of your existing transaction monitoring program, through analysis of your business model in relation to you requirements, regulatory expectations, and standard industry practices.

Why KPMG's AML Services?

- Strong AML Advisory practice
- Track record of AML/CFT assessment-related work
- Integrated team of professionals
- Relevant industry experience

If you have any questions, please let us know

Povilas Akstinas

Director

KPMG Baltics, Lithuania

E: pakstinas@kpmg.com

Vitalija Liktorė

Manager

KPMG Baltics, Lithuania

T: +370 60 840 465

E: vliktore@kpmg.com

Rūta Bajarūnaitė

Senior

KPMG Baltics, Lithuania

T: +370 61 676 074

E: rbajarunaite@kpmg.com

kpmg.com/socialmedia