# REFINITIV'S RESPONSE TO THE EU'S AML ACTION PLAN CONSULTATION

**Prepared by** Che Sidanius
Global Head of Financial Crime and Industry Affairs

*Thanks for the invaluable input from Phil Cotter, Vivienne Artz, James Mirfin, John Cowling, Ernst Pienaar and Jan Eger*

REFINITIV®
DATA IS JUST THE BEGINNING®

## It's time we inform policy makers on what we already know. The anti-financial crime regime doesn't work.

For practitioners, the following statistic is well-known: Less than 1% of global illicit financial flows is being seized and frozen.[1] Europe is aiming to take radical action as policy makers now acknowledge that the global and pervasive nature of financial crime is increasingly affecting a wide range of EU sectors while criminals effectively adopt technologies to target our communities in the pursuit of illicit profits with devastating societal effect. Over 40 million people are estimated to be victims of modern-day slavery globally today. That should be a shocking number by itself. However, this is not just about today. Financial crime has an insidious impact on future generations. Criminals don't pay tax, so $1 billion of missing tax revenues could be invested in school systems and pay for 150,00 toddlers to have a high-quality education in Spain or employ 64,000 teachers in Poland, for example.[2] In other words, these are not just issues that concern EU policy makers who are committed to more effective means to combat financial crime, but they should be adopted as priorities that affect us all.

**Over 40 million people** are estimated to be victims of modern-day slavery globally today.

1 https://www.unodc.org/unodc/en/frontpage/2011/October/illicit-money_-how-much-is-out-there.html
2 https://www.refinitiv.com/en/resources/special-report/true-cost-of-financial-crime-global

The EU's 5th Anti-Money Laundering (AML) Directive rightfully extends the scope of the requirements to other sectors including crypto-assets and custodian wallet providers, estate agents and art dealers, to name a few. It also places greater emphasis on transparency in ultimate beneficial ownership as part of a focused attempt to fight back against criminals who hide behind complex and opaque corporate structures which are otherwise shrouded in secrecy. In addition, the 5th AMLD requires Member States to create functional Politically Exposed Person lists that include titles, roles or functions of individuals deemed to be politically exposed.

Despite these efforts, only five Member States are said to have met the deadlines to transpose AMLD5.[3] The European Commission now aims for a comprehensive Union policy on preventing money laundering and terrorism financing by converting the provisions of the 5th AML Directive into a regulation, thereby directly transposing these provisions into national law. On May 7, 2020, it published an unprecedented "AML Action Plan" to address a number of shortcomings: First, it recognizes that the complexity of the Union's financial system has opened the door to new financial crime risks. Second, the EU rightfully focuses on effectiveness as it delivers better enforcement of existing rules and strengthens its role as a world leader in the fight against financial crime. Thus far, legislative measures have aimed to broaden regulatory requirements. However, the central tenant of measuring effectiveness has, historically, been lost. To date, the discussion around AML rules has been unhelpfully transfixed on the choices around a "risk-based" approach (i.e., a flexible but tough to manage) versus a "rules-based" approach (inflexible but easier to manage). This is a false choice and focuses on input frameworks rather than on outputs (i.e., policy effectiveness).

Furthermore, the interaction of other regulatory efforts, such as the implications of how money laundering can trigger the winding-up of a bank under the Bank Recovery and Resolution Directive (Directive 2014/59/EU) and the uncertainty about the application of data protection rules in sharing information between public and private sectors internationally needs proper attention. The AML Action Plan aims to address these. These reforms are welcomed but more is needed to address the fact that only 2.3% of the estimated proceeds of crime are provisionally seized or frozen, 1.1% of the criminal profits are confiscated at the EU level.[4]

The collective experience of anti-financial crime practitioners suggests that the current model misaligns incentives. The regulatory approach focuses on technical compliance and control failures which lead to overreporting of suspicious activity. The ultimate aim, therefore, is not a reduction of money laundering, but on protecting the obligated entities' bottom line. According to a Refinitiv survey, 63% of respondents in the private sector are willing to take regulatory risks "in order to win new business."[5] Fundamentally there needs to be a change in approach to transform reactive financial crime "compliance" cultures into proactive "risk management."[6] To improve efficiency, organizations should increase organizational agility, deploy new technology, and improve partnerships with other risk-intelligence providers and the public sector. This entails expanding the legal and technical frameworks for fostering intelligence sharing; aligning incentives on the objective of reducing financial crime; and identifying and sharing best practices in integrating financial crime risk into risk management governance structures.

**1.1%**

of the criminal profits are confiscated at the EU level.

**63%**

of respondents in the private sector are willing to take regulatory risks "in order to win new business."

3 https://www.globalwitness.org/en/press-releases/only-handful-eu-countries-meet-key-money-laundering-deadline/
4 https://www.europol.europa.eu/print/newsroom/news/does-crime-still-pay%20and
5 https://www.refinitiv.com/en/resources/special-report/innovation-and-the-fight-against-financial-crime
6 https://rusi.org/publication/occasional-papers/deep-impact-refocusing-anti-money-laundering-modelevidence-and

## To ensure a more effective implementation of the rules, Refinitiv recommends the following to be considered:

1. Create a public-private sector "Working Group" to conduct regular assessments of the financial crime risks to the EU. This should include a cooperative framework with detailed analysis of what information concerning financial crime is currently collected and held by the public and private sectors so that a full picture of its levels is understood. This forum would also allow the sharing of best practices and highlight financial crime trends that are cross-cutting and involve law enforcement, AML policy makers, customs authorities, tax authorities, asset recovery offices and the private sector, including risk intelligence data providers. This Working Group could participate or feed into the existing European Commission Supranational Risk Assessment.
2. Develop key performance indicators (KPIs) in collaboration with the competent authorities and the private sector so that levels of financial crime – and, in turn, EU legislative actions – can be measured appropriately. Currently, assessing the effectiveness of AML policies is challenging, as scientific/comparable data on criminality is hard to collect and measure.
3. Reform suspicious transaction reporting (STR) – Financial crime statistics do not distinguish between different types of offenses and the data is dispersed over various industry sectors. Common formatting of how statistics are recorded is needed so that trends and actionable intelligence are more easily identifiable.
4. Financial investigation teams should be cross-cutting and horizontal so that they are able to recognize the interlinkages of criminal activity such as environmental crime, migrant smuggling, wildlife trafficking and the loss of biodiversity. We, at Refinitiv, call this "green crime."[7]

Turning the directive into a regulation, however, will only be effective if commensurate enforcement mechanisms are in place to ensure Member States properly prioritize these requirements and consider the fight against money laundering and terrorism financing as not just another compliance requirement, but as a necessity to safeguard the integrity of the EU's economic system. Some of the requirements which would benefit from becoming a regulation include:

1. Harmonize the whistleblower protection regimes. The protection of whistleblowers has been at the forefront of the G20 Anti-Corruption Working Group since 2010.[8] Of particular interest is to clarify the definition of a whistleblower and to agree on what constitutes protected communications and disclosures, and to encourage reporting by strengthening laws designed to deter retaliation.
2. Harmonize the recognition and standards around digital identity. Currently the landscape is fragmented and in need of a consistent approach to help greater levels of efficiency and security. This would accelerate the EU becoming an attractive, secure and dynamic data-agile economy and support wider policy objectives such as the "Digital Single Market," and the "EU Data Strategy." The work of the eIDAS Regulation is encouraged so that government-issued electronic identities can better address the patchwork of identity systems across the EU. Providing open access would accelerate the aim of eIDAS which is to enhance trust in electronic transactions in the internal market by providing a common framework for secure and efficient cross-border electronic interactions between citizens, business and the public sector. In addition to encouraging issuance of government-issued identities, it is recommended that the EU drives consistent adoption of the Financial Action Task Force (FATF) recommendations on Digital Identity across the EU.[9] Currently, there are a variety of verification identification processes using different documents and formats. There is also a variety of access rights with respect to public information that can be used for verification purposes. In some countries it is very open, in others it is very restrictive. Supporting the Digital Identity solutions that protect individual privacy and also enable identities to be verified through open source data, including a variety of government-issued documents (i.e., not just passports), is essential to the future of the fight against financial crime.

7 https://www.regulationasia.com/green-crime-a-global-challenge-requiring-a-global-response/
8 http://www.g20.utoronto.ca/2010/g20seoul-anticorruption.pdf
9 https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

3. Reforming the beneficial ownership registers is vital to enhance effective implementation of the rules. Global Witness, in its March 2020 report, reminds us that 63% (17 of 27) of the Member States do not yet have a centralized register with the beneficial owners of companies that is available to the public.[10] Knowing who ultimately owns or controls a firm is a necessity to properly assess the financial crime risks. Currently it is enormously challenging to identify companies that have been banned, censured or cited by sanctions authorities, which in turn makes it difficult for firms to understand their supply chain risks. Furthermore, where such registers do exist in Europe, their usability and accessibility are often limited by being behind a paywall. Legislative harmonization is urgently needed through a regulation to ensure completeness, consistency and accessibility in order to improve efficiency and effectiveness. The prerequisites to achieve these goals and interoperability require open access to data, minimum formatting and common data structures. A consistent approach should include full names of entities and individuals, dates of birth and other identification numbers that would be easily and freely accessible to obligated entities, and risk-intelligence data providers who support obligated entities for compliance purposes would be extremely helpful. This would also more easily allow the comingling of various data sources (e.g., EU sanctions, enforcement lists). There are several principles needed to make beneficial ownership data easy to use, accurate and interoperable:[11]
   a. Data should be accessible to the public and beneficial ownership should be defined in law
   b. Disclosure should comprehensively cover all types of legal entities and natural persons
   c. Information should be submitted in a timely manner and kept up to date
   d. Historic records should be kept and published
   e. Adequate enforcement measure should be taken against noncompliance
4. A renewed focus on how the EU General Data Protection Regulation (GDPR) can support the AMLD5 requirements is needed. The Action Plan rightfully raises concerns that both public and private sector organizations have identified limitations of information exchange and access to certain public owned registers, respectively. Through the important work of the EU AML Task Force lead by the Centre for European Policy Studies, the European Data Protection Supervisor (EDPS) helpfully indicated that data protection is not an obstacle in the fight against money laundering. GDPR (EU 2016/679) is intended to be enabling in nature, and it is not intended to block data processing and data sharing per se. In the case of fighting money laundering and financial crime more broadly, the legal bases for processing personal data include: The consent of the individual (GDPR Art. 6 (1) (a)); compliance with a legal obligation (GDPR Art. 6 (1) (c)); performance of a task in the public interest (GDPR Art. 6 (1) (e)); and processing in the legitimate interests of the data controller (GDPR Art. 6 (1) (f)). The breadth of processing grounds reflects the roles of both the public and private sector, including (i) obliged entities under the AMLD5 (ii) those entities which support and provide services to obliged entities to meet their obligations and (iii) financial markets infrastructure and other firms who perform the wide range of due diligence to identify and manage risks, and comply with an increasingly wide range of both reporting and transparency obligations such as modern slavery and environmental crime.

**63%**

(17 of 27) of the Member States do not yet have a centralized register with the beneficial owners of companies that is available to the public.

Given the global reality of the fight against financial crime, it is increasingly important that cooperation at the global level takes place to address key privacy issues such as the bases for processing data and the sharing of data, including criminal data and special category data, both within and external to the EU. One of the areas where Member States could help facilitate the fight against financial crime is through leveraging Article 23 of the GDPR to provide greater clarity around the processing grounds and scope of personal data in the context of financial crime. Financial crime is global in nature and obligations stem from a multitude of legal, regulatory, industry and international requirements including FATF, over 60 sanctions authorities, law enforcement, regulators and international commitments such as the UN Global Compact, to name a few. In addition, restrictions on international transfers both through privacy and localization measures, and the reality that many AML laws still require certain AML data to be held locally, create unhelpful restrictions that inhibit the ability to address the global threat posed by financial crime to individuals, firms and countries.

10 https://www.globalwitness.org/en/press-releases/only-handful-eu-countries-meet-key-money-laundering-deadline/
11 https://www.openownership.org/framework/

It is essential to ensure the effectiveness of the evolving approach to the fight against financial crime that privacy laws allow for appropriate information sharing and the use of innovative technological solutions to help identify and combat evolving financial crime risks. Financial crime extends well beyond the FATF definitions of "predicate offense." One such example is the focus on "green crime" which recognizes the intersection of criminal activity not defined as a predicate offense. Green crime raises awareness of the massive adverse impact that environmental and wildlife trafficking crimes have on peace and security, as well as the devasting consequences for biodiversity. Green crime is a global industry estimated to be worth up to $258 billion and not only harms the environment, but businesses, their supply chains and our health. The COVID-19 pandemic has been a watershed moment on this issue and has helped to highlight how the wildlife trade has many facets and implications, which are not confined to the impact on animals, but has also demonstrated how these actions can facilitate diseases leaping to humans. It is also reported to contribute to the sixth mass extinction. According to a survey conducted by Refinitiv of 3,138 managers, 81% said that data privacy restricts their ability to collaborate against financial crime.[12] The fight against financial crime should be considered as a "Data Space" as defined by the EDPS' paper "on the European strategy for data" and make it easier for businesses and public authorities to collaborate and access high-quality data.[13]

5. Harmonize and enhance cooperation not just between the financial intelligence units (FIUs), but also customs authorities, tax authorities, Asset Recovery Offices and law enforcement authorities. This is in keeping with the recommendations of the Council of Europe.[14]
6. Establish public-private partnerships to fight financial crime between competent authorities, private sector obligated entities and other third parties in the wider financial services ecosystem including risk intelligence providers, with the aim of informing a risk-based approach on material financial crime threats. Studies conducted by the Future of Financial Intelligence Sharing program demonstrate how these information sharing frameworks can improve the detection and prevention of criminal activity.[15]

**81%**

said that data privacy restricts their ability to collaborate against financial crime.

## How do we address the age of digitization and crime?

Digital products that involve payment transfers should be subject to proportionate screening obligations and be considered within the scope to the list of obligated entities. Europol points to increasing evidence that online platforms and digital assets are being used to launder money and to finance terrorist activities. At the EU level, there is no consistent recognition of know your customer (KYC) tools in an online environment. It is widely accepted that the rise of new digital financial products has meant that they are not immune to being exploited in the proliferation of financial crime. It has made it much easier for criminals to conceal the identity of the ultimate beneficial owner of a company or financial asset. If we look at instant payment systems, the possibility of fraud is evident without robust AML due diligence checks. According to the European Central Bank, the scale of fraud using credit and debit cards, for instance, amounts to €1.8 billion[16], 73% of it through the internet or the telephone, e.g.,"card-not-present". The same can be said of any digital payment product or payment platform that is built on anonymity.

12 https://www.refinitiv.com/en/resources/special-report/innovation-and-the-fight-against-financial-crime
13 https://edps.europa.eu/data-protection/our-work/publications/opinions/european-strategy-data_en
14 'Council conclusions on enhancing financial investigations to fight serious and organized crime', June 17, 2020
15 The Future of Financial Intelligence Sharing (FFIS) programme leads independent research into the role of public-private financial information-sharing partnerships to detect, prevent and disrupt crime
16 https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html#toc4

# €1.8 billion

73% resulted from card-not-present, i.e., payments via the Internet, post or telephone.

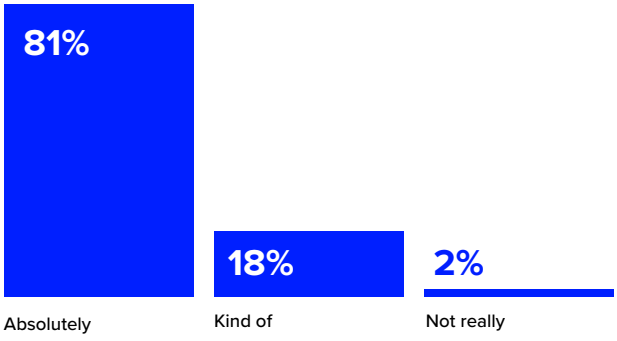
## We need stop treating financial crime as a compliance issue

The European Banking Authority's (EBA) role in working with the prudential supervisors in relation to identifying money laundering and terrorism financing risks in the context of the supervisory review and evaluation process is very welcome. There is a recognition that regulatory technical standards of the Capital Requirements Directive require competent authorities to consider money laundering risks across an increasingly wide range of areas such as governance and internal control, authorization, financial innovation and loan origination.[17] It is important to note that financial crime is not simply an issue of compliance; it also has significant consequences for financial stability and safeguarding citizen deposits. The possibility of a large financial institution becoming insolvent due to money laundering is real; it has the potential to become one of the most important sources of systemic risk in a Member State with significant ramifications to the rest of the EU. Therefore, the EU's capital regime, CRD IV, should explicitly consider financial crime risk by prudential supervisors as part of their assessment of a bank's operational risk framework.[18] This also means that there should be a harmonized approach and consistency of the subcategories belonging to operational risk and related losses. Out of seven of the EBA's internal risk taxonomies on operational risk, four are already directly related to fraud, negligence and failure to uphold a bank's fiduciary responsibilities. The EBA also recognizes that operational risk is only expected to increase in the near future. In 2018, the sum of just the five largest losses in operational risk is estimated to account for 2.1% of common equity (CET1) for EU banks, not including the loss of shareholder value overall. Operational risk capital levels should, however, not solely rely on negative enforcement (e.g., higher capital), but also contain positive incentives rewarding compliance practices and innovation (e.g., lower capital).

The focus on customer due diligence should also be aligned with the supply chain due diligence legislative package for the sustainability corporate governance area that is being considered by the European Commission. The COVID-19 pandemic presents an opportunity for the EU to position itself as a leader in promoting due diligence on environmental risks, including human rights violations, that should lead to a more sustainable economic model. Promoting more "stakeholder capitalism" with a focus on the "societal purpose" of the public and private sectors' fight against financial crime is warranted.

Through a survey conducted by Refinitiv of nearly 1,800 professionals, 65% are aware or suspect that their third parties may have been involved in illegal activities and 43% are not subject to any due diligence checks. Substantive additional policy actions are needed to accelerate the sustainability transition of the EU financial sector and the fight against financial crime also implicates environmental crime and biodiversity. In fact, according to a June 2020 poll, 81% agreed that "green crime," referencing environmental and wildlife crimes, should receive equal attention as money laundering and terrorist financing. The standard has already been set out in detail in the UN Guiding Principles on Business and Human Rights and the OECD's Due Diligence Guidance. It is now time for the EU to build on these precedents and harmonize these requirements. Not only will they provide much needed confidence by consumers, savers, retail investors and stakeholders that products and services are free from human rights abuses and environmental damage, but they will enhance the EU's reputation as a leader in promoting responsible business conduct.

**Do you agree that green crime is a threat to peace and security?**




**Source:** The Rise of Green Crime webinar
https://youtu.be/_wiUeQrTzVE

17 Article 8(2) of the Capital Requirements Directive

18 Operational risk means the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events

## How do we empower financial intelligence units?

Suspicious Transaction Reporting (STR): Obligated entities and regulators find the STR regime inadequate as it fails to deliver on investigative outcomes. Through the adoption of a regulation, there is an urgent need for common approaches and adoption. There is an Asian Development Bank initative to encourage a feedback loop between regulators, law enforcement/financial intelligence units and obligated entities that allows for common and relevant data to be shared across the EU with the aim of increasing actionable intelligence and improving benchmarking. This would allow organizations to understand the types of data needed to fight financial crime; enable resources to focus on materiality and risk; facilitate the development of better indicators and typologies; better cross-agency (domestic) and cross-border information sharing; and promote better public-private and private-private collaboration.

**65%**

are aware or suspect that their third parties may have been involved in illegal activities.

**43%**

are not subject to any due diligence checks.

The remit and powers of FIUs are currently not harmonized, which has an adverse impact on FIUs' ability to access and share relevant information. It has been reported that 97% of suspicious reporting from obligated entities is of no immediate value to FIUs while the annual volume of reporting is growing at 11% across major financial centers. Europol plays an essential role and is a well-recognized and respected agency internationally. Its legal and operational capability should be strengthened to enable Europol to provide the technical support and guidance to Member State FIUs as needed.

An intelligence-led approach is required to make the fight against crime more effective, and supervisors need to enable it. Law enforcement should take the lead, which requires it to have sufficient resources and expertise available. Europol, in particular, needs a stronger mandate and its legal framework should be adjusted to ensure it can perform its duties, as highlighted by the FIU.net case. The EDPS imposed a ban on Europol's personal data processing activities (based on concerns regarding individuals not considered as suspects) for the purposes of the technical administration of the FIU.net. Europol plays an essential role in the fight against financial crime, and the European Commission's priority should be to strengthen the operational capacity of Europol and, in particular, addressing limitations inherent in the sharing of information across law enforcement, competent authorities and FIUs is most welcome.

## Let's promote cross-border public and private sector collaboration

The emergence of an EU-wide public-private information sharing arrangement was previously called for by the European Parliament in its special committee reports and recommendations on tax and terrorism (TAX3 and TERR committees). Over recent years, it has been shown that public-private partnerships (PPPs) can provide for dynamic information sharing on financial crime risks between public and private sectors as evidenced in the Netherlands, the UK, the U.S., Australia, Hong Kong, Singapore and Canada. Other EU Member States that have recently announced similar arrangements include Germany, Austria and Sweden. The Future of the Financial Intelligence Sharing program states that "the public–private partnership model is delivering benefits in terms of increasing the value and responsiveness of suspicious activity reports and improving criminal justice outcomes; such as arrests, asset recovery other disruption of criminal networks."[19] It is also a vital component to improve the quality and accuracy of STRs while promoting a risk-based approach, rather than a compliance-based approach.

There is also an urgent need to promote a public-private sector forum at the policy level to discuss best practices, promote more effective mechanisms to identify emerging threats, identify pressure points in the current AML framework and propose tangible policy solutions to these. One such initiative is the Global Coalition to Fight Financial Crime, a unique consortium of organizations that represent the banking sectors, law enforcement, NGOs and other private sector actors[20]. This coalition shares financial crime trends, thought leadership and actively engages

19. https://www.future-fis.com/thought-leadership-in-partnership-development.html
20. https://www.gcffc.org

with AML authorities globally. This type of consortium was also an explicit policy recommendation by the Business20 (B20) in an upcoming report to the G20 that stresses the need for more partnerships between the public and private sectors in this area. Cross-border collaboration and coordination can and should be harnessed to promote integrity, root out corruption and build on current cross-border enforcement.

## The European Union needs a collective voice

The EU's active participation in global forums is strongly recommended. Financial crime is global by nature and so should be the response to fight financial crime. International collaboration is a prerequisite to fight crime more effectively. FATF is a key global standard setter and the European Commission should be given the task of representing the EU.

However, there are other additional international forums to consider including the G20, MONEYVAL, the Egmont Group and the Global Coalition to Fight Financial Crime. The Action Plan sets out an ambitious and a most welcomed road map to address issues that are global in nature. The policy actions to be considered by the European Commission include the following:

1. Enhance international standards of public registries to ensure completeness, consistency and accessibility. The prerequisites to achieve these goals and international interoperability of public registers require global minimum data standards, formatting and structure. According to research conducted by Refinitiv, out of the 237 jurisdictions in which companies can be incorporated, only 51% provide director information and only 57% disclose shareholders. In addition, where such registers do exist, their usability and accessibility are often limited by being behind a paywall. These standards should include:
   a. Data should be accessible to the public and beneficial ownership should be defined in law
   b. Disclosure should comprehensively cover all types of legal entities and natural persons
   c. Information should be submitted in a timely manner and kept up to date
   d. Historic records should be kept and published
   e. Adequate enforcement should exist for noncompliance
2. Support whistleblower programs, clarify international definitions and strengthen laws designed to deter retaliation. The protection of whistleblowers has been at the forefront of the G20 Anti-Corruption Working Group agenda since 2010. More recently, under the Japanese presidency in 2019, the G20 adopted the High-Level Principles for the Effective Protection of Whistleblowers. The EU should take steps to foster a robust information exchange between governments and the private sector and evaluate whistleblower protection frameworks.
3. Support a more consistent and international approach to digital identity standards recognition; leverage the work of FATF, and adopt their recommendations consistently across the EU.
4. Promote cross-border public-private partnerships that are cross-cutting and involve law enforcement, AML policy makers, customs authorities, tax authorities, asset recovery offices and the private sector, including risk intelligence data providers.
5. Promote a dialogue on how the application of global data protection legislations, which now cover over 60% of the world, can better support the fight against financial crime by helping to facilitate data sharing while respecting privacy obligations.
6. Reform international Suspicious Transaction Reporting (STR) regimes. There should also be a feedback loop between regulators, law enforcement/FIUs and obligated entities that allows for common data points to be shared across the EU, and increase actionable intelligence and improve benchmarking.
7. Create an international public-private sector working group to conduct regular assessments of the financial crime risks to the EU. This should include a cooperative framework with detailed analysis of what information concerning financial crime is currently collected and held by the public and private sectors so that a full picture of its levels is understood. This forum would also allow the sharing of best practices and highlight financial crime trends that are cross-cutting, and involve law enforcement, AML policy makers, customs authorities, tax authorities, asset recovery offices and the private sector, including risk intelligence data providers.
8. Support for lower-capacity countries should be strengthened so that they can fully action a risk-based approach. These countries may be less familiar with the flexibility provided by the FATF's revised 2012 methodology. For instance, when new digital products, such as mobile money, come to market, supervisors may not have the expertise to identify either the benefits these represent for financial inclusion or how to best manage any associated financial crime risks.

Refinitiv is one of the world's largest providers of financial markets data and infrastructure, serving over 40,000 institutions in approximately 190 countries. It provides leading data and insights, trading platforms, and open data and technology platforms that connect a thriving global financial markets community – driving performance in trading, investment, wealth management, regulatory compliance, market data management, enterprise risk and fighting financial crime.

Visit **refinitiv.com**

@Refinitiv Refinitiv

REFINITIV®

DATA IS JUST
THE BEGINNING®

RE1257904/8-20