



UK
FINANCE

ACCESS TO PAYMENT ACCOUNT SERVICES: Good practice guidelines

March 2019



EXECUTIVE SUMMARY

This good practice guide is aimed at both credit institutions providing access to payment account services¹ and applicants seeking access to such an account within the UK. It aims to bring together the most relevant guidance around access to payment account services for applicants and credit institutions in a way that focuses on the responsibilities of both parties.

This guide is purely voluntary and does not supersede, nor enhance, the regulatory and legal requirements to which credit institutions and applicants are already subject. It is recommended that applicants and credit institutions obtain their own legal opinion on what aspects of their business may be covered by a legal requirement. This could be as a result of the Payment Services Regulations 2017 (PSRs 2017), including the Financial Conduct Authority's (FCA) Approach document and the Payment Systems Regulator's (PSR) Approach document; the requirements of HMRC registration for Supervision under the Money Laundering Regulations (MLRs); the PSR's powers under the Financial Services (Banking Reform) Act 2013 (FSBRA) or the requirements of the PSR's Specific Direction 1 (SD1).

This document was created to assist the industry in implementing the requirements of proportionality, objectivity and non-discrimination (POND) set out in the Payment Services Regulation 2017 (PSRs), Regulation 105. The guide's primary role is to signpost credit institutions and applicants to the relevant rules and guidance, in order to constructively help the provider and applicants by clearly presenting existing requirements for both parties with regards to the provision of payment account services. Unless otherwise specified, this good practice applies equally to decisions regarding

new applications and to decisions on continuing to provide bank account services under pre-existing agreements.

The provision of payment accounts is a complex space with multiple actors and competing priorities. It is anticipated that this guide, and its reference materials, will help to increase transparency for all parties, reduce misunderstandings and support a better functioning market. It is not expected that a 'standardised' market will be enabled by this document, as firms are expected to maintain their own risk appetites and application processes. However, these guidelines are published in order to encourage an improvement in market practice and provide a point of departure for other efforts to promote a transparent, effective and functioning market for both those applying for payment accounts and those providing access.

This document has been developed by UK Finance and its members with the input and co-operation of the Association of Foreign Exchange and Payment Companies (AFEP), the Emerging Payments Association (EPA) and the Electronic Money Association (EMA). This group will review the impact of this document on the market in early 2020 and investigate what changes may need to be incorporated within the guide.

¹ In the context of this document when we refer to 'access to payment account services' we are primarily referring to payment and safeguarding accounts as provided by a credit institution.

STRUCTURE OF THE DOCUMENT

This document is split into three main parts:

1. The first part provides an initial introduction to the scope of firms covered by the good practice guidelines and is intended to be read in conjunction with a firm's own legal advice;
2. The second part is generally addressed to credit institutions providing, or seeking to provide, access to payment account services for the purposes of enabling access to the payment systems. It includes:
 - a. references to the PSRs 2017, specifically Regulation 105 which covers access
 - b. references to the FCA's and PSR's approach documents with specific reference to the implementation of Regulation 105
 - c. reference to the Joint Money Laundering Steering Group (JMLSG) guidance, specifically the expectation that relationships are treated on a case-by-case basis.
3. The third part is generally addressed to applicants seeking access to a payment account for the purpose of facilitating customer transactions, including accessing the payment systems. It includes:
 - a. details of the expectations of banks providing access, including anti-money laundering (AML), sanctions and wire/funds transfer responsibilities
 - b. references to both the supervisory arrangements of HMRC and the FCA.

Please note that firms are encouraged to read all sections in order to inform themselves of the expectations on both parties.

1. SCOPE

1.1. Application of Regulation 105

This document contains guidance only for firms operating within the regulatory environment of the UK and either applying for, or providing, services covered under Regulation 105 of the PSRs 2017.

Regulation 105 requires that credit institutions provide access to payment account services on a proportionate, objective and non-discriminatory (POND) basis. The regulation also requires credit institutions to:

- provide PSPs that enquire about access to payment account services with the criteria that the credit institution applies when considering requests for such access
- maintain arrangements to ensure those criteria are applied in a manner which ensures that access to payment account services is granted on a POND basis
- ensure that, where access is provided, it is sufficiently extensive to allow the PSP to provide payment services in an unhindered and efficient manner
- notify the FCA of the reasons where access is refused or withdrawn.

Both HMT and the FCA note that the regulation:

“does not impose an absolute obligation for credit institutions to grant access. The decision to work with a given payment institution is still a commercial one, with credit institutions able to take into account cost and risk”.²

While the requirements of Regulations 103 and 104 of the PSRs 2017 are not considered within scope of this document; firms are invited to consider the alignment of the requirements of these Regulations with Regulation 105. Further, the Payment Systems Regulator’s Specific Direction³ concerns services offered under Regulations 103, 104 and 105 of the PSRs 2017. This Direction is applicable to indirect access providers offering sponsor bank services; however, it represents a standard of good practice that this document has attempted to emulate.

1.2. Application to Firms

There are three broad types of regulatory supervised institutions of relevance to this document. They are as follows:

Credit Institution – where used in this document, this term has the meaning given to it by the PSRs 2017, derived from Article 4(1) of Regulation (EU) 575/2013; that being “an undertaking the business of which is to take

deposits or other repayable funds from the public and to grant credits for its account”, and is subject to the requirements of this, and other relevant, regulation. Specifically, these institutions operate under the supervisory purview (for conduct and financial crime) of the FCA.

Payment Service Provider (PSP) – where used in this document, this term has the meaning given to it by the PSRs 2017; however it should be noted that, for the explicit application of POND as required by part 105 of this same regulation, the PSRs consider this requirement to only apply to the following firms when they carry out payment services:

- a. authorised payment institutions
- b. small payment institutions
- c. registered account information service providers
- d. EEA authorised payment institutions
- e. EEA registered account information service providers
- f. electronic money institutions, including branches located in the EEA of such institutions whose head office is outside the EEA, in so far as the payment services provided by those branches are linked to the issuance of electronic money.

The FCA and PSR Approach documents also set out that they cover a party which has made an application to the FCA or the relevant competent authority in its home EEA state to be authorised or registered as any of the PSPs listed above. Therefore, references to PSPs in this document include prospective PSPs for the purposes of Regulation 105.

2. Section 16.8 of the FCA Approach to Payment Services and Electronic Money.

3. At the time of publication, the PSRs SDI is currently under review. The content of this document concerns the text of the proposed direction

In addition PSPs may also operate as a Money Service Business or Money Service Bureau (MSB); – where used in this document, this term has the meaning given to it by the Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017 (MLRs), that being “an undertaking which by way of business operates a currency exchange office, transmits money (or any representation of monetary value) by any means or cashes cheques which are made payable to customers”, and is subject to the requirements of this, and other relevant, regulation.

It is pertinent to note that credit institutions, including branches located in the EEA (point (g) within the PSRs 2017) are not within scope of the application of Regulation 105. Where appropriate in this document, PSPs and MSBs are referred to collectively as ‘applicants’. There are specific requirements that may rest solely on PSPs or MSBs, or providers in their dealings with PSPs or MSBs, and firms should seek their own legal guidance as to these requirements.

1.3. AML Supervision

There are two AML supervisors that oversee firms operating services based on access to payment accounts:

1. The FCA
2. HMRC

The appropriate supervisory authority is dependent on the regulatory environment within which a firm has chosen to offer its services. Firms are recommended to seek their own legal guidance as to the appropriate regulatory environment they are required to engage in, as this may impact the types of services that they can offer.

Given the changing payments market environment, there may be firms engaging in related activities that are not addressed by current regulation, or whose regulatory status is yet to be clarified. This document is unable to address possible issues raised by emerging business practices, technologies or regulatory decisions.

1.4. Interpretation and Implementation by Firms

As noted previously, firms are recommended to obtain their own legal opinion on what aspects of their business may be covered by a legal or regulatory requirement. These could derive from the following non-exhaustive list:

- The PSR’s 2017:
 - ◊ the FCA’s Approach Document
 - ◊ the PSR’s Approach Document
- HMRC’s registration requirements under the MLRs
- The PSR’s powers under FSBRA
- The PSR’s SD1.

2. PROVIDING ACCESS TO PAYMENT ACCOUNT SERVICES

2.1. Scope

The first part of this document is addressed generally to credit institutions that are providing, or seek to provide, access to payment account services to an applicant in the UK.

2.2. Good Practice Principles

2.2.1. Transparency and Clarity

- One of the main ways credit institutions can help improve the functioning of the market around access to payment account services for an applicant is by ensuring there is objectivity, clarity and transparency in their criteria for providing access to such services, including any minimum eligibility criteria such as acceptable payments volumes, indicative details of a firm's risk appetite and any items of regulatory compliance.⁴
- This information should be made available through standard responses to initial enquiries, or summary information on a publicly available and clearly signposted website.⁵
- Any initial criteria statement should contain sufficient information to potential applicants⁶ and be kept up to date.⁷
- The criteria should not seek to prescribe upfront conditions that are unnecessarily restrictive, for example, requiring membership of industry bodies/ organisations.
- Credit institutions should make clear to the applicant all the information, and any particular format of this information, that the applicant will need to submit, whether

at the start of an application or during the application.

- Credit institutions are reminded that clear and specific details of their own requirements and risk appetites are very helpful to an applicant in preparing for the application. Providing detailed guidance early on in the process may reduce the amount of manual intervention required in an applicant's application process, as the applicant is able to understand which elements of their business model or customers may require the provision of further information or justification and assist credit institutions in their assessment.
- It is good practice for a provider of payment account services to establish a justifiable pricing hierarchy within their framework of acceptable risk, that aligns with POND principles. This, or a fee guide structure, should be shared with an applicant, unless the institution considers this information to be commercially sensitive.
- It is not good practice for credit institutions to use unjustifiably excessive pricing as an alternative means of refusing an application.

2.2.2. Timescales

- A provider of payment account services should, having received an application for access, issue a formal recognition of its receipt and a written indicative timeline for the consideration of the application.
- While timescales will vary depending on the nature of application, as a guideline credit institutions should seek to reach a decision on an application in a timescale of between three to six months, or quicker where possible.

4. Sections 16.3 and 16.4 of the FCA Approach Document and Regulation 105(1) (b)

5. Section 16.14 of the FCA Approach Document and Regulation 105

6. Section 16.18 of the FCA's Approach Document

7. Section 16.19 of the FCA's Approach Document

- It is recognised that complex applications may take longer, and it is considered that a credit institution should respond within the above three to six months in order to clarify details of a longer review process.
- Where the credit institution considers it necessary to adjust the indicative timeline, they should discuss with the applicant these changes and the reasons for these changes.
- In order to keep the application process flowing smoothly, providers should ensure that any communication is timely and that requests for further information are made clearly.

2.2.3. Application Requirements

- Credit institutions should keep up a regular dialogue/correspondence with applicants throughout the application process, particularly to request any additional relevant information needed to make a decision.
- Where the independent verification of an applicant's submission is required by a credit institution, it is good practice that these auditing requirements are kept proportionate to the size of the applicant, and that any associated costs are not unnecessarily prohibitive to the applicant.
- Credit institutions should consider whether the submission of a similar external audit undertaken by an applicant prepared for another application may satisfy their internal policies.
- Where the risk profiles of the credit institution, as set out in its initial criteria statement, and the applicant differ, it is recommended that both parties communicate clearly and transparently regarding their differing risk assessments.

2.2.4. Dealing with New Entities

- When dealing with an applicant in the process of applying, or preparing to apply, for FCA authorisation, a credit institution should provide, if requested, the applicant with a letter of intent addressed to the FCA, stating that it is considering the applicant for an account, provided that the account application has progressed to a sufficient stage. Where an applicant has not begun, or is only at an early stage in the FCA authorisation process, a credit institution may consider whether or not it is appropriate to provide such a letter of intent.
- Where the FCA has given a decision in principle as to the authorisation of an applicant, pending the opening of suitable accounts, a credit institution that has previously provided a letter of intent as described above should continue to process the account opening request as though the relevant PSP was sufficiently authorised.

2.2.5. Declining Applications and Handling Appeals

- Credit institutions are reminded that their obligations under Regulation 105 include the notification to the FCA of reasons for their rejection of an application for payment account services, or withdrawal of existing services. This information is subsequently shared with the PSR.⁸
- To the extent that it is lawful, when considering the application, credit institutions should inform applicants as early in the application process as possible what issues are impeding or may impede their application and give the applicant time to address these issues.

8. FCA Approach Document 16.27 and Regulation 105

- The credit institution should provide an opportunity to discuss the application meaningfully and constructively with the applicant if the credit institution has specific concerns with the application. When exiting a customer, the credit institution should provide similar opportunities during the exiting process.
- As far as possible, credit institutions should ensure governance and application processes used to evaluate an application are specific and appropriate to the type of applicant, and that any final decision on an application has been reviewed by a person with sufficient authority before it is communicated to the applicant.
- If an application is refused, it is good practice for a credit institution to share relevant information with the applicant that would allow them to make a more successful application. This may include referring the applicant to this guidance document and noting which sections they should investigate in greater detail.
- When a credit institution decides to review the current provision of payment account services, to the extent possible (given lawful considerations, e.g. 'tipping off'), they should endeavour to inform the other party of the initiation of such a review and abide by industry good practice principles upon reaching a decision to no longer provide payment account services to their customer.
- Credit institutions should take into account best practice on exiting firms, such as the '[Principles for Exiting a Customer](#)' developed by UK Finance, when deemed necessary to no longer provide services to a firm.
- Credit institutions should have a mechanism to assist the applicant to make representations or appeal against a final decision relating to their application.
- Credit institutions are reminded of their obligation to provide to the FCA their duly motivated reasons for refusing a prospective PSP's request for access or withdraw such access from a PSP. This should include sufficient detail as requested by the FCA and PSR.

2.2.6. Ensuring Appropriate Knowledge of Applicant's Sector

- It is good practice that, as far as possible, a credit institution's decision-making process should be based on a good knowledge of the business sector of the applicant.
- Where the credit institution does not have detailed knowledge of a particular business sector, it is recommended that they request suitable engagement with the applicant and engage with other market participants or industry trade bodies in order to increase their knowledge of the sector, though this engagement may not affect the risk assessment the institution has made of the sector.
- It is considered good practice for the credit institution to take into account the risk mitigation measures and processes that the applicant has implemented, in order to reduce the risk associated with operating in particular jurisdictions and/or offering certain payment instruments.

2.3. Regulatory and Other Guidance

2.3.1. The Payments Services Regulations 2017: Regulation 105

The [Payment Services Regulations 2017](#) are the transposed UK law of the EU's Second [Payment Services Directive \(2015/2366\)](#). Regulation 105 of the PSRs 2017 requires that credit institutions must grant PSPs access to payment account services on a proportionate, objective and non-discriminatory (POND) basis. While the competent authority for the Payment Services Regulations is primarily the FCA, the PSR has responsibility as a competent authority in this context for Part 8 of the PSRs 2017, which concerns access to payment systems and bank accounts. Both the PSR and the FCA are competent authorities and a [Protocol](#) exists between the FCA and the PSR on the enforcement of Regulation 105 of the PSRs 2017.

2.3.2. The FCA's Approach Document

The FCA has published its [Approach Document](#) to the PSRs 2017. Part 16 of the Approach Document, PSPs' access to payment account services, covers the FCA's expectations around Regulation 105. Credit institutions offering payment account services should review this regulation in order to ensure that they reach compliance.

The guidance from the FCA (and PSR) also covers refusal of access and instances where access is withdrawn; this is covered in sections 16.28-16.31. A credit institution may refuse a PSP's request to access payment account services, or withdraw existing services, only for duly motivated reasons which must be proportionate, objective, and non-discriminatory. Refusals to grant access and withdrawal of access must be notified to the FCA (using the FCA's 'NOT002 Payment Account Service rejections or withdrawals' form).

2.3.3. The PSR's Approach

The PSR has published its [Approach Document](#) to the monitoring and enforcement of PSD2 which replicates the text of the FCA Approach Document.

2.3.4. The Joint Money Laundering Steering Group's (JMLSG) Expectations

The Joint Money Laundering Steering Group (JMLSG) recommends that relationships are treated on a case-by-case basis. This body is made up of the leading UK trade associations in the financial services industry. Its aim is to promulgate good practice in countering money laundering and to give practical assistance in interpreting the UK Money Laundering Regulations. This is primarily achieved by the publication of industry guidance. JMLSG has been producing money laundering guidance for the financial sector since 1990, initially in conjunction with the Bank of England, and latterly to provide regularly updated guidance on the various money laundering regulations in force. JMLSG periodically reviews its guidance and makes changes and additions as required.

The latest versions of the guidance documents are available [here](#). There are three parts to the guidance. Part II includes a section (part 1A) on Money Service Businesses (as customers of banks) (MSBs). The section includes:

- an overview of the sector
- an analysis of the money laundering and terrorist financing risks associated with Money Service Businesses (MSBs)
- recommended risk assessment considerations
- recommended customer due diligence
- enhanced due diligence advice
- ongoing monitoring guidance.

The section on Risk Assessment makes clear that:

“the risk inherent in the MSB sector is not the nature of the sector itself, but the potential for the abuse of the sector by criminals. It is therefore important that firms understand these potential risks and manage them effectively. This risk will be greater in some MSBs than in others, and firms should be able to carry out a risk assessment that allows such a judgement to be made”.

Part II also includes a section (Sector 3) on e-money which may help credit institutions understand the obligations on Electronic Money Institutions.

2.3.5. Code of Conduct for Indirect Access Providers

The voluntary [Code of Conduct for Indirect Access Providers](#) has been developed by Indirect Access Providers (IAPs) in consultation with the Payment Systems Regulator (PSR) to address concerns around the commercial access arrangements they provide to Payment Service Providers (PSPs) requiring Indirect Access Services to UK payment systems. Credit institutions are invited to consider whether the suite of services they offer are relevant to this code of conduct and how they could commit to upholding this code.

GAINING ACCESS TO PAYMENT ACCOUNT SERVICES

3.1. Scope

This second part of the document is addressed generally to applicants seeking access to payment account services from a credit institution or bank in the UK.

3.2. Good Practice Principles

3.2.1. Key Application Expectations

- As per sections 16.3 and 16.4 of the FCA Approach document, a credit institution should clearly signpost “the channels through which potential applicants can make enquiries about access to payment account services (e.g. a dedicated email address or telephone line). Through these channels, information should be readily available about the payment account services offered by the credit institution, how to apply and the estimated timeframe for decisions to be made on applications”.
- Any credit institution that receives an application is likely to request copies of appropriate compliance policies, in particular policies drafted in relation to the regulation and good practice principles highlighted in this document, and may additionally request evidence of compliance with these policies and any other relevant rules, regulations and guidance by way of a programme review or – if necessary – an audit.
- The kinds of questions that credit institutions might typically ask during an application can be found in the Annex.

- The applicant should endeavour to gather as much information known or expected to be required by the bank or credit institution during an application prior to beginning the application. Examples of points of compliance that are recommended may be found in Sections 3.3 and 3.4.
- Applicants are reminded that an application process should be seen as an opportunity to demonstrate their competence and knowledge of the sector in which they operate, and not solely as an exercise in providing the requested documentation in support of an application.

3.2.2. Transparency

- Applicants should be transparent about the nature of their business, for example, being clear as to whether intermediaries are used in business processes, or whether key risk management functions are outsourced and how third party’s performance and compliance is monitored by the applicant.
- In some instances, the credit institution may ask an applicant to provide further information to support their application.
- For example, this may be required where the applicant provides services to industries, counterparties or jurisdictions that the credit institution deems pose a higher money laundering, terrorist financing or sanctions risk; where the applicant provides high risk

instruments; or where the applicant has a complex ownership structure, etc. This risk assessment may be based on existing international guidance (such as sanctions policy) or internal policies.

- As connectivity to certain payment systems may carry additional requirements, it is important to clearly inform the credit institution of any connectivity requests. An applicant may be required to provide additional information to support this or it may be necessary for the credit institution to specify additional functional requirements (e.g. formatting of payment messages).
- Where the risk profiles of the credit institution, as set out in its initial criteria statement, and the applicant differ, it is recommended that both parties communicate clearly and transparently regarding their differing risk assessments.
- Information pertinent to the risk mitigation strategies that have been undertaken by the applicant should be shared openly with the credit institution in order to assist the credit institution in understanding the risk profile of the applicant.

3.2.3. Timescales

- In order to keep the application process flowing smoothly, applicants should answer questions promptly and provide documentation in a timely manner and, where this is not possible, inform the credit institution when it can expect a response.

3.2.4. Complaints

- Applicants are recommended to discuss with the credit institution reviewing their application any concerns that they have with the application process or final decision prior to making any formal complaint to a relevant regulator.
- Both parties to a complaint should engage openly and constructively with each other in their attempt to resolve a complaint.

3.2.5. Undertaking FCA Application

- Under the PSRs 2017/EMRs, the FCA is unable to grant an authorisation to an applicant firm unless the relevant conditions are satisfied. For PSPs, this includes “adequate measures for the purpose of safeguarding payment service users’ funds”; typically, through placing them in a designated account with an authorised credit institution. The FCA’s expectation is that an application for authorisation will be able to confirm with whom the applicant is in discussion for such an account(s), not that the account is opened at the time of application. Instead, the FCA recognises that the applicant will likely be in ongoing discussions with a credit institution(s) in parallel to the application for authorisation.
- An applicant should request from the institution from which they are requesting payment account services a letter of intent addressed to the FCA stating that it is considering the applicant for an account.
- Where the FCA has completed its assessment of the application but discussions with the credit institution(s) are still ongoing, it may nevertheless be able to provide the applicant with a decision in principle. This

may be conditional on the account(s) being opened. Although not yet authorised, it does provide certainty that the FCA will authorise the applicant subject to receiving confirmation of the account(s) being opened. In such circumstances, credit institutions should be able to open such accounts for applicants prior to them receiving their full authorisation as a PSP and being entered on the Financial Services Register.

3.2.6. Other Considerations

- As noted above, the decision for a credit institution to work with a PSP is also a commercial one, and therefore PSPs should expect that there will be commercial considerations as part of the application process, alongside the previously discussed factors of internal policies, AML considerations and other factors.
- It is recommended that an applicant clearly communicate to credit institutions any such factors that may affect the commercial viability of any agreement and ensure the credit institution is aware of items such as the expected payment volumes or other business metrics at an early stage in the process.

3.3. Relevant Guidance Documents: FCA Regulated Firms

This section contains links to documents that explain the expectations of banks providing access, including anti-money laundering (AML), sanctions and wire transfer responsibilities. A PSP seeking access to a bank account should be familiar with the following rules and regulations⁹ and may be required by the bank to provide evidence of policies or compliance.

The table overleaf outlines the documents recommended for consideration regarding the compliance of institutions with regards AML/CTF concerns. Where necessary further information is available in subsequent sections. Not all of the documents noted below may be a matter of regulatory compliance, depending on the firm in question. However, these references have been provided as relevant documentation of good practices and other key principles associated with the purpose of this document.

9. Rules and regulations cited are current at time of publication, though several are under review or in the process of being updated.

Document	Sections of note	Source
FCA Financial Crime Guide for Firms		https://www.fca.org.uk/publication/policy/ps16-19.pdf
FCA Financial crime: a guide for firms – Part 1	<ul style="list-style-type: none"> • 6 – Bribery and Corruption • 7 – Sanctions and Asset Freezes 	https://www.handbook.fca.org.uk/handbook/document/FC1_FCA_20150427.pdf
FCA Financial crime: a guide for firms – Part 2	<ul style="list-style-type: none"> • All relevant anti-fraud procedures 	https://www.handbook.fca.org.uk/handbook/document/FC2_FCA_20160307.pdf
UK Finance [BBA] Anti-Bribery and Corruption Guidance		https://www.bba.org.uk/policy/financial-crime/anti-bribery-and-corruption/anti-bribery-and-corruption-guidance/
Ministry of Justice: The Bribery Act 2010 – Guidance		https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf
SYSC – Systems and Controls	<ul style="list-style-type: none"> • 6.3.9 – The money laundering reporting officer <p>[Provided for guidance only for firms where the SYSC does not apply.]</p>	https://www.handbook.fca.org.uk/handbook/SYSC/6.pdf
JMLSG – Final Guidance Part I	<ul style="list-style-type: none"> • Chapter 4 – Risk-based approach (including annexes) • 5.5.13-5.5.36 – Politically exposed persons; • 5.7.9-21 – Ongoing Transaction Monitoring; • Annexes 5-1-IV – Risk Factors SDD & EDD; • SARS 	http://www.jmlsg.org.uk/
JMLSG – Final Guidance Part II	<ul style="list-style-type: none"> • Part II, 1A – Money service businesses (as customers of banks). 	http://www.jmlsg.org.uk/

Document	Sections of note	Source
The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017	<ul style="list-style-type: none"> • Regulation 3 – General interpretation; • Regulation 28 – Customer due diligence measures; • Regulation 33 – Obligation to apply enhanced customer due diligence; • Regulation 35 – Enhanced customer due diligence: politically exposed persons; • Regulation 37 – Application of simplified customer due diligence; • Regulation 38 – Electronic money; • Schedule 2 – Activities listed in points 2 to 12, 14 and 15 of Annex I to the Capital Requirements Directive. 	http://www.legislation.gov.uk/uksi/2017/692/contents/made
Terrorism Acts 2016	<ul style="list-style-type: none"> • Part 3 	https://www.gov.uk/government/publications/the-terrorism-acts-in-2016
Proceeds of Crime Act 2002(3)	<ul style="list-style-type: none"> • Part 7 – Money Laundering. 	https://www.legislation.gov.uk/ukpga/2002/29/contents
Criminal Finances Act 2017		http://www.legislation.gov.uk/ukpga/2017/22/contents/enacted
Criminal Finances Act 2017 (implementation notes)		https://www.gov.uk/government/collections/criminal-finances-act-2017
Wolfsberg Guidance on Risk Assessments		https://www.wolfsberg-principles.com
FCA Financial Crime Guide for Firms		https://www.fca.org.uk/publication/policy/ps16-19.pdf
Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds ¹⁰		https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32015R0847
UK Finance Funds Transfer Regulation 'How To' Guide		https://www.ukfinance.org.uk/wp-content/uploads/2018/08/UK-Finance-How-To-Guide-for-the-Funds-Transfer-Regulation-Aug-2018-002.pdf
National Risk Assessment		https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017

10. Also known as the 'Wire Transfer Regulations' or 'Funds Transfer Regulations'.

3.3.1. JMLSG

Firms should familiarise themselves with the relevant sections of the [Joint Money Laundering Steering Group Guidance](#). For PSPs seeking access this includes Part II, 1A.

3.3.2. Anti-money laundering

The [Money Laundering, Terrorist Financing and Transfer of Funds \(Information on the Payer\) Regulations 2017](#) apply to banks, building societies and credit unions. They also apply to other firms undertaking certain financial activities (see Schedule 2 of the regulations). These will normally include investment managers and stockbrokers, e-money institutions, payment institutions, consumer credit firms offering lending services, financial advisors, investment firms, asset managers and those providing safety deposit services. These regulations require firms to apply risk-based customer due diligence measures, ongoing monitoring of transactions and take other steps to prevent services from being used for money laundering or terrorist financing.

3.3.3. Wire Transfers Regulations / Funds Transfer Regulations

[Regulation \(EU\) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds \(known as the Wire Transfer Regulations or Funds Transfer Regulations\)](#). The Funds Transfer Regulations sit alongside the Money Laundering, Terrorist Financing and Transfer of Funds Regulations.

As regards scope, the regulation applies to transfers of funds, in any currency, sent or received by a PSP or an intermediary PSP established in the EU.

The PSP of the payer is required to provide specific information on both payer and payee, for example, the name of the payee and the payee's payment account number and to check the accuracy of the information provided.

The PSP of the payee and any intermediary PSP are required to have effective procedures in place for detecting whether the information provided on payer or payee is missing or incomplete. In the case of missing or incomplete information, the PSPs must have effective risk-based procedures for deciding whether to execute, reject or suspend a transfer of funds lacking the required information.

3.3.4. UK Finance Funds Transfer Regulation 'How To' Guide

In 2018 UK Finance published a '[How To' Guide on the Wire Transfers Regulation](#)' (also known as the Fund Transfers Regulation). This interpretative guidance is intended to provide clarity and encourage market harmonisation. The objective is to support firms to ensure that systems and processes can identify the highest risk transactions, that 'false-positives' are reduced wherever possible, and that straight-through-processing is not hindered.

3.3.5. Senior Manager Arrangements for Systems and Controls (SYSC) - SYSC 6: Compliance, internal audit and financial crime

The SYSC is part of the FCA Handbook of rules and guidance. The FCA Handbook contains the complete record of FCA Legal Instruments. Part of the Handbook covers the Senior Manager Arrangements for Systems and Controls (SYSC). Section 6 of these SYSC rules deals with compliance, internal audit and financial crime. Whilst SYSC may not apply to all applicants, it is recommended to consider the contained guidance in the implementation of policies alongside guidance similarly articulated in the MLRs.

For example, it states that “A firm must ensure that the policies and procedures established under SYSC 6.1.1 include systems and controls that:

1. enable it to identify, assess, monitor and manage money laundering risk
2. are comprehensive and proportionate to the nature, scale and complexity of its activities

3.4. Relevant Guidance Documents: HMRC Regulated Firms

The HMRC [website](#) details its money laundering supervision for MSBs. Documented guidance on the anti-money laundering supervision required for a MSB is available [here](#) and the online application form is available at [this link](#).

According to the website:

“If you’re already supervised by the [FCA](#), you do not also need to register with HMRC. You must not run a money service business until you’ve registered. The term money service business has a special meaning under the [Regulations](#). Businesses that transfer money (money transmitters) must follow the [EU Funds Transfer Regulation](#) in order to reduce the risk of money laundering and terrorist financing. When you put anti-money laundering policies and procedures in place, you must make sure they cover all your activities carried out under the regulations.”

Firms are expected to register with HMRC if they:

- act as a bureau de change or currency exchange office
- transmit money, or any representation of money, including if the business has an exemption certificate from the FCA to be a small e-money issuer – just collecting and delivering money as a cash courier is not transmitting money
- cash cheques that are payable to their customers
- take payments on telecommunications, digital and IT devices and act as an intermediary between a payer and supplier
- provide a payment service for utility and other household bills.

SUMMARY

In summary, applicants seeking access to payment account services should:

- establish their own view as to what regulatory and legal requirements they should be governed under in relation to the form of service that they wish to offer
- familiarise themselves with the JMLSG Part II.1A because that sets out industry good practice of banks providing access: <http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current>
- familiarise themselves and comply with either [JMLSG](#) guidance or HMRC's guidance for [money laundering supervision that has been issued to MSBs](#), depending on who the relevant money laundering supervisor is for your business
- familiarise themselves (if relevant) with the additional documents referred to in HMRC's guidance to MSBs (e.g. FCA's guidance on Politically Exposed Persons)
- for firms subject to the MLRs, review: <https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing>
- familiarise themselves with the expectations of banks that provide access to you as payer/payee
- it may also be useful for PSPs to familiarise themselves with the responsibility of credit institutions providing access under Regulation 105 of the PSRs, under JMLSG. This is to help them understand the responsibilities of the credit institution and what these firms will therefore consider when taking applications from PSPs.

ANNEX 1

This annex provides a high-level overview of the kind of questions/evidence that may be included in an applicant's application process – it is indicative and designed to help PSPs to anticipate the kinds of things they may need to prepare. This list is not to be considered exhaustive and each credit institution offering access will have an application process that reflects their business and risk appetite.

Information

You are likely to be asked to confirm and/or provide evidence for some or all of the following:

- information about your business – such as business plan including activity profile, your organisational structure, public documents about what you do, your regulatory permissions, who you provide services to and where; beneficial ownership, officials, regulated status
- information on your total client base (for example, total numbers, the percentage of business and individual clients, the industry types of the business clients, locations of client base, number of PEP clients)
- the type of service/s being applied for (for example corporate accounts, payment accounts, safeguarding accounts, foreign exchange liquidity services)
- the level of knowledge, experience and independence of your Money Laundering Reporting Officer or nominated officer
- your approach to governance and understanding and controlling your risks
- your adherence to industry good practice guidance, such as the Wolfsberg Transparency Principles
- your AML reporting, training and record keeping procedures.

Document submissions

You may also be asked to provide further documentary evidence, such as the following:

- latest fulfilled unabbreviated accounts which should include a profit and loss statement. Being loss-making or a start-up will not necessarily be an issue, provided you can show adequate sources of funding to support your business:
 - ◊ if the last year's accounts are more than six months old, either interim or monthly management accounts from the end of the last year to date
 - ◊ current business plan and cash flow forecast for 12 months (especially if entity is less than two years old).
- financial crime policy (and procedures):
- client identification and verification requirements and processes
- KYC policy (and procedures) - If not contained within your Financial Crime Policy KYC/ Due Diligence & Risk Categorisation (onboarding and in-flight);
- Suspicious Activity Reports (SARs) & Reporting Procedures; PEPs procedures and policies

-
- AML and CTF policy (and procedures), transaction monitoring and training - If not contained within your Financial Crime Policy
 - ◊ sanctions procedures and policies (including systems used, fuzzy logic settings, lists screened against)
 - ◊ prohibited business policy / standards (for example, does the business deal with cryptocurrency, gambling companies, military contracts, pornography?).
 - Anti-Bribery and Corruption procedures and policies (to include Gifts and Hospitality, Whistle Blowing Policy)
 - Fraud policy (and procedures) - if not contained within your Financial Crime Policy
 - full ownership structure chart (including parents and subsidiaries).
 - ◊ If you have a Politically Exposed Person “PEP”(s) within your directorship, leadership, board or ownership structure, you may be asked for photographic identification in the form of a passport or driving licence, confirming the date of birth and current address of the individual(s). If the PEP is a foreign PEP you may be asked for the source of wealth.
 - Confirmation and supporting evidence, such as minutes, that the firm’s management holds regular meetings where financial crime is a prominent feature.
 - Business wide risk assessment
 - Your risk appetite statement
 - FCA submission document - for applicants seeking regulatory approval
 - If using agents or outsourcing key risk functions, evidence of how this is overseen
 - Audit reports or programme reviews.

