



GUIDANCE NOTES

For

AML/ATF REGULATED FINANCIAL INSTITUTIONS

On

**Anti-Money Laundering
&
Anti-Terrorist Financing
(AML/ATF)**

**Proceeds of Crime (Anti-Money Laundering & Anti-Terrorist
Financing) Regulations 2008**

PART 4 WIRE TRANSFERS

**Issued by the
Bermuda Monetary Authority**

Pursuant to Proceeds of Crime Regulations (Supervision & Enforcement) Act 2008 (Section 5(2))

March 2010

BERMUDA MONETARY AUTHORITY

GUIDANCE NOTES

For

AML/ATF Regulated Financial Institutions

On

Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing)
Regulations 2008

PART 4 – WIRE TRANSFERS

Note: This guidance issued by the Bermuda Monetary Authority is only relevant to AML/ATF regulated financial institutions engaged in wire transfer business.

Background

1. FATF issued Special Recommendation VII in October 2001, to enhance the transparency of electronic payment transfers (“wire transfers”) of all types, domestic and cross border, making it easier for law enforcement to track funds transferred electronically by terrorists and other criminals. A revised Interpretative Note to this Special Recommendation was issued by the FATF on 10 June 2005, and is available at the FATF website:

[FATF Revised Interpretative Note to Special Recommendation VII: Wire Transfers](#)

2. These Regulations implement Special Recommendation VII within Bermuda with effect from January 27th 2010.
3. These Regulations require a person whose business includes the provision of transfer of funds – a payment service provider (‘PSP’), to provide certain information in each wire transfer about the person who gives the instructions for the wire transfer to be made (‘the Payer’). The core requirement is that this information consists of the following information (‘Complete Information on the Payer’):

Customer name;
Customer address and
Customer account number

However, there are a number of permitted variations and concessions, as detailed below under “Information Requirements” (paragraph 10). The Regulations also place obligations on the PSP of the person who is the intended final recipient of the wire transfers (‘the Payee’) and on any other PSP that is involved in making the wire transfer. It should be noted that the Regulations provide only for complete information to be held by PSPs, and there is no obligation to pass information on the payer to the payee.

4. Whilst it is possible that a payee may in fact be a conduit for an undisclosed ‘final recipient’ to serve a criminal objective, within the context of the Regulations, ‘final recipient’ is to be understood as referring to the person named in the transfer as the beneficiary of the payment, unless there is evidence to suggest that another person will benefit.

Scope of the Regulations

Regulation 22

- 5.1 The Regulations are widely drawn and intended to cover all types of funds transfers falling within its definition as made “by electronic means”, other than those specifically exempted wholly or partially by the Regulations. For Bermuda based PSPs it therefore includes, but is not necessarily limited to, international payment transfers made via SWIFT, including various payment systems, and domestic transfers via CHAPS and BACS.
- 5.2 Regulation 22 specifically exempts the following payment types:
- (a) 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;
 - (b) transfers by credit or debit card or similar payment instrument, providing that the Payee has an agreement with the PSP permitting payment for goods or services and that the transfer is accompanied by a unique identifier permitting the transaction to be traced back to the Payer (see paragraph 10.3);
 - (c) transfers whereby the Payer withdraws cash from his/her own account. This is designed to exempt ATM withdrawals outside Bermuda which would otherwise attract the full information requirement;
 - (d) transfers to public authorities for taxes, fines or other levies;
 - (e) direct debits, subject to their carrying a unique identifier for tracing purposes;
 - (f) truncated cheques (cheques are otherwise paper to which the Regulation does not apply);
 - (g) regulation 22(3) provides a limited exemption for small pre-paid transfers carried out by means of a mobile phone or any other digital or IT device; and
 - (h) 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.

Pre-conditions for making payments

Regulation 23

6. Payment Service Providers (PSPs) of Payers must ensure that the Payer information conveyed in the payment relating to account holding customers is accurate and has been verified. The verification requirement is deemed to be met for account holding customers of the PSP whose identity has been verified, and where the information obtained by this verification has been stored in accordance with the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008. 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., institutions will be mindful of the provisions of paragraphs 5.37 to 5.40 of the general guidance

concerning customers with existing relationships (see paragraph 10.9 where the named Payer is not the holder of the account to be debited).

7. Before undertaking one-off payments in excess of \$1,000 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).
8. For non-account based transfers of \$1,000 and under, PSPs are not required by the Regulations to verify the Payer's identity except when several transactions are carried out which appear to be linked (see Regulation 23(4)) and together exceed \$1,000. Even in cases where the Regulations do 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.
9. Evidence of verification must be retained with the customer information in accordance with Record Keeping Requirements (see paragraphs 15.1 and 15.2).

Information Requirements: Complete payer information:

Regulation 23

- 10.1 Except as permitted below, complete information on the Payer must accompany all wire transfers. Effectively, the complete Payer information requirement applies where the destination PSP is located in a jurisdiction outside Bermuda. Complete Payer information consists of: name, address and account number.
- 10.2 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 an institution'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.
- 10.3 Where the payment is not debited to a bank account, the requirement for an account number must be substituted by a unique identifier which permits the payment to be traced back to the Payer. The Regulations distinguish between a 'customer identification number' and 'unique identifier'. The customer identification number (CIN) could be an internal reference number that is created by a PSP or a number that is contained in an official document such as a national identity number. However, it is key that it uniquely identifies a particular Payer. The unique identifier could be a transaction number that allows a payment to be traced back to a payer.
- 10.4 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 Regulations.
- 10.5 The account number could be, but is not required to be, expressed as the IBAN (International Bank Account Number).
- 10.6 The Regulations apply even where the Payer and Payee hold accounts with the same PSP.
- 10.7 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 Regulations, although it is also preferable for

the account number to be included where available. The same applies to Business Entity Identifiers (BEIs), although in that case the account number should always be included. As the use of BICs and BEIs is not specified in FATF Special Recommendation VII or the Regulations, there may be requests from Payee PSPs for address information.

- 10.8 Generally, institutions 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 account holder whose account number is stated on the payment transfer.
- 10.9 Where the named Payer is not the account holder 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 account holder. In the latter case, provided the Payer's PSP retains all relevant data for 5 years, the Payer PSP is required to verify only the information about the account holder being debited (in accordance with regulation 23(3)). PSPs should exercise a degree of control to avoid abuse of the discretion by customers. It is important to note that this flexibility should not undermine the transparency of Payer information sought by FATF Special Recommendation VII and the Regulations. It is designed to meet the practical needs of corporate and other business (e.g., attorneys) account holders with direct access who, for internal accounting reasons, may have legitimate reasons for quoting alternative Payer details with their account number.
- 10.10 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 of improper motive by a customer should be reported to the institution's reporting officer.
- 10.11 In the case of a payer that is a company, a wire transfer must be accompanied by an address at which the company's business is conducted, or at which it may be contacted. In the case of a Payer that is a trustee, a wire transfer must be accompanied by the address of the trustee.
- 10.12 In the case of a joint account, a PSP may demonstrate that it has met its legal obligation to provide a customer name where, dependent upon the size of the field, it provides the name of either or both account holders.

Information Requirements: Domestic Transfers:

Regulation 24

- 11.1 Where the PSPs of both Payer and Payee are located within Bermuda, wire transfers need be accompanied only by the Payer's account number or by a unique identifier which permits the transaction to be traced back to the Payer.
- 11.2 However, if requested by the Payee's PSP, complete information must be provided by the Payer's PSP within 3 working days, starting the day after the request is received by the Payer's PSP.

Information Requirements: Batch File Transfers from single payer to PSP outside Bermuda:

Regulation 25

12. Under Regulation 25 the batch file for transfers from a single Payer to multiple Payees outside Bermuda must contain complete Payer information. However, the individual transfers within the batch need carry only the Payer's account number or a unique identifier.

Payments via Intermediaries:

Regulations 30 & 31

13. Intermediary PSPs include those who act as agents for other PSPs or who provide correspondent banking facilities. Intermediary PSPs (IPSPs) must, subject to the following guidance on technical limitations, ensure that all information received on the Payer which accompanies a wire transfer is retained with the transfer. It is preferable for an IPSP to forward payments through a system which is capable of carrying all the information received with the transfer. However, where an IPSP within Bermuda is technically unable to on-transmit Payer information originating outside Bermuda, it may nevertheless use a system with technical limitations provided that -
 - (a) if it is aware that the Payer information is missing or incomplete it must concurrently advise the Payee's PSP of the fact by an agreed form of communication, whether within a payment or messaging system or otherwise;
 - (b) it retains records of any information received for 5 years, whether or not the information is complete;
 - (c) if requested to do so by the Payee's PSP, the IPSP must provide the Payer information within 3 working days of receiving the request.

Minimum standards

14. The above information requirements are minimum standards. It is open to PSPs to elect to supply complete Payer information with transfers which are eligible for a reduced information requirement and thereby limit the likely incidence of inbound requests for complete information.

Record Keeping Requirements

Regulations 23, 29 & 31

- 15.1 The Payee's PSP and any intermediary PSP must retain records of any information received on a Payer for 5 years, in accordance with Regulation 29 and Regulation 31(5) respectively.
- 15.2 The Payer's PSP must retain records of transactions and supporting evidence of the Payer's identity in accordance with Regulation 23(5).

Checking Incoming Payments

Regulations 26, 27 & 28

16. 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 Regulations specify that PSPs should have procedures to detect whether relevant information is missing. (This requirement is satisfied by the validation rules of whichever messaging or payment system is being utilised). Additionally, Regulation 27 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:

- (a) SWIFT payments on which mandatory Payer information fields are not completed will fail anyway and the payment will not be received by the Payee PSP. Current SWIFT validation prevents payments being received where the mandatory information is not present at all. However, it is accepted that where the Payer information fields are completed with incorrect or meaningless information, or where there is no account number, the payment will pass through the system. Similar considerations apply to non-SWIFT messaging systems which also validate that a field is populated in accordance with the standards applicable to that system, e.g., BACS.
- (b) 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, for example -
 - (i) the sampling could normally be restricted to payments emanating from PSPs outside Bermuda where the complete information requirement applies;
 - (ii) 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;
 - (iii) 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;
 - (iv) other specific measures might be considered, e.g., checking, at the point of payment delivery, that Payer information is compliant and meaningful on all transfers that are collected in cash by Payees on a "Pay on application and identification" basis.

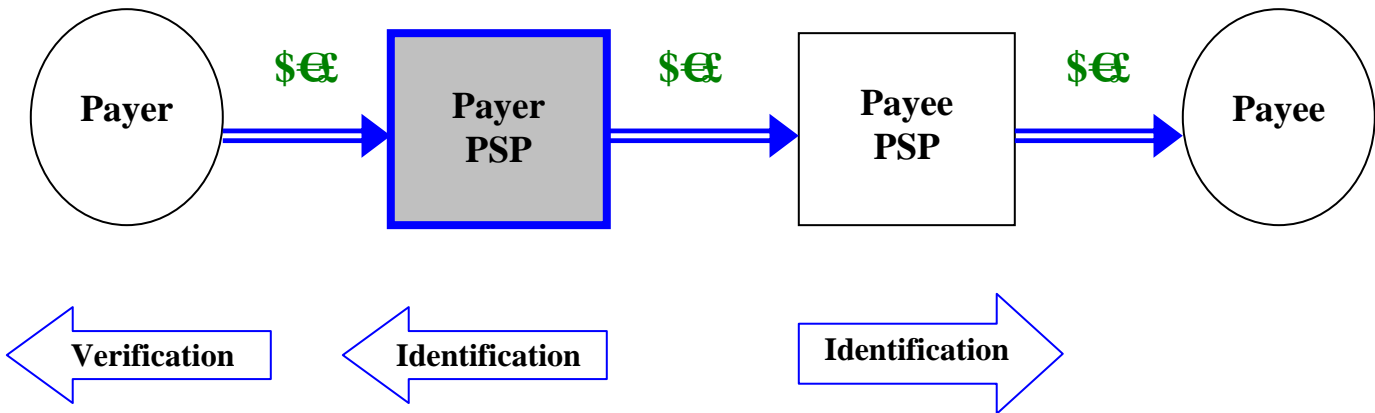
NB. None of the above requirements obviate the obligation to report suspicious transactions (see Chapter 6 of the General Guidance).

17. If a Payee PSP becomes aware in the course of processing a payment that it contains meaningless or incomplete information, under the terms of regulation 27(1) of the Regulations it should either reject the transfer or ask for complete information on the Payer. In addition, in such cases, the Payee PSP is required to take any necessary action to comply with any applicable law or administrative provisions relating to money laundering and terrorist financing. Dependent on the circumstances such action could include making the payment or holding the funds and advising the Payee PSP's reporting officer.

18. 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 -
 - (a) seek the necessary information on the Payer and/or
 - (b) take any necessary action under any applicable law, regulation or administrative provisions relating to money laundering or terrorist financing.
19. Where a PSP is identified as having regularly failed to comply with the information requirements, 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.
20. 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 reporting officer for possible disclosure to the Financial Intelligence Agency.
21. With regard to transfers from PSPs located in countries that are not members of either the CFATF or FATF, institutions 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 culture and policy and who accept the standards set out in the Interpretative Note to FATF Special Recommendation VII.
22. It should be borne in mind when querying incomplete payments that some FATF member countries may have framed their own regulations to incorporate a threshold of US\$1,000 below which the provision of complete information on outgoing payments is not required. This is permitted by the Interpretative Note to FATF Special Recommendation VII. The USA is a case in point. This does not preclude Bermudian 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.

March 2010

Example 1: Transfer of funds – Obligations on Payer PSP



If to PSP outside BERMUDA:

- Complete information

If batch file from single payer to PSP outside BERMUDA:

- Complete information on batch
- Account number (or unique identifier) on single transaction

If both PSPs within BERMUDA:

- Account number (or unique identifier)

Complete Information (CIP):

- Name
- Address (or date and place of birth, or customer identification number or national identity number)
- Account number (or unique identifier)

If transaction not from account with PSP:

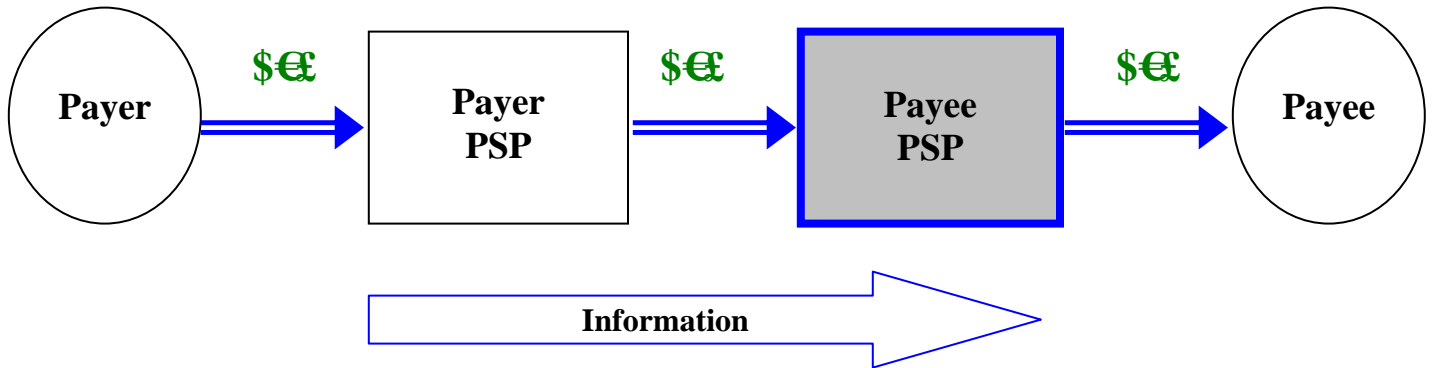
- If below \$1,000: No mandatory verification of CIP.
- If exceeds \$1,000 or series of linked transactions exceeding \$1,000: Verify CIP.

If transaction from account with the PSP (for any value):

- Verification deemed to have taken place if identity of account holder verified in accordance with the requirements of CDD under Part 2 of the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008

Records of CIP which accompanies transfer of funds to be kept for 5 years.

Example 2: Transfer of funds – Obligations on Payee PSP



Procedures:

- Detect whether appropriate type of information attached and whether fields complete

If fields incomplete or information inappropriate:

- Ask for information or reject transaction

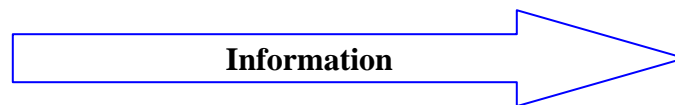
If fields regularly incomplete or information inappropriate:

- Report to the Bermuda Monetary Authority
- Issue warning to PSP of payer
- If no improvement, reject any further transactions or restrict / terminate business relationship
- Consider whether it is appropriate to make a report to the Financial Intelligence Agency

Note: In practice the procedures required to 'detect' may be met by a combination of system (e.g. SWIFT) validation and risk-based post event random sampling.

Records of any information received to be kept for 5 years

Example 3: Transfer of funds – Obligations on Intermediary PSP



Keep information received with the transfer where technical limitations prevent this)

Where information is not sent with transfer it must be kept for 5 years