the Wolfsberg Group

Banco Santander
Bank of America
Bank of Tokyo-Mitsubishi UFJ
Barclays
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC
J.P. Morgan Chase
Société Générale
Standard Chartered Bank
UBS

Wolfsberg Group
Payment Transparency Standards

Background

The 2007 Wolfsberg Group and Clearing House Association's statement on Payment Message Standards[1] was an important intervention to enhance transparency regarding parties to transactions in international payments. The four payment message Standards to be observed by all financial institutions (FIs) remain relevant today and are:

- Financial institutions should not omit, delete or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other financial institution in the payment process
- Financial institutions should not use any particular payment message for the purpose of avoiding detection of information by any other financial institution in the payment process
- Subject to all applicable laws, financial institutions should cooperate as fully as practicable with other financial institutions in the payment process when requested to provide information about the parties involved
- Financial institutions should strongly encourage their correspondent banks to observe these principles

Over the last decade the financial services industry has made significant progress in adopting these standards, such as through the introduction of MT202COV for cover payments[2] by SWIFT; the development of market practice guidelines by various bodies such as the Payments Market Practice Group (PMPG); Enhanced Due Diligence (EDD) arrangements in relation to correspondent banking relationships and the development and deployment of various tools by FIs to enhance the identification of any omission, deletion or alteration of payment information.

The Wolfsberg Group has recently reviewed its Transparency Standards and is publishing additional Standards. These additional Standards are aspirational in nature and the Group notes that full adoption will require investments to be made over time, for example, for FIs to realign policy, data and systems to these new requirements and/or foster the development of enhanced market infrastructures. Legacy payments infrastructures may limit the amount of information that can be included in a payment due to the absence of sufficient field space. In setting out these additional aspirational Standards, the Wolfsberg Group calls on providers of payments infrastructures and delivery channels, as well as FIs, to continue to address these limitations and coordinate their actions through the adoption of technology and consistent structured formats

[1] http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg_NYCH_Statement_on_Payment_Message_Standards_(2007).pdf
[2] http://www.wolfsberg-principles.com/pdf/comment/Joint_Industry_Letter_on_MT_202_COV_(20-05-09).pdf

to provide sufficient system capacity to transmit the volume of information required for increased transparency. Full adoption of ISO 20022 standards[3] would support addressing these limitations.

The Wolfsberg Group also welcomes efforts by the public sector to support progress on enhanced payment transparency, such as the Basel Committee Guidelines on Due Diligence and Transparency regarding Cover Payment Messages related to Cross-border Wire Transfers 2009;[4] Financial Action Task Force (FATF) Recommendation 16;[5] FATF Correspondent Banking Guidance 2016;[6] Basel Committee Guidelines on Correspondent Banking 2016[7] and through related regulations.

The Wolfsberg Group supports the view of the Bank for International Settlements' (BIS) Committee on Payments and Market Infrastructures (CPMI) that enhancing payment transparency has a role to play in addressing correspondent banking de-risking. In its 2016 report on Correspondent Banking, the CPMI identified further steps in this regard and made the following recommendation: [8]

By June 2017, SWIFT PMPG and the Wolfsberg Group are expected to develop an action plan for strengthening market guidance concerning the use-cases for payment messages, including (i) what data should be included in payment messages; (ii) how to include the Legal Entity Identifier (LEI) in payment messages (on an optional basis) and (iii) where to place the information on beneficiary and originator in the data fields.

In response, the Wolfsberg Group is proposing the below additional Standards.

The Standards

These Standards should apply to:

- cross-border transactions
- domestic transactions, to the extent possible with current national payment infrastructures
- all currencies
- all payments regardless of value
- all participants originating, intermediating or receiving payments

unless specifically excluded by FATF Recommendation 16[9] (e.g. transactions carried out using credit, debit or prepaid cards for the purchase of goods or services).

These Standards should additionally be used by parties working on the introduction of new payment methods and platforms, including for domestic payments, where covered by FATF Recommendation 16. As the payments landscape and supporting technologies continue to develop, the capability to support these Standards will further support enhancements in payments transparency. Where payment infrastructures do not provide for transmission of information as mentioned in these Standards, FIs should retain the originator and beneficiary information and have processes in place to make such information available to other relevant parties in the payment chain on request.

[3] ISO 20022 is an ISO standard for electronic data interchange between financial institutions that includes payment transactions, securities trading and settlement information, credit and debit card transactions and other financial information. More information can be found here: https://www.iso20022.org/faq.page
[4] http://www.bis.org/publ/bcbs154.pdf
[5] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
[6] http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf
[7] http://www.bis.org/cpmi/publ/d147.pdf
[8] http://www.bis.org/cpmi/publ/d147.pdf
[9] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

1. Originating FIs

The Originating FI is responsible for:

- verification, identification and due diligence of its customer, as well as related record keeping in line with all the regulations applicable to the FI
- accuracy and completeness of information in the payment message concerning the originating party
- maintaining adequate records that permit the reconstruction of messages if required
- ensuring that messages contain all required information in compliance with FATF Recommendation 16, as well as any other information stipulated by applicable regulations and guidance
- ensuring the correct use of payment messages so as to facilitate identification of payment information by all FIs in the payment process and
- including information on the beneficiary party as described below

When originating payments, an FI should:

A. Include the following information on the originator as the preferred approach to complying with the requirements of FATF Recommendation 16:

Name, Address and **Account number** of the customer of the FI, who is also the originator of the payment. In the absence of an account number, a unique transaction reference number or code must be included.

'Name' refers to the name of the customer as verified by the FI.

- For natural person customers, the name recorded in the FI's systems should be the full name of the customer that was verified as part of Customer Due Diligence (CDD). For accounts held in joint names, the FI should set out in its policy which names are to be recorded on its systems and which of those names should be used for payments. These policies must be in line with all the regulations applicable to the FI.
- For legal entity customers (e.g. companies, partnerships) multiple names may exist such as registered legal name, trading name, 'doing business as' name or commonly abbreviated name. For example:

	Registered Legal Name	**Trade Name/Doing Business As (DBA)**
Name	Eastern Finmark Corporation	Finmark or EFC
Purpose	The name given in the partnership agreement, articles of incorporation or other documents. It is used when communicating with the government or other businesses, e.g. when filing tax returns or buying property.	The name a business uses for advertising and sales purposes that is different from its legal name. A trade name can also be referred to as a DBA.

- The FI should place preference on the registered legal entity name verified as part of CDD. The FI should set out in its policy which names are to be recorded on its systems and which of those names should be used for payments.
- These policies must be in line with all the regulations applicable to the FI.

'Address' refers to an address of the customer as verified by the FI.

- Address information should be sufficient to identify clearly the location of the party/parties for screening and anti-money laundering (AML) monitoring. It should include Country and other aspects

of address in accordance with the resident country conventions such as City, State/Province/Municipality, Street Name, Building Number or Building Name and Postal Code. Having only a Post Office (P.O.) Box as an address should be avoided except where no alternative exists.

- Including full country names as recognised by the United Nations[10] will improve clarity. ISO 3166 2-Character country codes[11] may be used as a preferred approach for SWIFT MT 103, MT 202 COV and related structured messages[12] for originator and beneficiary fields as an alternative to full country name.
- Multiple addresses may exist, e.g. registered address, place of business address, mailing address. For example:

	Registered Address	**Place of Business Address**
Name	Eastern Finmark Corporation	Eastern Finmark Angola Branch
Address	17 Lords Avenue, London, United Kingdom, AC2V 5DV	Rua Cirilo da Conceo silva No.5, andar. Postal 1111. Luanda Angola
Purpose	A registered office is the official address of an incorporated company, association or any other legal entity. Generally, it will form part of the public record and is required in most countries where the registered organisation or legal entity is incorporated.	A business address is the place where the real activity of the company is carried out, i.e. where the operations of the company are planned, controlled, managed and executed.

- The FI should use the address verified as part of CDD. It is recognised that value may be found in utilising the most relevant address. The FI should set out in its policy which addresses are to be recorded in its systems, which are to be verified and used for payments. This includes managing situations where multiple account holders with different addresses may exist, in which case the address of the primary or first named account holder is likely to be sufficient.
- These policies must be in line with all the regulations applicable to the FI.

Policies may also set out where a unique identifier code such as a Business Identifier Code (BIC) is sufficient to identify the customer without full name and address information.

B. Include the following information on beneficiary party:

Name, Address and **Account number** of the beneficiary party. In the absence of an account number, a unique transaction reference number or code must be included. The inclusion of the address represents best practice but is not required by FATF Recommendation 16 and the associated Interpretive Note.[13]

'Name' refers to the name of the beneficiary as provided by the originator of the transaction. The name will not be subject to verification and the FI should pass on the name as supplied by its customer.

'Address' refers to the address of the beneficiary as provided by the originator of the transaction. Where possible, it should include Country, State/Province/Municipality, City, Street Name, Building Number or Building Name and Postal Code in accordance with the resident country conventions. The address will not be subject to verification and the FI should pass on the address as supplied by its customer.

10 http://www.un.org/en/member-states/index.html#gotoE
11 https://www.iso.org/iso-3166-country-codes.html
12 https://www.swift.com/node/82676
13 http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf - pages 73-78

The FI should set out in its policy which beneficiary name(s) and address(es) should be requested from its customers for use in payment messages. These policies must be in line with the regulation of the applicable jurisdiction of the FI. It is not expected that the policy of the FI will require that a transaction request be rejected if the customer does not provide the beneficiary's name and address in line with the request of the FI, unless it is required by the regulations of the applicable jurisdiction or is required to complete the payment. However, it is expected that the policy of the FI should require review of the customer relationship where the FI identifies through ongoing monitoring, over a number of transactions and over a period of time, that the required information:

- is repeatedly not provided or
- is repeatedly clearly meaningless. Examples of meaningless information include strings of random characters and terms such as 'our client.' The FI may set out in its policy commonly found terms which it considers to be clearly meaningless.

C. On Behalf of (OBO) Payments

An OBO payment is when a customer is making payments on behalf of an ultimate originator (e.g. as part of a transaction, a law firm who is the customer of the FI, is making a payment on behalf of its client who is the ultimate originator). In order to support transparency, the originating FI should:

- undertake sufficient due diligence on its customer to confirm to a reasonable degree that payments for third parties are consistent with the line of business of the customer
- set out in its policy what ultimate originator information should be provided by its customers, and clearly communicate those expectations to its customers
- to the extent identifiable from the customer instructions, and practically achievable with existing payment infrastructures, include the full name and address of the ultimate originator in addition to that of the customer in payment message. Information about the ultimate originator may be more relevant for AML/Counter Terrorist Financing (CTF) purposes than customer information in this scenario. The name and address will not be subject to verification and the FI should pass on the name and address as supplied by its customer
- where both ultimate originator and customer information cannot be provided in the same payment message, the FI should set out in its policy whether to provide accurate information on the customer as detailed in section 1A in preference to providing information on the ultimate originator. These policies must be in line with the regulations of the applicable jurisdictions for the FI and
- retain information on ultimate originators where not included in the payment message and make this information available to other FIs in the payment chain where requested.

It is expected that the policy of the FI should require review of the customer relationship where the FI identifies through ongoing monitoring, over a number of transactions and over a period of time, that the required ultimate originator information for OBO payments:

- is repeatedly not provided or
- is repeatedly clearly meaningless (as defined above)

D. Money or Value Transfer Services (MVTS) Payments

Where an account holder is a Money or Value Transfer Service[14] (MVTS) as defined by FATF (2016), it must be licensed or registered with a competent regulatory authority. Since an MVTS is likely to be subject to different regulatory oversight as compared to an FI, the FI must perform a detailed customer risk assessment of the MVTS (including an analysis of relevant AML/CFT controls) before on-boarding and continue to do so at regular intervals thereafter, as defined by their risk assessment process.

The MVTS will be responsible for:

- The activities of its agents
- Complying with the full range of AML/CFT requirements
- Complying with all the relevant requirements of FATF Recommendation 16 as well as those set out in section 1A of this document, either directly or through their agents
- In the case of bulk/batched transactions, particularly when cross-border, the MVTS must adhere to jurisdictional regulations on the information to be provided in the wire transfer with respect to transactional limits for all domestic and cross border transactions. It is noted that:
    - The information of ultimate originator and beneficiary must be recorded in MVTS' systems and should be made available to the relevant authorities and FIs involved in the payment chain on request
    - The originating and beneficiary MVTS are responsible for AML/CTF controls and due diligence on their underlying customers
    - The originating, intermediary and beneficiary FIs will not have all information on underlying originators or beneficiaries that in aggregate comprise the MVTS to MVTS transfer and thus cannot monitor for transparency or for underlying money laundering/terrorist financing risks

2. Intermediary FIs

The Intermediary FI is responsible for:

- passing on complete information that is received within payment messages to the next FI in the payment chain
- retaining a record of all the information received from the Originating FI or the Intermediary FI immediately upstream in the payment chain
- monitoring for compliance with FATF Recommendation 16 and implementing relevant regulation and
- risk based policies and procedures to determine when to execute, reject or suspend a payment and appropriate escalation.

3. Beneficiary FIs

The Beneficiary FI is responsible for:

- the verification, identification and due diligence of its customer (the beneficiary party), as well as related record keeping
- monitoring for compliance with FATF Recommendation 16 and implementing relevant regulations and
- risk based policies and procedures to determine when to when to execute, reject or suspend a payment and appropriate escalation.

[14] FATF (2016), Guidance for a Risk-Based Approach for Money or Value Transfer Services, FATF, Paris www.fatf-gafi.org/publications/fatfrecommendations/documents/rba-money-or-value-transfer.html

4. Addressing current limitations

Limitations across commonly used infrastructure such as SWIFT and National Payment Systems can result in a lack of sufficient capacity in certain payment message fields to transmit all the information set out in these Standards. In the event that the infrastructure does not support the passing of all information, for example when fields are absent, lack sufficient space, or where the information cannot be passed due to payments moving from cross border to domestic infrastructures (or domestic infrastructures to cross border), the FI should retain this information (for the periods specified under applicable law) and make it available on request from other FIs in the payment chain.

All FIs in the payment chain should set out in their policies the priorities for the information that is transmitted as part of the payment instruction when acting as originating or intermediary FI. This should be guided by how that information is commonly used in the industry:

- Name and address information is used for screening and monitoring purposes both in real time and post transaction. Both must be provided, which may result in truncation of both or either
- Country information is particularly important in this regard specifically for risk, sanctions and AML/CTF screening and monitoring processes

Recognising that certain payments infrastructures may limit the amount of information that can be included, the following is recommended:

- The name of the primary account holder should be provided in full before secondary account holder information is provided. Further, family name should receive priority over given names
- Address information should be provided to the fullest extent possible. Country should receive priority, followed by City, State/Province/Municipality, Street Name, Building Number or Building Name and Postal Code in accordance with the resident country conventions. Transmitting full name and address for the primary account holder should be prioritised over transmitting the names of all account holders in situations where name and address fields are not interchangeable
- For OBO payments, the Wolfsberg Group notes the current limitations within the SWIFT and other national payment infrastructure formats that may prevent including both customer (Originator) as well as ultimate originator information in full. The standards set out above recognise this existing limitation and the need for FIs to set out the approach they will take in their policy. It is important to note that this flexibility should not undermine the transparency of originator information sought by FATF Recommendation 16 and regulations of all the applicable jurisdictions of the FI
- Where the payments systems/infrastructure provides for a structured format to be used which aids in the collection of information (like country), this should be the preferred format for the Originating FI

<u>Related Market Guidance</u>

The Wolfsberg Group recognises and endorses the work of the SWIFT Payments Market Practice Group (PMPG) in relation to the practical compliance with these Standards, as below:

- Market practice guidelines to comply with FATF Recommendation 16[15]
- MT202COV guidance[16]

[15]https://www.swift.com/about-us/community/swift-advisory-groups/payments-market-practice-group
[16] https://www.swift.com/node/8426

The Use of LEI in Payments

In September 2016, the PMPG initiated an industry dialogue on the use of the Legal Entity Identifier (LEI)[17] in payment messages. The Wolfsberg Group supports further discussion on the benefits of including LEI within payment messages, particularly with respect to how this might be implemented and whether the potential benefits are sufficient to justify the investment that would be required to include the LEI in legacy payment message Infrastructures. Wide adoption of LEIs might support more rapid elimination of false positive alerts generated by commonly deployed screening and monitoring systems for sanctions and AML purposes, while ensuring more efficient payment processing through the provision of certainty of identity. While the existing adoption of LEI by large corporates may solve for a growing percentage of cross-border payments by value, in order to address transparency comprehensively the LEI initiative would need wider adoption by Small and Medium Enterprises and other legal entities. Furthermore, a comparable solution for Individuals would be required.

[17] The Legal Entity Identifier (LEI) is a 20-digit, alpha-numeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO). It connects to key reference information that enables clear and unique identification of legal entities participating in financial transactions. For more information: https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei