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. Following the United Kingdom's (UK) decision to leave the European Union, the FTRs were legislatively onshored through a statutory instrument (SI), The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations, which came into force on the 26th June 2017.

UK Finance has worked with its members to produce an additional voluntary guidance document. This 'How To' interpretative guidance is intended to provide some operational clarity and encourage market harmonisation on points material to, for example, straight-through processing.

These guidelines have been prepared for general guidance only, and should not be construed as legal guidance. 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.

Members may also find it helpful to refer to the ESA Guidelines as further context.

Articles		How-to comments
CHAPTER 1 - SUBJECT MATTER, SCOPE AND DEFINITION		
	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 United Kingdom (UK).	HOW TO: **For the avoidance of doubt, Non-Bank Payment Service Providers (NBPSPs) and Non-Bank Financial Institutions are in scope of the FTR and must identify where they are Payer Payment Service Provider (PSP) and ensure that true Payer information is included in Field 50 or the ISO20022 equivalent.**
	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 UK.	**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/FCA guidance to branches and subsidiaries located outside of the UK, where the parent company is located within the UK. 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: **With regards to payment message types in scope, any message which effects a transfer of funds shall be deemed to be in scope"**

Articles		How-to comments
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: **Payments that are made as an intrinsic part of wider business, e.g., securities services, which is not a payment services business can seek to use the negative scope under Article 2.** **This often has the effect that the PSP of the Payer is clear in their treatment of the payment but onward PSPs are not based on the content of the payment message.** **As a result, Requests for Information (RFI) are requested and responded to adding friction and cost to the payment process where missing or incomplete date is detected.** **To reduce friction, PSPs should where possible ensure the payment messages contain the complete information or where market practice used a different convention then a statement in a free text advising of its exclusion under Article 2 can be considered. It is easier to ensure the payment message contains the correct information at generation than respond to RFIs.** **Where the PSP of the Payer is responding to an RFI it can state the payment is out of scope under Article 2. It is optimal to provide the information requested as routine. Onward PSPs do not need to challenge the PSP of the Payer on the basis under which they content exclusion using Article 2, the remains the responsibility of the PSP of the Payer.** **Where such instances present recurrent problems, PSPs may enter into dialogue to understand and resolve the problems to reduce RFIs through common understanding.**
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 post-paid 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 post-paid device with similar characteristics, is used in order to effect a person-to-person transfer of funds.	Art 2(3)b states that the Regulation does apply for person-to-person transfers. Section 15 of the ESA guidelines states that the exemption will only continue to apply if PSP can demonstrate that it is for goods or services. 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 the UK; (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)	The UK 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 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.	**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 UK transfers. As noted in the ESA 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 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.**

Articles		How-to comments
	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.	HOW TO: **In line with Section 1.18 of Part III JMLSG Guidance, where an online based Payment Services Provider, that operates under a contractual agreement with a merchant (similar to a merchant acquirer) acting as a payment gateway to the payment clearing process, pays the funds owed to a merchant for their sales from multiple customers, in an aggregated and consolidated settlement payment following reconciliation and net of fees after an agreed period of time (pull payment), the online PSP entity is the Payer of this consolidated settlement payment.** **However, the online PSP is obligated to instruct disbursement of funds or settlements to Payees (online merchants) with complete and meaningful Payer and Payee information and have the necessary controls in place such as detection of missing information, etc.** **Ultimately, in the described scenario, it is the responsibility of the PSP of the Payer (the Bank or Non-Bank PSP holding the payment account of the online PSP) to monitor and ensure compliance and flag any data quality concerns to the online PSP client for remediation and should follow the relevant obligations under the Regulation.**
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;	HOW TO: **Firms have noted instances whereby a NBPSP is incorrectly reflected as Payer thereby misrepresenting a cross-border payment as a domestic one. This happens where the NBPSP does not have access to a channel such as SWIFT, so the IPSP / Bank initiates the message with their NBPSP client as Payer instead of Payer PSP where the underlying customer should be present.**
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	
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; (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 post-paid device with similar characteristics;	

Articles		How-to comments
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 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.	HOW TO: **Information to be included in messages: Payer Name** **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 noncompliance 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).**

Articles	How-to comments
	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.** **'The case study outlined below is an illustration for products where NBPSP utilise Banking PSPs to facilitate payments for the NBPSP's underlying clients.'** **Case study 1 - Virtual accounts for NBPSPs (excluding merchant acquiring type business models)** *PSPA Ltd ("PSPA") is an NBPSP which provides FX and cross border payments services to its customers. It is not a SWIFT participant and has a pooled Segregated Master account to process the FX/funds transfer instructions from its clients with Bank BAB Ltd. ("Bank BAB"). Underneath this Master account sit a series of Virtual Accounts ("VA") with virtual Ibans tied to the Master account. The VAs are not physical accounts that hold balances, but simply dummy accounts connected to the master account which are used to effectively allocate and reconcile PSPA's clients' receipts and payments. These VAs may be held in the name of underlying clients of PSPA, who have beneficial interest in the funds. As the underlying clients of PSPA are not direct clients of Bank BAB and no "physical" accounts are opened for them, Bank BAB does not conduct full CDD/KYC on them, which is undertaken by PSPA.* Outgoing Flow *Happy Goods Ltd .(Payer) is a customer of PSPA who wishes to pay its supplier based in Hong Kong (Payer). As the first FI in the chain, PSPA sends the payment instruction to Bank BAB (IPSP) via the Bank's agreed internal channel/system and Bank BAB then initiates SWIFT message using the information provided. Below is a simplistic version of the payment with no FX.* Happy Goods Ltd (Payer) requests transfer of funds ↓ PSPA orders payment to Bank BAB (IPSP) using agreed channel ↓ Bank BAB (IPSP) initiates SWIFT message ↓ Message received by Beneficiary Bank (PSP of the Payee) ↓ Beneficiary in HK (Payee) See Annex (table 1) Incoming Flow *Similarly, Happy Goods Ltd. (Payer) receives a payment from a customer, Buyer Inc. in the US. It provides its customer with its virtual IBAN. Below is a simplistic version of the payment with no FX.* Buyer Inc. (Payer) requests a transfer of funds ↓ Buyer Inc's Bank initiates SWIFT message ↓

Articles	How-to comments
	Bank BAB (IPSP) receives message, identifies Master account from the virtual IBAN and applies payment ↓ PSPA settles payment to Buyer Inc's as per agreed terms See Annex (table 2) **Case study 2 – Segregated accounts for NBPSPs (excluding merchant acquiring type business models)** *PSPA Ltd ("PSPA") is an NBPSP which provides payments wallets/e-money type accounts to its clients for the purpose of cross border payments services, online purchases etc. PSPA is not a SWIFT participant and has a segregated account in its own name with Bank BAB Ltd. ("Bank BAB") used to process the funds transfer instructions from its clients.* *As the underlying clients of PSPA are not direct clients of Bank BAB and no accounts are opened for them, Bank BAB does not conduct full CDD/KYC on them, which is undertaken by PSPA.* Outgoing Flow *Happy Goods Ltd (Payer). is a customer of PSPA who wishes to pay its supplier based in Hong Kong (Payee). As the first FI in the chain, PSPA sends the payment instruction to Bank BAB (IPSP) via the Bank's agreed internal channel/system and Bank BAB then initiates SWIFT message using the information provided. Below is a simplistic version of the payment with no FX.* Happy Goods Ltd (Payer) requests transfer of funds ↓ PSPA orders payment to Bank BAB (IPSP) using agreed channel ↓ Bank BAB (IPSP) initiates SWIFT message ↓ Message received by Beneficiary Bank (PSP of the Payee) ↓ Beneficiary in HK (Payee) See Annex (table 3) Incoming Flow *Similarly, Happy Goods Ltd. (Payee) receives a payment from a customer, Buyer Inc. (Payer) in the US. It provides its customer with its virtual IBAN. Below is a simplistic version of the payment with no FX.* Buyer Inc. (Payer) requests a transfer of funds ↓ Buyer Inc's Bank initiates SWIFT message ↓ Bank BAB receives message, identifies Master account from the virtual IBAN and applies payment ↓ PSPA settles payment to Buyer Inc's as per agreed terms See Annex (table 4) **Corporate 'On Behalf Of' (OBO)/Virtual Account Case Study** *There are instances where corporate clients may want to leverage virtual accounts for intra-group cash management without opening bank accounts for the subsidiary entities.* *The corporate client is not a PSP and cannot legally act as the first PSP in the payment chain regarding payments made out of the related virtual accounts.* *This in turn creates a challenge for firms attempting to establish the true payer if both the master and associated virtual accounts are controlled by the corporate client that holds the direct banking relationship.*

	Articles	How-to comments
		In the case of Corporate virtual account scenarios, either actual accountholder (Happy Goods Plc) or subsidiary (Happy Goods Ltd.) may be reflected as the Payer, as per interpretation of point 8 under 1.13 of Part III JMLSG. See Annex (table 5)
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).	HOW TO: **Where a Unique Transaction Identifier (UTI) is used where a transfer is not made from a Payment Account, there is no standardisation on what format this takes provided the payment messaging system can accommodate the character set. This presents a challenge in determining whether the information could be considered as meaningless.** **This means that the PSP of the Payer may enter UTI that is formatted to their system solution and not that of established banking conventions.** **Despite being permissible, this can have unintended consequences for automated monitoring solutions used by onward PSPs if the UTI character count is short in length or in a combination of characters that the automated solution is not configured for. In such instances the Firm should have procedures in place that ensure agreed/acceptable use of UTIs are in place to limit unnecessary RFI production or erroneous repeat failing financial institution reporting. The automated solution could be tuned accordingly once the convention being used is understood.** **The PSP of the Payer remains accountable for ensuring the UTI enables the transactions to link the PSP of the Payer and the PSP of the Payee accurately upon enquiry.**
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.	HOW TO: **It is acknowledgement that under SEPA, where a UK Debtor Bank (PSP of the Payer) receives an incomplete Direct Debit mandate-related data with the Debtor address missing from an EU Creditor Bank (PSP of the Payee) the Debtor Bank must reject such a payment in order to avoid a breach of the absolute obligations under ART 4(1).** **This presents a technical risk where the Debtor Bank knows the Debtor address but does not enhance the mandate and payment message under the scheme. The financial crime risk presented remains low however in order to act in accordance with the FTR obligations a risk-based approach is not permitted.**
	Article 5 – Transfers of funds within the UK	
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 UK, 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.	

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	**Discussion**: The Final ESA Guidelines did 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 diligence is not necessary The period of time depends on the customers, product and destination countries. HMRC recommends that businesses

	Articles	How-to comments
	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.	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 UK	
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 UK, 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 carry the payment account number of the payer or, where Article 4(3) applies, the unique transaction identifier.	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 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 UK, 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.	
SECTION 1 - OBLIGATIONS ON THE PAYMENT SERVICE PROVIDER OF THE PAYER		
	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.	

	Articles	How-to comments
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 UK, the information referred to in Article 5; (b) for transfers of funds where the payment service provider of the payer is established outside the UK, 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 UK, the information referred to in Article 4(1) and (2) in respect of that batch file transfer.	**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 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." 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

	Articles	How-to comments
		has been identified as egregiously noncompliant 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; • 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 down in Articles 69 and 70 of Directive 2007/64/EC.	
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.	

	Articles	How-to comments
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.	
	Article 8 – Transfers of funds with missing or incomplete information on the payer or the payee	
		Suspending payments for missing information Section 31 of the ESA 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. Section 30(2) of the Guidelines gives suggested high-risk indicators, which includes 'missing 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. **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 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 the information is immediately available to the firm, the firm should provide the information within the appropriate timeframes.** **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.**

Articles	How-to comments
	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 additional information on the client payment. 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.** **Discussion**: As the ESA guidelines captured under Article 3(9) outline, '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.' However, there is uncertainty over the obligations on the payer bank in the event of incomplete or inconsistent payer information. As the UK is no longer a member of the EU/EEA, payer address details are mandatory on all inbound payments from EU/EEA to UK and all outbound payments from UK to EU/EEA. The European Payments Council (EPC) has issued advice to all participants to include payer address details on SEPA Credit Transfers and SEPA Direct Debits to/from UK. As such, inbound SEPA Credit Transfers, including those with missing information, can be treated like other cross border payments using a risk-based approach. Inbound SEPA Direct Debits pose more of a problem as the sending PSP (Creditor PSP) does not have a relationship with the payer (Debtor) and cannot provide the payer's address without contacting the Creditor. The concept and process of sending requests for information (RFI) is difficult to apply and for this reason, PSPs may, in line with a risk-based approach, decide to reject SEPA Direct Debits that do not contain full payer details. HOW TO: **Since the regulatory onshoring of the FTRs, UK-based SEPA payment scheme participants acting as a recipient PSP can credit payments with missing information or make the funds available to the payee using a risk-sensitive approach to payments.** **Where the Creditor PSP fails to provide full payer details in a SEPA Direct Debit instruction, the risk-sensitive approach adopted by the Payer or Debtor PSP could include reliance on information obtained from the client (the payer or debtor) and verified as part of the CDD/KYC process. This approach recognizes the fact that the the payer is not a client of the Creditor PSP and as a result, the Creditor PSP relies on information provided by the Creditor which cannot be verified by the Creditor PSP.**

Articles		How-to comments
		If PSPs decide to process SEPA Direct Debits lacking full payer details, RFIs can be sent via SWIFT to the Creditor PSP, or to the Direct Participant BIC. There is no RFI inquiry message in SEPA so if SWIFT is not an option as the Creditor BIC is SEPA only or a TEC BIC is used, EBA Clearing's SDD Operational Directory could be used to obtain an email address to make contact with the Creditor PSP. **PSPs should leverage available communication channels to engage repeatedly failing Creditor PSPs prior to taking further actions to restrict or reject payments.**
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 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.	
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.	HOW TO: I**n 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.** **Firms should also set out their interpretation of which factors and scenarios they consider a payment to be non-compliant in order to consistently assess payment messages and raise Requests for Information appropriately (RFIs).** **This should include the role the prior PSPs play in the payment message and an assessment of materiality of the nature of the non-compliance. This supports engagement with the repeatedly failing PSP to establish the underlying reason for non-compliance and the resolution to ensure messages are complaint in the future.** **It must be noted that some aspect of payment messaging completeness are subjective and reflect the Firms own risk appetite and local practice. This means that resolution between Firms may not be achieved as PSPs have discretion in determining non-compliance.** **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.** **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); • Additional, factors such as PO boxes, Chinese Character Code and Unique Transaction identifiers over account numbers require a consistent and proportionate approach often with discussion with the remitting PSP.

- **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;**
- **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.**

Discussion: Firms note that it is at time challenging to establish how or when to determine a IPSPs as 'repeatedly failing' consistently across different types of incomplete information, including minor technical requirements (e.g. postcodes or province fields left empty, inconsistent use of abbreviations), to a more substantial level (e.g. blank addresses) and potential higher risk failings (e.g. meaningless information).

It was also noted that there have been cases where a firm receiving payment information does not have an existing relationship with the payment originator (e.g. due to receiving the information through a correspondent banking relationship) and the IPSPs are forced to delay to respond to RFI requests about repeatedly incomplete information. Under the FTRs, the Originating PSP is ultimately responsible for providing the missing information, not the sending PSP/IPSP, however, there is uncertainty of how to respond if the IPSP is repeatedly processing incomplete information.

HOW TO: **Firms should approach this challenge in line with their risk appetite and informed by a risk-based approach. Firms may want to consider the following piece of Wolfsberg Group's guidance which specifies the critical payment information required for sanctions screening to focus initially on understanding the reason for repeatedly incomplete information (e.g. heightened screening, checks for technical limitations), and to focus EDD and payment interventions on higher risk cases (e.g. meaningless information, payment originator in high risk country).**

Firms should include both quantitative and qualitative assessments in determining when to report a failure. A PSP may be repeatedly failing based on quantitative criteria but qualitative factors like response to RFIs, materiality of the information missing (e.g. minor technicalities such as missing street address, postcodes, abbreviations etc. or high-risk errors such as missing or meaningless information) and existence of a clear course of action should be taken into consideration.

Firms should review where the repeat failing PSP has been engaged and explain the underlying reason for non-compliance. A proposal for the resolution of the issue should be provided along with a time frame. Often this is a data or systems issue that requires enhancement or remediation. This aids the assessment of seriousness of non-compliance.

Constructive dialogue and understanding between Firms is far favorable to no dialogue including poor engagement and/or negligent behavior. Poor engagement or negligence should be seen as an aggravating factor in making any report to the FCA.

Firms must also consider the jurisdiction of the repeat failing PSP and the jurisdiction of their regulator. It may be that a risk assessment by the PSP is required to determine whether they wish to continue to process the payment flows involving the repeat failing PSP where the regulator has no jurisdiction or limited influence over the repeat failing PSP.

		Firms should also consider IPSP's obligation to pass on payment messages as it is received. The regulation emphasizes the need to maintain straight through processes and not impede the flow of capital. Firms should consider that IPSPs may have adopted a risk-based approach to meet this requirement.
	Article 9 – Assessment and reporting	
	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.	

Articles	How-to comments

SECTION 3 – OBLIGATIONS ON INTERMEDIARY		
	Article 10 - Retention of information on the payer and the payee with the transfer	
Art 10	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.	**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 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.** **Discussion:** In some multi-leg transactions payment scenarios, the international originator can be obscured or missed without further information (e.g. due to a UK payment intermediary using CHAPS), when a cross-border payment moves into a domestic channel primarily. This is a payments transparency challenge that largely occurs with bulk or aggregated payments. HOW TO: **The following case study is an illustrative example of how this challenge arises in multi-leg transactions** **Correct Leg1 message flow: via SWIFT** **US NBPSP --> US Correspondent Bank of US NBPSP --> UK Correspondent Bank of UK NBPSP --> UK NBPSP (aggregated funds)** **Flow Type is described by NBPSP as liquidity movement between both NBPSPs although the purpose is to facilitate settlement of client funds.** **Details of underlying Payers/Payees whose payments have been aggregated are not available to UK Correspondent Bank.** **Correct Leg2 message flow: via local channel e.g., FPS** **US Payer --> US NBPSP --> UK Correspondent Bank of UK NBPSP --> UK Beneficiary Bank --> UK Beneficiary** **The original US Payer must be added in this leg of the payment under F50/ISO equivalent to ensure transparency requirement is met.** **In order that this settlement leg is not treated as a domestic payment, IPSPs should ensure that when the change from cross-border to domestic channel happens, that the cross-border Payer PSP i.e. US NBPSP, reflects in Field52/ ISO20022 equivalent this to correctly identify the transfer as a cross-border one.**
		If US NBPSP is not added as PSP of Payer, this settlement leg will be treated by UK PSPs as a domestic payment, impacting the type and extent of TM and PT checks applied.

	Articles	How-to comments
	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.	
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 UK, 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.	HOW TO: **The assessment of repeat failing PSPs is on the same basis as is considered in Section 8,2 albeit with the reporting Firm in the role of Intermediary PSP.**
	Article 13 – Assessment and reporting	
	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.	

Articles	How-to comments
Chapter 3 - Information, Data protection and Record-retention	**NO COMMENTS ON THE SUBSEQUENT CHAPTERS**
Chapter 4 - Sanctions and Monitoring	
Chapter 5 - Implementing Powers	
Chapter 6 - Derogations	
Chapter 7 - Final provisions	

CASE STUDY ANNEX

TABLE 1 - CASE STUDY 1

Party name	Role (as per FTR)	Party Field to be used	Comments
Happy Goods Ltd.	Payer	F50/ISO Equivalent Virtual Account number used as Payer account number.	Considerations: • No physical Bank/payment account is held by Happy Goods with PSPA • Payer account number used could be a virtual IBAN which gives the appearance of the Payer holding an account with Bank BAB • Adding Payer in F50 not only allows application of Payment Transparency controls (e.g. meaningless information checks) but also ensures effectiveness of transaction monitoring controls.
PSPSA	Payment Service Provider (PSP) of the Payer	F52/ISO Equivalent	
Bank BAB	Intermediary PSP (IPSP)	F53/ ISO Equivalent	
Beneficiary Bank	PSP of the Payee	F57/ ISO Equivalent	
Beneficiary	Payer	F59/ ISO Equivalent	

TABLE 2 - CASE STUDY 1

Party name	Role (as per FTR)	Party Field to be used	Comments
Buyer Inc.	Payer	F59/ISO Equivalent .	Considerations: • No physical Bank/payment account is held by Happy Goods with PSPA • Payee account number used could be a virtual IBAN which gives the appearance of the Payer holding an account with Bank BAB • Adding Payer in F59 not only allows application of Payment Transparency controls (e.g. meaningless information checks) but also ensures effectiveness of transaction monitoring controls.
Beneficiary Bank	PSP of the Payer	F52/ISO Equivalent	
Bank BAB	IPSP	F53/ ISO Equivalent	
PSPSA	PSP of the Payee	F57/ ISO Equivalent	
Happy Goods Ltd	Payee	F50/ ISO Equivalent Virtual Account number used as Payer account number	

TABLE 3 - CASE STUDY 2

Party name	Role (as per FTR)	Party Field to be used	Comments
Happy Goods Ltd.	Payer	F50/ISO Equivalent .	Considerations: • Adding Payer in F50 not only allows application of Payment Transparency controls (e.g. meaningless information checks) but also ensures effectiveness of transaction monitoring controls
Beneficiary Bank	PSP of the Payer	F52/ISO Equivalent	
Bank BAB	IPSP	F53/ ISO Equivalent	
PSPSA	PSP of the Payee	F57/ ISO Equivalent	
Buyer Inc.	Payee	F59/ ISO Equivalent	

TABLE 4 - CASE STUDY 2

Party name	Role (as per FTR)	Party Field to be used	Comments
Buyer Inc.	Payer	F59/ISO Equivalent .	Considerations: • Adding Payer in F59 not only allows application of Payment Transparency controls (e.g. meaningless information checks) but also ensures effectiveness of transaction monitoring controls.
Beneficiary Bank	PSP of the Payer	F52/ISO Equivalent	
Bank BAB	IPSP	F53/ ISO Equivalent	
PSPSA	PSP of the Payee	F57/ ISO Equivalent	
Happy Goods Ltd.	Payee	F50/ ISO Equivalent	

TABLE 5 - CASE STUDY 3

Party name	Role (as per FTR)	Party Field to be used	Comments
Happy Goods Ltd.	Payer	The true payers to be captured in F50/ISO Equivalent	Considerations: • No physical Bank/payment account is held by Happy Goods with Bank BAB. • Happy People Plc controls both the Master and Virtual Accounts • Payments made from the Virtual Accounts are accompanied with the virtual IBAN, name and address of the subsidiary, in this example, Happy Goods Ltd • This gives the appearance of Happy Goods Ltd holding an account with Bank BAB.
Happy Goods Plc	PSP of the Payer	F52/ISO Equivalent	
Bank BAB	Actual account holder	F53/ ISO Equivalent	
Beneficiary Bank	PSP of the Payee	F57/ ISO Equivalent	
Beneficiary	Payee	F59/ ISO Equivalent	