2017 REVIEW **23 June 17**

**POST CONSULTATION**

The Joint Money Laundering Steering Group


# Prevention of money laundering/ combating terrorist financing

# 2017 REVISED VERSION

GUIDANCE FOR THE UK FINANCIAL SECTOR
PART III: SPECIALIST GUIDANCE

June 2017

Doc 479960

Draftsman/Editor: David Swanney

## PART III: SPECIALIST GUIDANCE

***This specialist guidance is incomplete on its own. It must be read in the context of the main guidance set out in Part I of the Guidance.***

***This material is issued by JMLSG to assist firms by setting out guidance on how they may approach meeting certain general obligations contained in legislation and regulation, or determining the 'equivalence' of particular overseas jurisdictions or markets, where there is no expectation or requirement in law that such guidance be formally approved by HM Treasury.***

***With the exception of sections 1 and 5, therefore, the guidance in this Part does not carry the same Ministerial approval as the guidance in Parts I and II.***

**CONTENTS**



*These sections will carry HM Treasury Ministerial approval in due course

## 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). Part A refers to FATF R16 and Part B to Cover Payments.***

**PART A – FATF R16**

**Background**

1.1 FATF issued Recommendation 16 in February 2012 (previously Special Recommendation VII, first issued in 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 Recommendation was also issued by the FATF in February 2012. R16 and the Interpretive Note are available at http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

1.2 Recommendation 16 is addressed to FATF member countries, and was implemented in member states of the European Union, including the UK, through Regulation 2015/847, at :http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847.

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 and the beneficiary (Payee), the recipient of the payment. 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 1.14ff**).**

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 1.31 and Annex 1-II.

1.6 In April 2017, the European Supervisory Agencies issued draft Guidelines on measures that should be taken in order to comply with Regulation 2015/847. Payment Service Providers should read the JMLSG text in conjunction with these Guidelines, which are at:

https://www.eba.europa.eu/documents/10180/1807814/Consultation+Paper+on+draft+Joint+Guidelines+to+prevent+transfers+of+funds+can+be+abused+for+ML+and+TF+%28JC-GL-2017-16%29.pdf

**Scope of the Regulation**

1.7 The Regulation is widely drawn and intended to cover all types of funds transfer falling within its definition as made "at least partially 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 202/202COVs **are**, however, in scope – see Part B of this guidance);

- Services listed in points (a) to (m) and (o) of Article 3 of Directive 2007/64/EC.

- transfers by a payment card, an electronic money instrument or a mobile phone, or any other digital or IT prepaid or postpaid device with similar characteristics, ~~credit or debit card or similar payment instrument,~~ providing that the card, instrument or device ~~Payee has an agreement with the PSP permitting~~ is used exclusively for payment for goods or services and that ~~the~~ any transfer flowing from the transaction is accompanied by the number of the card, instrument or device ~~a unique identifier permitting the transaction to be traced back to the Payer (see paragraph 1.18).~~; It should, however, be noted that the use of 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 in order to effect a person-to-person transfer of funds does fall within the scope of the Regulation;~~:~~

- 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;~~

- transfers carried out through cheque images exchanges, including 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.~~

**Formatted:** Indent: Left: 2 cm, No bullets or numbering

**Formatted:** Indent: Left: 1.5 cm, Hanging: 0.5 cm, Bulleted + Level: 2 + Aligned at: 1.9 cm + Tab after: 2.54 cm + Indent at: 2.54 cm, Tab stops: Not at 2.54 cm

**Formatted:** Indent: Left: 2 cm, No bullets or numbering

~~It should, however, be noted that the use of a payment card, an electronic money instrument, a mobile phone, or any other digital or IT prepaid or post paid device with similar characteristics in order to effect a person-to-person transfer of funds does fall within the scope of the Regulation.~~

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

- Article 2 (5), 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;

1.9 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 the intended 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 1.19 below in relation to the merchant acquisition payment process.

**Pre-conditions for making payments**

1.10 Payment Service Providers (PSPs) of Payers and Payees must ensure that the 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, i.e., in the UK in accordance with the Money Laundering Regulations 2017, which gave effect to the Fourth 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 5.317 – 5.3.20, concerning customers with existing relationships. (See 1.14ff where the named Payer is not the holder of the account to be debited.)

1.11 PSPs of Payers must only verify the information on the Payer if the transfer exceeds €1,000 (single or linked), if the funds have been received in cash or anonymous electronic money, or if there are reasonable grounds for suspecting money laundering or terrorist financing. Similarly, PSPs of Payees must only verify the information on the Payee if the transfer exceeds €1,000 (single or linked), if the funds are paid out in cash or anonymous electronic money, or if there are reasonable grounds for suspecting money laundering or terrorist financing. ~~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).~~

1.12 ~~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.~~

1.13 Evidence of verification must be retained with the customer information in accordance with **Record Keeping Requirements** (see 1.21-1.22).

**Information Requirements**

**1.14 Complete payer and payee information:**

Except as permitted below, complete Payer and Payee information must accompany all wire transfers. Effectively, the complete Payer and Payee 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. Complete Payee information consists of: name 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 the account number(s) 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 16 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 16 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.

- Payee PSPs are not obligated to pass on to the payee all the payer information they receive with a transfer. However, Regulation 38 of the Payment Services Regulations 2009 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;"

**1.15 Reduced Payer Information:**

Where the PSPs of both Payer and Payee are located within the European Union, wire transfers need be accompanied only by at least the payment account number of both the payer

and the payee. The account number of the payer can be substituted for unique transaction identifier where the payment is not being debited from an account.

- 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 24 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 4.94).

**1.16 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.

**1.17 Payments via Intermediaries:**

Intermediary PSPs (IPSPs) must, subject to the following guidance on technical limitations, ensure that all information received on the payer and payee which accompanies a wire transfer is retained with the transfer. On a risk based approach the IPSP must determine whether to execute, reject or suspend a transfer of funds lacking the required payer or payee information.

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 or payee 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.

Where the IPSP 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 IPSP's risk-based approach, it must:

(i) seek the necessary information on the Payer and Payee

and/or

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

Where a PSP repeatedly fails to provide the required information on the payer or payee, the ISPSP must take steps, which may include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from the PSP or restricting or terminating its business relationship with the PSP. Such repeated failures must be reported to the NCA.

~~**1.18 Card transactions**~~

~~As indicated in paragraph 1.7, 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 1.15.~~

~~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'. FCA 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.~~

**1.19 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 October 2009 Approach document of the regulator (the FSA, now the FCA) in relation to the Payment Services Regulations. https://www.fca.org.uk/publication/archive/payment-services-approach.pdf

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.

**1.20 Minimum standards**

The above information requirements are minimum standards. It is open to PSPs to elect to supply complete Payer and Payee 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**

1.21 The Payee's PSP and any intermediary PSP must retain records of any information received on a Payer for five years, at which point the personal data must be deleted, unless otherwise provided for by national law.

1.22 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**

1.23 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 and Payee 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 and Payee 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 and Payee 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).

1.24 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 or Payee. 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.

1.25 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 or Payee

and/or

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

1.26 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.

1.27 Where a PSP is identified as having regularly failed to comply with the information requirements, under Article 8(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.

1.28 Under Article 9 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.

1.29 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 16.

1.30 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 16. 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.

1.31 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

1.32 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.

1.33 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.

1.34 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:

1.35 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.

1.36 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.

1.37 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.

1.38 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**

1.39 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:**

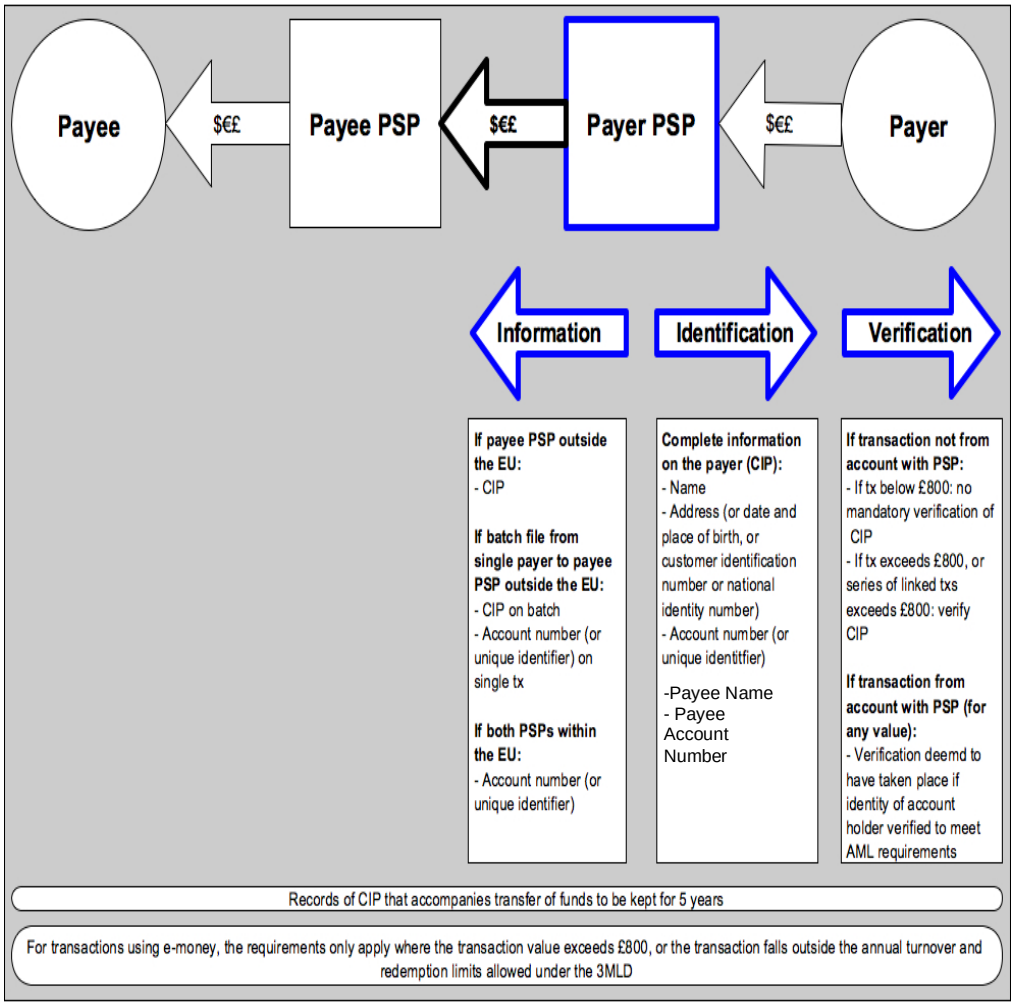
1. SWIFT Press release. 'New Standards for Cover Payments' (May 19 2009), available at http://www.swift.com/.

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

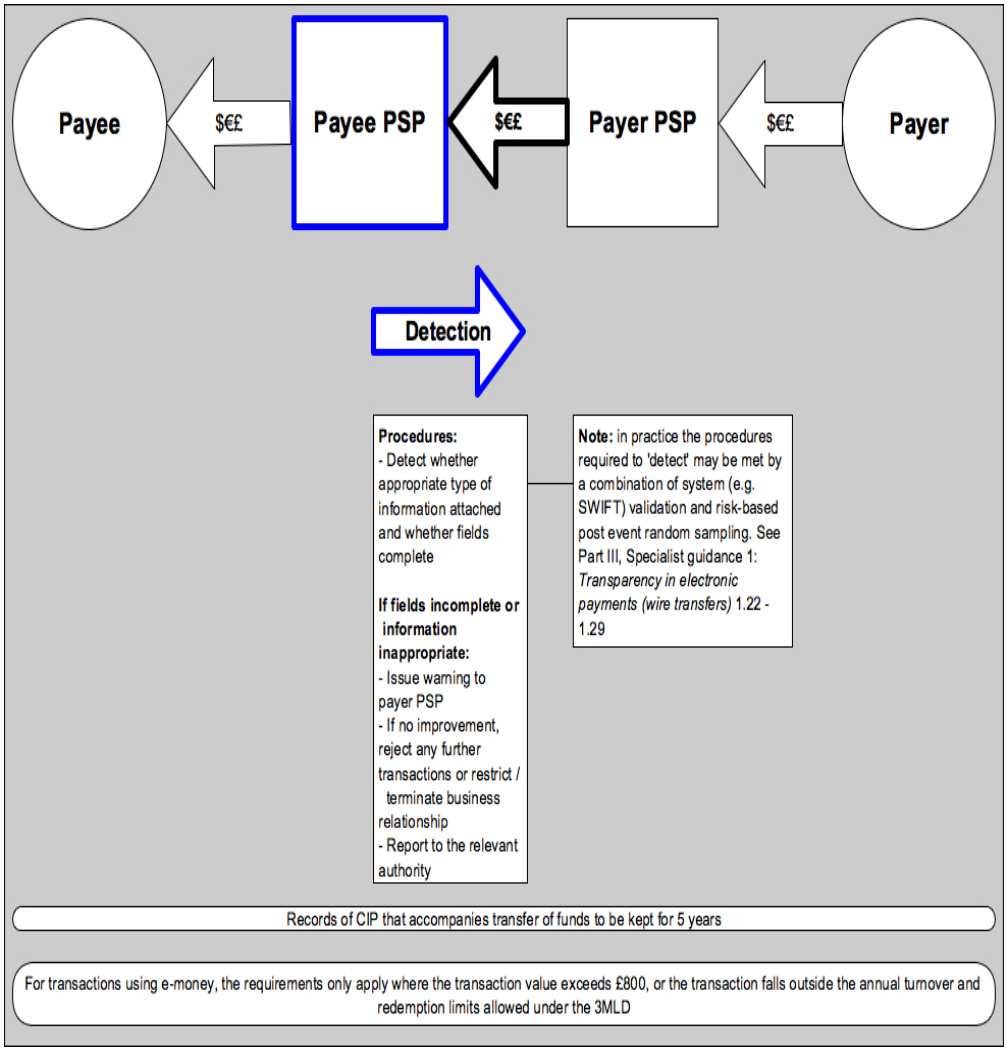
3. 'Cover Payments: Background Information and implications of the new SWIFT Message Format' and 'The Introduction of the MT202COV in the International Payment Systems,' issued jointly in May 2009 by the Bankers' Association for Finance and Trade, the Clearing House Association LLC, the European Banking 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**

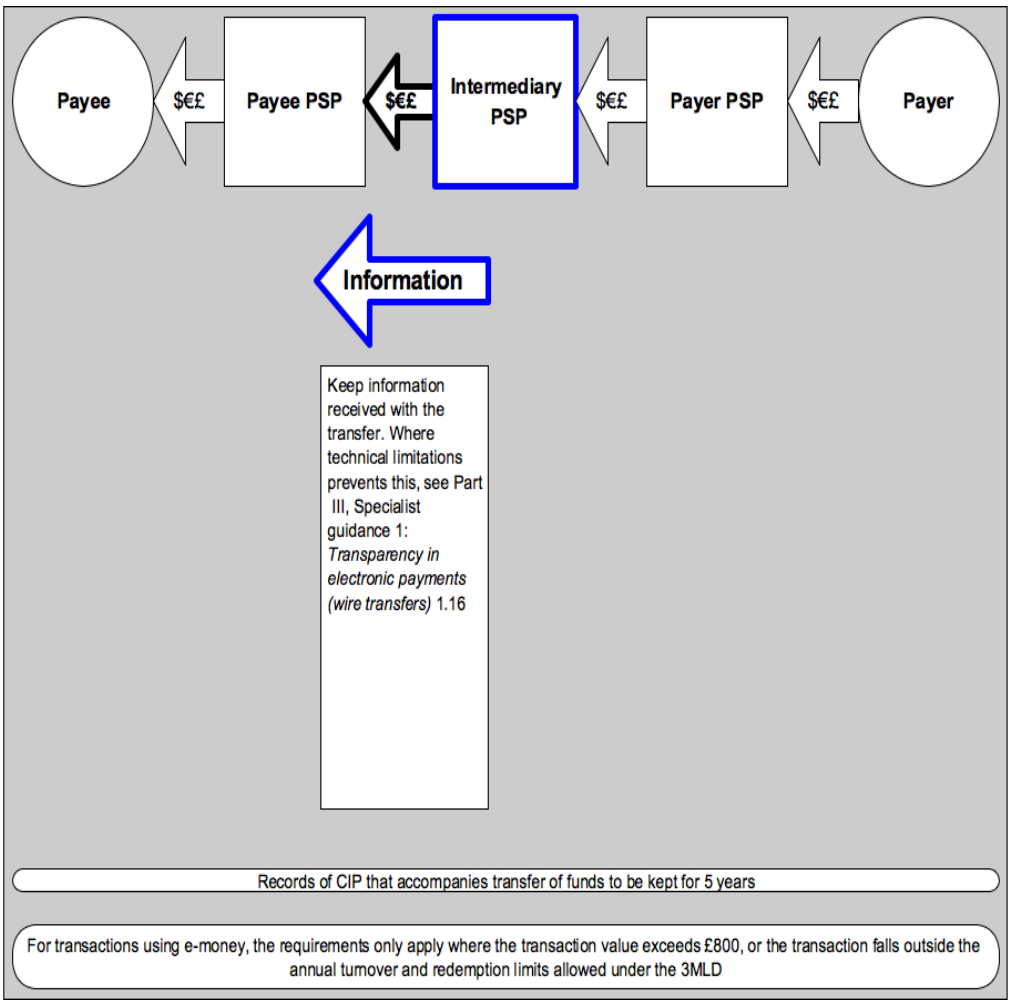
**Scenario 1: Transfer of funds – Obligations on Payer PSP**



**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.

## 4: Compliance with the UK financial sanctions regime

***The international and UK legislative frameworks for financial sanctions do not prescribe the processes which firms have to adopt to achieve compliance with their legal obligations. This guidance is intended to provide an indication of the types of controls and processes that firms might adopt in order to enable them to comply with sanctions obligations in an effective and proportionate manner. It is not intended to prescribe the manner in which firms must comply with the regime, as much will depend on the nature of the customer base and the business profile of each individual firm. Rather, t~~T~~he guidance is intended to assist firms in designing their own processes.***

***~~Although it is not formal guidance that has been given Ministerial approval, t~~This guidance ~~has been discussed with the Office of Financial Sanctions Implementation, HM Treasury, and reflects input from~~should be read alongside ~~its~~ the Office of Financial Sanctions Implementation, HM Treasury's publication Financial Sanctions: Guidance (April 2017), available at:https://www.gov.uk/government/publications/financial-sanctions-faqs.***

### *Introduction*

*General*

4.1 Sanctions can take the form of any of a range of restrictive/coercive measures. They can include arms embargoes, travel or investment bans, asset freezes, reduced diplomatic links, reductions/cessation of any military relationship, flight bans, suspension from international organisations, withdrawal of aid, trade embargoes, restriction on cultural /sporting links and other.

4.2 This guidance focuses on financial sanctions and asset freezes, although firms must also be aware of the nature and requirements of other sanctions, especially trade embargoes.

4.3~~2A~~ Although financial sanctions have been in force for many years, their scope and application, and how they are followed, has changed considerably over time. Exceptions and exclusions have always formed part of the regime, but in recent years it has become increasingly important to distinguish relationships which are unambiguously prohibited from those which are permitted. The latter category has always extended to humanitarian transactions, but the decision whether the relationships are permitted or prohibited has over the years become a more complex process of assessing the involvement of types of goods, geographical destinations and specially designated persons and entities and the resulting risk exposure, ~~but the nature of permitted/prohibited relationships has over the years become a more complex combination of types of goods, geographical destinations and specially designated persons and entities~~. Increasingly, too, sanctions have been extended to certain terrorist groups or geographical areas, without individual members being listed. This adds to the complexity for firms of ensuring compliance with financial sanctions, whilst at the same time not ~~harming~~ obstructing the carrying out of transactions permitted under the sanctions regime.

**Formatted:** Font: (Default) Times New Roman, 11 pt, Not Italic, Font color: Auto

**Formatted:** Font color: Auto

4.4~~2B~~ The UK regime also incorporates ~~a~~ licensing ~~arrangement~~provisions, under which permission can be given to carry out particular transactions~~, which then protects a firm from allegations of a breach of the regime~~. It is important for firms to be fully conversant with the licence

arrangements that apply to their business and/or customers.

4.53 The sanctions regime requires absolute compliance and any person in breach of an obligation under a relevant Statutory Instrument will be guilty of an offence, unless a defence is successfully made out. The nature of the legislation means that firms risk breaching a sanctions obligation as soon as an individual or entity is listed in an EU Regulation, or falls within the remit of a UK Statutory Instrument, the timing of which is outside their control (in contrast to AML approaches, which generally allow firms to set their own timetables on checking and updating customer due diligence details). The Terrorist Asset-Freezing etc. Act 2010 provides a primary legislative basis for the UK's domestic asset freezing regime.The penalties for committing an offence are covered in each individual Statutory Instrument, and through powers granted to HM Treasury in s146 of the Policing and Crime Act 2017.

4.64 Notwithstanding the absolute nature of the regime, firms are likely to focus on implementing appropriate systems and controls to identify persons who are subject to financial sanctions, given their assessment of the likelihood of dealing with such persons and associated risk of breaching their obligations. This may involve less immediate or frequent screening and/or being more selective with regard to those who are screened. Firms should note, however, that any provision of funds or financial services ~~etc~~etc. directly or indirectly to, or failure to freeze the assets of, a sanctioned person will expose the firm to the risk of prosecution or a monetary penalty.

4.75 The fact that the sanctions regime is absolute provides a challenge for compliance. Some firms, for example large firms with millions of customers or which process many millions of transactions every day, will use automated screening systems. Other firms with smaller numbers of customers and transactions may achieve compliance through other processes. Firms must use sanctions checking processes that are proportionate to the nature and size of the firm's business and that in their view are likely to identify all true matches.

*Code for Crown Prosecutors*

4.86 If an individual or a firm breaches a financial sanctions prohibition, it will have committed a criminal offence unless a defence is successfully made out. However, in line with the principles set out in the Code for Crown Prosecutors (see Annex 4-IV), prosecution of a firm or individual would only be likely where the prosecuting authorities consider this to be in the public interest, and where they believe that there is enough evidence to provide a realistic prospect of conviction.

***What is the financial sanctions regime?***

4.9 The UN has called for all member states to act to prevent and suppress the financing of terrorist acts. United Nations Security Council Resolutions are not directly applicable in UK law. However, the EU implements the 28 Member States' UN obligations by adopting an EU Regulation, which gives effect to the UN measures in UK law. A set of UK Regulations is required to introduce criminal penalties for breaches of the EU Regulation.

*The UK regime*[2]

4.106B EU Regulations imposing and/or implementing sanctions are part of ~~Community~~ European Union law and have direct effect in the Member States. EU Regulations either implement UN sanctions regimes or implement autonomous EU regimes. A set of UK Regulations made

[2] The text describes the present UK regime, which will change post-Brexit. The UK government issued a White Paper in April 2017 inviting responses to questions posed on the possible scope and application of a post-Brexit regime.

under section 2(2) of the European Communities Act 1972 is required to introduce criminal penalties for breaches of ~~the~~ EU Regulations into UK law~~.~~, although~~-~~ penalties for breach of EU Regulation 2580/2001 are imposed under TAFA.

4.11~~6C~~ There is no single over-arching piece of financial sanctions legislation in the UK. With the exception of the domestic Terrorism and Terrorist Financing regime, which is implemented by primary domestic legislation, for every individual financial sanctions regime there are two types of legislative instruments:

(1) an EU Regulation which imposes obligations on UK persons to freeze the assets of designated persons, to refrain from making funds and economic resources available to them and any other financial prohibitions or restrictions; and

(2) a set of UK regulations made under section 2(2) of the European Communities Act 1972, which enforces the EU Regulation by making it a criminal offence in the UK to breach the EU Regulation's measures.

4.12~~6D~~ Under the Terrorism and Terrorist Financing regime there is:

(1) an EU Regulation, 2580/2001, which gives effect to UN Security Council Resolution 1373(2001), and which imposes specific financial sanctions against certain listed targets; and

(2) The Terrorist Asset-Freezing etc. Act 2010 which (a) enforces the asset freezes in respect of the EU-listed targets and (b) provides HM Treasury with powers unilaterally to freeze the funds and economic resources of those suspected or believed to be involved in terrorist activities, and restricts the making available, directly or indirectly, of funds, financial services, and economic resources to, or for the benefit of such persons.

The Anti-terrorism Crime and Security Act also empowers OFSI to designate targets. For current listings see: https://www.gov.uk/government/publications/financial-sanctions-uk-freezing-orders

**Formatted:** Font: 11 pt

**Formatted:** Normal, Indent: Left: 0 cm, First line: 0 cm

**Formatted:** Font: 11 pt

**Field Code Changed**

4.13~~7E~~ A number of organisations have been proscribed under UK anti-terrorism legislation. Where such organisations are also subject to financial sanctions (an asset freeze), they are included on the Consolidated List maintained by the Office of Financial Sanctions Implementation, HM Treasury. The primary source of information on proscribed organisations, however, including up-to-date information on aliases, is the Home Office. Firms can find the list of proscribed organisations at: https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2

*Country-specific*

4.14~~7F~~ The UN Security Council also maintains a range of country-based financial sanctions that target specific individuals and entities connected with the political leadership of targeted countries. Each UN sanctions regime has a relevant Security Council Committee that maintains general guidance on the implementation of financial sanctions and current lists of targeted persons and entities. The list of currently applicable Security Council Resolutions can be found at www.un.org/Docs/sc/committees/INTRO.htm.

4.15~~7G~~ The EU directly implements all UN financial sanctions against countries/regimes; it can also initiate autonomous measures under the auspices of its Common Foreign and Security Policy. Detail on UN-derived and EU autonomous financial sanctions regimes (including targets) is

**Formatted:** Left

available on the EC sanctions website, http://ec.europa.eu/external_relations/cfsp/sanctions/docs/measures_en.pdf.

4.167H The EU has published FAQs on the implementation of its sanctions regime against Russia. The FAQs cover several topics, including the meaning of providing financial assistance in the context of the arms embargo, when financing restrictions apply generally, how banks should ensure their compliance, the extent of the restrictions on access to capital markets, and the status of pre-existing loans. The FAQs are available at http://europa.eu/newsroom/files/pdf/1_act_part1_v2_en.pdf

4.177I Unlike the arrangements under the terrorism measures, the UK would not normally make autonomous additions to the target lists for country-specific sanctions. The prohibition in these sanctions regimes apply in respect of funds and economic resources in the same manner as those in the terrorism sanctions. Where relevant, any specific individuals and entities subject to such targeted countries/regimes will be included on the HM Treasury Consolidated List.

4.187H OFSI will now add new sanctions listings made by a UN Security Council committee to the consolidated list for 30 days, or until the EU adds the new listings to an existing sanctions regulation, whichever is sooner. Where listings have been made under a new UN Security Council Resolution, OFSI's intention is that the Linking Regulations will be amended to include the new Resolution within 48 hours.

4.197J The number of regimes can change from time to time. A full list of the financial sanctions regimes in force is available at: https://www.gov.uk/government/organisations/hmtreasury/series/financial-anctions-regime-specific-consolidated-lists-and-releases. Each entry on the list of current regimes gives access to full details of that regime, including the relevant UN and EU decisions, UK legislation, and Treasury information.

4.207K Annex 4-I summarises the relevant legislation in the UK.

*What is a financial sanction?*

4.217L A key element of many ffinancial sanctions ~~invariably include~~is an asset freezing regime. Asset freezes comprise two elements:

- A prohibition on dealing with the funds or economic resources belonging to or owned, held or controlled by a designated person, and
- A prohibition on making funds or economic resources available, directly or indirectly, to, or for the benefit of, a designated person.

4.227M An asset freeze prevents anyone "dealing" with funds or economic resources which belong to, or which are owned, held or controlled by, a designated person. "Deal with", in relation to funds, includes to move, transfer, alter, use, allow access to, or deal with in any way that would result in any change in the funds' volume, amount, location, ownership, possession, character, destination, or any other change that would enable the funds to be used. This also includes the management of securities (shares, bonds, etc.) and other assets.

4.237N "Deal with", in relation to economic resources, generally means using the economic resources to obtain funds, goods, or services in any way, including, but not limited to, by selling, hiring or mortgaging them. The everyday use by a designated person of their own economic resources for personal consumption is not prohibited ~~means exchange, or use in exchange, for funds, goods or services. It is not prohibited for a designated person to use the economic resource for~~

Formatted: Left

Formatted: Normal, Indent: Left: 0 cm, First line: 0 cm, Tab stops: 0.99 cm, Left + 4.95 cm, List tab

Formatted: Font: 11 pt

Formatted: Normal, Justified, Indent: Left: 0 cm, First line: 0 cm

Formatted: Left, Tab stops: Not at 0.99 cm + 4.95 cm

Formatted: Left

Formatted: Indent: Left: -0.19 cm, First line: 0 cm

~~normal use within the law~~ (e.g.~~,~~ using their car to do the shopping) but a designated person could not sell or use the resource to generate funds (e.g. by selling the car or using it for a taxi or courier business) without a licence from ~~the Treasury~~OFSI.

4.24~~7O~~ As well as placing a direct prohibition on dealing with a specified person or entity, some sectoral sanctions prohibit the supply of certain financial products (especially around the capital market). Thus firms need not just to flag a customer who is on a prohibited list, but to look through to the nature of the service involved.

*Insurance*

4.25~~7P~~ Generally, sanctions do not ban the provision of insurance. However it is prohibited to provide insurance to:

- persons designated under TAFA 2010, and
- certain state entities and persons in Syria

The Russian sanctions include prohibitions on export credit insurance.

4.26~~7Q~~ There are special provisions for the insurance supplied to designated persons. There is more about the financial restrictions in force:

- in respect of Syria, at: ~~http://www.hm-treasury.gov.uk/fin_sanctions_syria.htm and at~~ https://www.gov.uk/sanctions-on-syria

- in respect of Russia, at https://www.gov.uk/government/news/doing-business-in-russia-and-ukraine-sanctions-latest

4.27~~7R~~ Additionally, sanctions prohibit the payment of funds to or for the benefit of designated persons, which would impact on the payment by the designated person and others of insurance premiums and the payment of claims to a designated person, which could not take place unless licensed. This prohibition would, without a licence, prevent the payment of benefits due under a policy to a beneficiary who is a designated person.

4.28~~7S~~ If someone is listed by the UN or EU under a country sanctions regime, the fact of their designation does not make any insurance cover that they enjoy at the time of their designation, or any cover that might be taken out after that date, illegal. However, if they are listed under the Syrian regime, it may be illegal to provide them with cover regardless of their designation, because of the broad insurance bans referred to above.

4.29~~7T~~ Except as already described, t~~T~~here is no legal requirement to discontinue cover to listed persons. Insurers making an assessment of whether they wish to discontinue cover to a designated person will wish to take into account the potential social harm that might be caused if they terminate a contract that is either not subject to any restriction or is permitted under a general licence.

4.30~~8~~ When delegating any underwriting or claims authority to a third party an underwriting insurer may not have direct ~~Whilst Insurers may not have~~ knowledge of the identities of the underlying clients /customers and so be unable themselves to identify any potential sanctioned party exposure, the underwriting insurer should satisfy themselves that the third party's systems and controls are commensurate with the UK financial sanctions obligations as they apply to the delegated activity. Insurers should consider measures such as making specific reference to sanctions compliance within their Terms of Business and/or from time to time requiring positive affirmation from their third parties of their financial sanctions systems and controls.

**Formatted:** Indent: Hanging: 0.5 cm

**Formatted Table**

**Formatted:** Font: 11 pt, Not Italic

4.319 In respect of each prohibition, it is a defence for the provider of the funds, economic resources, or where applicable financial services, not to have known or have had reasonable cause to suspect that the prohibition was being breached. ~~Where it is impossible to draw a conclusion due to non-availability of additional data the firm may lack the requisite knowledge or suspicion to fall foul of any of the sanctions prohibitions.~~

*Exemptions*

4.329A There are exemptions to regimes which permit s~~S~~ome activities which would otherwise amount to a breach of the asset freezing requirements are automatically exempted under the legislation. For example, funds due to designated persons in relation to contractual or other obligations entered into prior to the designated person's listing can be credited to the designated person's frozen account. Regard should always be had to the latest version of the relevant legislation.

*Licence regime*

4.339B A licence is a written authorisation from OFSI to allow an activity which would otherwise be prohibited. A licence may include associated reporting requirements or other conditions. Generally there are two sorts of licence:

1. General licences. These are available to every potential beneficiary subject to whatever terms or conditions apply under the sanctions regime concerned; so a general licence allows every transaction, or category of transaction, that is described in the licence to be lawful, whoever the persons who are engaging in them. General licences are available in a limited number of circumstances, and are published ~~publicly identified and are available~~ on the gov.uk web pages.

2. Individual or specific licences. These are granted to specific parties, and may permit specific transactions or types of spending for example. They are not usually published.

4.349C Sanctions regimes generally provide carve-outs for humanitarian payments, although some offer specific licensing provisions for these.

4.359D If the designated person is listed under the domestic terrorism regime (the only regime under which it is prohibited to provide insurance to listed persons), two general licences are currently in place which cover insurance. General licences allow:

• the provision of insurance to designated persons, and

• the immediate and temporary provision of goods and services in respect of an insurance claim such as courtesy cars or emergency hotel accommodation to designated persons.

~~4.9E There is more information on general licences at: http://www.hm-treasury.gov.uk/fin_sanctions_general_licences.htm~~

4.369F Licences can be granted for a range of purposes. The permitted purposes are typically set out by the UN or EU, and may include allowing the release of frozen funds to pay obligations due by the designated person under a contract entered into prior to their listing, to meet bank charges, to cover basic household or business expenses and reasonable legal costs.

4.379G Licences can also allow other arrangements to permit transactions and protect third parties who are not sanctions targets – for example to allow staff salaries to be paid, to allow humanitarian transactions, and to allow the assets of designated persons to be safeguarded and managed.

4.389H The terms of the relevant EU Regulation typically prescribe the circumstances in which licences can be issued and the conditions that need to be satisfied in order for HM TreasuryOFSI to issue a licence.

4.399I OFSI licences do not cover activities in other jurisdictions, nor trade imports or exports subject to trade sanctions. If the firm, or the activity it is seeking to have licensed, is subject to more than one sanctions regime (because of overseas ownership, for example) the firm may need to apply to the overseas authorities for a separate licence from them.

*Penalties*

4.4010 The penalties for a breach of UK financial sanctions (including breach of EU Regulations containing sanctions, which are applicable in the UK) are set out in the relevant statutory instrument, and in s146 of the Policing and Crime Act 2017. Any person guilty of an offence is liable on conviction to imprisonment and/or a fine.

*OFSI website*

4.4111 OFSI's website includes the sanctions legislation applicable in the UK, HM Treasury's sanctions notifications, Guidance notes and related materials. See https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation ~~https://www.gov.uk/sanctions-embargoes-and-restrictions~~.

Formatted: Indent: Left: 0 cm, First line: 0 cm

*The Consolidated List*

4.4212 The obligations under the UK financial sanctions regime apply to all firms in the financial sector and not just to banks. In order to assist compliance with the UK regime, OFSI maintains a 'consolidated list' of individuals and entities that are based in the UK or elsewhere that are subject to financial sanctions. The Consolidated List is available at https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.

~~*UK Investment Ban List*~~

~~4.13~~ ~~A list of investment ban targets designated by the European Union under legislation relating to current financial sanctions regimes is available at www.hm-treasury.gov.uk/d/investmentban.pdf~~

~~4.14~~ ~~Investment ban targets are not included in the Consolidated List of financial sanctions targets. UK financial firms are prohibited from making new investments in the entities named on the list of investment ban targets. They are not prohibited from making other payments to them or receiving payments from them. This guidance may assist financial institutions in designing processes to prevent new investment in those parties.~~

*Responsibilities*

4.4315 Responsibilities for the UK sanctions regime lies with three Government departments:

(i) Office of Financial Sanctions Implementation, HM Treasury
(ii) The Foreign and Commonwealth Office ("FCO"), and
(iii) The UK Department for International Trade, through the Export Control Organisation

The Financial Conduct Authority also has a role in relation to firms' systems and controls. Under its objective of enhancing the integrity of the UK financial system, it requires firms, under Principle 3, to have in place appropriate policies and procedures to counter the risk that they might be used to further financial crime. These include adequate systems and controls to comply with the asset freezing regime. Annex 4-II provides a summary of the responsibilities of the UK authorities.

*Overseas jurisdictions*

4.4416 Where a firm is active in jurisdictions outside the UK, it may be required to comply with the requirements of the sanctions regimes in other jurisdictions. Some jurisdictions' requirements may also apply without a firm having an actual presence in that jurisdiction.

4.4517 Firms will need to understand which sanctions regimes impact on which parts of their business and ensure they correctly comply with applicable sanctions while not incorrectly applying regimes of other jurisdictions to UK business. Annex 4-IV contains links to some useful websites.

***Approach, procedures and training***

*Approach – what does an asset freeze do?*

4.4618 An asset freeze prohibits dealings with the funds or economic resources of a sanctions target. It also prohibits making funds or economic resources (and in relation to those designated under the terrorism regime, financial services) available, directly or indirectly, to or (in the case of those designated under the terrorism regime) for the benefit of sanctions targets. Firms should therefore implement appropriate means of control to prevent breaches of prohibitions. It is a criminal offence for a firm to breach a sanctions prohibition.

4.4719 In order to reduce the likelihood of breaching obligations under financial sanctions regimes, firms are likely to focus their resources on areas of their business that carry a greater likelihood of involvement with sanctions targets and where meaningful information on their clients, counterparties and transactions is held. Within this approach, firms are likely to focus their prevention and detection procedures on direct customer relationships, and on transactions, having appropriate regard to other parties involved. However, firms cannot ignore "low risk" areas and must ensure that systems and controls also pay attention to areas where dealings with a sanctions target are unlikely, but possible.

*Policy and senior management responsibilities*

4.4820 Firms should have a sanctions policy that is informed by a thorough understanding of legal requirements applied to an assessment of the risks in their firm. Senior management and/or the Board of a firm should understand the firm's obligations and take responsibility for the firm's sanctions compliance policies and procedures.

*Approach tailored to business model*

4.4921 Firms should take an approach which is appropriate for their business model, when assessing where and how their business is most likely to encounter sanctioned parties, and to focus resources and tailor systems and controls accordingly.

4.2250 Firms, particularly those with many different client types, product types and/or geographical markets, should consider carrying out an assessment in order to be able to understand which parts of their business may carry a greater likelihood of breaching the requirements of

economic or terrorist-related sanctions. Any assessment may usefully include a high level assessment of the firm's view of its business profile in specific business areas, and information on periodic CDD and other checks relating to those areas.

4.5123 An assessment should start with identification and assessment of the issues that have to be managed. A firm should develop its approach in the context of how it might most likely be involved in breaching economic and country-related sanctions. A firm may take into account a range of factors when conducting its assessment, including:

- Its customer, product and activity profiles
- Its distribution channels
- The complexity and volume of its transactions
- Its processes and systems
- Its operating environment
- The screening processes of other parties
- The geographic risk of where it does business
- The sanctions regulations of relevant countries.

*Documenting the assessment*

4.5224 Firms should document the assessment and approach adopted on the basis of that assessment. Firms should also identify where a decision is taken to adopt a different approach where this may go beyond a particular requirement.

*Firms' activities outside the UK*

4.5325 UK sanctions legislation typically applies to UK persons and persons in the UK, including bodies incorporated or constituted under UK law. Where firms operate in a number of countries or territories, a consistent group wide 'umbrella' policy should be established, which can assist local business units in ensuring that their local procedures meet minimum group standards. Firms will also need to take account of any particular local, legal requirements. Foreign subsidiaries of UK firms that have a separate legal personality outside the UK (as distinct from branches) would not be covered by UK sanctions law, but by the law of the jurisdiction in which they are based.

4.5426 Firms should ensure that appropriate policies and procedures are in place across the organisation. A firm's procedures should be appropriate to its business, and readily accessible and well understood by all relevant staff. Senior management must understand and stress the importance of understanding and complying with the firm's policies and procedures.

4.5527 Firms should ensure that their procedures remain up to date and fit for purpose in a changing environment. Firms may use internal review, other appropriate functions or external review to achieve this.

4.5628 Firms should ensure that they communicate in a timely manner to relevant staff changes to the sanctions requirements, including any internal changes to systems, procedures and controls.

4.5729 Firms should adequately monitor their systems processes and controls to support full compliance with sanctions requirements.

*Staff training*

4.5830 A firm should have staff training programmes commensurate with its business and risk

profile. Firms should consider implementing arrangements for:

- providing material containing the firm's financial sanctions policies and procedures which is readily available and simple to understand;
- providing training that is appropriately tailored for different groups of staff to reflect the likelihood of different degrees of staff involvement with sanctions issues, including what to do in the event of a reportable match;
- providing refresher training, delivered at appropriate intervals.

*Circumvention*

4.5931 Firms' policies and procedures should include provisions to prohibit and detect attempts to circumvent sanctions, by, for example:

- omitting, deleting or altering information in payment messages for the purpose of avoiding detection of that information by other firms in the payment process, or
- structuring transactions with the purpose of concealing the involvement of a sanctioned party.

Employment contracts should make any such attempt a serious disciplinary offence.

4.6031A Generally, financial sanctions apply to specifically designated persons. It is important to note that an asset freeze and some financial services restrictions also apply to businesses and other organisations owned or controlled by a designated person. More information is available in OFSI's Guide to Financial Sanctions[3]. ~~However, there may be cases where the assets of persons who are not expressly listed as a designated person may nevertheless have to be treated as frozen. This is because a sanctions regime *may* target a list of named persons and other, unnamed, persons that are, for example, owned or controlled by the named persons.~~ This will be a matter of case-by-case analysis and if in doubt, OFSI should be consulted.

4.6131B It can be unclear whether an unlisted person and its assets are owned or controlled by a designated person. There is no absolute legal rule as to when an entity is owned or controlled by another. The matter must be subject to a case-by-case evaluation, taking into account the *degree* to which the entity concerned is owned or controlled. The EU's best practices guide[4] says the following:

- The criterion to be taken into account when assessing whether a legal person or entity is owned by another person or entity is the possession of more than 50% of the proprietary rights of an entity or having majority interest in it. If this criterion is satisfied, it is considered that the legal person or entity is owned by another person or entity.

***Screening of customers and transactions***

4.6232 Firms should have processes to manage the risk of conducting business with or on behalf of individuals and entities on the Consolidated List[5] (which includes all the names of sanctioned persons and entities under UN and EU sanctions regimes which have effect in the UK).

4.6332A A firm's internal policy and procedures should determine the frequency of ~~scanning~~screening.

[3] https://www.gov.uk/government/publications/financial-sanctions-faqs

[4] http://data.consilium.europa.eu/doc/document/ST-10254-2015-INIT/en/pdf

[5] The Consolidated List is available at https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets.

**Formatted:** Font: 11 pt

**Formatted:** Font: 11 pt

**Formatted:** Default, Justified, Indent: First line: 0 cm

**Formatted:** Font: Times New Roman

**Formatted:** Font: Times New Roman

**Formatted:** Justified, Indent: Left: 0 cm

**Formatted:** Font: 10 pt

**Formatted:** List Paragraph

It is each firm's responsibility to comply with the relevant legislation. However, if a firm fails to identify and block a target account, this may lead to a breach of the legislation. It should be noted that a critical aspect of the listing of a target is that the target's assets must be frozen immediately~~, before they can be removed from UK jurisdiction~~.

4.~~32~~64~~B~~ Where a prohibition is against business with certain geographical areas, for example, Crimea, there are additional practical challenges in picking up transactions for screening. It may be helpful, at least in part, to screen against specific locations – such as known towns, cities or ports within such a geographical area. This however should be considered on a firm by firm basis within the context of business activities and profile.

*Taking a tailored approach*

4.~~33~~65 As already noted, it is for individual firms to assess how best to comply with the financial sanctions legislation within the context of their business activities and profile. The prohibitions in the legislation extend beyond payments made directly to sanctions targets, i.e., payments which are made indirectly to, or which are made to others for the benefit of, sanctions targets are within the scope of the legislation.

4.~~34~~66 An "indirect payment" is one that is made to someone acting on behalf of the sanctions target. In contrast, the prohibition on making payments to others for the benefit of a sanctions target is intended to prevent payments being made to third parties to satisfy an obligation of that person.

4.~~35~~67 As explained in paragraphs 4.~~18~~46ff, firms should adopt an approach informed by the profile of their business model and client base. Firms are likely to focus their screening processes on areas of their business that carry a greater likelihood of involvement with sanctions targets, or their agents, although as outlined earlier, low risk areas cannot be ignored.

*Record of screening policy*

4.~~36~~68~~6~~ Firms should keep a written record of their screening policy and be able to justify the timescales and frequency of screening, resolution of screening matches and regulatory reporting if required.

*Review of processes*

4.~~37~~69 Firms should review, and update their processes periodically, so that they remain appropriate for their needs and ensure that any internal guidance is updated to reflect major changes to the sanctions regime, such as the addition of a new jurisdiction or regime.

*Elements of screening process*

4.~~38~~70 The scope and complexity of the screening process will be influenced by the firm's business activities, and according to the profile of the firm. An effective screening process should include the following elements:

- it should flag up potential name matches against the Consolidated List and names against which measures have been issued under the Counter-Terrorism Act
- potential matches should be reviewed by appropriately trained staff
- where matches are confirmed as true, appropriate action should be taken to freeze the account
- true matches should be reported as soon as is practicable to OFSI (see paragraphs 4.62ff for the reporting of matches) and

- it should maintain an audit trail of actions around potential and true matches.

*Screening software*

4.~~39~~71 Many firms use automated customer screening software provided by a commercial provider; other firms rely on manual screening. Firms may consider whether and what type of screening software to use in line with the nature, size and risk profile of their business. A key element of a screening system is that it will flag potential matches clearly and prominently. Firms should document the reasons for choosing whichever screening method they decide to use.

4.7240 Where commercially available automated screening software is implemented, firms should understand its capabilities and limits, and make sure it is tailored to their business requirements, data requirements and risk profile. Firms should also monitor the ongoing effectiveness of automated systems. Where automated screening software is used, firms should be satisfied that they have adequate contingency arrangements should the software fail and should periodically check the software is working as they expect it to.

*Legacy systems*

4.~~41~~73 Firms should be alert to any operational issues which may arise from having the risk of customer or transaction data in legacy systems.

*'Fuzzy matching'*

4.~~42~~74 It is important to consider "fuzzy matching", as names might be missed if only exact matches are screened. "Fuzzy matching" describes any process that identifies non-exact matches. Fuzzy matching software solutions identify possible matches where data - whether in official lists or in firms' internal records - is misspelled, incomplete, or missing. They are often tolerant of multinational and linguistic differences in spelling, formats for dates of birth, and similar data. A sophisticated system will have a variety of settings, enabling greater or less fuzziness in the matching process.

4.~~43~~75 Where a firm uses a screening system which has a fuzzy matching capability, it should ensure that the fuzzy matching process is calibrated as appropriate in line with the risk profile of their business.

4.~~44~~76 Application of a fuzzy matching process to a screening system will result in the generation of an increased number of apparent matches which have to be checked. The generation and resolution of an undue number of false positives may have a negative impact on the efficacy of the resolution process. Firms should therefore consider the level of appropriate human intervention to assess which results may be false positives.

*Use of false personal information*

4.~~45~~77 Sanctioned parties are known to use false personal information to try and evade detection of their illicit activities. Typical approaches are to use name variations, e.g., name reversal and removing numbers from the names of entities, etc. For this reason, many firms use screening tools which screen using several protocols – e.g., name reversal, number removal, number replaced by word, etc.

*Outsourcing and reliance*

4.~~46~~78 A firm may outsource screening and/or other financial sanctions compliance processes to a contractor, but will remain fully responsible for discharging all of its regulatory obligations.

Firms may therefore consider putting in place an appropriate Service Level Agreement with contractors and should satisfy themselves that the outsourced party is providing an effective service.

4.~~47~~79 There is no "reliance" provision in the UK financial sanctions regime. When screening customers and related parties that are new to the firm but who are or were already clients of another FCA-authorised firm, firms might choose to consider this in their assessment when determining their screening policy. However, it should not be assumed that such clients have already been screened.

*Timing of screening*

4.~~48~~80 All customers should be screened during the establishment of a business relationship or as soon as possible after the business relationship has commenced. Firms should be aware of the risks associated with screening customers after a business relationship has been established and/or services have been provided i.e., that they may transact with a sanctioned party in breach of sanctions prohibitions. Firms must be aware of the absolute restrictions embedded in the financial sanctions regime. Where there is any delay in screening, firms face a risk of breaching the legislation.

4.~~49~~81 For low-risk business a firm might choose post-event screening, provided the nature of the business allows the firm to prevent movement or withdrawal of the asset(s) concerned until the sanction check has been completed.

4.82~~50~~ In accordance with a firm's business profile, consideration should be given to how often customer re-screening should be carried out. Some firms carry out regular periodic systems-based screening of their entire customer data. Others develop a programme to re-screen for changes to their customer list and changes to the Consolidated List. Firms should ensure that they have adequate arrangements to screen when changes are made to the Consolidated List.

*Screening of associated parties*

4.~~51~~83 The sanctions prohibitions also apply to both indirect payments to and payments for the benefit of sanctions targets. Where practicable, screening should cover any other related parties, for example beneficial owners (including trustees, or company directors), that are identified by the firm in question as requiring verification under its risk-based approach to customer due diligence. A firm's judgement in these matters will need to be consistent with its approach for AML purposes, and whether or not full identity details are collected.

4.~~52~~84 Firms may choose not to undertake financial sanctions checks in respect of particular related parties associated with an investment if its assessment considers such checks would be disproportionate in particular cases. Firms should be aware, however, that this will increase the risk of sanctions legislation being breached. Firms may be liable to prosecution in respect of any such breaches.

4.~~52A~~85 Particular challenges arise in respect of entities which, whilst not ~~directly~~ explicitly listed, ~~might become so~~may still be subject to financial sanctions by virtue of their ownership/control structure.

*Dormant accounts*

4.~~53~~86 Firms may wish to consider whether dormant accounts should be screened, and if so how and when they should be screened. This decision is likely to reflect the firm's risk policy, and the availability or otherwise of dormant account data on a system that is able to be screened.

*Transaction screening*

4.~~54~~87 Firms should monitor higher-risk payment instructions to assist in preventing a breach of the prohibitions. Transactions screening involves screening of payment information to identify potential sanction targets.

4.~~55~~88 Transaction screening should take place on a real-time payment basis, i.e., the screening or filtering of relevant payment instructions should be carried out before the transaction is executed.

4.~~56~~89 Firms will approach transaction screening in line with their assessment of their business risks. Firms are likely to focus on screening international transactions where there is adequate information on third parties, and parties to trade finance deals plus walk-in customers wishing to send payments both within and outside the UK. Firms that operate client money accounts or provide safe custody services are likely to focus on third party payments and asset transfers.

4.~~57~~90 Banks will wish to consider screening both data in the payment and relevant advice messages (e.g., MT103, MT910, MT202 etc) and for intermediary banks data in the cover payments e.g., MT202COV.

4.~~58~~91 Factors that firms may consider when determining which transactions should be screened include:

- whether automated screening is possible
- industry best practice
- international / domestic connections
- adequate information to ascertain whether it is a potential match
- materiality of transaction
- the nature of the client's business
- analysis of historical sanction matches

4.~~59~~92 When funds are received electronically by a financial firm as payee (i.e., not a Payment Service Provider in the transaction – see Part I, paragraph 5.2.11), the name of the payer will typically not be passed on by the PSP to the payee. The payee firm is not expected to screen the payer nor to screen the incoming payment, unless there is reason to believe the payer is not their customer.

4.~~60~~93 When funds are received electronically by a Payee Payment Services Provider from within the EU, the payer's name and address may not be included in the transfer (as it is not required in the relevant legislation – see section 1: *Transparency in electronic payments (wire transfers)*, paragraph 1.1~~5~~4). The PSP may need to consider whether to request additional information in order to meet its sanctions obligations.

*Audit trail and record keeping*

4.~~61~~94 Whether firms screen using automated systems or manually, an audit trail should be maintained for a period of no less than five years. This should record all relevant information to a likely match, how it was resolved and the rationale applied. Firms should ensure that their processes are kept under review, and remain up to date, and appropriate for the needs of the institution.

***Reporting matches and breaches of the regime***

*Assessing possible matches*

4.~~61A~~95 **A target match** is where a firm is satisfied that the transaction or account held is that of a specific person who is a target of financial sanctions. **A name match** is where a firm has matched the name of an account holder with the name of a target included on HM Treasury's Consolidated List. This does not necessarily mean that the account holder is one and the same as the target. If a firm has a name match it needs to decide, using the information it has about the account holder, whether they are a sanctions target or not.

4.~~62~~96 Firms may often find it difficult to determine if there are true matches i.e., they involve a sanctioned party. Potential matches should be investigated and reviewed as appropriate to confirm if they are true matches. The majority of matches are likely to be "false positives" and after this is confirmed there will be no need for further review. Sophisticated screening software permits adjustment of screening rules, so as to prevent repetition of specific false matches.

4.~~63~~97 True matches are where a firm has no doubt that the account held is that of a target of the financial sanctions regime. It is also possible to have a potential match where a name of a customer may appear to match the name of a target included on HM Treasury's Consolidated List. Firms should seek to obtain sufficient information to enable them to confirm or eliminate a partial match. This process should be documented in writing.

4.~~61B~~98 Firms are required to inform OFSI of all funds and economic resources that they have frozen in accordance with the relevant legislation and provide all relevant information necessary for ensuring compliance with the legislation, subject to the obligations of legal professional privilege. Under existing financial sanctions legislation applicable in the UK, a firm is guilty of an offence if it knows or has reasonable cause to suspect that a person is a listed person or has committed an offence under the legislation, and the institution does not disclose the information to OFSI as soon as is reasonably practicable after that information comes to its attention.

4.~~61C~~99 OFSI have published a template for reporting breaches, which is ~~attached as Annex 4 V.~~available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/512772/ofsi_breach_form_template_march_2016.docx. ~~The form is not mandatory but~~ OFSI strongly encourage firms to use it. OFSI would expect to see it used for all new suspected breach disclosures going forward, but do not expect to see previous disclosures resubmitted. All emails to OFSI upon receipt receive an automatic acknowledgement. All disclosures will be considered internally by OFSI and then shared with law enforcement. The ~~bank~~ firm can expect to be contacted by either OFSI or a law enforcement agencies at an appropriate juncture in the consideration of the information provided.

Formatted: Left

Formatted: Font: 11 pt

Formatted: Font: 11 pt

*What is a false positive?*

4.~~64~~100 A "false positive" is the identification of an apparent match to a record on the Consolidated List (or a party against which measures have been issued under the Counter-Terrorism Act) which is assessed on investigation not to relate to a sanctions target or entity.

4.~~65~~101 Time constraints are also particularly relevant in the context of payments. Firms may make further enquiry either from the counter-party bank or from their client or both, so as to assist in determining whether the match is a true match. Firms should seek sufficient information to enable them to confirm or eliminate an potential match. This process should be documented in writing. For cases that are assessed to be not a true match, firms should ensure that there is a clear rationale for deciding that an apparent match is a false positive and that this rationale

can be demonstrated.

4.~~66~~102 Every potential match of a customer account should be checked, and if appropriate investigated. This process should be documented in writing. Firms are advised to keep an appropriate audit trail about every likely match. This is likely to include a record of who made the decision and on what grounds.

*Reporting to OFSI*

4.103~~66A~~ Firms are required to provide OFSI with information where they know, or have reasonable cause to suspect, that a person is a designated person or that someone has committed an offence under specific sections. Those offence provisions include both an actual breach and participation in activities where the purpose of those activities is to directly or indirectly circumvent the prohibitions. The EU Regulations also generally contain a requirement that individuals and entities should supply all information which would facilitate compliance with the regulations. While an example of information on the initial freezing of the account is provided, this is non-exhaustive. As such, HM Treasury have advised it is their view that attempted breaches, which the financial institution stops, could well be the appropriate subject of a suspected breach disclosure.

4.104~~66B~~ OFSI have also advised **not** to put the word "Notification" in the title of the email - as the inbox automatically filters those into a different process. OFSI have specifically requested that the words "suspected breach disclosure" be put in the title, so that these can be allocated to the correct case worker and dealt with promptly.

4.105~~67~~ Where ~~firms~~ financial institutions believe that they hold funds or assets for a sanctioned party, this must always be reported to OFSI as soon as practicable – see Annex 4-II. Firms must ensure that they have clear internal and external reporting processes for reporting matches to OFSI as soon as practicable and that individuals within the firm dealing with matters in relation to which a report has been made to OFSI understand their obligations.

*What information to report?*

4.106~~68~~ Firms are generally required to report the following information:

- the information or other matter on which the knowledge or belief is based;
- any information held by the financial institution about the sanctions target by which the person can be identified; and
- the nature and amount or quantity of any funds or economic resources held by the financial institution for the sanctions target.

*Legislative reporting requirements*

4.107~~69~~ Firms should comply with the specific requirements of the applicable legislation, which may be contained in a UK Statutory Instrument or in an EU Regulation (available from the HM Treasury sanctions website) as regards their obligations in dealing with sanctioned parties. As legislation relating to different sanctioned parties may vary, the detail of the relevant legislation covering the asset freeze should be examined. Firms may also seek advice from ~~HM Treasury's Financial Sanctions Unit~~OFSI on the action required, including where serious practical difficulties arise with regard to compliance.

4.~~70~~108 In the case of sanctions contained in UK Statutory Instruments, HM Treasury may (depending on the applicable Statutory Instrument) in addition ask any UK person (as defined in the relevant Statutory Instrument) to provide information that they may reasonably require

for the purpose of monitoring compliance and detecting evasion of the sanctions regime ~~[see for example the Terrorism (United Nations Measures) Order 2009 Schedule Part I (4)].~~

*Contacting customer's branch*

4.~~71~~109 Where a customer's account has been frozen, firms may need to contact the customer's local branch or appropriate business area informing them of the asset freeze.

*Notifying customer of asset freeze - does "tipping off" apply?*

4.~~72~~110 Firms are not legally required to advise customers that their account has been frozen. The listing authority will have made efforts to inform the designated person that they have been designated and what that means for them. The Consolidated List is a public document and there is no prohibition on discussing a customer's listing with them (as compared to the prohibitions relating to 'tipping off' under the wider anti-money laundering regime).

4.~~73~~111 It will, however, generally be good practice to tell the customers involved that they are subject to financial sanctions such as an asset freeze, and to explain the effect of any restrictions to them, and how to contact OFSI. When discussing matters with the customer a firm should still be aware that it is a criminal offence to circumvent, or enable or facilitate circumvention of sanctions.

*Does a SAR have to be filed?*

4.~~74~~112 Holding an account for a sanctioned party or rejecting or processing a transaction (whether or not in breach of financial sanctions prohibitions) which involves a sanctioned party, is not in itself grounds for filing a SAR under either POCA or the Terrorism Act.

4.113~~75~~ However, should a suspicion of crime or terrorism arise, firms should consider their obligations under the legislation and whether they should submit a SAR.

*Reporting to the FCA*

4.~~76~~114 There is no formal legal requirement to report a true match other than to OFSI.

4.~~77~~115 Both t~~T~~he FCA and the PRA have~~has~~ indicated that they~~it~~ regard~~s~~ breaches (not true matches) of financial sanctions to be a matter that would be appropriate for firms to report to the FCA via their usual points of contact. This disclosure should be consistent with the FCA's Principle 11 which requires a firm to "deal with its regulators in an open and co-operative way" and to "disclose to the FCA anything relating to the firm of which the FCA would reasonably expect notice". Firms with a dedicated FCA and/or PRA relationship manager may wish to discuss the practicalities of this as part of their usual supervisory dialogue.

*Review customer relationship*

4.~~78~~116 Firms may wish to review their relationship with a customer confirmed as a true sanctions match.

*Breaches of Statutory Instruments*

4.~~79~~117 OFSI must be informed as soon as practicable where a firm knows or suspects that an offence under any one of the various sanctions has been committed either by itself or by a sanctions target. Failure to do so constitutes an offence.

**ANNEX 4-I**

**Summary of relevant legislation**

*Note: This summary focuses on legislation relating to terrorism and terrorist financing. Not all country-based regimes are, however, in place for this purpose; some are more human rights based.*

***United Nations***

| | |
|---|---|
| UNSCR 1373 (2001) | The UN Security Council has passed UNSCR 1373 (2001) which calls on all member states to act to prevent and suppress the financing of terrorist acts. Guidance issued by the UN Counter Terrorism Committee in relation to the implementation of UN Security Council Resolutions regarding terrorism can be found at www.un.org/Docs/sc/committees/1373/ |
| UNSCR 1267 (1999) | The UN has published the names of individuals and organisations subject to UN financial sanctions in relation to involvement with Usama Bin Laden, Al-Qa'ida, and the Taliban under UNSCR 1267 (1999), 1390 (2002) and 1617 (2005). All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities. |

***European Union***

| | |
|---|---|
| EC Regulation 2580/2001 as amended | The EU directly implements all UN financial sanctions, including financial sanctions against terrorists, through binding and directly applicable EU Regulations. The EU implemented UNSCR 1373 through the adoption of Regulation EC 2580/2001 (as amended). This Regulation introduces an obligation in Community law to freeze all funds and economic resources belonging to named persons and entities, and not to make any funds, economic resources or financial services available, directly or indirectly, to those listed. |
| EC Regulation 881/2002 (as amended) | UNSCR 1267 and its successor resolutions are implemented at EU level by Regulation EC 881/2002 (as amended).<br><br>The texts of EC Regulations referred to and the lists of persons targeted, are available at http://ec.europa.eu/external_relations/cfsp/sanctions/docs/measures_en.pdf |

***UK legislation***

| | |
|---|---|
| | The UK has implemented its obligations under UNSCR 1373 under the Terrorist Asset-Freezing Act 2010 (which replaced the Terrorism (United Nations Measures) Orders of 2001, 2006 and 2009). The 2001 and 2006 Orders had been replaced and revoked by the 2009 Order save that directions designating persons under article 4 of the 2001 and 2006 Orders which remained in force on the date of the 2009 Order came into force continued to apply and the provisions of the 2001 and 2006 Orders continued to apply to such directions.<br><br>UNSCR 1267 and its successor resolutions are implemented in the UK by |

EC Regulation 881/2002 (as amended). The Al-Qa'ida and Taliban (Asset-Freezing) Regulations 2010 provide for penalties of Regulation 881/2002 and, amongst other things, reporting obligations on financial institutions.

Acting under the Terrorist Asset-Freezing etc Act 2010, where HM Treasury has reasonable grounds for suspecting that the person is a person who commits, attempts to commit, facilitates or participates in the commission of acts of terrorism, and it considers the designation necessary for the purposes of protecting members of the public from a risk of terrorism, it can designate that person for the purposes of the Order. This might result in the addition of a name to the HM Treasury list that might not appear on the equivalent UN or EU lists.

A number of organisations have been proscribed under UK anti-terrorism legislation. Where such organisations are also subject to financial sanctions (an asset freeze), they are included on the Consolidated List maintained by OFSI.

***Regimes currently in place***

A list of the financial sanctions regimes currently in place can be found on the OFSI website at: https://www.gov.uk/government/organisations/hm-treasury/series/financial-sanctions-regime-specific-consolidated-lists-and-releases.

***Other regimes***

The Department for International Trade is the UK department responsible for trade sanctions.

Certain trade sanctions regimes, such as those involving an arms embargo, also include measures that place restrictions on the provision of financial assistance related to specific activities, such as military activities.

Below are details of those trade sanctions regimes in effect in the UK, which include restrictions on the provision of finance directly to the prohibited trade activities:

Lebanon

The Counter Terrorism Act 2008

Schedule 7 to the CTA gives power to HM Treasury to issue directions to firms in the financial sector. The kinds of requirement that may be imposed by a direction under these powers relate to

customer due diligence;
ongoing monitoring;
systematic reporting ;
limiting or ceasing business.

The requirements to carry out CDD measures and ongoing monitoring build on the similar obligation under the Money Laundering Regulations. The requirements for systematic reporting and limiting or ceasing business are new.

HM Treasury may give a direction **if one or more** of the following

conditions is met in relation to a non-EEA country:

- that the Financial Action Task Force has advised that measures should be taken in relation to the country because of the risk of terrorist financing or money laundering activities being carried on

  1. (a) in the country,

  (b) by the government of the country, or

  (c) by persons resident or incorporated in the country.

- that the Treasury reasonably believe that there is a risk that terrorist financing or money laundering activities are being carried on

  (a) in the country,

  (b) by the government of the country, or

  (c) by persons resident or incorporated in the country,

  2. **and** that this poses a significant risk to the national interests of the UK.

- that the Treasury reasonably believe that

  (a) the development or production of nuclear, radiological, biological or chemical weapons in the country, or
  (b) the doing in the country of anything that facilitates the development or production of any such weapons,
  poses a significant risk to the national interests of the UK.

**ANNEX 4-II**

**Summary of responsibilities for the UK regime**

Responsibilities lie with three Government departments and the Financial Conduct Authority also has a role:

1. The Foreign and Commonwealth Office ("FCO") has responsibility for negotiating in the UN and in the EU on sanctions

2. The Department for International Trade ("DIT") has responsibility for trade sanctions.

3. HM Treasury, through OFSI, has responsibility for administering sanctions in the UK, compliance and issuing exemptions to prohibitions by way of licence.

4. The Financial Conduct Authority ("FCA") has responsibility for ensuring that financial services firms have adequate systems and controls for compliance with the UK financial sanctions requirements.

**The FCO**

The FCO has overall responsibility for UK policy in relation to the scope and content of the sanctions regime. The FCO also has responsibility for representing and negotiating the UK's position with respect to the terms of financial sanctions related United Nations Security Council resolutions and European Union Regulations. UNSCRs provide the basis on which the legal sanctions framework is constructed, and EC Regulations give effect to UN obligations in the EU, including in the UK.

The EU can also impose autonomous sanctions within the framework of the Common Foreign and Security Policy.

The FCO maintains a list of current restrictions and information on the countries that are under export controls and sanctions: see https://www.gov.uk/guidance/sanctions-embargoes-and-restrictions

**DIT**

DIT has responsibility for trade sanctions, setting export controls and administering the FCO list of about 50 countries subject to trade measures. Trade sanctions, such as embargoes on making military hardware or know-how available to certain named countries of jurisdictions, can be imposed by governments or other international authorities, and these can have financial implications. Firms which operate internationally should be aware of such sanctions, and should consider whether these affect their operations; if so, they should decide whether they have any implications for the firm's procedures.

DIT also has specific responsibility for implementing United Nations Security Council Resolutions on weapons of mass destruction. Within DIT the Export Control Organisation ("ECO") has responsibility for legislating, assessing and issuing export licences for specific categories of "controlled" goods. This encompasses a wide range of items including so-called dual-use goods, torture goods, radioactive sources, as well as military items. A licence may be required depending on various factors including the nature of the items exported and any sanctions in force on the export destination.

**HM Treasury**

HM Treasury is the lead UK Government department on administering the financial sanctions regime,

which it does through OFSI. OFSI's aim is to help ensure that financial sanctions are properly understood, implemented and enforced in the United Kingdom ~~The key objective of OFSI is to ensure a proactive and effective UK asset freezing regime in partnership with stakeholders.~~ OFSI has four branches, covering Counter-terrorism, International, Licensing and Compliance.

**FCA**

The FCA Handbook, in particular Principle 3 and SYSC 6.1.1, places specific responsibilities on firms regarding financial crime prevention. Authorised firms are therefore subject to regulatory requirements relating to the UK's financial sanctions regime.

The following are the specific requirements:

> Principle 3: Management and control
>
> "A firm must take reasonable care to establish and control its affairs responsibly and effectively with adequate risk management systems" and
>
> SYSC 6.1.1
>
> "A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime. [Note: article 13(2) of MiFID.]"

**Application in law**

Sanctions apply in UK law through both EC Regulations and Statutory Instruments (which have been used as the UK's enabling legislation for the application of UN financial sanctions). With regard to EC Regulations, there is direct applicability in EU Member States, so that entities incorporated or constituted under EU law, and persons and entities doing business in the EU (including non-EU nationals) are subject to their provisions. Statutory Instruments apply to any person in the UK and any British citizen, and any body incorporated or constituted under law of any part of the UK (but not subsidiaries operating outside the UK with no UK legal personality). Annex 4-I provides details of international, EU and UK legislation relevant to financial sanctions and asset freezing.

Each Statutory Instrument is unique in terms of detail, restrictions, exceptions, prohibitions the penalties for non-compliance and information requirements.

**Who must comply with financial sanctions in the UK?**

The relevant Statutory Instruments generally apply to any person in the UK, to any person elsewhere who is a British citizen or subject, and to any body incorporated or constituted under the law of any part of the UK, although the exact wording may differ from one Statutory Instrument to another. UK Statutory Instruments do not apply to subsidiaries operating wholly outside the UK and which do not have legal personality under UK law.

EU Regulations imposing and/or implementing sanctions are part of Community law, are directly applicable and have direct effect in the Member States. The measures apply to nationals of Member States, as well as persons and entities doing business in the EU, including nationals of non-EU countries.

**Is it an offence to make funds available to a target of financial sanctions legislation?**

This is covered specifically in each relevant Statutory Instrument and EU Regulation. In general terms, any person to whom the relevant legislation applies who, except under the authority of a licence granted by OFSI under the relevant legislation makes any funds, economic resources or, in some circumstances, financial (or related) services available directly or indirectly to or for the benefit of persons listed under the relevant Statutory Instrument or EU Regulation is guilty of an offence.

**What are the penalties for committing an offence under the legislation?**

These are covered specifically in each relevant Statutory Instrument, and in s146 of the Policing and Crime Act 2017. However, in general terms, any person guilty of an offence under the relevant Statutory Instrument is liable on conviction to imprisonment and/or a fine. The maximum term of imprisonment is currently seven years or two years in the case Statutory Instruments providing penalties for breaches of EU Regulations.

Where any body corporate is guilty of an offence under the relevant Statutory Instrument, and that offence is proved to have been committed with the consent of connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary or other similar officer of the body corporate, or any person who was purporting to act in any such capacity, that person as well as the body corporate is guilty of that offence and is liable to be proceeded against and punished accordingly.

HM Treasury, through OFSI, may impose a monetary penalty on a person if it is satisfied, on the balance of probabilities, that

(a) the person has breached a prohibition, or failed to comply with an obligation, that is imposed by or under financial sanctions legislation, and
(b) the person knew, or had reasonable cause to suspect, that the person was in breach of the prohibition or (as the case may be) had failed to comply with the obligation.

OFSI's monetary penalties guidance is available at:
https://www.gov.uk/government/publications/monetary-penalties-for-breaches-of-financial-sanctions

Formatted: Font: 11 pt

**Subscribing to HM Treasury notification service**

OFSI offers a free subscription facility for notification by e-mail when a Financial Sanctions-related release is published on this website and the consolidated list of targets is updated. ~~In order to subscribe, an email should be sent from the email address to be subscribed to AMLsubscribe@hmtreasury.gsi.gov.uk with the words **SUBSCRIBE SANCTIONS** in the subject field, and providing your name, company name, address and telephone number as appropriate.~~Those wishing to subscribe can do so at: https://www.gov.uk/government/publications/monetary-penalties-for-breaches-of-financial-sanctions

Formatted: Font: 11 pt

**The BBA alert service**

The BBA provides an additional alert service by notifying its members and drawing their attention to amendments published by HM Treasury. The alert service is provided to all BBA member banks and principal contacts.

**International requirements**

Firms active in non-UK jurisdictions will wish to be aware of the sanctions requirements in each and every country where they operate.

**ANNEX 4-III**

**Summary of Licensing Regime**

**What is a licence?**

A licence is a written authorisation from ~~HM Treasury~~OFSI to allow an activity which would otherwise be prohibited by financial sanctions legislation. The obligations and responsibilities attached to a licence are generally imposed on a sanctions target, but a licence may be issued to a relevant financial institution in order to allow such institution to engage in an activity, such as dealing with funds belonging to a sanctions target, which would otherwise be prohibited. A licence may include associated reporting requirements or other conditions on a financial institution, and these will be made clear in the terms of an individual licence.

Applications for a licence should be made using the application form on the OFSI website[6] and either emailed or posted to OFSI.

Applications to release funds from frozen accounts, or to make funds, economic resources or financial services available to or for the benefit of a sanctions target must be made in writing to the Office of Financial Sanctions Implementation, ~~HM Treasury,~~ 1 Horse Guards Road, London SW1A 2HQ, or emailed to ofsi@hmtreasury.gsi.gov.uk.

OFSI will normally provide guidance letters when issuing licences to banks. Such guidance will specify the purpose for which the licence is being issued, together with any specific obligations on financial institutions including any monitoring requirements.

**Operation of frozen accounts under a licence**

OFSI does not instruct financial institutions on how they should operate frozen accounts that are licensed to permit specific transactions to take place. Some financial institutions operated such accounts by blocking all electronic functionality, or permitting only specified standing orders/direct debits. Other financial institutions allow the accounts to operated without restrictions, but apply specific monitoring. Where accounts are operated openly, financial institutions must ensure that there is sufficient monitoring to satisfy them that any breaches by a sanctions target, for example withdrawals in excess of a ~~-~~cash limit stated in the licence, are identified as soon as possible and reported to OFSI.

There are primarily four different models by which frozen accounts are operated:

i. frozen accounts of sanctions targets subject to a licence are run as standard accounts with cash cards and full electronic functionality. Monitoring is in place on such accounts to ensure any unauthorised activity by the sanctions target is detected and communicated to HM Treasury without delay.

ii. the original account is frozen and a new account is opened that benefits or other licensed income can be paid into. The sanctions target has no access to funds in the original frozen account. Again, monitoring is in place on such account to detect any unauthorised activity.

iii. access to a cash card is withdrawn. However, the sanctions target is permitted to set up payments, e.g., for rent and utilities, by standing order or direct debit. Remaining funds required (up to a limit specified in the licence) must be withdrawn in person at the branch

[6] https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation

Formatted: Font: 10 pt

counter.

iv. the account is blocked to remove all electronic functionality, and the sanctions target must withdraw cash over the branch counter – there may be a limit on the amount of cash that can be withdrawn, depending on the terms of the licence.

Depending on the model of account operation adopted, there is a balance between ensuring that sufficient controls are in place on such accounts and ensuring that the impact of the asset freezing regime on the individual is not disproportionate.

In respect of the insurance industry, especially general insurance, there may be instances where legitimate third party claims may arise. In such circumstances any payments or services provided may require a licence or amending the current licence. In all instances the advice of HM Treasury should be obtained before any payment is made.

Even where no obligations on a bank are specified in a licence, there are relevant obligations contained in the legislation itself. ~~Part 4 of the 2009 Terrorism Order imposes certain reporting obligations on financial institutions in relation to offences committed under Article 8 and Part 3 of the Order.~~ Where a financial institution is aware of breaches of the asset freeze by a sanctions target, there is a requirement to inform ~~the Financial Sanctions Unit~~OFSI as soon as it is practicable to do so. One example is that in a circumstance where a bank is aware, through monitoring of an account, that a sanctions target is in breach of their licence conditions, e.g., through withdrawing more cash than they are permitted, the bank is required by the legislation to inform HM Treasury of the sanctions target's breach as soon as is practicable.

Guidance on the licensing process can be found in~~, and examples of, General Licences is available on the OFSI website at https://www.gov.uk/sanctions-embargoes-and-restrictions~~. OFSI's guide to ~~has also issued general guidance on~~ financial sanctions, available at: https://www.gov.uk/government/publications/financial-sanctions-faqs.

**ANNEX 4-IV**

**Useful sources of information**

UN Security Council: www.un.org/Docs/sc/committees/INTRO.htm.

~~HM Treasury~~OFSI: https://www.gov.uk/government/organisations/office-of-financial-sanctions-implementation
~~https://www.gov.uk/sanctions-embargoes-and-restrictions~~

FCO: http://www.fco.gov.uk/en/global-issues/counter-terrorism/

Code for Crown Prosecutors: www.cps.gov.uk/publications/docs/code2004english.pdf

Home Office: https://www.gov.uk/government/organisations/home-office

NCA: www.soca.gov.uk

European Commission: http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.htm

FCA report on firms' compliance with UK sanctions requirements: www.fsa.gov.uk/pubs/other/Sanctions%20Final%20Report.pdf

Department for ~~Business Innovation and Skills~~International Trade
https://www.gov.uk/government/organisations/department-for-international-trade

US Treasury: http://www.ustreas.gov/offices/enforcement/ofac/programs/

OFAC: http://www.treas.gov/offices/enforcement/ofac/

FATF: www.fatf-gafi.org/

Wolfsberg Group: http://www.wolfsberg-principles.com/

.

Formatted: Font: Times New Roman

Formatted: Font: 11 pt