Financial Data and Technology Association
c/o The University of Edinburgh
13-15 South College Street
Edinburgh
EH8 9AA

6 July 2020

Dirk Haubrich
Head of Conduct, Payments & Consumers
European Banking Authority
20 Avenue André Prothin
Courbevoie, 92400
France

Sent via Email to:

Dear Dirk,

RE: FDATA Europe Response to EBA's Consultation on Revised Guidelines on Money Laundering and Terrorist Financing Risk Factors: JC 2019 87 CP (https://eba.europa.eu/node/99760)

Please find below FDATA's formal submission of response to the EBA's Consultation on Revised Guidelines on Money Laundering and Terrorist Financing Risk Factors. Due to the limitations of the response form provided online and the lack of option to attach supporting evidence, we take this opportunity to send our analysis and position via email.

We ask that you kindly share this Consultation submission with the team for review and consideration; we also ask that you consider the following analysis, and take actions recommended herein to ensure the continued viability of Open Banking in Europe.

Yours sincerely,

Ghela Boskovich

FDATA Europe Chapter Lead

Forward:

The Financial Data and Technology Association (FDATA Europe), on behalf of its members, is grateful for the opportunity to provide comments on the Guidelines on money laundering risk factors, specifically Guideline 18: Sectoral guideline for payment initiation service providers (PISPs) and account information service providers (AISPs).

Legal and regulatory provisions for third party providers (TPPs) that are beyond risk-based and proportionality principles can endanger a successful open banking market in Europe. A current example is AML regulation for TPPs. AML rules should apply to cases where business models have a clear connection with money laundering risks. For example, where businesses are responsible for executing transactions and come into possession of customer funds.

When the new Payment Services of Account Information Service (AIS) and Payment Initiation Service (PIS) were introduced by PSD2, providers of both services were automatically classed as obliged entities under AMLD, despite the fact that neither type of provider executes transactions or comes into possession of funds.

As the EBA itself acknowledges in its Draft Guidelines “the inherent ML/TF risk associated with [these services] is limited” for these very reasons. The inclusion of these services needs to be re-examined as part of the Commission’s AML action plan, to remove duplication and friction which will ultimately prevent consumer take-up of these innovative new services and hamper innovation and competition.

We ask that the EBA’s Risk Sector AML Guidelines are not finalised until the conclusion of the Commission’s AML Action Plan initiative - particularly given the contention around whether AIS and PIS were intended to be included as obliged entities, or whether this was the unintentional result of cross referencing between PSD2, CRD and AMLD.

The inclusion of these services under European AML legislation will very negatively impact the intended outcome of PSD2, which the European Commission noted in its press release addressing frequently asked questions about PSD2 in January 2018, was to *‘help stimulate competition….[that] would then allow consumers to benefit from more and better choices between different types of payment services and service providers’.*

Asking new providers of AIS and PIS to serve a *separate* purpose - to be watchdogs for illegal money flows through the ASPSs - is disproportionate, contrary to existing law, and was never initially outlined as an objective of PSD2. Under PSD2 and GDPR (data minimisation), these companies must only use data strictly to provide the services customers request.

Requirements to conduct due diligence and verification (e.g. proof of identity and address checks) would dissuade many customers from using the services in the first place. Customers will wonder why they have to repeat the KYC process to allow an AISP to access their payment account transaction data, having already done this to open their payment account. Requirements to notify authorities of

suspicious transactions would require each AISP and PISP to build costly systems, and, even if feasible, would lead to double counting of reports already received from ASPSPs. The cumulative impact of these requirements could lead businesses to exit the emerging open banking market before it has taken off.

Additionally, authorities have supported PISPs to encourage competition with card schemes and reduce merchant fees alongside the Interchange Fee Regulations. If PISPs have to stop customers mid-checkout to ask for proof of identity and address documents (which incidentally is not a requirement for card acceptance), opportunities for competition and innovation in payments will be snubbed out.

Our response to specific questions, and our recommendations follow below, specifically in regards to additional sector-specific Guidelines 18 on account information and payment initiation service providers.

Q18: Do you have any comments on the additional sector-specific Guideline 18 on account information and payment initiation service providers?
Yes. It is FDATA Europe's position, based on the reasons set out below, that there should be no application of AML to either AISPs or PISPs.

<u>Arguments for re-considering inclusion of AIS and PIS in scope of AMLD</u>

<u>AISPs</u>

Account information service providers (AISPs) can, with the payment service user's explicit consent, access customer transaction data, in order to provide services based on this data - e.g. a dashboard of all bank accounts for accountancy platforms; providing enhanced credit scores; or using the data to inform lending decisions (please see the Appendix to this document for a detailed description of some of the types of account information services currently being offered). AISPs only allow PSUs to see their data in different ways and to be used for different purposes, and cannot access accounts to make payments. They never come into possession of funds or execute payments.

No risk that money-laundering or terrorist financing can occur through an AISP platform

AISPs have read-only access to PSU bank account information and neither the AISP nor the AISP's PSU can conduct financial transactions on a bank account from within the 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 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.

AISPs enable customers to share data - and only data - with their selected service providers, including third party providers. Data itself is neutral and not a means for money laundering. When a customer selects an AISP, and authorises its ASPSP to share data to a TPP AISP via the required consent mechanism, there are essentially three parties that hold the exact same data: the regulated ASPSP, the Technical Service Provider (TSP), and the AISP. In some cases, those three parties are the ASPSP, AISP, and an agent; and often it only involves two parties: the ASPSP and AISP.

However, only one actor is, and should be, subject to full regulation – the ASPSP. The TSP and AISP should not be subject to regulation as holding the data is not indicative of facilitating money laundering, nor is the act of sharing that data a means to money laundering.

Limited value at high cost

Proposed Guidelines Section 18.11 obligates AISPs to monitor for unusual transactional activity, however, AISPs are not in the business of monitoring transactions – they provide account aggregation services. They have access to customer data that is consented to and authorised by the customer for the sole purpose of providing a service to the customer *with the lightest touch possible*: this means the minimum processing required. To require AISPs to undertake transaction monitoring would, as noted above, require disclosure as to the purpose of additional transaction monitoring. We are of the view that this over the top approach is in direct violation to PSD2, which states that AISPs should only access the data needed for the services they provide, which is data consolidation, not execution of transactions..

To require AISPs to monitor all transactions on the customer account is tantamount to asking AISPs to police the entire banking ecosystem. For customers with multiple payment accounts, this means an AISP is therefore burdened with monitoring the transactions across all the accounts and ASPSPs to which they are connected. This is beyond the scope of PSD2, and beyond the service an AISP provides. It is also virtually impossible to assess whether transactions are suspicious or not without knowing the purpose for which the accounts were created and the transactions were made. It is burdensome, and counter to PDS2 both from a role and responsibility perspective. It is also an additional cost layer, which performs a redundant purpose and will stifle innovation, ultimately impacting consumers ability to access new and innovative services.

Furthermore, because AISPs are required to reauthenticate the customer's consent every ninety (90) days under current rules, most AISPs only have 90 days worth of transactional data on which to perform heavier transaction monitoring. This limited data set stymies the ability to perform transaction monitoring. AISPs are unlikely to identify suspicious transactions
in relation to their read-only access to

the data without bringing in additional algorithms to run across the data and/or without seeking further information about the activity in question from the ASPSP.

Any transaction monitoring would be a duplication of work already being performed by ASPSPs, and would come at an additional cost. There is a real risk of an increase in the number of false positives that are generated by this additional level of transaction monitoring. This directly increases the number of notifications generated across the system and would likely result in AISPs adopting a 'defensive filing' approach to Suspicious Activity Reports to the detriment of the Financial Intelligence Units. An AISP is in a position to only send out a suspicious activity notification. Considering the limitations of no real-time analysis, as well as an increase in false positives, these notifications would increase the cost of investigation and reconciliation. They would also defeat the efficiencies created by the ASPSP performing the same level of transaction scrutiny as part of the AML requirements.

For these reasons, requiring AISPs to do heavy handed transaction monitoring for suspicious AML/CTF activity is redundant, costly, and will have a negative impact on the number of competitive AISP actors in the market. not to mention likely serve to distract Financial Investigation Units causing them to wade through high volumes of defensive Suspicious Activity Reports (SAR) from AISPs/PISPs.

AISP Authorisation Requirements do not include AML/CTF Controls

FDATA Europe believes it was always the intention for AISPs to be carved out of these obligations. PSD2 (Article 33) specifically exempts AISPs from having to submit at authorisation, a description of the internal control mechanisms which the applicant has established in order to comply with AML obligations.

By explicitly omitting AISPs from having to detail AML/CTF controls from the AISP authorisation requirements, it is clear that no such obligations were intended to apply to AISPs. To continue to obligate AISPs to perform AML/CTF checks is in conflict with the requirements of Article 33 of PSD2.

Where internal AML/CTF control mechanisms are not required as part of the AISP application process, it is our firm belief that no such obligations were intended to apply to AISPs and no obligation should exist.

Onerous and redundant

In the interest of reducing the overall burden of regulation on participants, we believe that a number of the requirements of AML regulations are already satisfied prior to an AISP consuming transaction data from a financial institution. For example, ASPSPs will have already conducted customer due diligence measures on account holders using AISP services, and are required to keep such CDD up to date by actively monitoring account activity throughout the relationship lifecycle; this means that further AISP CDD checks are 'doubling up'.

In all cases, the ASPSP is best placed to undertake the appropriate checks and monitor transactions for suspicious behaviour. Requiring an AISP to perform the same measure the ASPSP has already taken is redundant and would serve no purpose other than burdening AISPs with unnecessary overhead costs and compliance. This redundancy runs counter to the guidance provided by the JMLSG in 5.6.2 of Part 1, which states: “Several firms requesting the same information from the same customer in respect of the same transaction not only does not help in the fight against financial crime, but also adds to the inconvenience of the customer”. The sentiment behind that guidance should equally apply to money laundering considerations as it does to financial crime.

In the case of Account Information Verification Services, the service provided by the AISP ordinarily requires a single, one-off connection by the customer in order to prepare and provide specific information about the customer's bank account for a corporate such as a lawyer, accountant, pension provider or wealth manager. In the simplest of cases (for example, the verification of account details) the AISP never obtains the transaction information of the end customer, and even where transaction-level information is provided, the AISP simply reflects the data from the customer's bank to the corporate. Due to the one-off nature of the connection, customers are significantly less likely to invest time in onboarding with the AISP, instead seeing the process as being driven by the corporate who requires their financial information - many of whom are already subject to KYC and AML requirements in verifying their customers' bank account information, and whom in many cases do not want the end customer's details to become known to the AISP providing Account Verification services. Onboarding the customer by the AISP therefore necessitates a simple, frictionless connection process in order to realise the benefits being offered, and requiring these companies to undertake due diligence such as KYC and AML on their customers would be sufficient friction to effectively cripple their business model. It would duplicate many of the processes being undertaken by both the corporates requesting the information and the ASPSPs providing the information. Notably, as this type of service simply passes through facts about the customer's account once approved by the customer, it is not possible for the AISP to facilitate any kind of Money Laundering.

One of the objectives of the 4MLD and 5MLD is to balance the objective of protecting society from crime against the need to create a regulatory environment that allows companies to grow their businesses without incurring disproportionate compliance costs. Any onerous and redundant double-up compliance on an AISP would be counter to the objectives of the 4/5MLDs. It would negatively impact competition and customer choice and convenience as we believe the significant and unnecessary compliance costs will have the effect of creating a barrier of entry to the market, with any value that firms see in entering the AISP market outweighed by the regulatory costs of complying with AML regulation.

Other sectors, with a higher risk than AISPs, are carved out

Even for **e-money issuers**, the proposed guidelines (section 10.12) provide an exemption from identification and verification of the customer’s and beneficial owners’ identities and assessment of the nature and purpose of the business relationship for certain e-money products (in accordance with Article 12 of Directive (EU) 2015/849), if national or member state legislation provides for that exemption. For example:

> See **MLD4/MLRs 2017 Para. 7, Preamble MLD4**: "...in certain proven low-risk circumstances and under strict risk-mitigating conditions, Member States should be allowed to exempt electronic money products from certain customer due diligence measures, such as the identification and verification of the customer and of the beneficial owner"
>
> and
>
> **MLD4/MLRs 2017 Reg. 38, para. 1 MLRs 2017:** Exemption for electronic money cards with 250 euros or less.

The EBA's guidance requires AISPs to conduct CDD on each customer's identity even though *there is absolutely no movement of money in the AISP platform*, but e-money products by definition are mobile and at risk of potential AML/CFT and are able to be exempted from similar requirements. This simply does not make sense in the fight against financial crime.

Even where e-money issuers have to perform only Simplified Due Diligence, as noted under section 10.18 (b), they may verify the customer's identity on the basis of a payment being drawn from an account with an EEA-regulated institution over which the customer has control. This is tantamount to using the ASPSPs AML/KYC process as a proxy. They are even allowed to reduce monitoring as long as a certain monetary threshold is not reached (section 10.18 (g)). E-money transactions *below* a certain threshold do not require monitoring, and yet based on the current guidance AISPs who do **not** move money/funds are required to put monitoring measures in place.

In addition to exemptions for e-money issuers, the following further exemptions are provided for:

- **Money remitter's agents** under the new proposed guidelines are acknowledged to often provide payment services as an ancillary component to their main business, but may not themselves be obligated entities under applicable AML/CFT legislation (section 11.2); the guidelines further acknowledge that there is a limited amount of accountability a remitter can take for a break in the value chain at the agent level
    - In some cases an agent has more access and visibility over funds and may execute payments, but have fewer AML obligations than a AISP, and none of the reporting responsibilities
- **Letting agents** are exempted from CDD for agents letting for amounts under EUR 10.000 a month.
- **Gambling service providers** are exempted from AML requirements, with the exception of non-remote and remote casinos, based on evidence that indicated the gambling sector was low risk relative to other sectors.

- **Limited financial activity** is also exempted, for businesses with a low annual turnover, in order to reduce the administrative burden on business.

All of these sectors conduct financial transactions and enter into the flow of funds, and therefore present a much higher risk for money laundering than AISPs. It is incorrect to obligate AISPs to perform AML when they do **not** conduct financial transactions, while exempting sectors who do touch the money from any AML/CFT obligation.

As noted in the proposed guidelines (in section 18.2 (a) & (b)), account information service providers do not have capability for financial transactions, are not involved in the payment chain, and should be considered nil risk.

In summary and based on the arguments above, we strongly urge the EBA to revise its guidelines so that there is no application of AML to AISPs.

PISPs

Payment initiation service providers (PISPs) can, with the customer's explicit consent, submit payment orders to the customer's ASPSP, on the customer's behalf i.e. initiate payments which the customer's own ASPSP then executes. They are not allowed to come into possession of funds. The only data they are allowed to see are the payee's account details, and information on the initiation, and subsequent execution of the payment (which they get from the customer's ASPSP).

However, unlike other payment service providers (banks, money remitters, e-money institutions), who come into possession of funds in the provision of their services, PISPs are prohibited from being part of the flow of funds. Instead, PISPs sit in the shoes of the customer, and submit payment orders on the customer's behalf, just as a customer would do, if they were to make a credit transfer using online banking. A PISP is dependent on the customer's bank to actually execute the payment, and move the money from the customers bank to the payee's bank. As PSD2 states:

"When exclusively providing payment initiation services, the payment initiation service provider does not at any stage of the payment chain hold the user's funds".

The same arguments for removing AML obligations from AISPs also apply to PISPs, with some additional considerations.

PISPs would need to undertake customer due diligence on each end-customer

Depending on the 'risk profile' this could involve requesting name and address from each customer, **storing** these details, and using a paid-for electronic identification verification system. This adds considerable friction to the customer journey; friction leads to customer abandonment of the service, which has a detrimental effect on competition. This additional CDD burden adds considerable cost. This additional cost will prevent many PISPs from being commercially viable and merchants from moving to this payment method. Again, one of the objectives of the 4MLD and 5MLD, is to balance the objective of protecting society from crime against the need to create a regulatory environment that allows companies to grow their businesses without incurring disproportionate compliance costs

Requiring additional due diligence for each end customer is inconsistent with PSD2

According to Article 66.3(f), a PISP should not request from the PSU any data other than those necessary to provide the payment initiation service; requiring a full electronic ID verification process violates the minimum information standard set in Article 66.3(f). In the very next clause of Article 66 [3(g)], it goes on to say that a PISP should not use, access or **store** any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer. Under AML/CTF requirements, a PISP would need to store this data. Moreover, this requirement also contradicts Article 5(1)(c) of the General Data Protection Regulation (GDPR) on the principle of data minimisation.

Unlevel playing field between PISPs and card processors/ scheme

In a merchant context, a customer has a 'one-off' interaction with the PISP, in the same way as a customer paying by card has a 'one-off' interaction with whichever card-acquirer happens to be serving the merchant. AML obligations would mean the PISP having to stop the check-out process to ask the customer for their name and address. This would lead to friction that would mean PISPs were not on a level playing field with the card payment services they are competing with, thereby frustrating the PDS2 mandate to increase competition.

Card Processors do not perform AML on payment service users at the check-out. However, unlike PISPs, Card Processors can be in possession of a payment service user’s authentication data (card details including PAN/CVV/PIN). PISPs rely upon authentication procedures set by the ASPSP during the payment flow, so are inherently at lower risk of being used to commit fraud.

This cost and friction serves no purpose as PISPs never come into possession of funds other than duplication and additional cost

In every PIS transaction there is already one party undertaking CDD on the customer - the customer’s ASPSP. To double up on the KYC obligations is unnecessarily onerous to the PISP in terms of cost and redundant effort, it is also onerous for the customer.

Obliging PISPs to conduct AML checks on end customers is a significant barrier to providing payment initiation services

These requirements undermine the very principle of “fair competition among all payment service providers” postulated in PDS2: PISPs are subject to stricter requirements in comparison with Card Processors who have a similar business model.

Not only will it not “allow for the development of a user-friendly, accessible, and innovative means of payment”, it will not “ensure technology and business-model neutrality”, both of which are PSD2 requisites. It goes further to damage competition, as it will cause payment service user dissatisfaction, and lead to increased abandonment during the payment process.

Requiring PISPs to conduct AML checks on end customers is restricted to a manual process

Under PSD2, PISPs are prohibited from using APIs to obtain account information such as name and address. They cannot bypass the manual process. This adds an additional cost layer, making the requirement additionally burdensome for PISPs to comply. It also does not ensure technology and business model neutrality in accessing and sharing the data required to fulfill a payment service user’s order. Obligating PISPs to conduct AML checks on the customer would lead to Open Banking forfeiting its initial goal of encouraging innovation, and providing the customer with competitive choice. By rendering the initial goal moot, the massive investment already made into the payment ecosystem would be in vain.

This limited risk is disproportionate to the requirement for AIS and PIS to perform AML. In point of fact, there is no risk at all, and therefore no AML requirements should exist.

<u>General Comments on Guideline 18</u>

The EBA consultation acknowledges that they and other ESAs ‘consider that the ML/TF risk associated with their activities is limited’. However, it then proposes some actions for AISPs and PISPs which would prove extremely burdensome, and go beyond what these businesses would usually do to provide open banking services:

- As part of their CDD processes, PISPs and AISPs should ensure that their AML/CFT systems are set up in a way that alerts them to unusual or suspicious transactions. Even without holding significant information on the customer, PISPs and AISPs should use their own, or third party typologies, to detect unusual transactional activity.
- PISPs and AISPs should apply CDD measures to their customers (which are clarified as the payment service user).
- Each time an account is added, the AISP should ask the customer whether the account is his own account, a shared account, or a legal entity’s account to which the customer has a mandate to access (e.g.: an association, a corporate account).

FDATA believes these requirements are:

- Disproportionate and not compatible with existing law (PSD2)
- A risk to the take-up of open banking services and the competition

objectives of PSD2 Disproportionate and not compatible with existing law

(PSD2)

The European Commission noted in its press release in January 2018, that PSD2 was intended to 'help stimulate competition….[that] would then allow consumers to benefit from more and better choices between different types of payment services and service providers'.

However, asking new providers of AIS and PIS to serve a separate purpose - to be watchdogs for illegal money flows through the ASPSs - is disproportionate, and was never initially outlined as an objective of PSD2.

Third party providers are restricted by law to only using data for account information services. They are not permitted to use this data for AML purposes. As Article 67(f) makes clear, AISPs must '*not use, access or store any data for purposes other than for performing the* ***account information service*** *explicitly requested by the payment service user, in accordance with data protection rules.*

Risk to the take-up of Open Banking

Requirements on AISPs and PISPs to conduct due diligence (CDD) and verification (e.g. proof of identity and address checks) would dissuade many PSUs from using the services in the first place. PSUs will wonder why they have to repeat the KYC process to allow an AISP to access their payment account transaction data, having already done this to open their payment account in the first place. Requirements to notify authorities of suspicious transactions would require each AISP and PISP to build costly systems, and, even if feasible, would lead to double counting of reports already received from ASPSPs. The cumulative impact of these requirements could lead businesses to exit the emerging open banking market before it has taken off.

Additionally, authorities have supported PISPs to encourage competition with card schemes and reduce merchant fees alongside the Interchange Fee Regulations. If PISPs have to stop customers mid-checkout to ask for proof of identity and address documents (which incidentally is not a requirement for card acceptance), opportunities for competition and innovation in payments will be snubbed out.

Specific comments on Guideline 18

Question 18: Do you have any comments on the additional sector-specific Guideline 18 on account information and payment initiation service providers?

FDATA Europe's specific comments follow the quoted Guideline text.

> 18.1. When applying this Guideline, firms should have regard to the definitions referred to in point 18 and 19 of Article 4 of Directive (EU) 2015/2366 in accordance with which:
>
> a) a payment initiation service provider (PISP) is a payment service provider pursuing payment initiation services;
>
> b) an account information service provider (AISP) is a payment service provider offering account information services.

Article 113 of PSD2 should be amended to ensure that AIS and PIS are not classed as obliged entities (via cross referencing between CRD and AMLD).

> 18.2. Firms should take into account that despite PISPs and AISPs being obliged entities under Directive (EU) 2015/84965, the inherent ML/TF risk associated with them is limited due to the fact that :
>
> a) PISPs, although being involved in the payment chain do not execute themselves the payment transactions and do not hold payment service user's (PSU) funds;
>
> b) AISPs are not involved in the payment chain and do not hold payment service user's funds.

FDATA Europe fully agrees with the conclusion that PISPs and AISPs pose limited risks. In accordance with this, the EBA should consider making the requirements set out in the guidelines less onerous for PISPs and AISPs (we provide specific comments below).

> 18.3. When offering payment initiation services or account information services, PISPs and AISPs should take into account, together with Title I, the provision set out in this sectoral guideline.

This guidance should not come into effect until there has been further discussion with the Commission about the inclusion of AIS and PIS under the scope of AMLD.

Risk factors

> 18.4. When assessing ML/TF risks, PISPs and AISPs should take into account the following factors as potentially contributing to increased risk:

> a) The customer transfers funds from different payment accounts to the same payee that together, amount to a large sum without a clear economic or legitimate rationale;
>
> b) For AISPs: the customer transfers fund from different accounts to the same payee that give grounds to suspect that the customer is trying to evade specific thresholds using various payment accounts;
>
> c) The customer receives funds from, or sends funds to, jurisdictions associated with higher ML/TF risk or to someone with known links to those jurisdictions.

18.4(a): A PISP could not detect this scenario. PISPs submit payment orders which include the payee account details, but PISPs do not obtain the payer account details from ASPSPs (this is something banks are not providing currently). Therefore, for each payment initiated, the PISP will not be able to identify whether or not the payer is using different accounts. That is, unless ASPSPs are required to provide payer BIC and IBAN to PISPs via API.

To detect this scenario, an AISP would need to breach PSD2 Article 67(2)(f). The AIS would need to look at the accounts (and account data, including transactions) it aggregated, which would involve using the data for purposes other than the provision of performing account information services. In reality, AISPs do not 'read' any of a PSU's data, as this is not required for the provision of AIS. AISPs usually encrypt the data so it is only readable to the PSU to whom it belongs. Additionally, if the AISP did 'look into' the accounts it aggregated for the PSU and the transactions, it would not be able to see where the transactions were going to determine whether multiple payments were being made to the same payee, because the BIC/IBAN of the payee would not be included in the transaction data collected.

18.4(b): As above, to detect this scenario, an AISP would need to breach Article 67(2)(f). However, we also consider that this risk is highly unlikely to materialise: For an AISP to be able to identify whether this risk is materialising, the malicious actor (i.e., money mule agent) would have to be using an AISP to aggregate all their accounts (i.e., mule accounts). We think it is very unlikely that a criminal money mule agent would expose themselves to the risk of detection by using an aggregator service to view all their criminal mule accounts.

18.4(c): As above, to detect this scenario, an AISP would need to breach Article 67(2)(f) in order to view and assess who a PSU is receiving funds from. Additionally, requiring an AIS to

make judgements on the risk of incoming funds would duplicate the efforts that the PSU's ASPSP should already be undertaking to comply with its own AML requirements.

With regard to sending funds to high risk jurisdictions, as above, even if the AIS were to breach Article 67 and access data for a purpose other than providing AIS, the AIS would not have enough information about the transactions it could see to determine whether they were made to high risk jurisdictions.

With regard to sending funds to high risk jurisdictions, a PISP's role is to assemble and submit a payment order under the instruction of a PSU. It should ultimately be the ASPSP's role to assess whether there are specific risks before acting on the payment order and executing the transaction. To require PISPs to screen payees to identify jurisdictional risks is duplicative and not something PISPs will be able to sustain without significant ongoing cost and investment.

> 18.5. When assessing ML/TF risks, PISPs and AISPs should take into account the ESAs' Opinion on the use of innovative solution in the customer due diligence process .

The EBA'S Opinion (para 4) acknowledges that CDD is often associated with significant cost and customer inconvenience. We consider that requiring the PSU to undergo any CDD, even using innovative means, such as scanning a passport with a phone, would be enough to dissuade that customer from proceeding to use the open banking service. In e-commerce, for example, it is very unlikely that a customer would consider providing facial recognition just so they could use PIS to pay, as opposed to using their debit card, which wouldn't require any facial recognition.

> 18.6. When assessing ML/TF risks, PISPs and AISPs should take into account the following factors as potentially contributing to increased risk in particular if the customer uses multiple accounts held with different ASPSPs to make payments:
>
> a) For PISPs: the customer's initiate a payment to a jurisdiction associated with higher ML/TF risk or a high-risk third country.
>
> b) For AISPs: the customer connects payment accounts hold in the name of multiple natural or legal persons in more than one jurisdiction; or the customer connects payment accounts in jurisdictions associated with higher ML/TF risks.

18.6(a): As above, PISPs only act on instructions from PSUs, which include the payee details. PISPs would not be able to determine whether the PSU uses accounts held with different ASPSPs because PISPs cannot currently obtain the BIC and IBAN from the ASPSP.

With regard to sending funds to high risk jurisdictions, a PISP's role is to assemble and submit a payment order under the instruction of a PSU. It should ultimately be the ASPSP's role to assess whether there are specific risks before acting on the payment order and executing the transaction. To require PISPs to screen payees to identify jurisdictional risks is duplicative and not something PISPs will be able to sustain without significant ongoing cost and investment, which may ultimately hamper innovation and competition.

18.6(b): This scenario could only arise if there were weaknesses in ASPSP SCA processes allowing an individual to take over the accounts of multiple other individuals (i.e.. fraud victims), and then choose to connect the accounts to an AIS. It is unlikely a fraudster would choose to do this. Furthermore, as above, in order to access the account data to check whether there are multiple individuals, an AIS would need to breach article 67.

> 18.7. When assessing ML/TF risks, AISPs and PISPs should take into account the following factors as potentially contributing to decreased risk:
>
> c) For PISPs: the customer initiates a payment transaction to an EEA member country or to third country that has AML/CFT requirements that are not less robust than those required by Directive (EU) 2015/849.
>
> d) For AISPs: the customer's payment accounts are held in an EEA member country.

18.7 (c): The ASPSP will ultimately make a risk decision about whether to execute a transaction to a particular jurisdiction (whether initiated directly by the PSU or by a PISP).

18.7 (d): N/A

Measures

> 18.8. The customer is:
>
> a) 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).
>
> b) For AISPs: the customer is the natural or legal person who has the contract with the AISP. This can be the natural or legal person who holds the payment account(s).

18.8(a): Clarifying that the customer of the PISP is the PSU sets an expectation that PISPs will need to conduct CDD on the PSU. This will be damaging to PISPs who contract only with merchants. The PSU would have to be stopped at the online check-out to perform CDD with the PISP. This would dissuade any PSU from using PIS to make payments, because they would be able to make payments using a card (and they would not have to undergo CDD at the checkout using this method). This creates an unlevel playing field and defeats one of the objectives of PSD2:to support payment methods to compete with cards.

Under PSD2, PISPs do not have a contract with the PSU (framework contracts govern the execution of transactions, not the initiation of transactions - as per PSD2 Article 4(21)). Instead, the customer of the PISP will usually be the merchant - as discussed in recital 21 of PSD2:

> “In particular, payment initiation services in the field of e-commerce have evolved. Those payment services play a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer’s account servicing payment service provider in order to initiate internet payments on the basis of a credit transfer.”

Accordingly, the account owner is not the “customer” of the PISP in the sense of AML. The PISP does not establish a “business relationship” with the account owner in the sense of Art. 11 (a) AML-Directive. CDD, therefore, cannot refer to the account owner.

This has been confirmed by the ESAs in charge of licensing PISPs: While PISPs need to provide documentation of their internal AML control mechanisms under Art. 5 (1) lit k PSD2, this has not referred to the identification of account-owners, but to the identification and CDD of online-merchants.

We suggest the EBA Guideline should be amended to read:

> For PISPs: The customer is the online-merchant (the payee) that is offering PIS as a payment alternative, e.g. on a website.
>
> Only in exceptional cases, where the PISP has a direct and enduring contractual relationship with the account holder (the payer) in the sense of Article 3 (13) of the AML-Directive, the latter may be regarded as the “customer” of the PISP.

18.8(b): Clarifying that the customer of the AISP is the PSU sets an expectation that AISPs will need to conduct CDD on the PSU. Conducting due diligence and verification (e.g. proof of identity and address checks) would dissuade many customers from using AIS in the first place. Customers will wonder why they have to repeat the KYC process to allow an AISP to access their payment account transaction data, having already done this to open their payment account with their ASPSP. The cumulative impact of these requirements will lead businesses to exit the emerging open banking market before it has taken off.

18.9. PISPs and AISPs should take adequate measures to identify and assess the ML/TF risk associated with their business.

18.9: As discussed previously, many of the risk scenarios highlighted above either do not apply to AIS and PIS, or are not possible to detect, either because they would imply an AIS breached Article 67 of PSD2, or because the PISP does not receive the necessary information about the payer from the ASPSP.

If PISPs are to be required to undertake transaction monitoring, banks must be required to return certain information about the PSU (payer) to the PISP via API including BIC, IBAN, and name of the account holder, as a minimum. This is necessary to allow PISPs to uniquely identify transactions, without adding extra dissuasive steps into the PSU's payment experience.

> 18.10.PISPs and AISPs should determine the extent of CDD measures on a risk-sensitive basis. In most cases, the low level of inherent risk associated with these business models means that SDD will be the norm.

We welcome this acknowledgement that there is a low level of inherent risk with AIS and PIS. We make a suggestion below for further clarifying the requirements on AISPs and PISPs for SDD.

> 18.11.Monitoring: As part of their CDD processes, PISPs and AISPs should ensure that their AML/CFT systems are set up in a way that alerts them to unusual or suspicious transactional activity. Even without holding significant information on the customer, PISPs and AISPs should use their own, or third party typologies, to detect unusual transactional activity.

18.11: PSD2 Article 67(2)(f) states that AISPs "must not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules."

The EBA Guideline is asking AISPs to access and store data for a different purpose, i.e. to monitor transactions for suspicious activity.

Besides asking AISPs to breach Article 67(2)(f), the EBA Guidance is asking AISPs to serve a purpose that was not outlined in the objectives of PSD2, i.e. to be watchdogs for illegal money flows through the banks. The costs of implementing systems to serve this purpose would be disproportionate and burdensome for AISPS.

Additionally, even if such a use of the data was permitted under Article 67, it would require the PSU's explicit customer consent as well as disclosure as to the purpose of additional transaction monitoring. This would likely dissuade a PSU from agreeing to the service as they would consider transaction monitoring to be invasive and not a worthwhile price to pay for the original account information service.

With regard to PISPs, such theoretical monitoring is also redundant/ duplicative, considering that the transactions should be verified with regards to their AML compliance by the entities that actually execute the transactions, namely, ASPSPs.

Additionally, because the PISP will not necessarily have visibility of the details of the payer (i.e. their BIC/IBAN - because some banks don't share this data with the PISP) it would be difficult to judge fully whether a transaction was suspicious or not.

Customer due diligence

18.12.PISPs and AISPs should apply the CDD measures to their customers

in line with Title I. This guidance should be deleted as it duplicates the guidance

given in 18.10.

18.13.Pursuant to Article 13 of Directive (EU) 2015/849 each time an account is added, the AISP should ask the customer whether the account is his own account, a shared account, or a legal entity's account to which the customer has a mandate to access (eg: an association, a corporate account).

Article 26 of Directive (EU) 2015/849 enables the obliged entity to rely on the CDD of a third party. As such, an AISP could meet Article 13 requirements through obtaining the identity of the account holder from the ASPSP (i.e. obtaining the name via the API) - although this will require the EBA to ensure that

banks are sharing this information, which is not currently the case. They could use these details each time the account is added, and thereby detect whether the account belongs to the same account holder (The guideline should be changed to reflect this possibility). Therefore, the AIS should not have to ask these questions each time an account is added. To be required to do so, would introduce friction into the customer journey and dissuade PSUs from using open banking services.

Enhanced due diligence

18.14.In higher risk situations, firms should apply the EDD measures set out in Title I.

This guidance should be deleted, as the EBA has already made clear that AIS and PIS

are

inherently low risk.

Simplified customer due diligence

18.15.Firms should always know the name of their customer. PISPs and AISPs and may consider applying SDD such as:

a) Relying on the source of funds as evidence of the customer's identity where the payment account details of the customer are known, and the payment account is held at an EEA-regulated payment service provider;

b) Postponing the verification of the customer's identity to a certain later date after the establishment of the relationship. In that case, firms should ensure that their policies and procedures set out at what point CDD should be applied;

c) Assuming the nature and purpose of the business relationship;

We take 18.15 (a) to mean that PISPs and AISPs can rely on obtaining the name of the account holder from the ASPSP via the dedicated interface for the purpose of the verification required under Article 13 of AMLD. Since ASPSPs are required to provide name of the account holder under Article 36 RTS 389/2018, and ASPSPs will already have verified the identity of the PSU through their own KYC, the ASPSP should be relied on by the AISP or PISP to provide verification of identity of the PSU:

We suggest the guidance is amended:

18.15.Firms should always know the name of their customer. PISPs and AISPs and may consider applying SDD such as:

a) Relying on the ASPSP to provide the name of the account holder (as required under Article 36 RTS 389/2018 as verification of the customer's identity, providing the payment account is held at an EEA-regulated payment service provider;

Summary:

FDATA Europe strongly recommends the EBA await issuing final Revised Guidelines until the European Commission has concluded its own consultation on AML requirements.

FDATA Europe strongly believes that AISPs should be carved out from any application of AML requirements in the EU. AML requirements to AISPs do not serve the purpose for which they were intended, and are disproportionate to the risk (there is none) of any money laundering or terrorist financing occurring through AISP platforms. It would be onerous and redundant to apply AML requirements to AISPs, and have a negative impact on the innovation and competition that PSD2 and Open Banking were intended to create.

To the extent the EBA is unable to carve-out AISPs from application of AML requirements, any application of the requirements to AISPs (and PISPs) should be limited to the requirement to undertake a risk assessment of their activities, taking into account the nature of the activities the AISP/PISP is partaking in and the likelihood of AISP/PISP services being used to aid the flow of illicit finance.

If, based on the outcome of that risk assessment, the AISP/PISP believes that there is negligible risk of money laundering occurring, it is our view that it should not be subject to any further AML requirements.

In the AISP use case, the AISP can only access transaction information from an ASPSP if the payment service user provides its consent and authenticates with its bank in order to allow the AISP to access their payment account. In this scenario, the payment service user will already have undergone CDD at the banks' end, and any further CDD requirement on AISPs would be onerous and unnecessary.

Given that PISPs do not come into possession of funds, or execute transactions themselves, (but rather rely on banks to do this), it would be duplicative for PISPs to monitor and report transactions.

It may be possible for an AISP/PISP to rely on CDD measures conducted by the bank but this would not relieve the AISP/PISP of responsibility for the CDD obligation. Performance of CDD should be the sole responsibility of the bank and an AISP/PISP should not have any liability for it.

FDATA Europe strongly recommends that the EBA (and the European Commission) remove AISP and PISP AML/CFT requirements from the scope of the 5AMLD as soon as the opportunity arises.

ANNEX 1

Costs of the Application of AML to AISPs and PISPs

FDATA has undertaken the exercise of estimating the costs of implementing AML controls outlined in the EBA Guidelines, using the base assumption that a TPP is building the process from a blank page. Costs include legal fees for implementation assistance, as well as ongoing full-time compliance employees, the internal resources to build KYC into user flows and ongoing monitoring of transactions, as well as the third-party technology costs to help manage KYC and transaction monitoring.

It should be noted that a vast amount of AISP services are provided at no cost, or no additional cost (to the software that the AIS forms part of) to SMEs and consumers. However, additional AML requirements add a significant amount of operational costs to the service, and put the no-cost-to-consumer model in significant jeopardy. Firms new to market, as well as existing providers, will require significant additional capital in order to remain in business, to comply with a requirement to which they have no risk exposure, as they do not touch or move funds.

Some of these have been offered to customers for years and are just now being captured under the regulation (e.g., bank feed for cloud accounting providers).Since many of these services are offered for free, asking AISPs to implement AML controls would make these businesses unviable, which is ultimately to the detriment of consumers and SMEs.

Not once have FDATA members been made aware of any concerns of money laundering occurring through use of these services prior to them becoming regulated (given that it is impossible for an AISP to be involved in any of the placement, layers, or integration stages of money laundering), and no bank has ever asked them to consider implementing AML controls to access the data - which prior to Open Banking they were doing by way of a direct contract with the bank.

The primary purpose of bringing AISPs into the regulated landscape is to ensure that they meet a uniform set of standards to ensure the security of customer data and prevent fraud. There is no Money Laundering risk with AISP services and the security/fraud risk is already covered off by Open Banking/PSD2 standards.

A number of FDATA members have undertaken cost estimate exercises for implementing KYC/AML requirements, including additional human resource overhead, systems administration, and monitoring costs. The following matrix shows a high level breakdown of those costs. The matrix below details the additional average costs per annum for maintaining an AML team at current market salary rates, and solution, including a conservative estimate of new customers requiring KYC/AML checks at onboarding.

The costs relating to systems/solutions is an averaged cost based on quotes from the following AML/KYC providers in the market: Trulioo, Onfindo, Sanctions Search, Ondato, GB Group, and Jumio.

However, the matrix below details costs associated with the costs of doing AML checks, and does not examine the additional opportunity costs of the following:

Opportunity costs:

- Friction placed on entire AISP community
  - Costs of additional fraud prevention & false positives
- Impact on take-up of TPP services if AML is required
  - Decreased attractiveness of PIS proposition contra Card Schemes, as CDD is not required for use of card
  - Detrimental impact on competition against Card Schemes overall
- Attrition costs

  - Point of sale/online transactions incompletion
    - Friction of verifying a PIS customer engaging for the first time with a merchant

- ■ Identity & KYC documentation requirement for first time users and inconvenience of onboarding at time of sale
- ○ POS friction for PIS vs. Card Schemes, as CDD is not required for use of card

AML Fixed Cost per Annum Total Amount		
ML Requirements Officer	Full Time Employee (FTE)	£100,000 / €110,400
Administrator	FTE for monitoring	£80,000 / €88,300
Transaction Monitoring Analyst	FTE	£60,000 / €66,200
SAR Analyst	FTE	£60,000 / €66,200
Onboarding Analyst	FTE	£45,000 / €49,700
Transaction Monitoring License KYC Set up & License fees Screening Services £10,000 / €11,000 Sensitive Documentation Storage External AML/CDD Audit £20,000 / €22,000 **£450,000 / €496,600**		Transactions £25,000 / €27,600 £50,000 / €55,200
AML Variable Cost per Annum (assume 20k new users p.a.) KYC verification*		**Cost Per Unit Total Amount** £1.25 £25,000 / €27,600
PEP & Sanctions monitoring **		£2.00 £40,000 / €44,150
*Least expensive solution price topped out at £3.00 per KYC for 'selfie' and document verification **on-going monitoring, risk based screen frequency		**£65,000 / €71,700**
		Grand Total
(£1.00 = €1.10) **£515,000 / €568,300**		
This matrix does not include the requisite one-time set-up fees for the solution, which run between £100,000-£145,000 (€110,000 - €160,000) on average. Nor does it include the legal consultation fees for assisting in the implementation, which run from £130,000 - £150,000 (€143,500 - €165,500), depending on business model complexity. These one-time costs can add an additional £230,000 - £295,000 (€253,800 - €325,500) in operational costs to a TPP's		

overall first year budget, bringing the **overall costs of year 1 AML**

requirement compliance to well over £700,000 (€772,500).

Annex 2

Examples of AISP Services in the Market Today

Type of service	Description
Cloud Accounting Software	Cloud accounting platforms support customers in reconciling their bank transactions with the accounting transactions created in their accounts. In order to reconcile the transactions created within the cloud accounting software, the customer needs accurate and up-to-date transaction data from their bank in order to see what transactions have not been paid or accounted for, and to identify errors such as duplicate transactions. The customer can either do this manually (by downloading a transaction statement from a bank and uploading it to the cloud accounting providers platform), or use the cloud accounting providers account information services to import data directly from the customer's account with selected banks into their cloud accounting account. These types of services have been offered well before they became regulated by PSD2. For example, in the case of Xero, they have offered these services since 2011 through direct bilateral agreements with major banks in the UK. Never has there been any concern (by banks or customers) that this type of service could be used for any kind of money laundering.
Account Information Verification Services	Account Information Verification Services support corporates such as lawyers, accountants, pension providers and wealth managers, many of whom are already subject to KYC & AML requirements, in verifying their customers' bank account information. This can be for many reasons including assisting with simple KYC/AML account ownership checks, verification of account ownership prior to payments, balance confirmation, specific transaction verification and income verification. In many cases the corporate does not want the end customer's details to become known to the AISP

	providing Account Verification, and where the relationship between corporate and customer requires AML checks to be done these are completed by the corporate directly with their customer. Requiring Account Information Verification Services to onboard their corporate clients' customers and perform KYC/AML checks would duplicate many of the processes being undertaken by the corporates, and it would create friction to the verification process that would render it inefficient and in many cases would deter corporates from using it. In the simplest of cases (such as verification of account details) the AISP never sees the transaction information of the end customer, and even where transaction-level information is provided, the AISP simply reflects the data from the customer's bank to the corporate. As this type of service simply passes through facts about the customer's account once approved by the customer, it is not possible for the AISP to facilitate any kind of Money Laundering.
Digital Account check for Purchase Financing	Purchasing Finance facilitation requires evaluating the legal capacity of a customer, based on creditworthiness. AISP makes this possible by automating the consolidation and categorization of business accounts transactional information, in order to assess the financial position and creditworthiness of a customer.
Categorised Account View for Factoring	It is possible to reconcile a purchase invoice against a genuine receivable using AIS. By gaining a complete view of the business customer's revenue history via the account transaction history, along with categorisation, a factor has the relevant information to verify if an invoice is genuine or not. The categorisation provides the factoring company with exactly what it needs to know: whether or not a certain receivable actually exists. Even where transaction-level data is provided to the Factor, the AISP simply reflects the data from the customer's bank accounts to the Factor. As this type of service simply passes through facts about the customer's account once consent is granted, it is not possible for the AISP to facilitate any kind of money laundering.