EPIF response to the Commission's Consultation on an action plan for a comprehensive Union policy on preventing money laundering and terrorist financing

August 2020

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 190 authorised payment institutions and other non-bank payment providers as our members offering services in every part of Europe. **EPIF** thus represents roughly one third of all authorized Payment Institutions ("PI") in Europe. All of our members operate online. Our diverse membership includes a broad range of business models, including:

- Three-party Card Network Schemes
- E-Money Providers
- E-Payment Service Providers and Gateways
- Money Transfer Operators
- Acquirers
- Digital Wallets
- FX Payment Providers and Operators
- Payment Processing Services
- Card Issuers
- Independent Card Processors
- Third Party Providers
- Payment Collectors

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as a provider for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).

Response to Consultation

A. Ensuring effective implementation of the existing rules

Ensuring correct transposition and application of the EU anti-money laundering / countering the financing of terrorism rules is a priority for the Commission. The Commission adopted a tough approach in relation to the transposition of both the 4th and 5th Anti-Money Laundering Directives and launched or will soon launch infringement proceedings against Member States for failure to fully transpose these provisions.

The Commission monitors the effectiveness of Member States' anti-money laundering / countering the financing of terrorism frameworks in the context of the European Semester cycle. In 2020, 11 countries have seen their frameworks assessed

The European Banking Authority has seen its mandate recently strengthened, and is now responsible to lead, coordinate and monitor AML/CFT efforts in the financial sector. Among its new powers are the performance of risk assessments on competent authorities, the right to request national authorities to investigate individual institutions and adopt measures when breaches are detected. These new powers complement existing powers to investigate potential breaches of Union law.

This section aims to collect stakeholder views regarding the effectiveness of these measures and on whether other measures could contribute to strengthening the enforcement of anti-money laundering / countering the financing of terrorism rules.

1. How effective are the following existing EU tools to ensure application and enforcement of anti-money laundering / countering the financing of terrorism rules?

	Very effective	Rather effective	Neutral	Rather ineffective	Not effective at all	Don't know
Infringement proceedings for failure to transpose EU law or incomplete/incorrect transposition						x
Country-specific recommendations in the context of the European Semester						x
Action following complaint by the public						x
Breach of Union law investigations by the European Banking Authority						x
New powers granted to the European Banking Authority		x				

2. How effective would more action at each of the following levels be to fight money laundering and terrorist financing?

	Very effective	Rather effective	Neutral	Rather ineffective	Not effective at all	Don't know
At national level only				x		
At national level with financial support and guidance from the European Union			x			
At the level of the European Union (oversight and coordination of national action)		x				
At international level	x					
No additional action at any level					x	

3. **Should other tools be used by the EU to ensure effective implementation of the rules?**

EPIF generally supports the proposals by the European Commission to move to greater harmonization in the EU Anti-Money Laundering (AML) framework and would like to see part of the Directives turned into a maximum harmonization Regulation.

In building a new EU AML framework, EPIF calls on policymakers to focus on the following key areas:

- Reduce reporting burden by streamlining technology and the data elements, as well as standardising the reporting framework.
- Adoption of a risk based approach and a more principles-based and less prescriptive approach to fighting financial crime. Obliged entities must be able to use innovative techniques to mitigate AML risks.
- Move away from paper-based Know-Your-Customer (KYC) to online and innovative on boarding and KYC solutions building on e-ID. The rules should not stifle the incentives for industry to develop new technological solutions.
- An open approach to non-face-to-face and electronic KYC, taking into account the risk mitigation techniques.
- AML Frameworks should be used to support online and cross-border provision of payment services. Create legal certainty around the application of the GDPR. There needs to be legal certainty allowing obliged entities to meet their AML obligations without constraints while complying with the GDPR or any national regulations such as professional secrecy.
- Support the actions to facilitate information exchange between the FIUs, between the obliged entities and the public sector, as well as between private sector obliged entities.
- Not make a debate on new institutional arrangement in the EU a substitute for effective progress on the above priorities. Moreover, the Commission should define key goals and metrics to measure the effectiveness of AML legislation.

Compliance with AML regulations can be very costly. These costs include staffing for the Money Laundering Reporting Officer (MLRO), a Compliance Officer and operational staff; support functions such as engineering, information technology, data privacy, and third-party systems to enable screening and monitoring which is becoming increasingly sophisticated; and external counsel to ensure the firm understands each Member State's changing requirements.

EPIF supports greater harmonisation in targeted areas, combined with the effective application of a risk-based approach.

Having minimum harmonisation rules AML rules has a number of implications. One of these implications is that companies have to report different information in different formats using different technologies in different Member States, which creates inefficiencies and loopholes; this also serves to undermine the EU single financial services initiatives and the EU financial services passporting regime while skewering the competition in favour of larger organizations that have the financial capacity to adapt to those different regimes and potentially stifle innovation. It also makes it more difficult for payment companies to devise cross-border digital solutions because they must take into account multiple different national standards. This effectively disrupts the functioning of the Single Market. Already, such disruptions are evident in the fact that for example passporting e-money distributors is a process requiring 3 months. EPIF supports the creation of a more harmonised AML framework, moving to maximum harmonization in many parts of the current Directive.

Many Member States are also gold plating the EU legislation through the transposition into their national legislation. Navigating the multiple local nuances, especially areas such as Know-Your Client/Client Due Diligence ("KYC/CDD"), data privacy and reporting of suspicious activity, is a barrier to entry for firms attempting to operate cross-border.

EPIF supports the development of common reporting templates and practices for Suspicious Transaction Reports/Suspicious Activity Reports ("STR/SAR") and additional reporting such as annual compliance reports and internal Money Laundering Reporting Officer ("MLRO") reports. Common reports and templates will result in more effective reporting and increased efficiency in the fight against AML, promote the use and development of new technologies that can build on these common templates and reduce barriers to entry to new companies and costs to the consumer.

EPIF also recommends that conflicts between the AML/CTF and data privacy legislations are resolved so that companies do not breach one regulation when complying with the other. Screening of employees is a good example where data protection legislation is sometimes preventing or limiting the extent of the background checks.

EPIF also supports efforts to strengthen the dialogue and feedback between the AML supervisors, FIUs, law enforcement and the industry on the effectiveness and usefulness of reporting. EPIF would recommend that obliged entities be allowed to share regulatory developments and best practices through a pan European roundtable forum.

EPIF believes that FinTech has the potential to democratize financial services across the EU. With the right technical and regulatory pan-European framework, financial technology companies can provide consumers with the flexible, convenient and safety. The three principles, which EPIF proposes as a guide for the regulatory approach to FinTech - technology neutrality, proportionality and integrity -, should help EU FinTech thrive.

Regulators should foster growth and innovation by cooperating with innovators and by exploring sandboxes. The ultimate responsibility for KYC and CDD checks should fall to the obliged entity. Nonetheless, the EBA or other National Competent Authority (NCA) should assess RegTech solutions and these should be expected to comply with a set of standards to help businesses ensure that the technical solution in place is helpful for compliance.

EPIF members are at the forefront of developing and applying AI solutions for security and consumer protection issues, including fraud prevention and AML.

The use of new technologies such as Artificial Intelligence and Machine-Learning to combat AML and TF improve effectiveness and efficiency. Therefore, EPIF invites EU policy makers to review barriers in existing EU regulation to the adoption of new technologies by the private sector.

In addition, a harmonised e-ID system would significantly reduce the cost of compliance for digital businesses and would offer new opportunities for companies to meet their compliance obligations, while increasing customer convenience. A harmonised EU wide online (i.e. non-face-to -face) KYC framework would facilitate the introduction of a truly cross-border financial services market, and markedly reduce the cost of compliance for digital businesses.

Additional comments (5000 character(s) maximum)

With regard to the risk assessments and its effectiveness, EPIF recommends that National Risk Assessments ("NRAs") and Supranational Risk Assessments ("SNRAs") be monitored for their compliance with the new risk assessment mechanism introduced by AMLD4 and 5.

Specifically, EPIF recommends that the Commission changes the methodology of this SNRA. Instead of focusing on sectors, EPIF would recommend using a risk-based approach analysing existing risks and the mitigation measures currently in place to tackle these.

While EPIF recognises that the non-bank payment sector as a whole could be targeted for AML/CFT purposes, the SNRA of the European Commission failed to adequately recognise the wide-ranging risk mitigation techniques that the industry has put in place. The assessment implicitly reinforced the misperception that non-face-to-face and once-off payment solutions would be riskier than account-based or face-to-face transactions. This has contributed to the current challenges parts of the non-bank payment sector are facing in the area of bank de-risking.

The reality is quite different. AML-related efforts and compliance costs are in many cases the single largest costs factors for our members. Companies are constantly investing in new technology and training to stay ahead and manage these risks. By the nature of their business, EPIF's members are at the forefront of developments on AML/CFT in Europe and globally.

We urge the European Commission will take due account of these risk mitigation techniques in the next iteration of the SNRA. EPIF would like to contribute to this important work by the European Commission and would welcome the opportunity of a structured dialogue around current market practices, challenges and developments with the European Commission at an early stage in the drafting of the next SNRA.

B. Delivering a reinforced rulebook

While the current EU legal framework is far-reaching, its minimum harmonisation approach results in diverging implementation among Member States and the imposition of additional rules at national level (e.g. list of entities subject to anti-money laundering obligations, ceilings for large cash payments). This fragmented legislative landscape affects the provision of cross-border services and limits cooperation among competent authorities. To remedy these weaknesses, some parts of the existing legal framework might be further harmonised and become part of a future Regulation. Other Union rules might also need to be amended or clarified to create better synergies with the AML/CFT framework.

As criminals continuously look for new channels to launder the proceeds of their illicit activities, new businesses might become exposed to money laundering / terrorist financing risks. In order to align with international standards, virtual asset service providers might need to be added among the entities subject to anti-money laundering / countering the financing of terrorism rules (the 'obliged entities'). Other sectors might also need to be included among the obliged entities to ensure that they take adequate preventive measures against money laundering and terrorism financing (e.g. crowdfunding platforms).

This section aims to gather stakeholder views regarding a) what provisions would need to be further harmonised, b) what other EU rules would need to be reviewed or clarified and c) whether the list of entities subject to preventive obligations should be expanded.

4. The Commission has identified a number of provisions that could be further harmonised through a future Regulation. Do you agree with the selection?

	YES	NO	DON'T KNOW
List of obliged entities			x
Structure and tasks of supervision	X		
Tasks of financial intelligence units	X		
Customer due diligence	X		
Electronic identification and verification	X		
Record keeping	X		
Internal controls			x
Reporting obligations	X		
Beneficial ownership registers			x
Central bank account registers			x
Ceiling for large cash payments			x
Freezing powers for financial intelligence units			x
Sanctions	X		

5. **What other provisions should be harmonised through a Regulation?** (5000 Characters maximum)

EPIF recommends that the following Articles of the AMLD5 should become part of a Regulation:

- **Article 5** allowing Member States to adopt stricter provisions is too vague and leave a lot of discretion among Member States. This should move to maximum harmonisation to avoid gold platting.
- **Article 6 –** Assessment of AML/CFT risks: EPIF strongly encourages that mitigation measures are also taken into consideration when drafting the SNRA. (See comments on SNRA above). The Commission should also consider the approach on how this is carry out. There is a need for a clear methodology that ensures that updated and accurate information is collected to carry out the assessment. It should also add a call for industry consultation.
- **Article 7**: Generally, EPIF supports a risk-based approach but some of the current provisions should be subject to a Regulation limiting Member State discretion. The EU should have at least a common assessment methodology and effective communication among entities across EU Member States. The application of GDPR should be harmonised at EU level.
- **Article 8:** Companies should be further encouraged to adopt this approach in coordination with the respective competent authority. It is important not to use a blanket approach and take into account differences within a sector such as the size or resources. Mitigation measures in place by each sector should also be taken into account when assessing the level of risk. This should also involve the use of new technologies. There should be an EU wide methodology to carry out the risk assessment. This should of course take into account different situations in Member States and should consider the mitigation measures in place.

  These should be set at EU level to:

  - Ensure homogeneity
  - Help companies operating cross border
  - Avoid gold-platting
- **Article 11** - CDD Requirements: This should be turned into a Regulation.
- **Article 13**: CDD measures should be moved to a Regulation.
- **Article 15**: The Criteria to apply SDD should be established at EU level.
- **Article 25**: EU criteria would be helpful to assess when reliance on 3rd parties is possible. If applied

broadly, this could facilitate FinTech developments.

- **Article 28** Should be clarified at EU level.
- **Article 30**: Having EU assess criteria and common requirements on information to allow for an easily exchange cross borders.
- **Article 31**: The trust and other types of legal arrangements should be harmonised to allow for an easily exchange cross borders. This might include a standard trust databases.
- **Article 32: on FIUs:** Currently there are many differences between FIUs in different Member States making communication and coordination ineffective. The information exchange should be streamlined.
- **Article 36 -** Suspicious reporting practices and templates should be harmonised.
- **Article 39** - The FIU should be required to provide feedback on the suspicious transaction reporting in a consolidated form in certain intervals.
- **Article 40** on Record Keeping: These requirements should be harmonised among the EU.
- **Article 41** with regard to the processing of personal data: This should be further clarified. Link to **Article 43** unclear – further clarification needed.
- **Article 42** on systems to respond to enquiries from FIUs: There is a lot of fragmentation and this should be more harmonised.
- **Article 45. Paragraph 9** should be deleted. The requirements for CCPs varies among Member States and disrupts the use of online services. This should be further harmonised.
- **Article 50. a** - on exchange of information: This should be part of the Regulation.
- **Article 52** on FIUs cooperation: This should be strengthen.
- **Article 57** on definitions of predicate offences for FIUs cooperation: This should be harmonised.
- **Article 58** on sanctions: This should go under a Regulation.

6. What provisions should remain in the Directive due to EU Treaty provisions?

All other provisions could be kept in the Directive.

7. What areas where Member States have adopted additional rules should continue to be regulated at national level?

EPIF believes that in order to avoid gold platting the AML/CFT framework should be a maximum harmonisation framework where this is appropriate. EPIF members have witnessed how Member States create barriers instead of promoting a more efficient AML/CFT framework. The Central Contact Points (CCPs) are a good example of the challenges that companies face due to the diverse requirements of Member States, which has a negative impact on the Single Market and for competition.

With regard to Central Contact Points (CCPs) a results orientated approach would be preferable, whereby the Payment Institution (PI) is tasked with regulatory compliance but can decide on how to best to achieve this, as explained further below.

- **Level playing field**: If a Member State chooses to have CCPs, it shall oblige all issuers of electronic money and payment service providers ('obliged entities') established in its territory so as not to distort competition between the obliged entities in that market and to avoid regulatory arbitrage. In addition, FinTech companies providing services on a cross-border digital basis should be brought within the provisions. Otherwise, PIs with an agent structure are discriminated against. It would act as a significant disincentive to provide cross-

border services with physical locations. It is recognised by FATF and the UN that it is desirable to have a regulated remittance sector rather than to drive monies under-ground, and the measures should reflect this overall goal.

- **Geographical flexibility**: As long as the obliged entities provide a contact point which possesses the necessary capability and knowledge of local AML/CFT requirements to each host country competent authority, the intended purpose of Article 45 (9) has been addressed. From an EU Single Market and a proportionality perspective, it should not be made mandatory to have the CCP physically located in the host country, as long as it is ensured that the CCP is available to meet with local authorities upon request at a reasonable notice. The CCP for a given host country could for instance be physically located in a neighbouring Member State and thus serve as CCP for more than one country (e.g. regional centres of excellence).
- **Language flexibility**: The CCP should be allowed to communicate with home and host state regulators in English in order to facilitate information sharing within the EU supervisory community. Passporting notifications and other PSD related communication (e.g. agent notifications) between supervisory authorities are already done in English, so there is an established practice to be built upon.
- **Affiliation**: The CCP should not be required to be directly employed by the obliged entity as this would stand in conflict with market practices of EU wide operating groups whereby certain functions are being outsourced to affiliated group entities or third parties (such as temporary personnel placement providers, unaffiliated agents, professional service firms, etc.). Again, EPIF would recommend a results orientated approach, with companies having the ability to achieve the result in the most efficient way possible.

8. Should new economic operators (e.g. crowdfunding platforms) be added to the list of obliged entities?

Crypto to crypto exchange transactions are currently not covered by the 5AMLD. EPIF believes that the most important policy concern for crypto-assets concerns the use of the assets for criminal payments. As a consequence, it is crucial that crypto-exchanges are in scope for all AML requirements at the point of exchange between fiat money and real assets.

9. In your opinion, are there any FinTech activities that currently pose money laundering / terrorism financing risks and are not captured by the existing EU framework? Please explain

Please see our response above.

10. The Commission has identified that the consistency of a number of other EU rules with anti-money laundering / countering the financing of terrorism rules might need to be further enhanced or clarified through guidance or legislative changes. Do you agree?

	YES	NO	Don't Know
Obligation for prudential supervisors to share information with anti-money laundering supervisors	X		
Bank Recovery and Resolution Directive (Directive 2014/59/EU) or normal insolvency proceedings: whether and under what circumstances anti-money laundering grounds can provide valid grounds to trigger the resolution or winding up of a credit institution			
Deposit Guarantee Schemes Directive (Directive 2014/49/EU): customer assessment prior to pay-out			
Payment Accounts Directive (Directive 2014/92/EU): need to ensure the general right to basic account without weakening anti-money laundering rules in suspicious cases	X		
Categories of payment service providers subject to anti-money laundering rules	X		

Integration of strict anti-money laundering requirements in fit&proper tests			

11. Are there other EU rules that should be aligned with anti-money laundering / countering the financing of terrorism rules? (5000 Characters maximum)

As previously mentioned the interaction with data privacy and professional secrecy requirements should be clarified. Conflicts exist in particular between AML and data privacy legislation. It would be helpful to establish clarity on the overlap between these requirements so that companies are not in breach of data protection regulations when complying with AML/CFT legislation.

Greater guidance should be given between the General Data Protection Regulation provisions (e.g. legitimate interest, right to be forgotten) as it relates to AML regulatory obligations which necessitate the processing of personal information.

The relationship between data protection and AML/CTF framework counter-terrorism is one of the most important issues related to information sharing. The requirement to monitor transactions and report on suspicious behaviour falls under the exemptions of GDPR that allows to share personal data for purposes of preventing and tackling crime. However, financial institutions report difficulties in implementing existing AML/CTF regulations because of lack of clarity of existing legislation, and the increased demand for information sharing by national authorities responsible for disrupting crime that go beyond existing data protection laws. Due to significantly increased number of Suspicious Activity Reports (SARs), law enforcement authorities face the difficulties to process and investigate them appropriately. There is a lack of clarity surrounding the purpose of data collection, how data is used, and how long it can be kept by data processors.

11.b. Additional Comments (5000 Characters maximum)

Account Information Services (AIS)/ Payment Initiation Services (PIS) under the revised Payment Services Directive (PSD2):

EPIF would also like to draw your attention to its comments on the revised EBA Guidelines on risk factors under PSD2 in relation to the scope of potential AIS/ PIS AML obligations. EPIF questions the need to include AISPs and PISPs in the scope of the AML obligations due to recognised low risk in particular in relation to AISPs.

AISPs do not have any relation to financial transactions, they do not conduct financial activities. Therefore, they should not be subject to AML obligations. This principle applies to any TPP: they rely on the Strong Customer Authentication ("SCA") procedures of the ASPSP in line with Article 97 PSD2 to authenticate payers and shall be able to rely on ASPSPs also for access to the identification details such as the name of the account-holder, where required. If there are any AML requirements for PISPs, it should be clarified that the "customers" of PISPs are in almost all cases the online-merchants (the payees), not the account holders (the payers).

EPIF welcomes the addition of sector-specific Guidelines to the Risk Factor Guidelines, but asks that the Guidelines remain risk and principle based and do not exclude certain business models by making statements that rule out any other market practice. The market for Account information Services (AIS) and Payment Initiation Services (PIS) is still in an early stage of development and many business models may yet arise which address a particular market need. PIS services specifically can be applied in a variety of market environments: a PISP may offer its services to account holders, consumers to enable them to pay another consumer for the purchase of a good on a marketplace, but may also offer the same services to an online merchant to enable it to accept payments via payment initiation / credit transfer. In the latter model, the Payer will not be a customer of the PISP as its relationship is with the online merchant only to enable payment acceptance in the same way as e.g. card acquirers do.

EPIF also questions whether the Guidelines should state that 'For PISPs: the customer is the natural or legal person who holds the payment account and request the initiation of a payment order from that account the (Payment service user)' but rather state that 'For PISPs: multiple business models can exist where the customer can either be the natural or legal person who holds the payment account and request the initiation of a payment order from that account the (Payment service user) in case of a stand-alone PIS, but where the PIS is provided to a merchant, the customer can be that merchant with the Payment service user not always being a customer as well'.

With regard to the sector specific Guidelines for Third Party Providers (TPPs), it is important to recognise that there are various PIS models in the market, and it will not be appropriate for all PIS models to need to conduct due diligence on the payer.

To give more colour, in a pure PIS journey, the Payment Initiation Services Provider (PISP) does not hold any funds to execute the payment themselves, rather they simply provide the technology to connect a payer to their ASPSP and provide the recipient's bank details to the payer's Account Servicing Payment Service Provider (ASPSP).

In some PIS models, the PISP contracts with Merchants to facilitate ecommerce transactions. All due diligence and KYC is done on the merchant as there is an ongoing relationship.

The PISP only facilitates the transaction for the merchant on behalf of the payer via the bank, there is no ongoing relationship with the payer and therefore no ability or need to conduct due diligence.

Based on the OBIE's technical specifications, a pure PISP will receive data on currency, amount of the transaction, classification of transaction and in certain instances the shipping address from the merchant.

There is insufficient information for a PISP to do any KYC, have an ongoing relationship with the payer, or connect future transactions by the same payer to identify linked transactions.

The ASPSP would have already conducted KYC checks on the payer prior to setting up the payers current account. They are best positioned to identify unauthorized access and transaction monitoring on the payers account. SCA and existing fraud alerts already exist and are leveraged by the ASPSP.

In the instance of a pure PIS, the merchant is the customer of the PISP, whom they have an established relationship and whose name they obviously know.

In relation to the scope of AISPs, EPIF questions the need for AISPs to fulfill AML obligations. AISPs do not provide payments and are not involved in the payment chain; they are simply information service providers. AISPs have read-only access to customer bank account information and neither the AISP nor the AISP's customer can conduct financial transactions on a bank account from within the pure AISP environment. Application of AML requirements to AISPs would not have the effect of restricting the flow of illicit finance as there is no chance for money laundering or terrorist financing to occur via an AISP platform. AML obligations properly sit with the financial institution (i.e. the bank/ASPSP) which provides the accounts in relation to which an AISP provides information services; this is where the transactions take place and where the relevant business relationship with the customer exists.

Bank de-risking – Article 36 PSD2:

EPIF would also like to point out that various money transfer operators (MTO) have experienced the unilateral closure of their bank accounts across various jurisdictions (i.e. Norway, Finland, Denmark, Belgium) and the refusal by any other banks to offer them banking services, which, in our view, is in breach of Article 36 PSD2. This poses an existential threat to their activities, their employees and their customers and the continuation of this practice threatens to undermine the AML/CFT protections in place by driving MTOs out of the market and leading customers to use unlicensed illegal channels.

MTOs foster financial inclusion by enabling remittance flows from countries with highly banked and technologically equipped customers to communities overseas whose residents have little access to formal banking services or

technology.

National and international policy makers, such as the Financial Action Task Force (FATF), have labelled the concerted closure of bank accounts, or the refusal to provide banking services to certain industry sectors including the money transfer industry, as 'de-risking' or 'de-banking' and analysed it in order find ways to stop, prevent and reverse it. FATF has subsequently issued specific Guidance to the banking sector in order to clarify applicable requirements and to stop further de-risking from taking place. The Wolfsberg Group has also published a new Due Diligence Questionnaire on Correspondent Banking as a primary initiative to help address the decline of Correspondent Banking Relationships which sets an enhanced standard for Correspondent Banking Due Diligence and reduce additional data requirements to a minimum. This will result in a less tedious and costly due diligence process for Correspondent Banks and provide a standard for all financial institutions.

Payment institutions including MTOs and their agents depend on access to accounts held with credit institutions for the transfer, clearing and settlement of funds received from customers and for 'client funds safeguarding' purposes as required under applicable laws.

In order to address 'de-risking', EU legislators adopted a specific provision in the PSD2 (Article 36). This article imposes an obligation on NCAs to ensure that payment institutions permit MTOs to have access to payment accounts held with credit institutions in order to allow for an unhindered and efficient provision of payment services. However, this is not always the case.

Several national regulators have taken various initiatives to deal with de-risking issue. The UK FSA and the Lithuanian Central Bank published the Guidelines clarifying the PIs access to Payments accounts. Polish Regulator published a template of questionnaires for banks to submit to PIs prior the opening of accounts, Romanian and Belgian Central Banks are consulting on de-risking. The EBA has announced that is going to work on de-risking in 2020 Q1. We therefore suggest providing a harmonised approach, i.e. the Guidelines across the member states to ensure the consistency and its homogeneous application.

E-Money Directive

EPIF is generally against requirements that discriminate against e-money. E-money issuers are subject to AML/CTF requirements since e-money leaves a digital footprint and is therefore traceable.

EPIF thinks that the e-money sector specific section of the SNRA should be revised as it does not reflect the actual level of ML/TF threat.

EPIF believes that the SNRA does not accurately reflect the efforts of the industry to fight ML/TF. The distinction between distributors and agents in e-money should be explicitly acknowledged.

C. Bringing about EU-level supervision

Supervision is the cornerstone of an effective anti-money laundering / countering the financing of terrorism framework. Recent money laundering cases in the EU point to significant shortcomings in the supervision of both financial and non-financial entities. A clear weakness is the current design of the supervisory framework, which is Member-State based. However, supervisory quality and effectiveness are uneven across the EU, and no effective mechanisms exist to deal with cross-border situations.

A more integrated supervisory system would continue to build on the work of national supervisors, which could be complement, coordinated and supervised by an EU-level supervisor. The definition of such integrated system will require addressing issues linked to the scope and powers of such EU-level supervisor, and to the body that should be entrusted with such supervisory powers.

Effective EU level-supervision should include all obliged entities (both financial and non-financial ones), either gradually or from the outset. Other options would rest on the current level of harmonisation and provide for a narrower scope, i.e. oversight of the financial sector or of credit institutions only. These options would however leave weak links in the EU supervisory system.

Linked to the issue of the scope is that of the powers that such EU-level supervisor would have. These may range from direct powers (e.g. inspection of obliged entities) to indirect powers (e.g. review of national supervisors' activities) only, either on all or some entities. Alternatively, the EU-level supervisor could be granted both direct and indirect supervisory powers. The entities to be directly supervised by the EU-level supervisor could be predefined or regularly reviewed, based on risk criteria.

Finally, these supervisory tasks might be exercised by the European Banking Authority or by a new centralised agency. A third option might be to set-up a hybrid structure with decisions taken at the central level and applied by EU inspectors present in the Member States.

12. What entities/sectors should fall within the scope of EU supervision for compliance with anti-money laundering / countering the financing of terrorism rules? -

- ☐ **All obliged entities/sectors**
- ☐ **All obliged entities/sectors, but through a gradual process Financial institutions**
- ☐ **Credit institutions**

13. What powers should the EU supervisor have? - at most 1 choice(s) -

- ☐ **Indirect powers over all obliged entities, with the possibility to directly intervene in justified cases**
- ☐ **Indirect powers over some obliged entities, with the possibility to directly intervene in justified cases**
- ☐ **Direct powers over all obliged entities**
- ☐ **Direct powers only over some obliged entities**
- ☐ **A mix of direct and indirect powers, depending on the sector/entities**

14. How should the entities subject to direct supervision by the EU supervisor be identified? Members to provide feedback

- ☐ **They should be predetermined**
- ☐ **They should be identified based on inherent characteristics of their business (e.g. riskiness, cross-border nature)**
- ☐ **They should be proposed by national supervisors**

15. Which body should exercise these supervisory powers? at most 1 choice(s) Members to provide feedback

- ☐ **The European Banking Authority A new EU centralised agency**
- ☐ **A body with a hybrid structure (central decision-making and decentralised implementation)**
- ☐ **Other**

If other: please explain: (5000 character(s) maximum

Additional Comments - (5000 character(s) maximum)

EPIF sees the benefits of having more coordinated or harmonised supervision. The aim is to remove friction in the compliance with AML, facilitate cross-border transactions. It is also important to stress that the body that is in charge

of supervision (whether at European or national level) must understand and take into account the uniqueness of the payments market.

EPIF has repeatedly been calling for a strengthened role for the EBA to ensure a consistent implementation of AML. Our members welcomed the changes introduced in the ESA Review and have been supporting efforts to also increase the resources and priority given to the coordination of AML policies in the EU through the EBA.

EPIF remains neutral on the question whether greater coordination and targeted harmonisation requires new institutional arrangements at EU level. Such an institutional debate should not distract from the immediate benefits of greater cooperation and harmonisation.

D. Establishing a coordination and support mechanism for financial intelligence units

Financial intelligence units (FIUs) play a key role in the detection of money laundering and identification of new trends. They receive and analyse suspicious transaction and activities reports submitted by obliged entities, produce analyses and disseminate them to competent authorities.

While financial intelligence units generally function well, recent analyses have shown several weaknesses. Feedback to obliged entities remains limited, particularly in cross-border cases, which leaves the private sector without indications on the quality of their reporting system. The cross-border nature of much money laundering cases also calls for closer information exchanges, joint analyses and for a revamping of the FIU. net – the EU system for information exchange among financial intelligence units. Concerns regarding data protection issues also prevent Europol, under its current mandate, to continue hosting this system.

An FIU coordination and support mechanism at EU level would remedy the above weaknesses. Currently, the only forum available at EU level to coordinate the work of FIUs is an informal Commission expert group, the FUI Platform.

This section aims to obtain stakeholder feedback on a) what activities could be entrusted to such EU coordination and support mechanism and b) which body should be responsible for providing such coordination and support mechanism.

16. Which of the following tasks should be given to the coordination and support mechanism?

- **Developing draft common templates to report suspicious transactions Issuing guidance**
- **Developing manuals**
- **Assessing trends in money laundering and terrorist financing across the EU and identify common elements**
- **Facilitating joint analyses of cross-border cases Building capacity through new IT tools**
- **Hosting the FIU.net**

17. Which body should host this coordination and support mechanism? at most 1 choice(s)

- **The FIU Platform, turned into a formal committee involved in adopting Commission binding acts**
- **Europol, based on a revised mandate A new dedicated EU body**
- **The future EU AML/CFT supervisor**
- **A formal Network of financial intelligence units**

Additional Comments (5000 character(s) maximum)

FIUs Cooperation:

EPIF members file STRs/SARs to report possible money laundering, terrorism financing, transactions considered to be "suspicious" under applicable law, and other transactions that may be the proceeds of crime, to law enforcement and other government agencies designated to receive such reports.

Expectations vary greatly by Member State, where some signal mere anomalies, but others suggest only detected well-grounded and substantiated criminal behaviours should be reported. Feedback from National/Member State FIUs is disseminated to obliged entities across a varied spectrum (i.e., informal and formal), and can appear contradictory to written laws and regulations. Feedback from National/Member State FIUs could be improved insofar as apparent inconsistencies between informal feedback and written guidelines, which can open obliged entities to reputational risk and non-compliance. EPIF members encourage the Commission to consider publishing consistent guidance across jurisdiction.

EPIF believes that obliged entities filing STRs/SARs across multiple Member States would greatly benefit from a centralized filing of STRs/SARs to a single contact point in the EU. EPIF's members employ significant resources in ensuring differentiated Member State requirements and expectations (e.g., with respect to subject matter, format, etc.) are met. Standardized formats, thresholds, and a centralized and automated filing system could significantly improve the process for all stakeholders.

EPIF's members operate in Member States where supervisory functions are housed in agencies that are separate from the agencies responsible for analysis of STRs, and in others where the functions are combined.

EPIF is supportive of consolidation of AML/CFT supervision into an EU supranational supervisory agency. Such consolidation could leverage resources, help ensure consistent guidance and approaches to firms operating across Europe, and help the European authorities to better manage ML/TF risks. It would be further beneficial if a single supervisor were to perform both safety and soundness supervision function and conduct-of-business regulation.

E. Enforcement of EU criminal law provisions and information exchange

Recent actions have increased the tools available to law enforcement authorities to investigate and prosecute money laundering and terrorist financing. Common definitions and sanctioning of money laundering facilitate judicial and police cooperation, while direct access to central bank account mechanisms and closer cooperation between law enforcement authorities, financial intelligence units and Europol speed up criminal investigations and make fighting cross-border crime more effective. Structures set up within Europol such as the Anti-Money Laundering Operational Network and the upcoming European Financial and Economic Crime Centre are also expected to facilitate operational cooperation and cross-border investigations.

Public-private partnerships are also gaining momentum as a means to make better use of financial intelligence. The current EU framework already requires financial intelligence units to provide feedback on typologies and trends in money laundering and terrorist financing to the private sector. Other forms of partnerships involving the exchange of operational information on intelligence suspects have proven effective but raise concerns as regards the application of EU fundamental rights and data protection rules.

This section aims to gather feedback from stakeholder on what actions are needed to help public-private partnership develop within the boundaries of EU fundamental rights.

18. What actions are needed to facilitate the development of public-private partnerships?

- ☐ **Put in place more specific rules on the obligation for financial intelligence units to provide feedback to obliged entities**
- ☐ **Regulate the functioning of public-private partnerships**
- ☐ **Issue guidance on the application of rules with respect to public-private partnerships (e.g. antitrust)**
- ☐ **Promote sharing of good practices**

F. Strengthening the EU's global role

Money laundering and terrorism financing are global threats. The Commission and EU Member States actively contribute to the development of international standards to prevent these crimes through the Financial Action Task Force (FATF), an international cooperation mechanism that aims to fight money laundering and terrorism financing. To strengthen the EU's role globally, and given the fact that the EU generally translates FATF standards into binding provisions, it is necessary that the Commission and Member States speak with one voice and that the supranational nature of the EU is adequately taken into account when Member States undergo assessment of their national frameworks.

While FATF remains the international reference as regards the identification of high-risk jurisdictions, the Union also needs to strengthen its autonomous policy towards third countries that might pose a specific threat to the EU financial system. This policy involves early dialogue with these countries, close cooperation with Member States throughout the process and the identification of remedial actions to be implemented. Technical assistance might be provided to help these countries overcome their weaknesses and contribute to raising global standards.

This section seeks stakeholder views on what actions are needed to secure a stronger role for the EU globally.

19. **How effective are the following actions to raise the EU's global role in fighting money laundering and terrorist financing?** at most 1 answered row(s) -

	Very effective	Rather effective	Neutral	Rather ineffective	Not effective at all	Don't know
Give the Commission the task of representing the European Union in the FATF		**X**				
Push for FATF standards to align to EU ones whenever the EU is more advanced (e.g. information on beneficial ownership)		**X**				

Additional Comments - 5000 character(s) maximum

Payment services are a global industry. EPIF therefore believes that the EU should not diverge from FATF Standards.

EPIF welcomed efforts by the European Commission and Member States to adopt a common EU approach towards their engagement and membership in the FATF. This should ensure a stronger voice for the EU within this important international standard setting body and ensure an alignment of EU and international standards.