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

25 February 2020

Eric Ducoulombier
Head of Unit, FISMA/B3
Retail Financial services
DG Financial Stability, Financial Services and Capital Markets Union
European Commission
Rue de Spa 2 (SPA 2 2/20)
B-1000 Brussels/Bruxelles
Belgium/Belgique

Sent via email to: eric.ducoulombier@ec.europa.eu
ralf.ohlhausen@etppa.org

Dear Eric,

RE: Risks to open banking due to scope of AML legislation

The Financial Data and Technology Association (FDATA), on behalf of its members, is asking the European Commission to amend the 5th Anti-Money Laundering Directive to remove account information services providers (AISPs) and payment initiation services providers (PISP) from its scope, as soon as the opportunity arises.

The inclusion of these services under European AML legislation was an unintended consequence of cross referencing between PSD2, CRD and AMLD4. It will very negatively impact the intended outcome of PSD2, which the 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 banks - 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 the services customers request.

Requirements to conduct due diligence and verification (e.g. passport 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 add their bank to an AISP, having already done this to open their bank 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 banks. 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 a passport or driving licence (which incidentally is not a requirement for card acceptance), opportunities for competition and innovation in payments will be snubbed out.

We hope you will consider these points and the further detail below, and take action to ensure the continued viability of open banking across the European market.

Yours sincerely

Ghela Boskovich

FDATA Europe Chapter Lead

fdata europe
Financial Data and Technology Association

FDATA Europe Members

Background

The Revised Payment Services Directive (PSD2) was implemented in the UK by the Payment Services Regulations 2017. A key objective of the PSRs is to support newly regulated 'account information service providers, and payment initiation service providers' to compete with traditional banking and payment providers:

- **Account information service providers (AISPs)** can, with the customers 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. AISPs only allow customers 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.
- **Payment initiation service providers (PISPs)** can, with the customers consent, submit payment orders to the customer's bank, on the customer's behalf i.e. initiate payments which the customer's own bank 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 bank). In the UK, customers are redirected to their bank to authenticate a payment initiated by a PIS provider, in compliance with strong customer authentication (SCA) and dynamic linking requirements.

Why are these services now in scope of AML?

All 'Financial Institutions' are subject to the MLRs 2017. 'Financial Institutions' are defined in regulation 10(2)(a) of the MLRs as those carrying out one or more of the listed activities set out in points 2 to 12, 14 and 15 of Annex 1 to the Capital Requirements Directive (CRD). Point 4 of the annex to CRD previously included payment services as defined under PSD1. PSD2 (article 113) updated Point 4 of CRD to include the new list of payment services in PSD2, which includes AIS and PIS and (unintentionally, or else with very little foresight) brought these services in scope of AML.

Discussions with FCA

We have raised this issue with FCA's Payments Supervision and policy team. In response, the FCA suggested that FDATA and its members become involved in work to develop guidance on the application of AML to AIS and PIS providers. That would include both their own financial crime guide, Payment Services Approach Document (Financial Crime Chapter), and the Joint Money Laundering Steering Group's Guidance, which we understand is approved by Treasury Ministers.

We consider such guidance to be a last resort, and the better outcome to be that Treasury removes AIS and PIS from the MLR requirements. We have set out arguments for the removal below.

European Banking Authority Consultation

We are also raising these issues at the EU level with the EU Commission. The EBA has taken the disappointing position of consulting on what requirements should mean for an AIS and PIS under AML legislation, before the Commission has had chance to consider any changes to the underlying law for AIS and PIS. The EBA consultation acknowledges that they and other ESAs 'consider that the ML/TF risk associated with their activities is limited'. However, it goes on to propose 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 transactional. 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 the CDD measures to their customers
- 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).

Discussion of impacts of AML application to Account Information Service Provider (AISP) businesses

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

In the HM Treasury's Impact Assessment in April 2017, it noted that the purpose of the EU's Fourth Anti-Money Laundering Directive (4MLD) is to restrict the flow of illicit finance by setting minimum common regulatory standards for Member States. Whilst the purpose of AML requirements is to restrict the flow of illicit finance, AML legislation also focuses on the idea that firms should take a risk-based approach to ensure proportionate duties on participants; striking a balance between regulating to protect the financial system and onerous administrative duties for legitimate businesses.

In its 2010 report on "Money Laundering Using New Payment Methods", the Financial Action Task Force (FATF) noted that, for the purposes of assessing money laundering risks and vulnerabilities in the context of new payment methods, it is essential to differentiate between mobile payments based on individual bank accounts for each customer (and recipient) held at a financial institution that is subject to adequate AML/CFT regulation and supervision, and those services offered separately from such accounts. In its Report, FATF said it may be helpful to differentiate according to various categories of payment systems, including, "financial information services: Users may view personal account data and general financial information, but there is no capability for any financial transaction and therefore may be considered low risk".

As set out in 4MLD, the European Commission needs to take account of information from international organisations and standard setters in the field of AML/CFT, such as FATF public statements, and adapt its assessments to the changes therein, where appropriate.

As the FCA acknowledged in its response to FDATA, and the EBA acknowledged in its consultation, 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 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) 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. However, only one actor is subject to full regulation: the ASPSP. It is clear that holding the data is not indicative of facilitating money laundering, nor is the act of sharing that data a means to money laundering.

2. AML will dissuade customer take-up of AIS and provide limited value at high cost

AISPs are required to gain the customer's explicit consent to read their data, and must clearly inform the customer to the purpose and use of that shared data.. This subjects AISPs to disclose to the end customer that they will be using their data to fulfill the additional transaction monitoring for anti-money laundering and counter terrorism financing. This disclosure alone will have an adverse effect on the customer experience. Moreover, since data is neutral, and neither holding nor sharing that data is a means to money laundering, it is also redundant, as the bank has the onus of performing ALM/CTF duties.

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 service to the customer *with the lightest touch possible*: this means minimum processing. AISPs can only do the minimum amount of transaction monitoring *at the customer request*. To require AISPs to do transaction monitoring would, as noted above, require explicit customer consent as well as disclosure to the purpose of additional transaction monitoring. This heavier approach is also in direct violation to PSD2, which states that AISPs should only access the data needed for the services they provide

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 bank accounts, this means an AISP is therefore burdened with monitoring the transactions across all the accounts and banks to which they are connected. This is beyond the scope of PSD2, and beyond the service an AISP provides. It is burdensome, and counter to PDS2 both from a role and responsibility perspective, as well as stifling the ability for customers to access innovative services. It is also an additional cost layer, which performs a redundant purpose.

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 robust fraud recognition. AISPs are unlikely to identify fraudulent activity in relation to their read-only access to the data without bringing in additional algorithms to run across the data.

These additional algorithms, which are proprietary services offered by other fintechs, would not actually run in real time, and therefore not provide any notification before the transaction order is

completed. They would discover suspicious activity after the fact. They would also be a duplication of work already being done by the banks, and 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. 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 serve as an interruption to executing the customers' orders, and 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 has a negative impact on the number of competitive AISP actors in the market.

3. AISP Authorisation Requirements do not include AML/CTF Controls

We believe 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.

It is for these reasons that FDATA concludes no such obligations were intended to apply to AISPs: where internal AML/CTF control mechanisms are not required as part of the AISP application process, no obligation exists.

4. Disproportionate and harmful to competition

PSD2/Open Banking was introduced to increase innovation and competition – providing consumers with more choice and options. Any application of AML requirements to AISPs is counterproductive to the purpose of this regime. Some AISPs will not be able to continue to operate with the compliance overhead of AML requirements, and others simply won't get off the ground due to the additional cost layers resulting from both the AML/CTF checks as well as the heavier touch transaction monitoring obligations. This will make it incredibly difficult for small businesses and consumers to effectively and efficiently access and use new and disruptive AIS such as online accounting and money management products. As a specific example, implementing identification and verification checks into the sign-up flows of AISPs will have a negative impact on customer adoption of new products and services affecting the future viability and success of these businesses, and ultimately of the open banking regime.

5. Onerous and redundant

As noted in the Treasury's consultation on 4AMLD transposition, the government's AML/CFT regime has the aim of making the UK financial system an increasingly hostile environment for illicit finances, whilst minimising the burden on legitimate businesses and reducing the overall burden of regulation.

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, banks will have already conducted customer due diligence measures on account holders using AISP services, meaning that further checks are 'doubling up'.

In nearly all cases the bank is best placed to undertake the appropriate checks and monitor transactions for suspicious behaviour. Requiring an AISP to perform the same measure the bank 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".

One of the objectives of the 4MLD 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 4MLD, and also negatively impact competition and customer choice and convenience.

6. Unintended consequence

The European Commission has already confirmed in discussions with FDATA that the catching of AIS activity for AML requirements was a drafting oversight, caused by the blanket construal of references to the repealed PSD1 (which did not have the concept of account information services in its definition of 'payment services') as references to PSD2. This blanket construal had flow on consequences for the definition of 'payment services' in the list of activities subject to mutual recognition in Annex I to Directive 2013/36/EU and, as a result, for the definition of 'financial institution' in 4MLD.

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

The government has already carved out other 'low-risk' sectors from the AML regime. For example, as set out in the Treasury's 2017 Impact Assessment:

- **Gambling service providers**: the government exempted all gambling service providers from AML requirements, with the exception of non remote and remote casinos (which 4MLD requires to be in scope). This was based on evidence that indicated the gambling sector was low risk relative to other sectors. (p5)
- **Limited financial activity**: the government widened the exception for those engaging in financial activity on a very limited basis by increasing the annual turnover limit from £64,000 to £100,000. The aim was to reduce the administrative burden on businesses whilst retaining a "sufficiently low" figure, as required by 4MLD. (p6)

Both examples involve businesses who do – or have the potential to – conduct financial transactions and therefore present a much greater risk for money laundering than AISPs. In each case, the government concluded that the level of risk each presented was low and carved them out from the scope of AML requirements. We strongly support a similar approach being taken for AISPs.

Examples of carve-outs/ reduced scope for other business types

Reference	Description
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"
Reg. 38, para. 1 MLRs 2017	Exemption for electronic money cards with 250 euros or less.
MLD5	
Art. 1 (1)(b)	Exemption from CDD for agents letting for amounts under EUR 10.000 a month
JMLSG	
4.9, Part 1	"A risk-based approach will, however, serve to balance the cost burden placed on individual firms and their customers with a realistic assessment of the threat of the firm being used in connection with money laundering or terrorist financing. It focuses the effort where it is needed and will have most impact."
5.6.2, Part 1	"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."
3.13, Part 2	As issuers of electronic money usually occupy the position of intermediaries in the payment process, situated between two financial or credit institutions, they are often able to provide additional transaction information to law enforcement that complements identity data provided by other financial institutions. ***This may be equally or more valuable evidence than a repetition of the verification of identity process.***

Conclusion regarding AISP AML Requirements

Data is neutral and therefore holding the data is not indicative of facilitating money laundering, nor is the act of sharing that data a means to money laundering. An AISPs holds and shares that data, therefore there is no risk of an AISP facilitating money laundering.

AISPs do not monitor transactions, and only do so at the customer's request. PSD2 states AISPs should provide a light touch as a conduit, with minimal processing. In order to fulfill AML/CTF compliance on transaction monitoring would be in direct violation of the PSD2 light touch requirement. The additional expense and burden on AISPs to comply runs counter to promoting competition, resulting in another violation of the desired outcomes of PSD2.

AISP authorisation requirements do not include AML/CTF controls, and it is clear that no such obligations were intended to apply to AISPS. Continued AML/CTF control obligations are both harmful to competition, as well as burdensome and redundant. Moreover, other sectors with a higher risk of money laundering have been exempted from AML/CTF requirements; AISPs should be carved out of the scope of AML requirements as well.

It is for these reasons that FDATA strongly believes that AISPs should be carved out from any application of AML requirements in the United Kingdom, and the EU more generally. AML requirements to AISPs would not serve the purpose for which they were intended, and be disproportionate to the risk (there is none) of any money laundering or terrorist financing occurring through AISP platforms, as well as burdensome and redundant.

Discussion of impacts of AML application to Payment Initiation Service Providers (PISP) businesses

The PSD2 regulated activity of 'payment initiation services' has been designed specifically as a 'light touch' regulatory regime for innovative firms - 'PISPs' - to compete with incumbent payment providers such as banks and card schemes.

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 customers 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".

Many of the arguments for removing AML obligations from AISPs apply equally to PISPs. However, the following are key considerations:

1. 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 ID 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. These checks run around £10 per check, a cost which is not passed on to the end consumer but may have to be passed on to merchants,. 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 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 a PISP would be counter to the objectives of the 4MLD, and also negatively impact competition and customer choice and convenience.

2. 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.

3. Unlevel playing field between PISPs and card processors/ schemes

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. It is also duplicative and redundant as the customer has already likely entered the name and address of the merchant. 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 bank during the payment flow, so are inherently at lower risk of being used to commit fraud.

4. **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 customer due diligence on the customer - the customer's bank. 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 end customer.

5. **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.

6. **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 end 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.

It is for these reasons that FDATA strongly believes that PISPs should be carved out from any application of AML requirements in the United Kingdom, and the EU more generally. AML requirements to PISPs would not serve the purpose for which they were intended, and be disproportionate to the risk (there is none) of any money laundering or terrorist financing occurring through AISP platforms, as well as burdensome and redundant.

Proposals for JMLSG guidance to AIS and PIS providers

The purpose of this section is to summarise the key requirements of AML regulations, and provide commentary on their applicability to AISPs and PISPs in the event that AISPs and PISPs remain subject to AML requirements, which we strongly believe they should not be.

The proposals below should be seen as a starting point for any guidance being developed, either by the FCA (Financial Crime Guide/ Approach Document), or the JMLSG. We look forward to developing these proposals further with the input of HM Treasury/ JMLSG/ FCA.

Obligation	Detail	Commentary/proposal
Risk-based approach	Firms are under an obligation to: ● Identify and assess the risks of money laundering and terrorist financing to which their business is subject by conducting a risk assessment. The risk factors a firm must take into account include those relating to: its customers, its services, countries or geographical areas in which it operates, its transactions and delivery channels ● Agree a risk tolerance threshold for the business e.g. whether to accept PEPs ● Determine and apply appropriate customer due diligence ("CDD") measures on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction	Any application of AML requirements to AISPs and PISPs should be limited to this 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. **AISPs**: As noted by FATF in its 2010 Report, financial information service providers do not have capability for financial transactions and may be considered low risk. **PISP:** As per PSD2, PISPs are prohibited from coming into possession of funds. In each transaction, the bank of the payer and payee has already undertaken KYC checks with its customers (as they are obliged to). 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.
Governance systems and controls	Requirements to: ● Identify, assess, and manage effectively, the risks in the businesses ● Appoint an MLRO with responsibilities of oversight of the firm's compliance with AML rules and dealing with the regulator ● Ensure adequate resources are devoted to AML / CTF ● Establish and maintain adequate and appropriate policies and procedures to prevent money laundering ● Establish a system of governance arrangements with effective procedures to identify, monitor and report any risks to which it might be exposed and adequate, relevant control mechanisms	N/A. Provided an AISP's/PISP's risk assessment evidences a negligible risk of money laundering occurring, it is our view that it should not be subject to any further AML requirements.
Money Laundering Reporting Officer (MLRO)	Firms are under an obligation to nominate an MLRO who will review internal disclosures and make external reports for FCA approval.	N/A. **AISPs:** Given that transactions do not take place in the AISP's environment there is no transaction activity for the AISP to monitor or report on. The monitoring and reporting obligation has to sit with the financial institution that provides the account. We would propose that the risk assessment is reviewed and approved by the board or management body of the AISP, and, provided it evidences a negligible risk of money laundering occurring, the AISP should not be required to appoint an MLRO.

		PISPs: 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.
Customer Due Diligence (CDD)	A firm that is subject to AML requirements has an obligation to undertake customer due diligence (CDD) measures when it: establishes a business relationship; carries out an occasional transaction; suspects money laundering or terrorist financing; or doubts the veracity of documents obtained for the purpose of identification.	N/A. Provided an AISP/PISPs risk assessment evidences a 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.

Recommended Course of Action

FDATA strongly recommends, and requests, that HM Treasury remove AISP and PISP AML/CTF requirements from the scope of the Money Laundering Regulations as soon as the opportunity arises.

Burdening AISPs and PISPs with this additional compliance requirement sets an unlevel playing field for providers not in scope who perform similar services; allocates undue burden on low risk service providers when others with similar risk assessments have already been exempted from the requirement; and adds additional cost layers to duplicate efforts already performed by the ASPSPs. The AML/CTF requirement is fundamentally counterproductive to promoting competition and innovation, and violates PDS2, details of which have been enumerated above.

While AML provisions continue to apply to AIS and PIS, we recommend revisions to the JMLSG guidance, to minimise the impact of the provisions on AIS and PIS providers.