Funds Transfer Regulation – 'How to' interpretative guidance

In 2015 the updated Funds Transfer Regulation (FTR) (also known as the Wire Transfer Regulation) was published. In 2017, the Council of the European Supervisory Authorities (ESAs) published their guidance for the FTR, with an implementation date of 16 July 2018. UK Finance engaged with its members on the issue of interpretation and compliance. It was clear that there were a number of areas where firms felt that there could be more clarity for the market. There were also areas where firms were taking different approaches with regard to how to implement the FTR requirements. This led to a lack of harmonisation that increased the volume of stopped and rejected payments, and led to inconsistent treatments.

As a result, UK Finance set out to work with its members to produce an additional voluntary guidance document. This 'How To' interpretative guidance is intended to provide clarity and encourage market harmonisation on points material to, for example, straight-through processing.

These guidelines have been prepared for general guidance only. The application of issues covered by them can vary widely depending on the specific facts and circumstances concerned, including the different activities, relationships and roles of the parties involved. This guidance is voluntary and is in no way intended to replace or add to the legal requirements laid out in the FTR. UK Finance does not accept any legal responsibility or liability for these guidelines. In addition, these guidelines are not intended to be used as a substitute for formal legal advice.

The objective of this 'How To' analysis is to support focused efforts by the industry to meet their AML and compliance objectives by ensuring that:

- systems and processes can identify the highest risk transactions
  'false-positives' are reduced
- wherever possible, straight-through-processing is not hindered.

*** Further updates to the guidance: The guidance will be reviewed periodically to ensure that it is still adding value for firms in the market and is accurate. In particular, in June 2018 the Bank of England published its consultation on its new ISO20022 message for the UK, the Common UK Credit Message (CCM). Generally speaking, the How To guide reflects the structure of the CCM (for example the use of names and addresses). However, there are some proposed new elements that, if accepted during the consultation process, will need to be factored in to the How To guide. These include: Purpose Codes, LEIs, and Personal Identifiers. UK Finance will review the How To guide following the finalisation of the CCM to ensure that it takes into account all relevant changes.*

Conclusion of the Brexit negotiations may also have an impact which will be considered in due course.

Funds Transfer Regulation – How To guide

	Articles	ESAs Guidelines	How-to comments
CHAPTER 1 - SUBJECT MATTER, SCOPE AND DEFINITIONS			
	Article 1 - Subject Matter		
Art 1	This Regulation lays down rules on the information on payers and payees, accompanying transfers of funds, in any currency, for the purposes of preventing, detecting and investigating money laundering and terrorist financing, where at least one of the payment service providers involved in the transfer of funds is established in the Union.		
	Article 2 - Scope		
Art 2(1)	This Regulation shall apply to transfers of funds, in any currency, which are sent or received by a payment service provider or an intermediary payment service provider established in the Union.		**Discussion**: It will be difficult to list all payment message types and may become quickly out of date. It is also important for firms to consider the applicability of MLRs/ESA guidance to branches and subsidiaries located outside of the EEA, where the parent company is located within the EEA. It is also noted that the Wolfsberg Group state in their 2017 Payment Transparency Standards that the introduction of MT202COV in 2009 was part of the broader industry efforts to comply with international

			ML/TF standards on payment transparency. MT202COV is to be used for cover payments and allows for the replication of both originator and beneficiary information. MT202 is to be used where the transfer of funds is unrelated to an underlying customer credit transfer sent by the cover method. **HOW TO: As regards payment message types in scope, any message which effects a transfer of funds shall be deemed to be in scope"**
Art 2(2)	This Regulation shall not apply to the services listed in points (a) to (m) and (o) of Article 3 of Directive 2007/64/EC.		**Discussion:** Securities payments are deemed out of scope for this regulation. We understand that some firms are treating these transactions as in scope which is causing issues for other firms. While supporting firms that wish to apply high levels of due diligence, there is a risk of causing unnecessary delay or impact if firms choose to treat securities transactions as if they are in scope. **HOW TO**: Firms are encouraged to review their procedures to ensure that they are clear on out of scope transactions.
Art 2(3)	This Regulation shall not apply to transfers of funds carried out using a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or	(14) When applying the exemption in point (3) of Article 2 of Regulation (EU) 2015/847, PSPs and IPSPs should ensure that the transfer of funds is accompanied by the number of the card, instrument or digital device, for example the Primary Account	Art 2(3)b states that the Regulation does apply for person to person transfers. Section 15 of the guidelines states that the exemption will only continue to apply if PSP can demonstrate that it is for goods or services.

	postpaid device with similar characteristics, where the following conditions are met: (a)that card, instrument or device is used exclusively to pay for goods or services; and (b)the number of that card, instrument or device accompanies all transfers flowing from the transaction. However, this Regulation shall apply when a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics, is used in order to effect a person-to-person transfer of funds.	Number (PAN), and that that number is provided in a way that allows the transfer to be traced back to the payer. 15. Where the card, instrument or device can be used to effect both person-to-person transfers of funds and payments for goods or services, PSPs and IPSPs will be able to apply this exemption only if they are able to determine that the transfer of funds is not a person-to person transfer of funds, but constitutes a payment for goods or services instead.	**HOW TO:** Firms are encouraged to review their procedures for identifying and documenting that transfers by card, instrument or device are for goods or services, where the exemption applies, as opposed to person-to-person transfers.
Art 2(4)	This Regulation shall not apply to persons that have no activity other than to convert paper documents into electronic data and that do so pursuant to a contract with a payment service provider, or to persons that have no activity other than to provide payment service providers with messaging or other support systems for transmitting funds or with clearing and settlement systems.		

	This Regulation shall not apply to transfers of funds: (a)that involve the payer withdrawing cash from the payer's own payment account; (b)that transfer funds to a public authority as payment for taxes, fines or other levies within a Member State; (c)where both the payer and the payee are payment service providers acting on their own behalf; (d)that are carried out through cheque images exchanges, including truncated cheques.		
Art 2(5)	A Member State may decide not to apply this Regulation to transfers of funds within its territory to a payee's payment account permitting payment exclusively for the provision of goods or services where all of the following conditions are met: (a)the payment service provider of the payee is subject to Directive (EU) 2015/849; (b)the payment service provider of the payee is able to trace back, through the payee, by means of a unique transaction	(11) To apply these exemptions and derogations, PSPs and IPSPs should have in place systems and controls to ensure the conditions for these exemptions and derogations are met. PSPs and IPSPs that are unable to establish that the conditions for these exemptions are met should comply with Regulation (EU) 2015/847 in respect of all transfers of funds.	Discussion: It is noted that some firms are not making use of the exemptions in the Regulations, namely on transfers below the EUR 1000 threshold and the intra-EU transfers. As per the Guidelines, firms that do not have in place the systems to "ensure the conditions for these exemptions and derogations are met" would not apply them. Nevertheless, there may be challenges around fragmentation. Variation in use of exemptions is partly determined by type of establishment, business model and geographical reach. Variation is also driven by well-known difficulties in identifying linked transactions, particularly in real

	identifier, the transfer of funds from the person who has an agreement with the payee for the provision of goods or services; (c)the amount of the transfer of funds does not exceed EUR 1 000.		time. It was agreed that, given these issues, full market convergence is not seen as a realistic goal. An alternative approach was noted where market practice converges around transparency and dialogue, both for sending and receiving firms. It was also noted that there may be benefits for the industry if more information is routinely provided, rather than less. **HOW TO**: Given the Regulation's overall goal of providing law enforcement and regulated firms with an adequate set of information to identify and prevent money laundering and terrorist financing, there are benefits if firms do not make use of the exemptions. Where firms choose or are required for technical reasons to make use of the exemptions, they are encouraged to take proactive steps to make this clear to receiving firms, including responding promptly and fully to queries. Likewise, receiving firms raising queries are encouraged to check in all cases whether sending firms are making use of the exemptions.
	Article 3 - Definitions		
Art 3(1)	'terrorist financing' means terrorist financing as defined in Article 1(5) of Directive (EU) 2015/849;		

Art 3(2)	'money laundering' means the money laundering activities referred to in Article 1(3) and (4) of Directive (EU) 2015/849;		
Art 3(3)	'payer' means a person that holds a payment account and allows a transfer of funds from that payment account, or, where there is no payment account, that gives a transfer of funds order.		
Art 3(4)	'payee' means a person that is the intended recipient of the transfer of funds;		
Art 3(5)	'payment service provider' means the categories of payment service provider referred to in Article 1(1) of Directive 2007/64/EC, natural or legal persons benefiting from a waiver pursuant to Article 26 thereof and legal persons benefiting from a waiver pursuant to Article 9 of Directive 2009/110/EC of the European Parliament and of the Council [(19)], providing transfer of funds services;	(8) A PSP should establish for each transfer of funds whether it acts as the PSP of the payer, as the PSP of the payee or as an IPSP. This will determine what information has to accompany a transfer of funds and the steps the PSP or IPSP has to take to comply with Regulation (EU) 2015/847.	
Art 3(6)	'intermediary payment service provider' means a payment service provider that is not the payment service provider of the payer or of the payee and that receives and transmits a transfer of funds on behalf of the payment service provider of the payer or of the payee		

	or of another intermediary payment service provider;		
Art 3(7)	'payment account' means a payment account as defined in point (14) of Article 4 of Directive 2007/64/EC;		
Art 3(8)	'funds' means funds as defined in point (15) of Article 4 of Directive 2007/64/EC;		
Art 3(9)	'transfer of funds' means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same, including: (a)a credit transfer as defined in point (1) of Article 2 of Regulation (EU) No 260/2012; (b)a direct debit as defined in point (2) of Article 2 of Regulation (EU) No 260/2012; (c)a money remittance as defined in point (13) of Article 4 of Directive 2007/64/EC, whether national or cross border;	(9) Where a transfer of funds is a direct debit as defined in point (9)(b) of Article 3 of Regulation (EU) 2015/847, the PSP of the payee should send required information on the payer and the payee to the PSP of the payer as part of the direct debit collection. The PSP of the payee and the IPSP may then assume that the information requirements in point (2) and (4) of Article 4 and points (1) and (2) of Article 5 of Regulation (EU) 2015/847 are met.	

	(d)a transfer carried out using a payment card, an electronic money instrument, or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics;		
Art 3(10)	'batch file transfer' means a bundle of several individual transfers of funds put together for transmission;		
Art 3(11)	'unique transaction identifier' means a combination of letters, numbers or symbols determined by the payment service provider, in accordance with the protocols of the payment and settlement systems or messaging systems used for the transfer of funds, which permits the traceability of the transaction back to the payer and the payee;		
Art 3(12)	'person-to-person transfer of funds' means a transaction between natural persons acting, as consumers, for purposes other than trade, business or profession.		
CHAPTER 2 - OBLIGATIONS ON PAYMENT SERVICE PROVIDERS			
Section 1 - Obligations on the payment service provider of the payer			
Art 4(1)	The payment service provider of the payer shall ensure that transfers of funds are		**How To:** Information to be included in messages: Payer Name -

	accompanied by the following information on the payer: (a) the name of the payer; (b)the payer's payment account number; and (c)the payer's address, official personal document number, customer identification number or date and place of birth.		The firm should document in its procedures which payer name is to be populated in outbound Wire Transfers. The firm should, for a customer who is a natural person, populate Wire Transfers with the full legal name of the customer that has been identified and verified as part of Customer Due Diligence (CDD). The firm should include the full legal names of joint account holders in Wire Transfers. The firm should, for body corporates (i.e. an entity with its own legal personality), populate Wire Transfers with the full legal name that was identified and verified as part of CDD, giving priority to the registered legal name where applicable. The firm should, for customers that do not have a legal personality that is separate from their officers (e.g. unincorporated trusts, clubs and societies), populate Wire Transfers with the name of the customer that has been identified and verified, rather than the names of the officers (e.g. the name of the trust as given on the trust deed). Firms should consider when to supplement a sole trader's full legal name in Wire Transfers with their trading name. **Information to be included in messages - Payer Address** The Business should set out in its procedures which of the addresses recorded in its customers systems are to be used to populate Wire Transfers. This includes

			managing cases where multiple account holders with different addresses may exist, in which case the address of the primary or first named account holder is likely to be sufficient. The firm should populate Wire Transfers with the address that has been identified and verified as part of CDD on the customer. To this end, the firm should prioritise full postal address in messages in accordance with the resident country conventions such as Country, Town, City, State/Province/Municipality, Street Name, Building Number or Building Name and Postal Code. Note: When determining the materiality of a PSP's non-compliance as identified through monitoring of inbound Wire Transfers, firms should consider whether the information on the payer's address is sufficient to identify the location of the payer for sanctions purposes and for law enforcement to trace the payer (e.g. at a minimum, country and city/town). Including full country names as recognised by the United Nations will improve clarity. ISO 3166 2-Character country codes may be used as a preferred approach for SWIFT MT 103, MT 202 COV and related structured messages for Payer and Payee fields as an alternative to full country name. Information to be included in messages - Technical Limitations

			Firms should, recognising that certain external payments infrastructures may limit the amount of information that can be included in Wire Transfers, have procedures in place for addressing these limitations following guidance as provided by the external payments infrastructure (e.g. SWIFT). Where character limits restrict the ability for the firm to provide the payer's full legal name (e.g. in the case of joint account holders), the firm should document the order of priority for populating Wire Transfers with payer information, giving priority to payer information used in sanctions screening and used by law enforcement to trace the payer (e.g. de-prioritising titles and full middle names, whilst prioritising the initial of the given name and the full family name). Firms should consider situations such as: Where there are primary and secondary accountholders, firms should populate Wire Transfers with the name of the primary account holder in full before the secondary account holder information is provided. In addition, the family name should receive priority over given names. Where there are joint accounts where there is no primary and secondary account holders, firms should provide both names, giving priority to family name over given names.

Art 4(2)	The payment service provider of the payer shall ensure that transfers of funds are accompanied by the following information on the payee: (a) the name of the payee; and (b) the payee's payment account number.		
Art 4(3)	By way of derogation from point (b) of paragraph 1 and point (b) of paragraph 2, in the case of a transfer not made from or to a payment account, the payment service provider of the payer shall ensure that the transfer of funds is accompanied by a unique transaction identifier rather than the payment account number(s).		
Art 4(4)	Before transferring funds, the payment service provider of the payer shall verify the accuracy of the information referred to in paragraph 1 on the basis of documents, data or information obtained from a reliable and independent source.		
Art 4(5)	Verification as referred to in paragraph 4 shall be deemed to have taken place where:		

	(a)a payer's identity has been verified in accordance with Article 13 of Directive (EU) 2015/849 and the information obtained pursuant to that verification has been stored in accordance with Article 40 of that Directive; or (b)Article 14(5) of Directive (EU) 2015/849 applies to the payer.		
Art 4(6)	Without prejudice to the derogations provided for in Articles 5 and 6, the payment service provider of the payer shall not execute any transfer of funds before ensuring full compliance with this Article.		
	Article 5 – Transfers of funds within the Union		
Art 5(1)	By way of derogation from Article 4(1) and (2), where all payment service providers involved in the payment chain are established in the Union, transfers of funds shall be accompanied by at least the payment account number of both the payer and the payee or, where Article 4(3) applies, the unique transaction identifier, without prejudice to the information requirements laid down in Regulation (EU) No 260/2012, where applicable.	(12) In order to apply the derogation in Article 5 of Regulation (EU) 2015/847: a) PSPs of the payee should be able to determine that the PSP of the payer is based in the Union or an EEA Member State; and b) IPSPs should be able to determine that the PSP of the payer and the PSP of the payee are based in the Union or an EEA Member State. (13) PSPs and IPSPs should treat countries as third countries if they are part of the Single Euro	

		Payments Area (SEPA) but are not also Member States of the Union or EEA. Where a Member State has concluded a bilateral agreement with a third country or territory outside the Union in accordance with Article 24 of Regulation (EU) 2015/847, PSPs and IPSPs in that Member State may treat transfers of funds from or to that third country or territory as domestic transfers of funds.	
Art 5(2)	Notwithstanding paragraph 1, the payment service provider of the payer shall, within three working days of receiving a request for information from the payment service provider of the payee or from the intermediary payment service provider, make available the following: (a)for transfers of funds exceeding EUR 1 000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked, the information on the payer or the payee in accordance with Article 4; (b)for transfers of funds not exceeding EUR 1 000 that do not appear to be linked to other transfers of funds which, together	(16) In order to apply rules in Articles 5, 6 and 7 of Regulation (EU) 2015/847 related to transfers of funds that do not exceed EUR 1 000, PSPs and IPSPs should have in place policies and procedures to detect transfers of funds that appear to be linked. PSPs and IPSPs should treat transfers of funds as linked if these fund transfers are being sent: a) from the same payment account to the same payment account, or, where the transfer is not made to or from a payment account, from the same payer to the same payee; and b) within a reasonable, short timeframe, which should be set by the PSP in a way that is	**Discussion:** The Final Guidelines do not specify what criteria should be used by firms to determine a suitable timeframe to assess transactions for being linked. The Final Guidelines refer to a 'reasonable, short timeframe…commensurate with the ML/TF risk to which their business is exposed' but it is not clear whether this allows firms to apply existing ML/TF monitoring for linked transactions. In some cases, these existing systems may not be relevant for the derogation scope (e.g. for transactions involving higher risk jurisdictions). In a related but different AML context, HMRC guidance on AML Supervision for Money Service Businesses notes "There is no specific time period over which transactions may be linked, after which enhanced due

	with the transfer in question, exceed EUR 1 000, at least: (i)the names of the payer and of the payee; and (ii)the payment account numbers of the payer and of the payee or, where Article 4(3) applies, the unique transaction identifier.	commensurate with the ML/TF risk to which their business is exposed. (17) PSPs and IPSPs should determine whether other scenarios might also give rise to linked transactions, and if so, reflect these in their policies and procedures.	diligence is not necessary. The period of time depends on the customers, product and destination countries. HMRC recommends that businesses consider checking for linked transactions over a minimum rolling 90-day period.". **HOW TO**: Transactions that are "deemed to be linked" should be individually assessed against the full set of required information (i.e. not against the set of information required under the exemption). Article 9 of the Regulation and para 44 – 46 of the Final Guidelines confirm that missing information may not, by itself give rise to suspicion but should be taken into account as part of a firms' wider criteria and procedures. **HOW TO**: It seems that a PSP can avoid the requirement to check for linked transactions by ignoring the derogation, and instead checking on all traffic for missing information. While the ideal approach would be for a harmonised approach across the market, known difficulties in identifying linked transactions makes this an unrealistic goal. Where firms choose or are required for technical reasons to make use of the exemptions, they are encouraged to take proactive steps to make this clear to receiving firms, including responding promptly and fully to queries. Likewise, receiving firms raising queries are encouraged to check in all cases

			whether sending firms are making use of the exemptions.
Art 5(3)	By way of derogation from Article 4(4), in the case of transfers of funds referred to in paragraph 2(b) of this Article, the payment service provider of the payer need not verify the information on the payer unless the payment service provider of the payer: (a)has received the funds to be transferred in cash or in anonymous electronic money; or (b)has reasonable grounds for suspecting money laundering or terrorist financing.		
	Article 6 – Transfers of funds outside the Union		
Art 6(1)	In the case of a batch file transfer from a single payer where the payment service providers of the payees are established outside the Union, Article 4(1) shall not apply to the individual transfers bundled together therein, provided that the batch file contains the information referred to in Article 4(1), (2) and (3), that that information has been verified in accordance with Article 4(4) and (5), and that the individual transfers		The Wolfsberg Group note in their 2017 Payment Transparency Standards that neither originating, intermediary nor receiving firms will be able to monitor batch transactions between Money or Value Transfer Services (MVTS; e.g. money transfer and remittances) and recommend that the MVTS retain information on the ultimate originator and beneficiary to be provided on request to all firms involved in the transfer. This may

	carry the payment account number of the payer or, where Article 4(3) applies, the unique transaction identifier.		provide a model by analogy for non-MVTS batch payments. **HOW TO:** Firms are encouraged to apply procedures for retaining information on the ultimate originator and beneficiary, and for responding to requests for this information from all firms involved in that transfer.
Art 6(2)	By way of derogation from Article 4(1), and, where applicable, without prejudice to the information required in accordance with Regulation (EU) No 260/2012, where the payment service provider of the payee is established outside the Union, transfers of funds not exceeding EUR 1 000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1 000, shall be accompanied by at least: (a)the names of the payer and of the payee; and (b)the payment account numbers of the payer and of the payee or, where Article 4(3) applies, the unique transaction identifier.	(16) In order to apply rules in Articles 5, 6 and 7 of Regulation (EU) 2015/847 related to transfers of funds that do not exceed EUR 1 000, PSPs and IPSPs should have in place policies and procedures to detect transfers of funds that appear to be linked. PSPs and IPSPs should treat transfers of funds as linked if these fund transfers are being sent: a) from the same payment account to the same payment account, or, where the transfer is not made to or from a payment account, from the same payer to the same payee; and b) within a reasonable, short timeframe, which should be set by the PSP in a way that is commensurate with the ML/TF risk to which their business is exposed. (17) PSPs and IPSPs should determine whether other scenarios might also give rise to linked transactions,	

		and if so, reflect these in their policies and procedures.	
Section 2 – Obligations on the payment service provider of the payee			
	Article 7 – Detection of missing information on the payer or payee		
Art 7(1)	The payment service provider of the payee shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using characters or inputs admissible in accordance with the conventions of that system.	(21) PSPs and IPSPs should monitor transfers of funds to detect whether or not the characters or inputs used to provide information on the payer and the payee comply with the conventions of the messaging or payment and settlement system that was used to process the transfer of funds. These checks should be carried out in real time. (22) PSPs and IPSPs may assume that they comply with point (1) of Article 7 and point (1) of Article 11 of Regulation (EU) 2015/847 respectively if they are satisfied, and can demonstrate to their competent authority, that they understand the messaging or payment and settlement system's validation rules and that the conventions of that system mean that it: a) contains all the fields necessary to obtain the information required by Regulation (EU) 2015/847. For example, PSPs and IPSPs may treat the International Bank Account Number (IBAN) or, where the transfer of funds is made using a payment	

		card, the number of that card (for example the PAN) as the payment account number on condition that the number used permits the fund transfer to be traced to the payer or the payee; b) automatically prevents the sending or receiving of transfers of funds where inadmissible characters or inputs are detected; and c) flags rejected transfers of funds for manual review and processing. (23) Where a PSP's or IPSP's messaging, or payment and settlement system does not meet all the criteria stipulated in point 22 of these guidelines, the PSP or IPSP should put in place controls to mitigate the shortcomings.	
Art 7(2)	The payment service provider of the payee shall implement effective procedures, including, where appropriate, *ex-post* monitoring or real-time monitoring, in order to detect whether the following information on the payer or the payee is missing: (a)for transfers of funds where the payment service provider of the payer is established in the Union, the information referred to in Article 5; (b)for transfers of funds where the payment service provider of the payer is	(24) PSPs and IPSPs must implement effective procedures to detect if the required information on the payer or the payee is missing. (25) To be effective, these procedures should a) enable the PSP or IPSP to spot meaningless information; b) employ a combination of real-time monitoring and ex-post monitoring; and c) alert the PSP or IPSP to high-risk indicators. *Meaningless information*	**Meaningless Information** Several firms have commented that it is in practice very difficult to identify 'meaningless' information. What is meaningful to one party may mean nothing to another. While some obvious strings of characters e.g. ABCDE or XXXX might be easier to identify, strings of numerical digits are less easy to design systems to identify. We do not believe that at present any authoritative and comprehensive 'lists' of meaningless information exist, either in the public domain or through commercial providers. The Wolfsberg Group recommends in its 2017 Payment Transparency Standards that firms may

	established outside the Union, the information referred to in Article 4(1) and (2); (c)for batch file transfers where the payment service provider of the payer is established outside the Union, the information referred to in Article 4(1) and (2) in respect of that batch file transfer.	(26) PSPs and IPSPs should treat meaningless information as though it was missing information. Examples of meaningless information include strings of random characters (e.g. 'xxxxx', or 'ABCDEFG') or designations that clearly make no sense (e.g. 'An Other', or 'My Customer'), even if this information has been provided using characters or inputs in accordance with the conventions of the messaging or payment and settlement system. (27) Where PSPs or IPSPs use a list of commonly found meaningless terms, they should periodically review this list to ensure it remains relevant. In those cases, there is no expectation that PSPs or IPSPs manually review transactions to detect meaningless information. *High-risk indicators* (30) PSPs' and IPSPs' systems should be configured in a way that triggers alerts should a high-risk indicator be detected. High-risk indicators may include, but are not limited to: a) transfers of funds that exceed a specific value threshold. When deciding on the threshold, PSPs and IPSPs should at least consider the average value of transactions they routinely process and what constitutes an unusually large transaction, taking into account their particular business model;	set out in their policies their own list of commonly found terms which they consider to be clearly meaningless (e.g. 'our client'). Current SWIFT standards prevent payments being received without mandatory information in its entirety. However, it is noted that payer information fields could include incorrect or meaningless information which must be reviewed by Payee PSPs. SWIFT continues to review its validation standards to support inward monitoring and have introduced structured remitter fields (50F), however, its use is not currently mandatory. It is expected that forthcoming work by the BoE and NPSO on new payment messages and architectures will provide opportunities to address these issues. **Real-time monitoring** The Final Guidelines state that "The Regulation is clear that real-time monitoring may be necessary in some cases, as this gives PSPs the option of suspending or rejecting the transfer of funds. It is down to PSPs to decide, on a risk-sensitive basis, which transfers of funds, or types of transfers of funds, should be monitored in real time. There is no expectation that all transfers of funds be monitored in real time."

		b) transfers of funds where the PSP of the payer or the PSP of the payee is based in a country associated with high ML/TF risk, including, but not limited to, countries identified as high risk by the European Commission in accordance with Article 9 of Directive (EU) 2015/849. When identifying countries associated with high ML/TF risk, PSPs and IPSPs should have regard to the ESAs' Risk Factors Guidelines; c) a negative AML/CFT compliance record of the IPSP or the PSP of the payer, whoever is the prior PSP in the payment chain; d) transfers of funds from a PSP or IPSP identified as repeatedly failing to provide required information on the payer without good reason (see points 47-55), or from a PSP or IPSP that has previously been known to fail to provide required information on the payer or the payee on a number of occasions without good reason, even if it did not repeatedly fail to do so; e) transfers of funds where the name of the payer or the payee is missing.	It is envisaged that firms will come up with their own risk models to determine how their monitoring should be undertaken, with some examples utilising existing AML / CTF risk models and systems. These examples include varied approaches in line with the different systems and procedures in place; one firm screens in real-time all inbound transactions from high risk jurisdictions, while another firm utilises its ex-post monitoring to identify cases of specific concern for real-time monitoring. Market variation in approaches to real-time monitoring can be partly driven by differences in risk appetite between individual firms. However, if transfers are selected for review and possible query as a result of real-time monitoring, then the sending firm can still provide a pre-prepared standard response of how they are addressing the Regulation and Final Guidelines. **HOW-TO**: Firms are encouraged to review their AML / CTF risk models, systems and procedures to identify where existing approaches can be utilised to check for missing payments information, or whether a new and bespoke approach is required. These approaches may include real-time monitoring, ex-post monitoring and sample testing. Whatever approach is taken, firms should seek to ensure that their checks for missing

			payments information is commensurate with AML /CTF risk. Risk factors that may be considered by PSPs when establishing the risk based approach to monitoring Wire Transfers: - Firms should implement three methods of Wire Transfer monitoring; Real-Time Monitoring, Post-Event Monitoring, and random Post-Event Sampling. Firms should document the level and frequency of each; - All Wire Transfers qualify for random Post-Event Sampling, with the population of Wire Transfer for sampling being taken from across the risk spectrum. Firms should document their approach to random sampling of Wire Transfers on a post-event basis (e.g. how the random sample population is determined, how often the sampled will be generated); - Firm should document the risk-based approach to determining which Wire Transfers are to be monitored in real time and which Wire Transfers are to be monitored on a post-event basis, and why; - Firms should adopt the following, high level, risk-based approach to monitoring Wire Transfers: - The highest risk Wire Transfers are to be subject to Real-Time Monitoring. Commonly a firm will impose Real-Time Monitoring on a PSP that has been identified as egregiously non-compliant and the pattern of non-compliant

			payments indicates a material money laundering risk to the firm (e.g. taking into account the high-risk factors below). In these circumstances firms may implement Real-Time Monitoring as one of a series of controls aimed to mitigate the material money laundering risk posed by the PSP as final step before considering exiting the Business Relationship; - High-risk Wire Transfers are to be subject to Post-Event Monitoring. Commonly a firm may implement Post-Event Monitoring to target PSPs identified as repeatedly failing, Wire Transfers where material high risk factors are present (refer to the list of risks below), or a combination of the two; - All Wire Transfers are in scope for Random Post-Event Sampling. - Firms should document which high-risk factors, or combination of high-risk factors, are to be considered when determining the risk-based approach. High-risk factors to be considered may include (but are not limited to): - The residual risk of the firm as identified in the enterprise-wide financial crime risk assessment to ensure that the approach to monitoring, including the level and frequency of post-event and real-time monitoring, is commensurate with the money laundering risk to which the

			firm is exposed. Consideration should be given to the risk posed by the type of PSP customers, and the types of products, services and delivery channels offered to these PSPs; - Wire Transfers that exceed a specific value threshold. When deciding on the threshold, firms should consider the average value of transactions they routinely process and what constitutes an unusually large transaction, taking into account their particular business model; - Wire Transfers where the Payer, Payer's PSP, Payee's PSP and/or Payee is in a country which, as identified from the information in the Wire Transfer, is: - Assessed by the firm as posing a high risk of money laundering; - Classified as a High Risk Third Country by the EU under the Fourth EU Money Laundering Directive; - Not a member of the Financial Action Task Force / not a FATF Associate Member; or - Subject to a relevant sanctions regime (e.g. UN, EU). - Whether the prior PSP in the payment chain is categorised as particularly high risk (e.g. because it has been subject to money

			laundering-related adverse media from reliable sources and/or a large number of suspicious activity reports submitted to the NCA); and - Wire Transfers from a PSP identified as repeatedly failing to provide the required information on the payer or payee in Wire Transfers (including repeatedly providing meaningless words (e.g. 'One of Our Customers'). - Conversely, the firm may take account of lower risk factors such as: - Domestic Wire Transfers which take place entirely within the UK or between the UK and a jurisdiction categorised by the firm as posing a low risk of money laundering.
Art 7(3)	In the case of transfers of funds exceeding EUR 1 000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked, before crediting the payee's payment account or making the funds available to the payee, the payment service provider of the payee shall verify the accuracy of the information on the payee referred to in paragraph 2 of this Article on the basis of documents, data or information obtained from a reliable and independent source, without prejudice to the requirements laid	(16) In order to apply rules in Articles 5, 6 and 7 of Regulation (EU) 2015/847 related to transfers of funds that do not exceed EUR 1 000, PSPs and IPSPs should have in place policies and procedures to detect transfers of funds that appear to be linked. PSPs and IPSPs should treat transfers of funds as linked if these fund transfers are being sent: a) from the same payment account to the same payment account, or, where the transfer is not made to or from a payment account, from the same payer to the same payee; and	

	down in Articles 69 and 70 of Directive 2007/64/EC.	b) within a reasonable, short timeframe, which should be set by the PSP in a way that is commensurate with the ML/TF risk to which their business is exposed. (17) PSPs and IPSPs should determine whether other scenarios might also give rise to linked transactions, and if so, reflect these in their policies and procedures.	
Art 7(4)	In the case of transfers of funds not exceeding EUR 1 000 that do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1 000, the payment service provider of the payee need not verify the accuracy of the information on the payee, unless the payment service provider of the payee: (a)effects the pay-out of the funds in cash or in anonymous electronic money; or (b)has reasonable grounds for suspecting money laundering or terrorist financing.	61. When verifying the accuracy of information on the payee pursuant to points (3) and (4) of Article 7 of Regulation (EU) 2015/847, PSPs should consider whether or not their relationship with the payee amounts to a business relationship as defined in point (13) of Article 3 of Directive (EU) 2015/849 and apply customer due diligence measures in line with point (1) of Article 13 of Directive (EU) 2015/849 should that be the case. 62. PSPs may consider that they have complied with the verification requirements in Article 7 of Regulation (EU) 2015/847 where they have previously verified the payee's identity in line with the national law transposing point (1)(a) of Article 13 and, where applicable, point (1)(b) of Article 13 of Directive (EU) 2015/849 or to an equivalent	

		standard, should the payee's identity have been verified before the legislation transposing Directive (EU) 2015/849 entered into force.	
Art 7(5)	Verification as referred to in paragraphs 3 and 4 shall be deemed to have taken place where: (a)a payee's identity has been verified in accordance with Article 13 of Directive (EU) 2015/849 and the information obtained pursuant to that verification has been stored in accordance with Article 40 of that Directive; or (b)Article 14(5) of Directive (EU) 2015/849 applies to the payee.		
Art 8	**Article 8 - Transfers of funds with missing or incomplete information on the payer or the payee**	(31) PSPs and IPSPs should put in place effective risk-based procedures to determine whether to execute, reject or suspend a transfer of funds where real-time monitoring reveals that the required information on the payer or the payee is missing or provided using inadmissible characters or inputs. (32) In order to determine whether to reject, suspend or execute a transfer of funds in compliance with Articles 8 and 12 of Regulation (EU) 2015/847, PSPs and IPSPs should consider the ML/TF risk associated with that transfer of funds before	**Suspending payments for missing information** Section 31 of the Guidelines refers to "procedures to determine whether to execute, reject or suspend a transfer of funds where real-time monitoring reveals that "the required information" is missing or incomplete (emphasis added). It would seem logical that the 'required information' differs depending on circumstances, e.g. whether the exemptions apply. For example, for an extra-EU transaction the 'required information' is different from that of intra-EU payments. Section 30(2) of the Guidelines gives suggested high-risk indicators, which includes 'missing

		deciding on the appropriate course of action. PSPs and IPSPs should consider in particular whether or not: a) the type of information missing gives rise to ML/TF concerns; and b) one or more high-risk indicators have been identified that may suggest that the transaction presents a high ML/TF risk or gives rise to suspicion of ML/TF (see point 30). Where PSPs or IPSPs have taken a risk-sensitive decision, in line with point 28 of these guidelines, to monitor transfers of funds ex post, they should follow the guidance in points 40-43. *The PSP or IPSP rejects the transfer* 33. Where a PSP or an IPSP decides to reject a transfer of funds, it does not have to ask for the missing information but should share the reason for the rejection with the prior PSP in the payment chain. *The PSP or IPSP suspends the transfer* 34. Where a PSP or an IPSP decides to suspend the transfer of funds, it should notify the prior PSP in the payment chain that the transfer of funds has been suspended and ask the prior PSP in the payment chain to supply the information on the payer or the	information'. It would seem logical to conclude that missing information can only qualify as a high-risk indicator if it was 'required information' under the relevant section of the Regulation. I.e. if a firm does not provide the payer/payee name on an intra-EU transaction, this ought not be considered a high-risk indicator, because that information is not 'required' under the Regulation if the exemption applies. **The process for asking for missing information** Some firms have indicated that it is not always clear which firm should be approached if it is detected that there is missing or incomplete information. The Guidelines repeatedly reference the fact that PSPs should contact the "prior" PSP in the payment chain. General consensus is that firms should be encouraged to always contact the prior firm in the payment chain, but it is also noted that some global groups will have both an earlier sending firm and a later receiving firm. It is also noted that firms can also jump straight to an earlier sending firm in their global group. **HOW TO:** Given (i) the practical difficulties such as the fact that some firms may not have relationships (e.g. RMA to send authenticated messages as it assumed that unauthenticated will not be sufficient) or contacts with the 'originating' PSP and/or will not know the

		payee that is missing, or to provide that information using admissible characters or inputs. 35. When asking for missing information, the PSP or IPSP should set the prior PSP in the payment chain a reasonable deadline by which the information should be provided. This deadline should not normally exceed three working days for transfers of funds taking place within the EEA, and five working days for transfers of funds received from outside the EEA. Longer deadlines may be necessary where payment chains are more complex. 36. PSPs or IPSPs should consider sending a reminder to the prior PSP in the payment chain should the requested information not be forthcoming. As part of this, a PSP or IPSP may decide to advise the prior PSP in the payment chain that, if the required information is not received before an additional deadline, the prior PSP in the payment chain may be subject to internal high-risk monitoring (see point 30) and treated as repeatedly failing, as set out in point (2) of Article 8 of Regulation (EU) 2015/847. 37. Where the requested information is not provided by the set deadline, the PSP or IPSP should, in line with its risk-based policies and procedures:	original transaction reference number required as part of the request for missing information, and; (ii) the fact that all firms in the payment chain should have an interest in receiving the full information (as required by the Regulation), firms are encouraged to always contact the prior firm in the payment chain when asking for missing information. This could be in parallel to firms also contacting an earlier sending firm where they are part of the same global group. The industry anticipate/ expect that any requests being sent between PSPs requesting Missing Information or qualification on Payment details would follow the usual course of business for Payment Investigation related activity and that requests will be sent using the SWIFT mechanism, and should further escalation be required then alternate methods of contact/ communication will be sought. **SLA for PSPs to respond to enquiries to drive consistency:** A firm should first assess the request for information considering the legal grounds for the request, whether the firm is authorized to release the information, and whether there have been agreements in place committing to releasing the specific information requested. Where it is reasonable for the firm to provide the payer / payee information to the requesting PSP, and where

		a) decide whether to reject or execute the transfer; b) consider whether or not the prior PSP in the payment chain's failure to supply the required information gives rise to suspicion; and c) consider the future treatment of the prior PSP in the payment chain for AML/CFT compliance purposes. 38. PSPs and IPSPs should document and record all of these actions and the reason for their actions or inaction, so that they are later capable of responding to possible requests by the competent authorities for information about compliance with legally binding acts of the Union, for example where, as a result of actions taken under Article 8 of Regulation (EU) 2015/847, the PSP or IPSP has been unable to comply with relevant obligations in Articles 83 and 84 of Directive (EU) 2015/2366 as incorporated into the applicable national legal framework. *The PSP or IPSP executes the transfer* 39. Where a PSP or IPSP executes the transfer of funds, or detects ex post that required information was missing or provided using inadmissible characters, it should ask the prior PSP in the payment chain to provide the missing information on the payer or the payee, or to provide that	the information is immediately available to the firm, the firm should provide the information within: - Three business days of receiving a request in relation to a Wire Transfer that takes place within the UK/EEA, or - Five working days for Wire Transfers into the UK/EEA The set timeframe starts the day after the request is received by the PSP. Where the information is not immediately available to the firm (e.g. in the case of complex transfers, such as when the firm is acting as an IPSP and needs to contact the prior PSP in the payment chain for the requested information) the firm should send a holding response to the requesting PSP within these timeframes. Note: Firms should take complex transfers into account when determining whether the PSP it has requested missing information from should be categorised as repeatedly failing to respond to its requests for information. The requesting PSP may set a shorter timeframe for receipt of the information. In such cases the firm should endeavour to respond to the request within the timeline provided by the requesting PSP. Where this is not possible, the firm should send the requesting PSP a holding response.

		information using admissible characters or inputs after the transfer has been executed. 40. A PSP or IPSP that becomes aware that required information is missing while carrying out real-time monitoring, but decides to execute the transfer of funds having considered all relevant risks, should document the reason for executing that transfer. 41. When asking for missing information, the PSP or IPSP should proceed in line with point 36 of these guidelines. 42. Where the requested information is not forthcoming within the timeframe set by the PSP or IPSP, the PSP or IPSP should, in line with its risk-based policies and procedures, consider the future treatment of the prior PSP in the payment chain for AML/CFT compliance purposes. 43. The PSP or IPSP should document and record all of these actions and the reason for their actions or inaction, so that they are later capable of responding to possible requests of the authorities.	**Discussion:** Another nuanced scenario identified is that of non-bank financial institutions (NBFI) or banking institutions (BI) that use an agent bank to clear cash. In such relationships, a client of this NBFI/BI may not have a separate physical bank account. Rather the NBFI/BI will distinguish their client monies via a customer or trade reference and an expectation of receipt, with the money all going into one Nostro bank account at its agent bank. From the perspective of the FTR, there might be a gap in the ability for this NBFI/BI to monitor complete final beneficiary account number. For example, the ordering party or ordering bank may fail to include the client's reference number at the NBFI/BI on their payment advice, or, due to character limitations the reference in the SWIFT message may be truncated. In this scenario the NBFI/BI, which may be a PSP, could mark the prior PSP as repeatedly failing due to non-provision of complete information. However, the prior PSP would regard themselves as having completed their obligations as their client and final beneficially is the NBFI/BI who has their client account with them. It is useful to recognise the kinds of examples where it may be difficult to obtain comprehensive beneficiary information, and firms may therefore rely upon other

			internal data to validate the ultimate beneficiary. For example, if the NBFI/BI expects to receive this money, then there is a reasonable assumption that the money is intended to be credited to the internal client at the NBFI/BI. In which case, the NBFI/BI would ideally take a risk-based approach, and consider whether additional information on the client payment with the missing account number. This would hopefully reduce instances where such NBFI/BI are identifying the prior PSP as a repeat offender. **Timing for suspending payments** As well as complying with the Funds Transfer Regulation firm will be considering their compliance with other legislation such as the Payments Services Directive (PSD2) which lays down requirements on firms regarding the timelines for making transactions. **HOW TO**: When suspending payments, firms will ultimately need to take a risk-based approach including being aware of the timeliness requirements under PSD.
Art 8(1)	The payment service provider of the payee shall implement effective risk-based procedures, including procedures based on the risk-sensitive basis referred to in Article 13 of Directive (EU) 2015/849, for	(18) PSPs and IPSPs should establish and maintain effective policies and procedures to comply with Regulation (EU) 2015/847. These policies and procedures should be proportionate to the nature, size and complexity of the PSP's or IPSP's business,	

	determining whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information and for taking the appropriate follow-up action. Where the payment service provider of the payee becomes aware, when receiving transfers of funds, that the information referred to in Article 4(1) or (2), Article 5(1) or Article 6 is missing or incomplete or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system as referred to in Article 7(1), the payment service provider of the payee shall reject the transfer or ask for the required information on the payer and the payee before or after crediting the payee's payment account or making the funds available to the payee, on a risk-sensitive basis.	and commensurate with the ML/TF risk to which the PSP or IPSP is exposed as a result of: a) the type of customers it services; b) the nature of the products and services it provides; c) the jurisdictions it services; d) the delivery channels it uses; e) the number of PSPs and IPSPs regularly failing to provide required information on the payer and the payee; f) the complexity of the payment chains in which it intervenes as a result of its business model; and g) the volume and value of transactions it processes. (19) When assessing the ML/TF risk to which they are exposed, PSPs and IPSPs should refer to the ESAs' 'Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions' (the Risk Factors Guidelines).	

Art 8(2)	Where a payment service provider repeatedly fails to provide the required information on the payer or the payee, the payment service provider of the payee shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider, or restricting or terminating its business relationship with that payment service provider. The payment service provider of the payee shall report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.	*When is a PSP or IPSP considered to be 'repeatedly failing' to provide required information?* 47. PSPs and IPSPs should put in place policies and procedures to identify PSPs and IPSPs that repeatedly fail to provide the required information on the payer or the payee. 48. To this end, PSPs and IPSPs should keep a record of all transfers of funds with missing information to be able to determine which PSP or IPSP should be classified as 'repeatedly failing'. 49. A PSP or IPSP may decide to treat a PSP or IPSP as 'repeatedly failing' for various reasons, but should consider a combination of quantitative and qualitative criteria to inform that decision. 50. Quantitative criteria for assessing whether or not a PSP or IPSP is repeatedly failing include: a) the percentage of transfers with missing information sent by a specific PSP or IPSP within a certain timeframe; and b) the percentage of follow-up requests that were left unanswered or were not adequately answered by a certain deadline.	**HOW TO:** In addition to the notification report template provided as an annex to the Final Guidelines, firms are encouraged to provide summary information on their specific reasons for notifying the FCA. The FCA may produce a webpage in future with further details on what specific information should be provided. In the meantime, notifications can be sent to repeatedlyfailingpsp@fca.org.uk. **Factors that may be considered when determining whether a PSP is a 'repeatedly failing PSP':** A firm should consider a combination of quantitative and qualitative criteria to inform its decision on whether a PSP is to be classified as 'repeatedly failing'. Quantitative criteria for assessing whether a PSP is repeatedly failing may include (but are not limited to): - The percentage of transfers with missing information sent by the PSP within a certain timeframe; - The number of requests for information that were repeatedly unanswered, even after a reasonable number of follow up requests; - Whether there has been any notification or agreement from the PSP notifying the firm that more time was required to provide the information.

		51. Qualitative criteria for assessing whether or not a PSP or IPSP is repeatedly failing include: a) the level of cooperation of the requested PSP or IPSP relating to previous requests for missing information; and b) the type of information missing (see, for example, point 30 e). *Notifying the authorities* 52. Once a PSP or IPSP has identified another PSP or IPSP as repeatedly failing to provide required information, a notification to the authorities specified in the second subparagraph of Article 8(2) of Regulation (EU) 2015/847 should include, in line with the Annex to these guidelines: a) the name of the PSP or IPSP identified as repeatedly failing to provide the required information; b) the country in which the PSP or IPSP is authorised; c) the nature of the breach, including: i) the frequency of transfers of funds with missing information,	Qualitative criteria for assessing whether or not a PSP is repeatedly failing include (but are not limited to): - The presence of material high risk factors as detailed above; - The materiality of missing payer / payee information. A firm should assess materiality on the importance of the missing information to trace the Wire Transfer to the payer / payee and to subject them to sanction screening e.g. - Name: A firm may consider an entirely missing payer or the payee name as material, but a missing title or shortened given name as less material (especially where external payment infrastructure imposes a character limit); - Address: A firm may consider missing payer's city/town and country as material but missing post code as immaterial (especially where other details, such as date and place of birth, national identity number, customer identification number has been provided); - A firm should also take account of the materiality of the missing payer / payee information when determining whether to request missing information from the previous PSP. - The level of cooperation of the PSP relating to previous requests for missing information;

		ii) the period of time during which the breaches were identified and iii) any reasons the PSP or IPSP may have given to justify their repeated failure to provide the required information; d) details of the steps the reporting PSP or IPSP has taken. 53. The obligation in the second subparagraph of point (2) of Article 8 of Regulation (EU) 2015/847 applies without prejudice to the obligation to report suspicious transactions pursuant to Article 33 of Directive (EU) 2015/849. 54. PSPs and IPSPs should notify relevant authorities upon identifying a repeatedly failing PSP or IPSP without undue delay, and no later than three months after identifying the repeatedly failing PSP or IPSP. 55. These authorities will then notify the EBA. *Steps to be taken* 56. The steps the PSP of the payee or the IPSP should take where another PSP or IPSP repeatedly	- The reasons given by the PSP for not providing the missing information; - Whether the missing information is required by the firm under the EU Wire Transfer Regulations or the form's policy, but not under the legal obligations of the PSP (e.g. beneficiary address); and - Where the PSP is the PSP or the payer (and so ultimately responsible for providing the information in the Wire Transfer) or another intermediary PSP in the Wire Transfer (and so reliant on its prior PSP to provide the missing information unless truncated by the intermediary PSP itself). - For correspondent banking relationships, a firm may take account of the due diligence undertaken on the respondent through its answers to the Wolfsberg Due Diligence Questionnaire.

		fails to provide information required by Regulation (EU) 2015/847 should be risk-based and may include one or a combination of the following (though other steps are possible): 19 a) issuing a warning to the prior PSP in the payment chain to inform the PSP or IPSP of the steps that will be applied should the PSP continues to fail to provide the information required by Regulation (EU) 2015/847; b) considering how the repeated failure by the prior PSP in the payment chain to provide information and that PSP's attitude to responding to such requests affects the ML/TF risk associated with that PSP, and where appropriate, carrying out real-time monitoring of all transactions received from that PSP; c) issuing a further warning to the prior PSP in the payment chain that it will reject any future transfers of funds; d) restricting or terminating the business relationship with the failing PSP.	

		57. Before taking the decision to terminate a business relationship, in particular where the prior PSP in the payment chain is a respondent bank from a third country, the PSP or IPSP should consider whether or not it can manage the risk in other ways, including through the application of enhanced due diligence measures in line with Article 19 of Directive (EU) 2015/849.	
	Article 9 – Assessment and reporting	44. PSPs and IPSPs should assess whether or not a transfer of funds is suspicious, taking into account any criteria set out in Union law, national legislation and their own, internal AML/CFT policies and procedures. 45. PSPs and IPSPs should note that missing or inadmissible information may not, by itself, give rise to suspicion of ML/TF. When considering whether or not a transfer of funds raises suspicion, the PSP or IPSP should take a holistic view of all ML/TF risk factors associated with the transfer of funds, including those listed in point 30, to the extent that these are known, and pay particular attention to transfers of funds that are likely to present a higher risk of ML/TF.	

		46. PSPs and IPSPs should be able to demonstrate that they comply with directly applicable Union law and national legislation in the area of AML/CFT. In some cases, national legislation may require them to take additional action, for example the reporting of unusual transactions that may not give rise to suspicion of ML/TF.	
	The payment service provider of the payee shall take into account missing or incomplete information on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious and whether it is to be reported to the Financial Intelligence Unit (FIU) in accordance with Directive (EU) 2015/849.		
		Section 3 – Obligations on intermediary	
	Article 10 - Retention of information on the payer and the payee with the transfer		
	Intermediary payment service providers shall ensure that all the information received on the payer and the payee that accompanies a transfer of funds is retained with the transfer.	58. IPSPs should satisfy themselves that their systems and controls enable them to comply with their duty to ensure that all information on the payer and the payee that accompanies a transfer of funds is retained with that transfer. As part of this, IPSPs should satisfy themselves of their system's ability to convert information into a different format without error or omission.	Discussion: Some firms have indicated that in certain circumstances they may turn a cross-border/international payment into a domestic payment (e.g. a BACS payment). In this case, the full information packet cannot be transmitted and the information must be truncated (with the additional information being retained). This is a practice that was recognised in FATF 16 and in the previous version of the Regulation. The

		59. IPSPs should use only payment or messaging systems that permit the onward transfer of all information on the payer or the payee, irrespective of whether or not this information is required by Regulation (EU) 2015/847. Where this is not possible, for example because a domestic payment system restricts the data that can be entered into that system, IPSPs should put in place alternative mechanisms to pass on relevant information to the PSP of the payee. Such alternative mechanisms should be used only during a short transition period while domestic systems are being adjusted to comply with Regulation (EU) 2015/847 and these guidelines.	Wolfsberg Group has also recommended this practice in their 2017 Payments Transparency Standards. • The Wolfsberg Group has also recommended that firms' policies should set out their priorities for information that may be truncated by system limitations, noting that: Name and address information is important as this is used for screening and monitoring purposes • Country information is particularly important as this is used for risk assessment, screening and monitoring purposes • Name and address of primary account holder should be provided in full before secondary account holder information. • Family name should receive priority over given names. Address information should be prioritised from the most general to the most specific (e.g. country first, building number last). The final Guidelines allow this 'alternative mechanism' to continue for a 'short period'. In the UK this short period is likely to continue until the domestic schemes have been transitioned to ISO20022 and the New Payments Architecture (NPA), a process that is underway and expected to take 2-5 years.

			HOW TO: Firms may take different approaches to 'alternative mechanisms' during the transition period. It seems that many firms will employ a referencing system that means that the additional data is stored and can be retrieved and shared with another firm if requested.
	Article 11 - Detection of missing information on the payer or the payee		
Art 11(1)	The intermediary payment service provider shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using characters or inputs admissible in accordance with the conventions of that system.	(21) PSPs and IPSPs should monitor transfers of funds to detect whether or not the characters or inputs used to provide information on the payer and the payee comply with the conventions of the messaging or payment and settlement system that was used to process the transfer of funds. These checks should be carried out in real time. (22) PSPs and IPSPs may assume that they comply with point (1) of Article 7 and point (1) of Article 11 of Regulation (EU) 2015/847 respectively if they are satisfied, and can demonstrate to their competent authority, that they understand the messaging or payment and settlement system's validation rules and that the conventions of that system mean that it: a) contains all the fields necessary to obtain the information required by Regulation (EU) 2015/847. For example, PSPs and IPSPs may treat the International Bank Account Number (IBAN) or,	

		where the transfer of funds is made using a payment card, the number of that card (for example the PAN) as the payment account number on condition that the number used permits the fund transfer to be traced to the payer or the payee; b) automatically prevents the sending or receiving of transfers of funds where inadmissible characters or inputs are detected; and c) flags rejected transfers of funds for manual review and processing. (23) Where a PSP's or IPSP's messaging, or payment and settlement system does not meet all the criteria stipulated in point 22 of these guidelines, the PSP or IPSP should put in place controls to mitigate the shortcomings.	
Art 11(2)	The intermediary payment service provider shall implement effective procedures, including, where appropriate, *ex-post* monitoring or real-time monitoring, in order to detect whether the following information on the payer or the payee is missing: (a)for transfers of funds where the payment service providers of the payer and the payee are established in the Union, the information referred to in Article 5;		

	(b)for transfers of funds where the payment service provider of the payer or of the payee is established outside the Union, the information referred to in Article 4(1) and (2); (c)for batch file transfers where the payment service provider of the payer or of the payee is established outside the Union, the information referred to in Article 4(1) and (2) in respect of that batch file transfer.		
	Article 12 - Transfers of funds with missing information on the payer or the payee		
Art 12(1)	The intermediary payment service provider shall establish effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information and for taking the appropriate follow up action. Where the intermediary payment service provider becomes aware, when receiving transfers of funds, that the information referred to in Article 4(1) or (2), Article 5(1) or Article 6 is missing or has not been filled in using characters or inputs admissible in		

	accordance with the conventions of the messaging or payment and settlement system as referred to in Article 7(1) it shall reject the transfer or ask for the required information on the payer and the payee before or after the transmission of the transfer of funds, on a risk-sensitive basis.		
Art 12(2)	Where a payment service provider repeatedly fails to provide the required information on the payer or the payee, the intermediary payment service provider shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider, or restricting or terminating its business relationship with that payment service provider. The intermediary payment service provider shall report that failure, and the steps taken, to the competent authority responsible for monitoring compliance with anti-money laundering and counter terrorist financing provisions.		

	Article 13 – Assessment and reporting	44. PSPs and IPSPs should assess whether or not a transfer of funds is suspicious, taking into account any criteria set out in Union law, national legislation and their own, internal AML/CFT policies and procedures. 45. PSPs and IPSPs should note that missing or inadmissible information may not, by itself, give rise to suspicion of ML/TF. When considering whether or not a transfer of funds raises suspicion, the PSP or IPSP should take a holistic view of all ML/TF risk factors associated with the transfer of funds, including those listed in point 30, to the extent that these are known, and pay particular attention to transfers of funds that are likely to present a higher risk of ML/TF. 46. PSPs and IPSPs should be able to demonstrate that they comply with directly applicable Union law and national legislation in the area of AML/CFT. In some cases, national legislation may require them to take additional action, for example the reporting of unusual transactions that may not give rise to suspicion of ML/TF.	
	The intermediary payment service provider shall take into account missing information		

	on the payer or the payee as a factor when assessing whether a transfer of funds, or any related transaction, is suspicious, and whether it is to be reported to the FIU in accordance with Directive (EU) 2015/849.		
CHAPTER 3 - INFORMATION, DATA PROTECTION AND RECORD-RETENTION **NO COMMENTS ON THE SUBSEQUENT CHAPTERS**			
	Article 14 – Provision and information		
	Payment service providers shall respond fully and without delay, including by means of a central contact point in accordance with Article 45(9) of Directive (EU) 2015/849, where such a contact point has been appointed, and in accordance with the procedural requirements laid down in the national law of the Member State in which they are established, to enquiries exclusively from the authorities responsible for preventing and combating money laundering or terrorist financing of that Member State concerning the information required under this Regulation.		
	Article 15 – Data protection		
Art 15(1)	The processing of personal data under this Regulation is subject to Directive 95/46/EC, as transposed into national law. Personal data that is processed pursuant to this Regulation by the Commission or by the ESAs is subject to Regulation (EC) No 45/2001.		
Art 15(2)	Personal data shall be processed by payment service providers on the basis of this Regulation only for the purposes of the prevention of money laundering and terrorist financing and shall not be further processed in a way that is incompatible with those purposes. The processing of personal data on the basis of this Regulation for commercial purposes shall be prohibited.		
Art 15(3)	Payment service providers shall provide new clients with the information required pursuant to Article 10 of Directive 95/46/EC before establishing a business relationship or carrying out an occasional transaction. That information shall, in particular, include a general notice concerning the legal obligations of payment service providers under this Regulation when processing personal data for the purposes of the prevention of money laundering and terrorist financing.		
Art 15(4)	Payment service providers shall ensure that the confidentiality of the data processed is respected.		
	Article 16 – Record retention		
Art 16(1)	Information on the payer and the payee shall not be retained for longer than strictly necessary. Payment service providers of the payer and of the payee shall retain records of the information referred to in Articles 4 to 7 for a period of five years.		

	(63) In line with Article 16 of Regulation (EU) 2015/847, PSPs must retain records of information on the payer and the payee that they receive in line with Articles 4 to 7 of that Regulation. (64) However, where the PSP has entered into a business relationship with the payee and the transfer of funds takes place in the context of that business relationship, PSPs should comply with the record-keeping requirements in Article 40 of Directive (EU) 2015/849.
Art 16(2)	Upon expiry of the retention period referred to in paragraph 1, payment service providers shall ensure that the personal data is deleted, unless otherwise provided for by national law, which shall determine under which circumstances payment service providers may or shall further retain the data. Member States may allow or require further retention only after they have carried out a thorough assessment of the necessity and proportionality of such further retention, and where they consider it to be justified as necessary for the prevention, detection or investigation of money laundering or terrorist financing. That further retention period shall not exceed five years.
Art 16(3)	Where, on 25 June 2015, legal proceedings concerned with the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing are pending in a Member State, and a payment service provider holds information or documents relating to those pending proceedings, the payment service provider may retain that information or those documents in accordance with national law for a period of five years from 25 June 2015. Member States may, without prejudice to national criminal law on evidence applicable to ongoing criminal investigations and legal proceedings, allow or require the retention of such information or documents for a further period of five years where the necessity and proportionality of such further retention has been established for the prevention, detection, investigation or prosecution of suspected money laundering or terrorist financing.
CHAPTER 4 - SANCTIONS AND MONITORING	
	Article 17 - Administrative sanctions and measures
Art 17(1)	Without prejudice to the right to provide for and impose criminal sanctions, Member States shall lay down the rules on administrative sanctions and measures applicable to breaches of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented. The sanctions and measures provided for shall be effective, proportionate and dissuasive and shall be consistent with those laid down in accordance with Chapter VI, Section 4, of Directive (EU) 2015/849.
Art 17(2)	Member States shall ensure that where obligations apply to payment services providers, in the event of a breach of provisions of this Regulation, sanctions or measures can, subject to national law, be applied to the members of the management body and to any other natural person who, under national law, is responsible for the breach.
Art 17(3)	By 26 June 2017, Member States shall notify the rules referred to in paragraph 1 to the Commission and to the Joint Committee of the ESAs. They shall notify the Commission and the Joint Committee of the ESAs without delay of any subsequent amendments thereto.

Art 17(4)	In accordance with Article 58(4) of Directive (EU) 2015/849, competent authorities shall have all the supervisory and investigatory powers that are necessary for the exercise of their functions. In the exercise of their powers to impose administrative sanctions and measures, competent authorities shall cooperate closely to ensure that those administrative sanctions or measures produce the desired results and coordinate their action when dealing with cross-border cases.
Art 17(5)	Member States shall ensure that legal persons can be held liable for the breaches referred to in Article 18 committed for their benefit by any person acting individually or as part of an organ of that legal person, and having a leading position within the legal person based on any of the following: (a) power to represent the legal person; (b) authority to take decisions on behalf of the legal person; or (c) authority to exercise control within the legal person.
Art 17(6)	Member States shall also ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 5 of this Article has made it possible to commit one of the breaches referred to in Article 18 for the benefit of that legal person by a person under its authority.
Art 17(7)	Competent authorities shall exercise their powers to impose administrative sanctions and measures in accordance with this Regulation in any of the following ways: a) directly b) in collaboration with other authorities c) under their responsibility by delegation to such authorities d) by application to the competent judicial authorities. In the exercise of their powers to impose administrative sanctions and measures, competent authorities shall cooperate closely in order to ensure that those administrative sanctions or measures produce the desired results and coordinate their action when dealing with cross-border cases.
	Article 18 – Specific provisions
	Member States shall ensure that their administrative sanctions and measures include at least those laid down by Article 59(2) and (3) of Directive (EU) 2015/849 in the event of the following breaches of this Regulation: (a)repeated or systematic failure by a payment service provider to include the required information on the payer or the payee, in breach of Article 4, 5 or 6;

	(b) repeated, systematic or serious failure by a payment service provider to retain records, in breach of Article 16; (c) failure by a payment service provider to implement effective risk-based procedures, in breach of Articles 8 or 12; (d) serious failure by an intermediary payment service provider to comply with Article 11 or 12.
	Article 19 - Publication of sanctions and measures
	In accordance with Article 60(1), (2) and (3) of Directive (EU) 2015/849, the competent authorities shall publish administrative sanctions and measures imposed in the cases referred to in Articles 17 and 18 of this Regulation without undue delay, including information on the type and nature of the breach and the identity of the persons responsible for it, if necessary and proportionate after a case-by-case evaluation.
	Article 20 - Application of sanctions and measures by the competent authorities
Art 20(1)	Member States shall establish effective mechanisms to encourage the reporting to competent authorities of breaches of this Regulation. Those mechanisms shall include at least those referred to in Article 61(2) of Directive (EU) 2015/849
Art 20(2)	Payment service providers, in cooperation with the competent authorities, shall establish appropriate internal procedures for their employees, or persons in a comparable position, to report breaches internally through a secure, independent, specific and anonymous channel, proportionate to the nature and size of the payment service provider concerned.
	Article 22 - Monitoring
Art 22(1)	Member States shall require competent authorities to monitor effectively and to take the measures necessary to ensure compliance with this Regulation and encourage, through effective mechanisms, the reporting of breaches of the provisions of this Regulation to competent authorities.
Art 22(2)	After Member States have notified the rules referred to in paragraph 1 of this Article to the Commission and to the Joint Committee of the ESAs in accordance with Article 17(3), the Commission shall submit a report to the European Parliament and to the Council on the application of Chapter IV, with particular regard to cross-border cases.
CHAPTER 5 - IMPLEMENTING POWERS	
	Article 23 – Committee procedure
Art 23(1)	The Commission shall be assisted by the Committee on the Prevention of Money Laundering and Terrorist Financing (the 'Committee'). The Committee shall be a committee within the meaning of Regulation (EU) No 182/2011.
Art 23(2)	Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

CHAPTER 6 - DEROGATIONS	
	Article 24 - Agreements with countries and territories which do not form part of the territory of the Union
Art 24(1)	The Commission may authorise any Member State to conclude an agreement with a third country or with a territory outside the territorial scope of the TEU and the TFEU as referred to in Article 355 TFEU (the 'country or territory concerned'), which contains derogations from this Regulation, in order to allow transfers of funds between that country or territory and the Member State concerned to be treated as transfers of funds within that Member State. Such agreements may be authorised only where all of the following conditions are met: (a)the country or territory concerned shares a monetary union with the Member State concerned, forms part of the currency area of that Member State or has signed a monetary convention with the Union represented by a Member State; (b)payment service providers in the country or territory concerned participate directly or indirectly in payment and settlement systems in that Member State; and (c)the country or territory concerned requires payment service providers under its jurisdiction to apply the same rules as those established under this Regulation.
Art 24(2)	A Member State wishing to conclude an agreement as referred to in paragraph 1 shall submit a request to the Commission and provide it with all the information necessary for the appraisal of the request.
Art 24(3)	Upon receipt by the Commission of such a request, transfers of funds between that Member State and the country or territory concerned shall be provisionally treated as transfers of funds within that Member State until a decision is reached in accordance with this Article.
Art 24(4)	If, within two months of receipt of the request, the Commission considers that it does not have all the information necessary for the appraisal of the request, it shall contact the Member State concerned and specify the additional information required.
Art 24(5)	Within one month of receipt of all the information that it considers to be necessary for the appraisal of the request, the Commission shall notify the requesting Member State accordingly and shall transmit copies of the request to the other Member States.
Art 24(6)	Within three months of the notification referred to in paragraph 5 of this Article, the Commission shall decide, in accordance with Article 23(2), whether to authorise the Member State concerned to conclude the agreement that is the subject of the request. The Commission shall, in any event, adopt a decision as referred to in the first subparagraph within 18 months of receipt of the request.

Art 24(7)	By 26 March 2017, Member States that have been authorised to conclude agreements with a country or territory concerned pursuant to Commission Implementing Decision 2012/43/EU [(20)], Commission Decision 2010/259/EU [(21)], Commission Decision 2009/853/EC [(22)] or Commission Decision 2008/982/EC [(23)] shall provide the Commission with updated information necessary for an appraisal under point (c) of the second subparagraph of paragraph 1. Within three months of receipt of such information, the Commission shall examine the information provided to ensure that the country or territory concerned requires payment service providers under its jurisdiction to apply the same rules as those established under this Regulation. If, after such examination, the Commission considers that the condition laid down in point (c) of the second subparagraph of paragraph 1 is no longer met, it shall repeal the relevant Commission Decision or Commission Implementing Decision.
	Article 25 - Guidelines
	By 26 June 2017, the ESAs shall issue guidelines addressed to the competent authorities and the payment service providers in accordance with Article 16 of Regulation (EU) No 1093/2010, of Regulation (EU) No 1094/2010 and of Regulation (EU) No 1095/2010, on measures to be taken in accordance with this Regulation, in particular as regards the implementation of Articles 7, 8, 11 and 12.
CHAPTER 7 - FINAL PROVISIONS	
	Article 26 - Repeal of Regulation (EC) No 1781/2006
	Regulation (EC) No 1781/2006 is repealed. References to the repealed Regulation shall be construed as references to this Regulation and shall be read in accordance with the correlation table in the Annex.
	Article 27 – Entry into force
	This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*. It shall apply from 26 June 2017.