Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance)

DIRECTIVE (EU) 2018/843 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 30 May 2018

amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank[(1)],

Having regard to the opinion of the European Economic and Social Committee[(2)],

Acting in accordance with the ordinary legislative procedure[(3)],

Whereas:

(1) Directive (EU) 2015/849 of the European Parliament and of the Council[(4)] constitutes the main legal instrument in the prevention of the use of the Union financial system for the purposes of money laundering and terrorist financing. That Directive, which had a transposition deadline of 26 June 2017, sets out an efficient and comprehensive legal framework for addressing the collection of money or property for terrorist purposes by requiring Member States to identify, understand and mitigate the risks related to money laundering and terrorist financing.

(2) Recent terrorist attacks have brought to light emerging new trends, in particular regarding the way terrorist groups finance and conduct their operations. Certain modern technology services are becoming increasingly popular as alternative financial systems, whereas they remain outside the scope of Union law or benefit from exemptions from legal requirements, which might no longer be justified. In order to keep pace with evolving trends, further measures should be taken to ensure the increased transparency of financial transactions, of corporate and other legal entities, as well as of trusts and legal arrangements having a structure or functions similar to trusts (‘similar legal arrangements’), with a view to improving the existing preventive framework and to

Status: *EU Directives are being published on this site to aid cross referencing from UK legislation. After exit day no further amendments will be applied to this version.*

more effectively countering terrorist financing. It is important to note that the measures taken should be proportionate to the risks.

(3) The United Nations (UN), Interpol and Europol have been reporting on the increasing convergence between organised crime and terrorism. The nexus between organised crime and terrorism and the links between criminal and terrorist groups constitute an increasing security threat to the Union. Preventing the use of the financial system for the purposes of money laundering or terrorist financing is an integral part of any strategy addressing that threat.

(4) While there have been significant improvements in the adoption and implementation of Financial Action Task Force (FATF) standards and the endorsement of the work of the Organisation for Economic Cooperation and Development on transparency by Member States in recent years, the need to further increase the overall transparency of the economic and financial environment of the Union is clear. The prevention of money laundering and of terrorist financing cannot be effective unless the environment is hostile to criminals seeking shelter for their finances through non-transparent structures. The integrity of the Union financial system is dependent on the transparency of corporate and other legal entities, trusts and similar legal arrangements. This Directive aims not only to detect and investigate money laundering, but also to prevent it from occurring. Enhancing transparency could be a powerful deterrent.

(5) While the aims of Directive (EU) 2015/849 should be pursued and any amendments to it should be consistent with the Union's ongoing action in the field of countering terrorism and terrorist financing, such amendments should be made having due regard to the fundamental right to the protection of personal data, as well as the observance and application of the proportionality principle. The Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions entitled 'The European Agenda on Security' indicated the need for measures to address terrorist financing in a more effective and comprehensive manner, highlighting that the infiltration of financial markets allows for the financing of terrorism. The European Council conclusions of 17-18 December 2015 also stressed the need to take rapidly further action against terrorist financing in all domains.

(6) The Communication from the Commission to the European Parliament and to the Council entitled 'Action Plan for strengthening the fight against terrorist financing' underscores the need to adapt to new threats and to amend Directive (EU) 2015/849 accordingly.

(7) Union measures should also accurately reflect developments and commitments undertaken at international level. Therefore, UN Security Council Resolution (UNSCR) 2195 (2014) on Threats to international peace and security and UNCSRs 2199(2015) and 2253(2015) on Threats to international peace and security caused by terrorist acts, should be taken into account. Those UNSCRs deal with, respectively, the links between terrorism and transnational organised crime, preventing terrorist groups from gaining access to international financial institutions and expanding the sanctions framework to include Islamic State in Iraq and Levant.

(8) Providers engaged in exchange services between virtual currencies and fiat currencies (that is to say coins and banknotes that are designated as legal tender and electronic money, of a country, accepted as a medium of exchange in the issuing country) as well as custodian wallet providers are under no Union obligation to identify suspicious activity. Therefore, terrorist groups may be able to transfer money into the Union financial system or within virtual currency networks by concealing transfers or by benefiting from a certain degree of anonymity on those platforms. It is therefore essential to extend the scope of Directive (EU) 2015/849 so as to include providers engaged in exchange services between virtual currencies and fiat currencies as well as custodian wallet providers. For the purposes of anti-money laundering and countering the financing of terrorism (AML/CFT), competent authorities should be able, through obliged entities, to monitor the use of virtual currencies. Such monitoring would provide a balanced and proportional approach, safeguarding technical advances and the high degree of transparency attained in the field of alternative finance and social entrepreneurship.

(9) The anonymity of virtual currencies allows their potential misuse for criminal purposes. The inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without such providers. To combat the risks related to the anonymity, national Financial Intelligence Units (FIUs) should be able to obtain information allowing them to associate virtual currency addresses to the identity of the owner of virtual currency. In addition, the possibility to allow users to self-declare to designated authorities on a voluntary basis should be further assessed.

(10) Virtual currencies should not to be confused with electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council[(5)], with the larger concept of 'funds' as defined in point (25) of Article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council[(6)], nor with monetary value stored on instruments exempted as specified in points (k) and (l) of Article 3 of Directive (EU) 2015/2366, nor with in-games currencies, that can be used exclusively within a specific game environment. Although virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications such as means of exchange, investment, store-of-value products or use in online casinos. The objective of this Directive is to cover all the potential uses of virtual currencies.

(11) Local currencies, also known as complementary currencies, that are used in very limited networks such as a city or a region and among a small number of users should not be considered to be virtual currencies.

(12) Business relationships or transactions involving high-risk third countries should be limited when significant weaknesses in the AML/CFT regime of the third-countries concerned are identified, unless adequate additional mitigating measures or countermeasures are applied. When dealing with such cases of high-risk and with such business relationships or transactions, Member States should require obliged entities to

Status: *EU Directives are being published on this site to aid cross referencing from UK legislation. After exit day no further amendments will be applied to this version.*

apply enhanced customer due diligence measures to manage and mitigate those risks. Each Member State therefore determines at national level the type of enhanced due diligence measures to be taken with regard to high-risk third countries. Those different approaches between Member States create weak spots on the management of business relationships involving high-risk third countries as identified by the Commission. It is important to improve the effectiveness of the list of high-risk third countries established by the Commission by providing for a harmonised treatment of those countries at Union level. That harmonised approach should primarily focus on enhanced customer due diligence measures, where such measures are not already required under national law. In accordance with international obligations, Member States should be allowed to require obliged entities, where applicable, to apply additional mitigating measures complementary to the enhanced customer due diligence measures, in accordance with a risk based approach and taking into account the specific circumstances of business relationships or transactions. International organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing may call for the application of appropriate countermeasures to protect the international financial system from the ongoing and substantial risks relating to money laundering and terrorist financing emanating from certain countries. In addition, Member States should require obliged entities to apply additional mitigating measures regarding high-risk third countries identified by the Commission by taking into account calls for countermeasures and recommendations, such as those expressed by the FATF, and responsibilities resulting from international agreements.

(13) Given the evolving nature of threats and vulnerabilities relating to money laundering and the financing of terrorism, the Union should adopt an integrated approach on the compliance of national AML/CFT regimes with the requirements at Union level, by taking into consideration an effectiveness assessment of those national regimes. For the purpose of monitoring the correct transposition of the Union requirements in national AML/CFT regimes, the effective implementation of those requirements and the capacity of those regimes to achieve an effective preventive framework, the Commission should base its assessment on the national AML/CFT regimes, which should be without prejudice to assessments conducted by international organisations and standard setters with competence in the field of preventing money laundering and combating terrorist financing, such as the FATF or the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism.

(14) General purpose prepaid cards have legitimate uses and constitute an instrument contributing to social and financial inclusion. However, anonymous prepaid cards are easy to use in financing terrorist attacks and logistics. It is therefore essential to deny terrorists this means of financing their operations, by further reducing the limits and maximum amounts under which obliged entities are allowed not to apply certain customer due diligence measures provided for by Directive (EU) 2015/849. Therefore, while having due regard to consumers' needs in using general purpose prepaid instruments and not preventing the use of such instruments for promoting social and financial inclusion, it is essential to lower the existing thresholds for general

purpose anonymous prepaid cards and to identify the customer in the case of remote payment transactions where the transaction amount exceeds EUR 50.

(15) While the use of anonymous prepaid cards issued in the Union is essentially limited to the Union territory only, that is not always the case with similar cards issued in third countries. It is therefore important to ensure that anonymous prepaid cards issued outside the Union can be used in the Union only where they can be considered to comply with requirements equivalent to those set out in Union law. That rule should be enacted in full compliance with Union obligations in respect of international trade, especially the provisions of the General Agreement on Trade in Services.

(16) FIUs play an important role in identifying the financial operations of terrorist networks, especially cross-border, and in detecting their financial backers. Financial intelligence might be of fundamental importance in uncovering the facilitation of terrorist offences and the networks and schemes of terrorist organisations. Due to a lack of prescriptive international standards, FIUs maintain significant differences as regards their functions, competences and powers. Member States should endeavour to ensure a more efficient and coordinated approach to deal with financial investigations related to terrorism, including those related to the misuse of virtual currencies. The current differences should however not affect an FIU's activity, particularly its capacity to develop preventive analyses in support of all the authorities in charge of intelligence, investigative and judicial activities, and international cooperation. In the exercise of their tasks, FIUs should have access to information and be able to exchange it without impediments, including through appropriate cooperation with law enforcement authorities. In all cases of suspected criminality and, in particular, in cases involving the financing of terrorism, information should flow directly and quickly without undue delays. It is therefore essential to further enhance the effectiveness and efficiency of FIUs, by clarifying the powers of and cooperation between FIUs.

(17) FIUs should be able to obtain from any obliged entity all the necessary information relating to their functions. Their unfettered access to information is essential to ensure that flows of money can be properly traced and illicit networks and flows detected at an early stage. The need for FIUs to obtain additional information from obliged entities based on a suspicion of money laundering or financing of terrorism might be triggered by a prior suspicious transaction report reported to the FIU, but might also be triggered through other means such as the FIU's own analysis, intelligence provided by competent authorities or information held by another FIU. FIUs should therefore in the context of their functions be able to obtain information from any obliged entity, even without a prior report being made. This does not include indiscriminate requests for information to the obliged entities in the context of the FIU's analysis, but only information requests based on sufficiently defined conditions. An FIU should also be able to obtain such information on a request made by another Union FIU and to exchange the information with the requesting FIU.

(18) The purpose of the FIU is to collect and analyse the information which they receive with the aim of establishing links between suspicious transactions and underlying criminal activity in order to prevent and combat money laundering and terrorist financing,