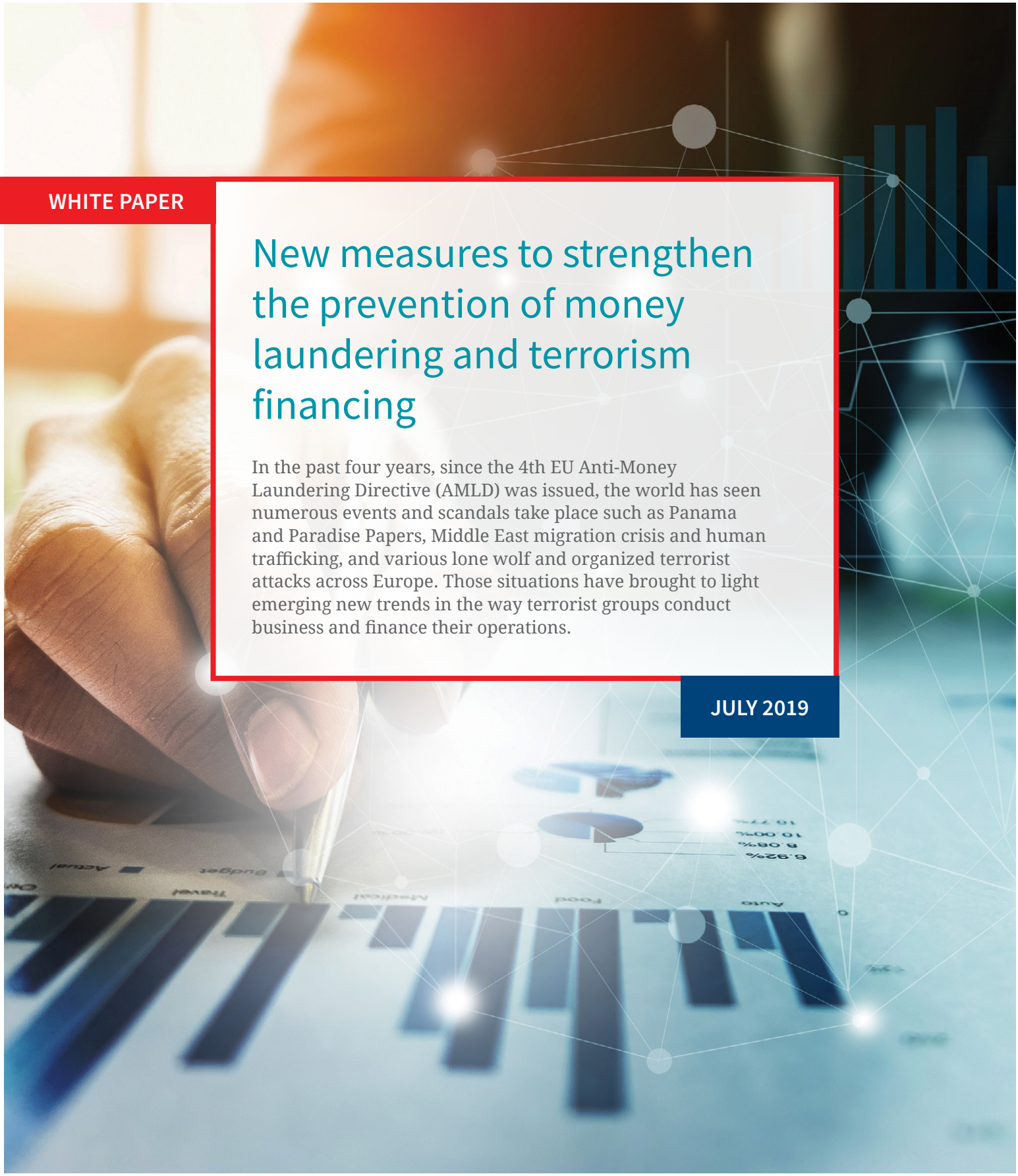
LexisNexis®
RISK SOLUTIONS



WHITE PAPER

# New measures to strengthen the prevention of money laundering and terrorism financing

In the past four years, since the 4th EU Anti-Money Laundering Directive (AMLD) was issued, the world has seen numerous events and scandals take place such as Panama and Paradise Papers, Middle East migration crisis and human trafficking, and various lone wolf and organized terrorist attacks across Europe. Those situations have brought to light emerging new trends in the way terrorist groups conduct business and finance their operations.

JULY 2019

# 5TH EU ANTI-MONEY LAUNDERING DIRECTIVE

Increasingly, modern technology is being used as an alternative to traditional financial systems. The 5th EU Anti-Money Laundering Directive (AMLD) introduces new measures that will ensure increased transparency and strengthen preventive frameworks to counter money laundering and the financing of terrorism.

On May 30, 2018, in response to the frequency of terrorist attacks and money laundering scandals, European Parliament and the Council have adopted the 5th AMLD that was published in the *Official Journal of the EU* on June 19, 2018. Member States are required to align their national legislation by January 10, 2020.

The main goal was to strengthen existing measures and to fight terrorism financing while keeping pace with technology and typologies that have emerged in the period between the 4th and 5th AMLDs.

Amendments to the 4th AMLD brought stricter rules and expanded its requirements to new obligated entities. New rules will:

- Prevent anonymous use of virtual currencies
- Limit use of prepaid cards
- Increase transparency of financial transactions, corporate and other legal entities as well as trusts and similar legal arrangements and transparency on beneficial ownership
- Strengthen the monitoring of transactions with high-risk countries
- Fortify the Financial Intelligence Unit (FIU) network
- Centralize data retrieval systems (central registers or central electronic data retrieval systems that facilitate identification)

Soon after the 5th AMLD was published, European Parliament and the Council have adopted a new 6th AMLD, published in the *Official Journal of the EU* on November 12, 2018. Those amendments are focused on criminal law provisions, and consequently sanctions, and will enable cross-border judicial and police cooperation, and jurisdictions cooperation terms.

## Seven Key Principles of the 5th AMLD

### 1 New Obligated Entities

Amendments in the 5th AMLD have included new obligated businesses to be registered and monitored by member states:

- providers engaged in exchange services of virtual and fiat currencies,
- custodian wallet providers and
- extension of existing groups:
  - to auditors, external accountants, tax advisors and any other person that undertakes to provide, directly or by means of other persons to which that other person is related, material aid, assistance or advice on tax matters as principal business or professional activity
  - high value goods—extension to intermediaries
    - estate agents including when acting as intermediaries in the letting of immovable property (only in relation to transactions for which the monthly rent amounts to EUR 10.000 or more)
    - persons trading or acting as intermediaries in the trade of works of art, including when this is carried out by art galleries and auction houses (in which the value of the transaction or a series of linked transactions amounts to EUR 10.000 or more)
    - persons storing, trading or acting as intermediaries in the trade of works of art when this is carried out by free ports (in which the value of the transaction or a series of linked transactions amounts to EUR 10.000 or more)

Recent typologies have shown that these businesses are widely exposed to financial crime. They have been used in all three phases of money laundering and in terrorism financing activities, especially virtual currency exchanges and custodian wallet providers. The anonymity of virtual and fiat currencies enabled criminals to move funds cross border without Suspicious Transaction Reports (STRs) being generated.

Virtual currencies are frequently used as means of payment, but they can also be used as means of exchange, investment, store-of-value products or in online casinos. With the number of users expanding daily, it was crucial to set up a monitoring process so all AML/CTF risks would be assessed and controlled.

FATF had issued a report on Key Definitions and Potential AML/CTF risks after conducting research and making preliminary assessment of the money laundering and terrorism financing risks associated with virtual currencies. Key risks they have identified were anonymity in trade, limitation in identification and verification of participants, lack of central oversight body and lack of clarity with regard to responsibility for AML/CTF compliance, supervision and enforcement for transactions that are segmented across several countries.

So far, providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers weren't under Union's obligation to identify suspicious activity. Because of the lack of identification and verification processes, terrorist groups had been able to transfer money into the EU financial system without exchange providers knowing if their customers were sanctioned or high-risk individuals as much as they weren't aware of the source of their funds. So, the 5th AMLD should, through competent authorities, monitor the use of virtual currencies in order to prevent money laundering and terrorism financing. However, monitoring of virtual currencies exchange service providers and custodian wallets will not entirely prevent potential misuses for criminal purposes. Because users can transact without such providers, the large part of the virtual currency environment will

remain anonymous. The 5th AMLD is addressing the possibility of allowing users to self-declare to designated authorities on a voluntary basis so the risk of anonymity in virtual currency trade could be better controlled.

### 2 New Risk Factors

The 4th AMLD is addressing the importance of applying a risk-based approach while performing risk assessments. To help obligated entities set the best risk scoring system and perform risk assessment, European Supervisory Authorities have issued Guidelines on risk assessment. The 5th AMLD continues addressing the importance of inclusion of various risk factors and variables.

There are new risk factors with regard to transactions related to oil, arms, precious metals, tobacco products, cultural artifacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species.

### 3 Increased Transparency on Trusts, Member States Cooperation and Data Centralization

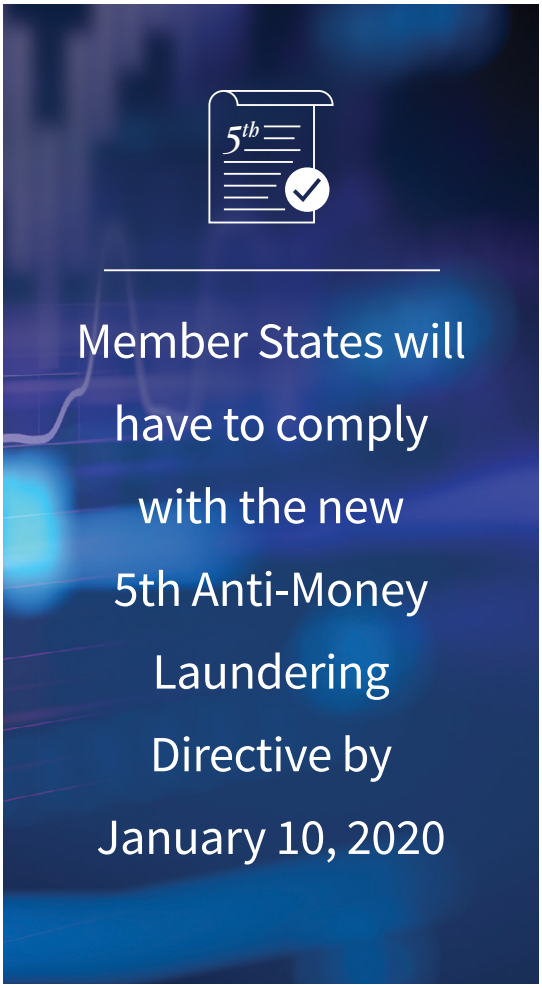
Due to lack of transparency and differences in legal systems of Member States, certain trusts and similar legal arrangements are not registered or monitored anywhere in the EU. The 5th AMLD states that "beneficial ownership information of trusts and similar legal arrangements should be registered where the trustees of trusts and persons holding equivalent positions in similar legal arrangements are established or where they reside."

In order to make their monitoring as efficient as possible, it is necessary for Member States to cooperate. In more detail, their Ultimate Beneficial Owners (UBO) registers with data of trusts, UBOs would be accessible and would ensure multiple registration of the same trusts. Access to beneficial ownership information of trusts should be granted to anyone able to demonstrate a legitimate interest or who files a written request in relation to a trust that holds or owns a controlling interest in any corporate or other legal entity incorporated outside the EU. In addition, each Member State shall identify the trusts or similar legal arrangements, considering that similar legal arrangements may have different legal characteristics throughout the Union. Coherent legal framework is being established to ensure better access to information related to beneficial ownership of trusts, purely for the purpose of preventing money laundering and terrorist financing, but also having in mind the data subjects' fundamental rights.

By January 20, 2020, all Member States should set up beneficial ownership registers for corporations and other legal entities, while the deadline for trusts and similar legal arrangements is set to March 10, 2020. By the same date, Central registers should be interconnected via the ECP (European Central Platform). By September 10, 2020, Member States should set up centralized automated mechanisms allowing the identification of holders of bank and payment accounts and safe deposit boxes.

## 4 Public Registers of Beneficial Owners

The previous legislation was the first initiative to increase transparency to tackle financial crime and tax evasion, however the 5th AMLD is putting even more scrutiny on beneficial owners and Member States to increase transparency. The 5th AMLD states that EU citizens will be granted access to beneficial ownership records. The general public shall be permitted to access general data such as name, month and year of birth, county of residence and nationality of the beneficial owner. It shall also be visible what type (what nature or interest held) of beneficial owner certain individual is. Member States will determine by local legislation whether they might provide access to additional information enabling the identification of the beneficial owner (date of birth or contact details), in accordance with data protection rules.




Registers should clearly state when a person is identified as beneficial owner only and not through ownership interest held or control exercised by other means.

GDPR-wise, the fair balance between general public interest in the prevention of money laundering and terrorist financing and data subject's fundamental rights is crucial. The set of publicly available data of beneficial owners should be of general nature: limited and clearly defined. In order to protect identified individual's privacy, Member States should be able to provide exemptions to the disclosure through the registers and to access such information in some extremely risky exceptional circumstances (e.g. in which such information would expose individuals to a disproportionate risk of violence, fraud or intimidation). Member States are left to consider if it's appropriate to make data of requestor and their legal grounds on beneficial owner's data available to the beneficial owner. Data access criteria and definition of legitimate interest will be further governed by the law of each Member State.

It will be possible for Member States to require a payment for access to the register. Data on beneficial ownership should be available within the registers for at least five years after the grounds for registration no longer exist. It is expected that public access to these records will help prevent the misuse of legal

entities for money laundering and terrorist financing purposes.

### 5 Enhanced Due Diligence (EDD) on High-Risk Countries

At present, Member States can determine their own levels of EDD measures towards riskier countries, which could potentially create deficiencies in managing relationships with entities in those territories.

The 5th AMLD proposes a standardized approach to treatment of those relationships throughout the EU. Enhanced due diligence measures to be applied require obligated entities to obtain additional information on the customer and the beneficial owner; on the intended nature of the business relationship; on the source of funds and wealth of both customer and beneficial owner and on the reason for transaction that is about to be performed.

Furthermore, senior management's approval should be obtained in order to establish or continue the business relationship. Also, an obligated entity should conduct enhanced monitoring of such business relationships by increasing the number and timing of controls that are being applied and selecting patterns of transactions that need to be further examined.

Member States can choose if they want to require obligated entities to ensure that the first payment is carried out through an account in the customer's name with a credit institution satisfying due diligence standards not less than those required per the 5th AMLD.

Member States shall require the performing of one or more additional measures to mitigate the risk related to person or legal entity carrying out transactions involving a high-risk Third World country:

- the application of additional elements of enhanced due diligence
- the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions
- the limitation of business relationships or transactions with natural persons or legal entities from the third countries identified as high-risk countries

The list of checks necessary to perform on high-risk countries is unified, and the Commission will include Third World countries with low transparency on beneficial ownership information, no appropriate sanctions or those that are less willing to cooperate in the exchange of information.

### 6 Pre-Paid Cards Thresholds

With lack of access to traditional banking, terrorism financing has moved to alternative payments methods, such as pre-paid cards. To reduce financial crime associated with pre-paid cards, the new Directive sets the threshold for transactions on such instruments on a monthly basis and reduced it to EUR 150. The maximum amount of money stored is also not to exceed this amount.

The Member States will have an option to allow anonymous use of such cards only when the pre-paid card is used in store for a maximum transaction of EUR 150, or a maximum transaction online of EUR 50. Anonymous prepaid cards issued outside of EU can be used only where they can be considered compliant to standards set out in the 5th AMLD.

### 7 Enhanced Powers of Financial Intelligence Units (FIUs)

FIUs will have access to more information through centralized bank systems as well as payment account registers or data retrieval systems. The Member States will be able to cooperate more easily through creating centralized automated mechanisms. FIUs should exchange information spontaneously or upon request, aiming to further increase transparency and improve the identification of account holders.

## The Need for an Increased Risk-Based Approach

Member States will have to bring into force the laws, regulations and administrative provisions necessary to comply with the 5th AMLD by January 10, 2020. As previously mentioned, the 6th AMLD was already adopted on October 23, 2018 and published in the *Official Journal of the EU* on November 12, 2018. Member States will have to comply with the new Directive by December 3, 2020.

The Directive showcases the need for an increased risk-based approach. With this, we are entering a new era of regulatory oversight, which will keep up the pace with today's ever-changing environment. The inclusion of virtual currencies, more pressure on services providing pre-paid cards, pressure on countries to take more responsibility in transparency and on FIUs to enhance their due diligence processes are all factors driving the change in how we continue to bank.

After the 3rd AMLD was introduced, it took a further 10 years for the 4th AMLD to come into action, but the rapid acceleration of changes in regulation calls for faster response to events surrounding us. With the evolving nature of threats, the EU is basing their assessments on international organizations and standard setters such as the FATF, in order to counter money laundering and financing of terrorism. It remains to be seen how quickly we can expect new changes to the just-adopted 6th AMLD, and on what those amendments will focus. Perhaps they will be driven by further technological developments and new challenges in the prevention of financial crimes.

To learn more, visit risk.lexisnexis.com/EMEA


## About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.