1: Transparency in electronic payments (Wire transfers)

Note: This section may only be relevant to a limited number of firms in the financial sector (see Part I, paragraphs 5.2.10ff). It previously formed the 'Wire Transfers' guidance in Part II and has now been moved to Part III and extended to include cover payments. Part A refers to FATF SR VII and Part B to Cover Payments.

PART A – FATF SRVII

Background

1.1 FATF issued Special Recommendation VII in October 2001, with the objective of enhancing the transparency of electronic payment transfers ("wire transfers") of all types, domestic and cross border, thereby making it easier for law enforcement to track funds transferred electronically by terrorists and criminals. A revised Interpretative Note to this Special Recommendation was issued by the FATF on 10 June 2005, further revised on 29 February 2008, and is available at http://www.fatf-gafi.org/dataoecd/34/56/35002635.pdf

1.2 Special Recommendation VII is addressed to FATF member countries, and was implemented in member states of the European Union, including the UK, through Regulation 1781/2006, which is at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:345:0001:0009:EN:PDF

1.3 The Regulation requires the ordering financial institution to ensure that all wire transfers carry specified information about the originator (Payer) who gives the instruction for the payment to be made. The core requirement is that this information consists of name, address and account number; however, there are a number of permitted variations and concessions, see below under **Information Requirements** (paragraphs 1.13ff**).**

1.4 As the text of this Regulation has EEA relevance, the three non-EU Member States of the EEA, i.e., Iceland, Liechtenstein and Norway, are expected to enact equivalent legislation. As and when this happens, references in this guidance to *intra-EU* can be understood to include these states. However, for the time being the reduced information requirement available within the EU will not apply to payments to and from those countries.

1.5 During 2008, the AML Task Force of the three Level 3 Committees (European Banking Supervisors, Securities Regulators and Insurance and Operational Pensions) investigated the varying approaches of Payment Service Providers across the EU to the inward monitoring obligations contained in the Regulation. Following consultation with industry and others, they published in October 2008 a 'Common Understanding' designed to achieve a more consistent approach by Payment Service Providers. Further details are set out at paragraphs 1.30 and Annex 1-II.

Scope of the Regulation

1.6 The Regulation is widely drawn and intended to cover all types of funds transfer falling within its definition as made "by electronic means", other than those specifically exempted wholly or partially by the Regulation. For UK-based Payment Service Providers (PSPs) it therefore includes, but is not necessarily limited to, international payment transfers made via SWIFT, including various Euro

payment systems, and domestic transfers via CHAPS and BACS. The Regulation specifically exempts the following payment types:

- transfers where both Payer and Payee are PSPs acting on their own behalf - this will apply to MT 200* series payments via SWIFT. This exemption will include MT 400 and MT 700 series messages when they are used to settle trade finance obligations between banks (*cover payments using MT 202/205COVs **are**, however, in scope – see Part B of this guidance);

- transfers by credit or debit card or similar payment instrument, providing that the Payee has an agreement with the PSP permitting payment for goods or services and that the transfer is accompanied by a unique identifier permitting the transaction to be traced back to the Payer (see paragraph 1.17);

- transfers whereby the Payer withdraws cash from his/her own account. This is designed to exempt ATM withdrawals outside the EU which would otherwise attract the full information requirement;

- transfers to public authorities for taxes, fines or other levies;

- direct debits, subject to their carrying a unique identifier for tracing purposes;

- truncated cheques (cheques are otherwise paper to which the Regulation does not apply);

- Article 3 (4) provides a limited exemption for small pre-paid transfers carried out by means of a mobile phone or any other digital or IT device;

- e-money transfers, as defined in Article 11(5)(d) of the Third EU Money Laundering Directive, where they do not exceed €1000. i.e., those transfers transacted using non-reloadable electronic money products on which the maximum load does not exceed € 150, or using reloadable e-money products which are subject to a maximum load of €2500 in a calendar year and maximum redemption of under €1000 in the same calendar year. (see also Part II Sector 3: *Electronic money*);

- post-paid funds transfers carried out by mobile phone, or any other digital or IT device, subject to various conditions, including their traceability and that they relate to the provision of goods and services.

1.7 The following payment types are also exempt under the Regulation (under derogations which are not used in the UK):

- Article 3 (6), which exempts small payments for goods and services, relates to giro payment systems in a few other member states;

- funds transfers of €150 or less for charitable, religious, cultural, educational, social, scientific or fraternal purposes to a prescribed group of non-profit organisations which run annual / disaster relief appeals and which are subject to reporting and external audit requirements or supervision by a public authority and whose names and supporting details have been specifically communicated by the Member State to the Commission. This applies only to transfers within the territory of the Member State. The exemption is designed to ensure that small charitable donations to certain bona fide bodies are not frustrated, but has limited practical relevance in the

UK, where typical mechanisms for making payments to charities, e.g., by credit transfer or by card payment within the EU, will either not be subject to the Regulation, or where they are, will be compliant with it in any case;

1.8 The UK credit clearing system is out of scope of the Regulation as it is paper-based and hence transfers are not carried out "by electronic means". Cash and cheque deposits over the counter via bank giro credits are not therefore affected by the Regulation.

Note: The Regulation defines "Payee" as a natural or legal person who is the intended final recipient of transferred funds. Recognizing that a perverse and wholly unworkable interpretation could be put on those words, where a named Payee might have been a conduit for an undisclosed 'final recipient' to serve a criminal objective, this Guidance takes the position that 'final recipient' can only practically be understood as referring to the party named in the transfer as the beneficiary of the payment.

See paragraph 1.18 below in relation to the merchant acquisition payment process.

Pre-conditions for making payments

1.9 Payment Service Providers (PSPs) of Payers must ensure that the Payer information conveyed in the payment relating to account holding customers is accurate and has been verified. The verification requirement is deemed to be met for account holding customers of the PSP whose identity has been verified, and where the information obtained by this verification has been stored in accordance with anti money laundering requirements, ie in the UK in accordance with the Money Laundering Regulations 2007, which gave effect to the Third EU Money Laundering Directive. This position applies even though the address shown on the payment transfer may not have been specifically verified. No further verification of such account holders is required, although PSPs may wish to exercise discretion to do so in individual cases; e.g., firms will be mindful of Part I, paragraphs 5.3.14 – 5.3.18, concerning customers with existing relationships. (See 1.13ff where the named Payer is not the holder of the account to be debited.)

1.10 Before undertaking one-off payments in excess of €1000 on the instructions of non-account holding customers, the PSP of the Payer should verify the identity and address (or evidence of a permitted alternative to address, such as date and place of birth if quoting that information on the transfer instead of address).

1.11 For non-account based transfers of €1000 and under, PSPs are not required by the Regulation to verify the Payer's identity except when several transactions are carried out which appear to be linked (see Article 5.4) and together exceed €1000. NB, even in cases where the Regulation does not require verification, the customer information has to be obtained and it may be advisable for the PSP to verify the identity of the Payer in all cases.

1.12 Evidence of verification must be retained with the customer information in accordance with **Record Keeping Requirements** (see 1.20-1.21).

Information Requirements

1.13 Complete payer information:

Except as permitted below, complete Payer information must accompany all wire transfers. Effectively, the complete Payer information requirement applies where the destination PSP is located in a jurisdiction outside the European Union. Complete Payer information consists of: name, address and account number.

- Address ONLY may be substituted with the Payer's date and place of birth, or national identity number or customer identification number. This Guidance recommends that these options are only deployed selectively within a firm's processes to address particular needs. It follows that in the event a Payee PSP demands the Payer's address, where one of the alternatives had initially been provided, the response to the enquiry should point that out. Only with the Payer's consent or under judicial compulsion should the address be additionally provided.

- Where the payment is not debited to a bank account, the requirement for an account number must be substituted by a unique identifier which permits the payment to be traced back to the Payer.

- The extent of the information supplied in each field will be subject to the conventions of the messaging system in question and is not prescribed in detail in the Regulation.

- The account number could be, but is not required to be, expressed as the IBAN (International Bank Account Number).

- The Regulation applies even where the Payer and Payee hold accounts with the same PSP.

- Where a bank is itself the Payer, as will sometimes be the case even for SWIFT MT 102 and 103 messages, this Guidance considers that supplying the Bank Identifier Code (BIC) constitutes complete Payer information for the purposes of the Regulation, although it is also preferable for the account number to be included where available. The same applies to Business Entity Identifiers (BEIs), although in that case the account number should always be included. As the use of BICs and BEIs is not specified in FATF Special Recommendation VII or the Regulation, there may be requests from Payee PSPs for address information.

- Generally, firms will populate the information fields from their customer database. In cases where electronic banking customers input their details directly the Payer's PSP is not required, at the time that the account is debited, to validate the Payer's name and/or address against the name and address of the accountholder whose account number is stated on the payment transfer.

- Where the named Payer is not the accountholder the Payer's PSP may either substitute the name and address (or permitted alternatives) of the account holder being debited (subject to any appropriate customer agreement), or execute the payment instruction with the alternative Payer name and address information provided with the consent of the accountholder. In the latter case, provided the Payer PSP retains all relevant data for 5 years, the Payer PSP is required to verify only the information about the accountholder being debited (in accordance with Article 5.3a. of the Regulation). PSPs should exercise a degree of control to avoid abuse of the discretion by customers.

  It is important to note that this flexibility should not undermine the transparency of Payer information sought by FATF Special Recommendation VII and the Regulation. It is designed to meet the practical needs of corporate and other business (e.g., solicitor)

accountholders with direct access who, for internal accounting reasons, may have legitimate reasons for quoting alternative Payer details with their account number.

- Where payment instructions are received manually, for example, over the counter, the Payer name and address (or permitted alternative) should correspond to the account holder. Any request to override customer information on a similar basis to that set out above for electronic banking customers should be contained within a rigorous referral and approval mechanism to ensure that only in cases where the PSP is entirely satisfied that the reason is legitimate should the instruction be exceptionally dealt with on that basis. Any suspicion arising from a customer's behaviour in this context should be reported to the firm's Nominated Officer.

- Beneficiary information: whilst Regulation 1781/2006 is concerned only with information relating to the Payer it is also important that Payer PSPs include sufficient beneficiary information to mitigate the risks of customer funds being incorrectly blocked, delayed or rejected.

- Payee PSPs are not obligated to pass on to the payee all the payer information they receive with a transfer. However, paragraph 38 of the Payment Services Regulations provides inter alia that:

  "The payee's payment service provider must, immediately after the execution of the payment transaction, provide or make available to the payee the information specified in paragraph (2).

  (2) The information referred to in paragraph (1) is—

  (a) a reference enabling the payee to identify the payment transaction and, where appropriate, the payer and any information transferred with the payment transaction;"

1.14 Reduced Payer Information:

Where the PSPs of both Payer and Payee are located within the European Union, wire transfers need be accompanied only by the Payer's account number or by a unique identifier which permits the transaction to be traced back to the Payer.

- However, if requested by the Payee's PSP, complete information must be provided by the Payer's PSP within three working days, starting the day after the request is received by the Payer's PSP. ("Working days" is as defined in the Member State of the Payer's PSP).

- Article 17 of the Regulation provides for the circumstances in which transfers of funds between EU Member States and territories outside the EU with whom they share a monetary union and payment and settlement systems may be treated as transfers within the Member State, so that the reduced information requirement can apply to payments passing between that Member State and its associated territory (but not between any other Member State and that territory). In the case of the UK such arrangements will include the Channel Islands and the Isle of Man.

- Firms which avail themselves of the option to provide reduced payer information in intra-EU transfers should bear in mind that they may face requests for additional information (especially name) from payee banks for the purpose of sanctions screening (see section 4: *Compliance with the UK financial sanctions regime*, paragraph [4.61]).

1.15 Batch File Transfers:

A hybrid complete/reduced requirement applies to batch file transfers from a single Payer to multiple Payees outside the EU in that the individual transfers within the batch need carry only the Payer's account number or a unique identifier, provided that the batch file itself contains complete Payer information.

1.16 Payments via Intermediaries:

Intermediary PSPs (IPSPs) must, subject to the following guidance on technical limitations, ensure that all information received on the Payer which accompanies a wire transfer is retained with the transfer.

It is preferable for an IPSP to forward payments through a system which is capable of carrying all the information received with the transfer. However, where an IPSP within the EU is technically unable to on-transmit Payer information originating outside the EU, it may nevertheless use a system with technical limitations provided that:

- if it is aware that the Payer information is missing or incomplete it must concurrently advise the Payee's PSP of the fact by an agreed form of communication, whether within a payment or messaging system or otherwise.

- it retains records of any information received for five years, whether or not the information is complete. If requested to do so by the Payee's PSP, the IPSP must provide the Payer information within three working days of receiving the request.

1.17 Card transactions

As indicated in paragraph 1.6, card transactions for *goods and services* are out of scope of the Regulation provided that a unique identifier, allowing the transaction to be traced back to the payer, accompanies the movement of the funds. The 16 digit Card PAN number serves this function.

Similarly, the Card PAN number meets the information requirement for all Card transactions for any purpose where the derogation for transfers within the European Union applies, as explained in and subject to the conditions set out in paragraph 1.14.

Complete payer information is required in all cases where the card is used to generate a direct credit transfer, including a balance transfer, to a payee whose PSP is located outside the EU. These are "push" payments, and as such capable of carrying the information when required under the Regulation.

Otherwise, Card transactions are "pull" payments, i.e., the transfer of funds required to give effect to the transaction is initiated by the merchant recipient rather than the Card Issuer and under current systems it is not possible for any information in addition to the PAN number to flow with the transfer in those cases where the transaction is arguably not for 'goods and services' but is settled to a PSP outside the EU. Examples include Card transactions used to make donations to charity, place bets, or purchase e-money products such as prepaid cards. As a matter of expediency these transactions must therefore be treated as 'goods and services'. FSA and HM Treasury have supported that interpretation for the time being, subject to further review at an unspecified future date on the basis that the transactions are traceable by the PAN number.

1.18 **Merchant Acquisition**

Part II sector 2: *Credit cards* paragraphs 2.9-2.11 briefly describe the payment processing service provided by merchant acquirers in respect of debit and credit card transactions undertaken at point of sale terminals or on the internet. For internet-based transactions a separate PSP, operating under a contractual agreement with the merchant in the same way as a merchant acquirer, may act as a payment gateway to the payment clearing process interfacing as necessary with the merchant's acquirer. These internet PSPs may also accommodate payment methods in addition to cards.

A more detailed explanation of the processing of card transactions may be found in Annex 5 of the FSA's October 2009 Approach document in relation to the Payment Services Regulations.http://www.fsa.gov.uk/Pages/About/What/International/psd/

There are two distinct funds transfers within the overall payment process: first, the collection by the merchant acquirer via the card schemes of the cardholder's funds from the card issuing firm where he holds his account (or where other payment methods are used the funds are collected by the internet PSP direct from the purchaser); secondly, the merchant acquirer (or the internet PSP for non-card transactions) pays the funds over in a separate transaction to the merchant's bank account. The second transfer will normally be a consolidated settlement payment following reconciliation, which aggregates many different transactions, and is made net of fees after an agreed period of time to safeguard against transaction disputes. Details of the underlying transactions are made available to the merchant for its own reconciliation purposes.

Consequently, for the purposes of the Regulation, the internet PSP or merchant acquirer is not an intermediary PSP but is rather the PSP of the payee and is subject to the obligations described in chapter 3 of the Regulation to the extent that they are relevant, i.e., in relation to electronic funds transfers other than card transactions which enjoy a qualified exemption under Article 3(2) of the Regulation. So far as the merchant's bank is concerned the merchant acquirer or the internet PSP is the 'Payer' of the separate consolidated settlement payment and that bank does not receive or require the underlying cardholder PAN number information (or payer details for non-card transactions).

Although the payment process operates in the way described, it should be noted that a full audit trail is available in case of need so that the traceability objective of the Regulation is in no way compromised.

1.19 Minimum standards

The above information requirements are minimum standards. It is open to PSPs to elect to supply complete Payer information with transfers which are eligible for a reduced information requirement and thereby limit the likely incidence of inbound requests for complete information. (In practice a number of large UK and European banks have indicated that they will be providing complete payer information for all transfers where systems permit). To ensure that the data protection position is beyond any doubt, it would be advisable to ensure that terms and conditions of business include reference to the information being provided.

Record Keeping Requirements

1.20 The Payee's PSP and any intermediary PSP must retain records of any information received on a Payer for five years, in accordance with the Regulation.

1.21 The Payer's PSP must retain records of transactions and supporting evidence of the Payer's identity in accordance with Part I, Chapter 8.

Checking Incoming Payments

1.22 Payee PSPs should have effective procedures for checking that incoming wire transfers are compliant with the relevant information requirement. In order not to disrupt straight-through processing, it is not expected that monitoring should be undertaken at the time of processing the transfer. The Regulation specifies that PSPs should have procedures to detect whether relevant information is missing. (It is our understanding that this requirement is satisfied by the validation rules of whichever messaging or payment system is being utilised). Additionally, the Regulation requires PSPs to take remedial action when they become aware that an incoming payment is not compliant. Hence, in practical terms it is expected that this requirement will be met by a combination of the following:

(i) SWIFT payments on which mandatory Payer information fields are not completed will fail anyway and the payment will not be received by the Payee PSP. Current SWIFT validation prevents payments being received where the mandatory information is not present at all. However, it is accepted that where the Payer information fields are completed with incorrect or meaningless information, or where there is no account number, the payment will pass through the system. Similar considerations apply to non-SWIFT messaging systems which also validate that a field is populated in accordance with the standards applicable to that system, e.g., BACS.

(ii) SWIFT has reviewed how its validation standards might be improved to facilitate inward monitoring, as a result of which Option F has been introduced as one of the three available formatting options. Option F structures information systematically by means of specified identifier codes and formatting conventions. However, use of this Option is not mandatory.

(iii) PSPs should therefore subject incoming payment traffic to an appropriate level of post event random sampling to detect non-compliant payments. This sampling should be risk based, e.g.,:

- the sampling could normally be restricted to payments emanating from PSPs outside the EU where the complete information requirement applies;

- the sampling could be weighted towards non FATF member jurisdictions, particularly those deemed high risk under a PSP's own country risk assessment, or by reference to external sources such as Transparency International, or FATF or IMF country reviews);

- focused more heavily on transfers from those Payer PSPs who are identified by such sampling as having previously failed to comply with the relevant information requirement;

- Other specific measures might be considered, e.g., checking, at the point of payment delivery, that Payer information is compliant and meaningful on all transfers that are collected in cash by Payees on a "Pay on application and identification" basis.

NB. Whenever these measures reveal potentially suspicious transactions, the normal reporting obligations apply (see Part I, Chapter 6).

1.23 If a Payee PSP becomes aware in the course of processing a payment that it contains meaningless or incomplete information, under the terms of Article 9 (1) of the Regulation it should either reject the transfer or ask for complete information on the Payer. In addition, in such cases, the Payee PSP is required to take any necessary action to comply with any applicable law or administrative provisions relating to money laundering and terrorist financing. Dependent on the circumstances such action could include making the payment or holding the funds and advising the Payee PSP's Nominated Officer.

1.24 Where the Payee PSP becomes aware subsequent to processing the payment that it contains meaningless or incomplete information either as a result of random checking or other monitoring mechanisms under the PSP's risk-based approach, it must:

(i) seek the necessary information on the Payer

and/or

(ii) take any necessary action under any applicable law, regulation or administrative provisions relating to money laundering or terrorist financing.

1.25 PSPs will be mindful of the risk of incurring civil claims for breach of contract and possible liability if competing requirements arise under national legislation, including in the UK the Proceeds of Crime Act and other anti money laundering and anti terrorism legislation.

1.26 Where a PSP is identified as having regularly failed to comply with the information requirements, under Article 9(2) the Payee PSP should take steps, which may initially include issuing warnings and setting deadlines, prior to either refusing to accept further transfers from that PSP or deciding whether to terminate its relationship with that PSP either completely or in respect of funds transfers.

1.27 Under Article 10 a Payee PSP should consider whether incomplete or meaningless information of which it becomes aware on a funds transfer constitutes grounds for suspicion which would be reportable to its Nominated Officer for possible disclosure to the Authorities.

1.28 With regard to transfers from PSPs located in countries that are not members of either the EU or FATF, firms should endeavour to transact only with those PSPs with whom they have a relationship that has been subject to a satisfactory risk-based assessment of their anti money laundering policies and procedures and who accept the standards set out in the Interpretative Note to FATF Special Recommendation VII.

1.29 It should be borne in mind when querying incomplete payments that some FATF member countries outside the EU may have framed their own regulations to incorporate a threshold of €/US$ 1000 below which the provision of complete information on outgoing payments is not required. This is permitted by the Interpretative Note to FATF Special Recommendation VII. The USA is a case in point. This does not preclude European PSPs from calling for the complete information where it has not been provided, but it is reasonable for a risk-based view to be taken on whether or how far to press the point.

1.30 As indicated in paragraph 1.5, the inward monitoring requirements of the Regulation were elaborated on in the *Common Understanding* (CU) published in October 2008 by the AML Task Force of three European regulatory bodies. The CU positioned itself as a "clarification" of the Regulation's requirements, not an "extension" of them. Whilst the final document was less

prescriptive than the Task Force's starting position the expectations set out are fairly detailed, covering the various elements within the Regulation, viz

- Sampling and filtering of incoming payments
- Deadlines for remediating deficient transfers
- Identifying regularly failing Payment Service Providers

all of which should be enshrined by firms within a clearly articulated set of policy and processes approved at an appropriately senior level defining the approach to be adopted to discharge these requirements Annex 1-II sets out a broad summary of the requirements, but firms should refer directly to the CU for the detail. See:

http://www.c-ebs.org/getdoc/d399f8d4-c2e4-4cce-8141-1aff447bb189/The-three-Level-3-Committees-publish-today-their-c.aspx

PART B – COVER PAYMENTS

Background

1.31 A customer funds transfer usually involves the ordering customer (originator) instructing its bank (the originator's bank) to make a payment to the account of a payee (the beneficiary) with the beneficiary's bank. In the context of international funds transfers in third party currencies, the originator's bank will not usually maintain an account with the beneficiary bank in the currency of the payment that enables them to settle the payment directly. Typically, intermediary (or covering) bank(s) are used for this purpose, usually (but not always) located in the country where the currency of the payment is the national currency. The alternative but less efficient method of making such payments is by serial MT103.

1.32 Cover payments are usually effected via SWIFT and involve two distinct message streams:

- A customer payment order (usually a SWIFT Message Type (MT)103) which is sent by the originator's bank direct to the beneficiary's bank and carries payment details, including originator and beneficiary information;
- A covering bank-to-bank transfer (the cover payment - historically, a SWIFT MT202) which is sent by the originator's bank to an intermediary bank (usually its own correspondent) asking the intermediary bank to 'cover' the originator bank's obligation to pay the beneficiary bank. The intermediary bank debits the originator bank's account and either credits the beneficiary bank's account under advice, or if no account is held, sends the funds to the beneficiary bank's correspondent with settlement usually being effected through the local Real Time Gross Settlement System (RTGS). The beneficiary bank is then able to reconcile the funds that it receives on its correspondent account with the MT103 received direct from the originator's bank.

1.33 Payments are sent using the 'cover method' primarily to avoid delays associated with differing time zones and to reduce the costs associated with commercial transactions.

Transparency Issues:

1.34 Historically, the MT202 has been used either to effect cover for an underlying customer transfer (MT103) or for inter-bank payments that are unconnected to customer transfers, such as wholesale money market or foreign exchange transactions. Consequently, an intermediary bank would not necessarily know that it was dealing with a cover payment when processing an MT202 message. Additionally, as there is no provision within the MT202 message format for it to carry the originator and beneficiary information that is contained in an underlying MT103 customer transfer, an intermediary bank has not, hitherto, been in a position to screen or monitor underlying customer information in relation to cover payments, from a sanctions or ML/FT perspective.

1.35 To improve transparency in respect of cover payments, and in order to assist financial institutions with their sanctions and AML/CFT obligations, SWIFT created a variant of the MT202, being the MT202COV[1], which has, since the 21st November 2009 go-live date, enabled originator and beneficiary information contained in the MT103 customer transfer to be replicated in certain fields of the MT202COV (further details can be found at www.swift.com):

[1] For cover payments effected between originator and beneficiary banks located in the same jurisdiction using a third party currency, an MT205COV can be used instead of an MT202COV and references in this guidance to MT202COV also relate to MT205COV.

1.36 The MT 202COV should be used for all outgoing cover payment transactions for which there is an associated MT103 and must replicate the originator/beneficiary information contained in the MT 103. The existing MT 202 should in future be used only for bank to bank transactions. As soon as technically feasible after the 21st November 2009 go-live date, firms should have the capability to receive MT202COV messages from other banks and, as a minimum, screen them against mandatory lists of individuals and entities whose assets must be blocked, rejected or frozen.

1.37 As an alternative to sending customer payments using the 'cover method', banks can choose to send their payments by the 'serial method' in which an MT103 is sent by the originator's bank to its correspondent asking for payment (and the corresponding covering funds) to be made available to the beneficiary bank for account of the beneficiary.

Further Guidance

1.38 After consulting with industry and regulators, in May 2009 the Basel Committee on Banking Supervision (BCBS) issued a paper entitled 'Due diligence and transparency regarding cover payment messages related to cross-border wire transfers', which is available at www.bis.org and provides further guidance for banks processing cover payments. This guidance is not mandatory and currently has no formal legal or regulatory force in the UK.,

Other Useful Sources of Information:

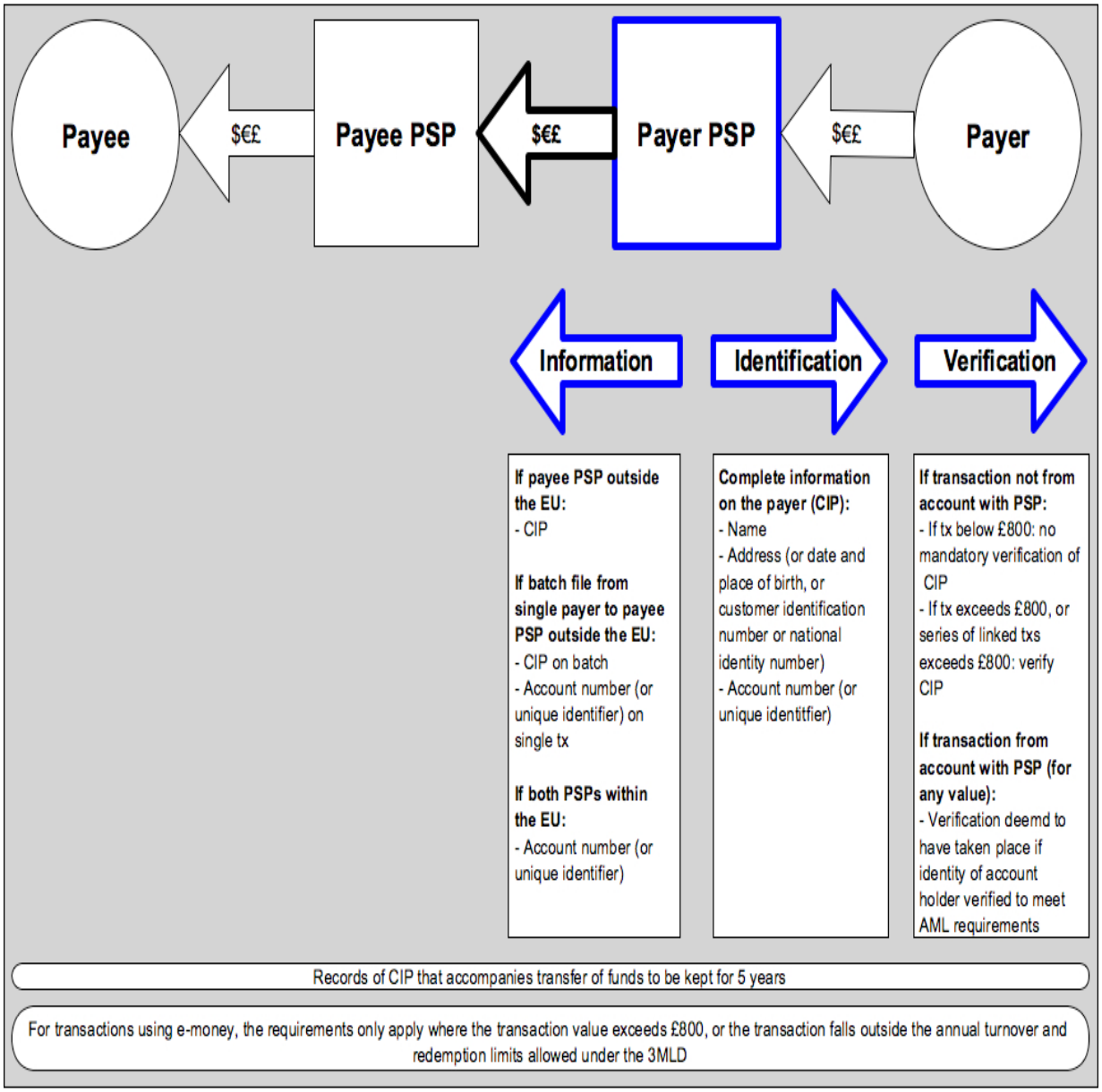
1. SWIFT Press release. 'New Standards for Cover Payments' (May 19 2009), available at http://www.swift.com/.

2. 'Guidelines for use of the MT202COV' issued by the Payments Market Practice Group, available at http://pmpg.webex.one.com/default.asp?link

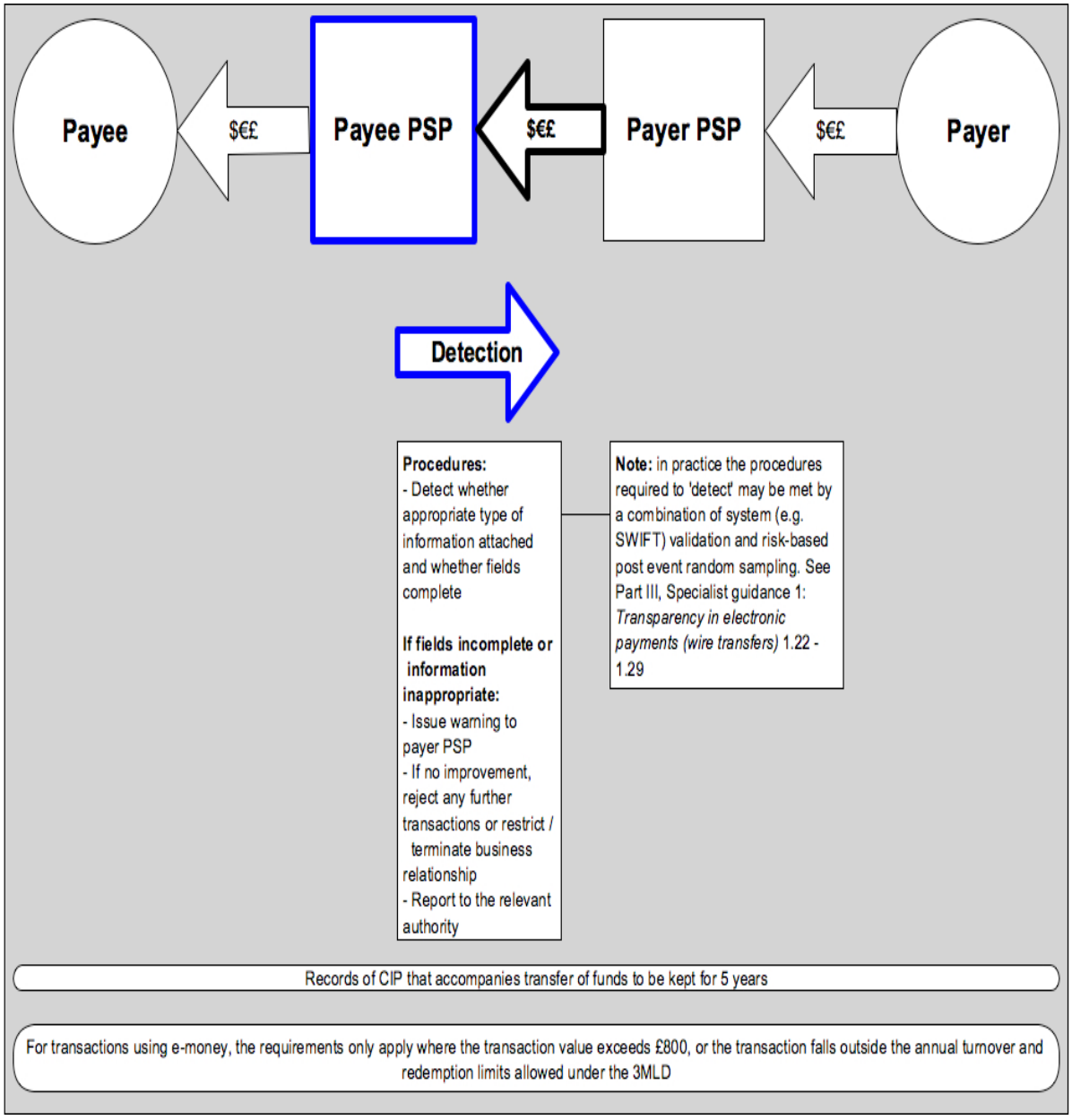
3. 'Cover Payments: Background Information and implications of the new SWIFT Message Format' and 'The Introduction of the MT202COV in the International Payment Systems,' issued jointly in May 2009 by the Bankers' Association for Finance and Trade, the Clearing House Association LLC, the European Banking Federation, the International Banking Federation, the International Chamber of Commerce, the International Council of Securities Associations, the International Financial Services Association, SWIFT and the Wolfsberg Group, available at the respective web sites of these organisations.

ANNEX 1-I

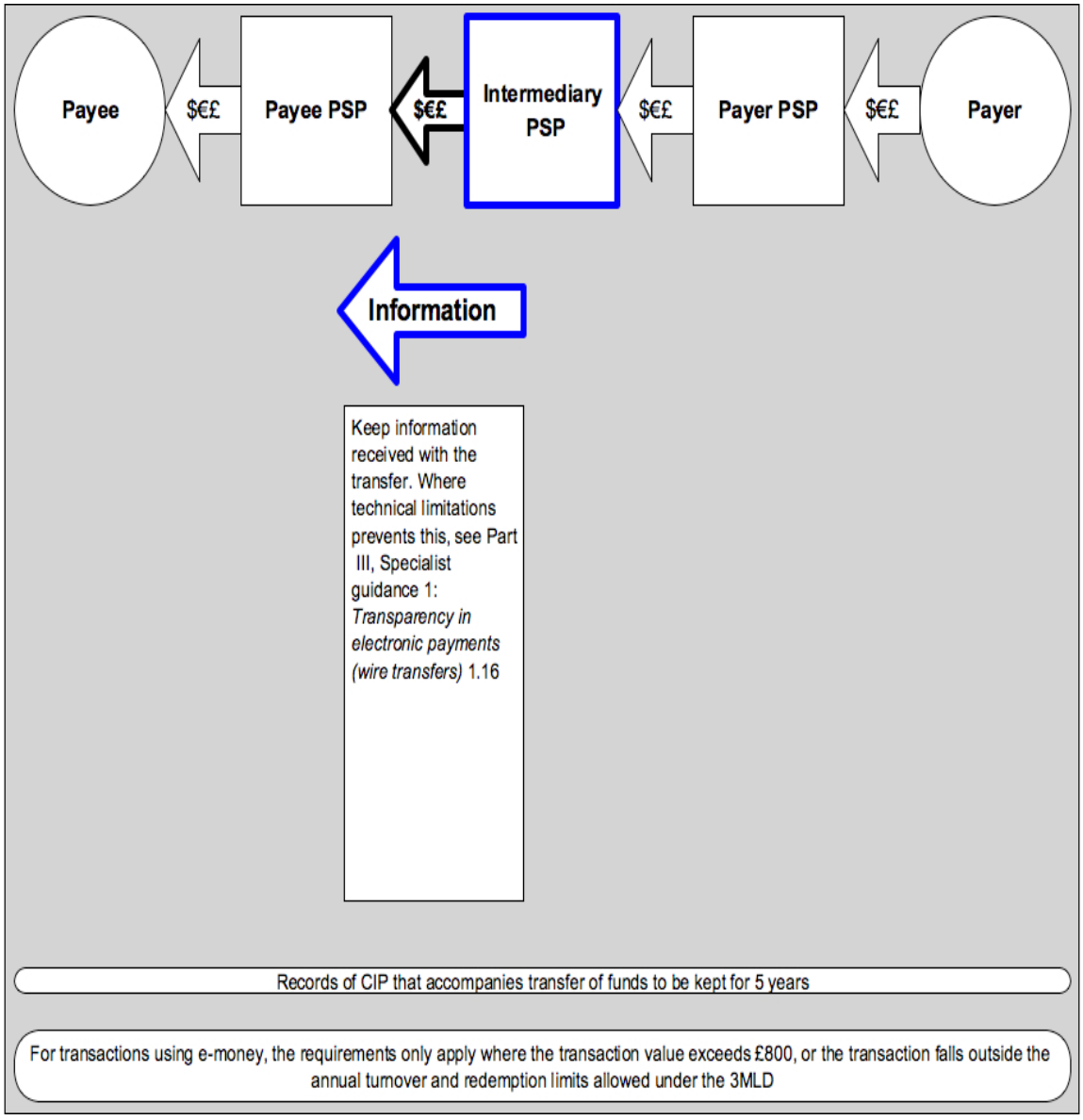
Scenario 1: Transfer of funds – Obligations on Payer PSP



Scenario 2: Transfer of funds – Obligations on Payee PSP



Scenario 3: Transfer of funds – Obligations on Intermediary PSP



ANNEX 1-II

Summary of the 'Common Understanding'

For background, refer to paragraphs 1.5 and 1.30.

The following is a summary only – firms should refer directly to the Common Understanding for the detail. See: http://www.c-ebs.org/getdoc/d399f8d4-c2e4-4cce-8141-1aff447bb189/The-three-Level-3-Committees-publish-today-their-c.aspx

1. Sampling / Filtering:

The CU accepted the basic premise of system validation as the first line of defence, which in the absence currently of a standard filter will inevitably allow some deficient payments to be accepted. Hence, PSPs should deploy two types of control

- **post event sampling**: unless PSPs can detect incomplete or meaningless payments at the time of processing a transfer the CU supports the position that there should be risk based, post event sampling to detect non compliant payments. To fulfil the risk based criterion, sampling could focus on transfers from higher risk sending PSPs, especially those previously identified as having failed to comply with the relevant information requirements.
- **filtering for 'obvious meaningless information'** defined as 'information clearly intended to circumvent the intention of the Regulation': this is not a mandatory control, rather PSPs are 'encouraged' to apply such filters. What is in mind here are formulations such as 'one of our customers' or any form of words which on the face of it is not providing genuine sender information.
- PSPs are expected to take action on all incomplete or meaningless transfers that they become aware of. Depending on whether they become aware at the time of processing or subsequently they should take action on all such defective transfers so identified in the form of one of the three response options: (1) reject the transfer, (2) hold it and ask for missing information, (3) process the payment and ask for missing information.
- Subject to any overriding legal restraints in their own jurisdiction PSPs are urged not to rely only on the No 3 post event follow-up option but to deploy the other options when appropriate. (N.B. The BBA took the position in their response to the consultation that other than in exceptional circumstances rejection of payment or delay in processing was quite unacceptable from a customer service perspective).

2. Deadlines for remediating deficient transfers:

When requesting missing information PSPs should work to appropriate and self imposed deadlines. The CU suggested what it considered to be reasonable timeframes for this purpose. In the absence of a satisfactory response the sending PSP should be warned that it may in future be subject to high risk monitoring (under which all or most of its future payments would be subject to scrutiny). Consideration should also be given as to whether the deficient payment is 'suspicious' and should be reported.

3. Identifying regularly failing PSPs

Mutual policing of PSPs is intended to go beyond the remediation of individual deficient payments to a systematic assessment of those PSPs who persistently fail to provide the information required under the Regulation. A receiving PSPs is therefore expected to establish criteria for determining when a PSP who is sending payments is 'regularly failing' such that some form of disciplinary reaction is called for. Five examples are given of the criteria that might be adopted for this sort of data analysis Thereafter it is expected firstly to notify the failing PSP that it has been so identified in accordance with the common understanding. Secondly, it must notify its regulator of the identity of the failing PSP. The CU acknowledges that whilst the Regulation states that a receiving PSP should decide whether in these circumstances to restrict or terminate its business relationship with a failing PSP, in practice such decisions must weigh up other factors and business considerations – implicitly it accepts that hasty action is not appropriate and should so far as possible be consensual with peer PSPs and have the benefit of supervisors' input before draconian disciplinary action is taken.

4. Articulation of internal policy, processes and procedures

A PSP is expected to have in place a clearly articulated policy approved at an appropriately senior level defining the approach to be adopted to discharge the obligations outlined under 1-3 above, e.g., covering inter alia.

- when to reject, execute and query, hold and query
- its risk criteria
- how soon after receipt of transfer it will raise the query (i.e., if batching up queries the CU recommends it should be no more than seven days)
- the deadlines it will impose for responses and further follow up
- how it will assess whether incomplete or meaningless transfers are 'suspicious'
- the criteria it will apply based on the guidelines in paragraph 43 to identify 'regularly failing' payer PSPs, who must then be notified as such and reported to the relevant authority.