Lyddon
CONSULTING SERVICES LTD
07939 132341
enquiries@lyddonconsulting.com
www.lyddonconsulting.com

WOLFSBERG GROUP 2017 PAYMENT TRANSPARENCY STANDARDS - "ON BEHALF OF" PAYMENTS AND RECEIPTS, AND THE VIRTUAL ACCOUNTS ESTABLISHED TO MAKE AND RECEIVE THEM

4th June 2018

Preface

This paper calls for the section in the Wolfsberg Group's Payment Transparency Standards 2017 on "On behalf of" payments to be completed as regards payments, and to be extended to have a section on receipts, which are not addressed at all.

It also asks that Wolfsberg Group confirm explicitly that any financial institution that issues unique banking details associated in its own records with a specific legal person is an Account Servicing Institution for that legal person and must have a compliant Customer Due Diligence file on the legal person.

There is a need for industry-wide clarity around "On behalf of" payments and receipts, and on the closely-related topic of Virtual Accounts. This clarity is absent from the section on this topic in Wolfsberg Group's 2017 Payment Transparency Standards, which is curious because the Wolfsberg Group members count in their number several of the main proponents of the usage of Virtual Accounts.

About the author

Bob Lyddon is an experienced management consultant both privately and with PwC in the fields of international banking, payments and cash management. Between 2003 and 2017 he was engaged as General Secretary of the IBOS international banking club. With PwC between 1997 and 2000 Bob managed several programmes at the time of the initial introduction of the Euro, and while at BankBoston between 1994 and 1997 Bob designed and brought to market the Connector international banking club. Bob's earlier career was spent at Chemical Bank/Manufacturers Hanover and Lloyds Bank International in international capital markets, big-ticket export finance, and aircraft finance.

Bob has written a series of online courses on Cash Management, Trade Finance and Corporate Treasury, as well as delivering such courses in person. Bob has acted an expert witness in connection with cross-border payments, and is a retained consultant to trade bodies in this same field.

Bob Lyddon holds a First Class degree in Modern Languages from the University of Cambridge.

Problem statement

Virtual Accounts – for making and receiving "On behalf of" payments – have become common in the corporate world where a Shared Service Centre operates both its own "real" accounts and the Virtual Accounts for group companies that are associated with them.

In the cases of both payment and receipt messages there is a specific risk of non-compliance with implementations of FATF Recommendation 16 – such as EU Regulation 2015/847 of 20 May 2015 on information accompanying transfers of funds - because messages may not contain the details of both (i) the party that owns the real account that funds are debited or credited to; and (ii) the party that has entered into the contract for the supply of goods/services that the payment or receipt relates to, and "on whose behalf" the payment or receipt is being made or received.

Contrary to the inference of the Wolfsberg Payment Transparency Standards, though, it is not the details of Party (ii) – the "On behalf of" party – whose details are normally missing, but the details of Party (i) - the owner of the real account at the start or end of the payment chain.

There are two other major problems with the Wolfsberg standards:

1. The standards infer that the real account sits in front of the virtual, or "On behalf of", account towards the outside world, but in fact it is normally the virtual account that is presented to trading counterparties, and the real account that is invisible to them;
2. These structures are principally used for receipts rather than for payments, such that the Wolfsberg standards are completely missing this side of it.

Virtual Accounts involve a bank issuing unique banking details to a specific legal person on the corporate side – and it is not the Shared Service Centre. In the bank's books the banking details are linked to records in which the name of this specific legal person is visible.

The bank is also aware that the specific legal person will use the banking details in their dealings with third-parties and will hold out to those third-parties that the financial institution identifiable through the banking details is their Account Servicing Institution or "ASI".

These circumstances make that bank an Account Servicing Institution to that specific legal person, and compel the ASI to carry out Customer Due Diligence on the specific legal person as laid down in applicable AML/CFT regulations.

This seems to be an obvious truth, but it is not adhered to in "On behalf of" structures, and so it is vital that Wolfsberg Group explicitly confirm the obvious.

Wolfsberg standards on "On behalf of" or "OBO" payments
The document which this paper comments on is the one entitled "Wolfsberg Payment Transparency Standards October 2017" and can be downloaded from this webpage: https://www.wolfsberg-principles.com/publications/wolfsberg-standards

The relevant section is on page 5 and is quoted in full below:

"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)"

The other documents referred to are:

- EU Regulation 2015/847 of 20 May 2015 on information accompanying transfers of funds: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R0847

- EU Directive 2007/64/EC, referred to solely for its definitions in Article 4 that are referred to in EU Regulation 2015/847: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007L0064&from=EN

Use case that is the focus of this paper

This paper concentrates solely on one of Wolfsberg's customer situations where OBO ("On behalf of") is used – the one where a centralised organisation for a multinational is managing the payments, accounting and reconciliation for companies belonging to the same group. The centralised entity may go by the name of "Payment Factory", or "Payment and Collection Factory", but in this paper we use the term "Shared Service Centre" abbreviated to "SSC".

As stated before, the subject is highly connected with so-called Virtual Accounts since the SSC only wants to have one set of real bank accounts with one ASI ("Account Servicing Institution" or bank), and preferably in one banking location only. The SSC's accounts are the real accounts, the balances on those accounts appear on the bank's and on the customer's balance sheets, and the SSC takes its statements and audit confirmation on these real accounts.

The group's Operating Companies – "OpCos" – are the OBO parties and have Virtual Accounts, which they use for their day-to-day payment operations. Indeed, the OpCo does not perform these operations itself: they are all transacted on its behalf by the SSC. The OpCo has no balance at the bank – the bank only recognises the SSC as a customer towards whom it has either an asset or liability.

This structure spares the complex sweeping and pooling arrangements, whose aim is to consolidate original balances from a set of individual "real" bank accounts held in various countries, currencies, banks and in the OpCo legal entity names, into just one bank account balance per currency, and possibly one single position in one currency.

The provision of an OBO structure has become a prime area of competition between banks in International Corporate Cash Management, and the Wolfsberg members count amongst their number several of the prime players in this market space.

If all the OpCos are in one country and have the same country of incorporation as the SSC, then the Virtual Account bank details follow the same convention as the details of the "real" account, and they are all identifiable to the same banking entity. This is the traditional application of OBO payments/receipts, where a firm – normally a professional services firm - holds one external bank account and then wants a service to break out the transactions going over it into internal accounts for the business of its individual clients.

This is not new and is common in the world of investment management, lawyers, indeed any entity that is holding client funds. Critically the client does not then use its "virtual account" for their own day-to-day expenditure, to pay their bills, to receive their salary as if it were a real account.

But this is not the normal configuration in the corporate world, because the OpCos have multiple countries of incorporation, and the OpCos want to look as if they have a local bank account with unique bank details, and held with a local banking entity. Under the multinational structure of Virtual Accounts, the OpCos do use their "account" for all their payment needs as if it were a real account, which, to all intents and purposes, it is.

Customer Service Proposition enabled by Virtual Accounts

We will exemplify the configuration using a putative "Security Home And Mortgage Trust Bank", in Europe, as the lead bank to the SSC and the co-ordinator of the scheme for the multinational client.

This bank, let's call it SHAM for short, has a few of its own branches and subsidiaries, supplemented by many partner bank arrangements, to cover off all the countries in the region.

Virtual Accounts is a pivotal part of their customer service proposition for multinationals:

- Only one set of Account Opening papers needs to be signed by the customer – SHAM's and only for their London branch
- Only one entity on the customer side needs to sign them: the SSC
- Quick to set up: a month from start-to-finish, compared to 12 weeks at best for real accounts in various banks
- "Real" accounts are all at SHAM and in their London branch: these are the accounts the customer reconciles and on which they get their statements and audit confirmation
- One place of relationship management and customer service – SHAM from a European centralised site, for argument's sake based in the UK in Hayes in south east London

The SSC has its real accounts, all identifiable to SHAM London branch through BBAN and local Bank Routing Code, and through IBAN and BIC (which could be SHAMGB2L).

The "OBO" parties – the OpCos whose financial business has been centralised into the SSC – need accounts in-country, normally in their country of incorporation:

- UK-registered OpCos will have their Virtual Accounts established at SHAM London branch as well;
- Non-UK OpCos will have their Virtual Accounts established at SHAM's European branches and subsidiaries where they have them, or at partner banks of SHAM in countries without a local SHAM banking entity.

Important benefits for the customer of the set-up focussed on SHAM London are:

- No need for the SSC to pass AML/CFT compliance of local banks
- No need to produce any Account Opening papers on the OpCos for either SHAM or its branches, subsidiaries or partner banks
- No need to interact at all with any bank except SHAM, London branch
- All statements can be supplied via file download in Edifact Bansta, or ANSI, or ISO20022 through a SHAM-supplied eBanking channel
- All payment orders can be submitted through a SHAM-supplied eBanking channel
- Bank account mandates – which only exist at SHAM London branch – can be operated via eBAM

How Single Euro Payments Area ("SEPA") supports a Shared Service Centre

SEPA is an enabler for the SSC to have one "real" account in EUR at one bank in the SEPA Area, and to make and receive EUR payments for the OpCos through it. This is enabled in the SEPA payment schemes, but in few other payment schemes, because the payment message format used does not always contain fields for both the holder of the real account and the "OBO" party.

The ISO20022 XML data format is used in SEPA, and there are fields for the "OBO" parties – known in SEPA as the Ultimate Debtor/Ultimate Creditor - so in principle the fields can be completed as the case demands:

- For payments away by credit transfer, the debit party is the SSC and Ultimate Debtor is quoted as the OpCo
- For collections through the direct debit scheme, the credit party is the SSC and the Ultimate Creditor is the OpCo
- For payments away through the direct debit scheme, the debit party is again the SSC and the Ultimate Debtor is the OpCo (although multinationals rarely act as the Debtor in the direct debit scheme)

More difficult is where an OpCo sends an invoice to its trading counterparty and requests payment by SEPA credit transfer:

- The OpCo should quote its bank details on its invoice as the SSC's account
- It then asks that it itself be quoted as Ultimate Creditor either by name or by a numerical identifier – which could be an IBAN
- It relies on its counterparty to insert the Ultimate Creditor details in the SEPA Credit Transfer
- In doing that it relies on the counterparty's bank to supply the counterparty with an eBanking system that enables the Ultimate Creditor details to be inserted…
- .. and it relies on the counterparty's bank and all intermediary clearing systems to pass that information through, and then on its own bank to show it

The usage of the approach based on Ultimate Debtor/Ultimate Creditor can stumble on this simple problem of relying on commercial counterparties and their banks to accommodate the full details in their credit transfers, failing which the SSC will have credit entries on its bank statement that it will not be able to apply.

However, while SEPA stands as an enabler for a compliant manner of using an SSC and showing both the SSC and the OpCo in the payment message, in practice this is not the way the service is set up and operated, either for SEPA or non-SEPA payments in EUR, or for payments inside, outside and one-leg-in the SEPA Area.

Market practice – not least as operated by Wolfsberg members themselves - renders the Wolfsberg OBO guidance on **payments away** at best **partial**, and it is **absent** as regards **receipts**.

Furthermore, the service as implemented hinges on **financial institutions** issuing unique bank details for OpCos that are identifiable to themselves, but the same financial institutions do not then draw the obvious conclusion that they are acting as **Account Servicing Institution** for the legal person with whom they associate the bank details.

OpCo operational requirements

The OpCos' requirement is to be able to put simple bank details on their invoices and preferably just an IBAN. At most it would be numeric domestic bank details like UK details.

The OpCos do not want to mention the SSC at all in their invoices, so as not to complicate the payment instructions and also so as to have their payments and receipts treated as local payments from the point of view of their trading counterparties and the banks in the payment chain.

The OpCos want to look as though they have a local ASI and banking connection, and to have the numbers and codes to go with it, and if they can do their payments and receipts just with IBAN, all the better. Even better still where the identity of the ASI is disguised as numeric characters and does not have the name of the ASI visible in it e.g. the UK IBANs all have an abbreviated name of the bank visible in them, whereas most other countries have IBANs composed entirely of numeric characters after the initial alpha country code.

What is driving this is a residual corporate reluctance – despite SEPA and despite various EU Directives and Regulations – to ask their trading counterparties to make cross-border payments or to cause their counterparties to receive them.

Multinationals usually trade with their counterparties out of a legal entity incorporated in the same country as the counterparty i.e. the OpCo is a resident entity of the same country as that OpCo's trading counterparties.

There are for sure business models where this is not the case, and where the OpCo is a non-resident towards its trading counterparties, but the normal modus operandi is to have resident OpCos.

Then the requirement is to have bank accounts that are:

- Established in the same country and currency
- Accessible through the local low-value payment clearing – so as to pay low or no payment fees
- Enabling payments to be made resident-to-resident, in local currency, and without the money crossing a national border
- Permitting the avoidance of the bureaucracy of Central Bank statistical reporting
- Mitigating or avoiding cross-border payment fees (aka lifting fees, per mille fees, cartel fees) which can be as high as 0.15% flat with a high minimum like EUR25

Multinationals will also use the structure, with care, where their OpCo is a non-resident: their counterparties will still be paying to or receiving from a non-resident's account in local currency and in the same country, but the multinational wants to avoid that their trading counterparty experience the charges, delay and bureaucracy that can come with cross-border payments. The multinational will want to eliminate or at least minimise the chance that the counterparty's bank has the right to impose these detriments – and of course the multinational does not want to experience such detriments itself.

Banking structure to meet OpCo operational requirements
The multinational wants to have access to local low-value payment clearings in each country where an OpCo is established, but does not want to run bank relationships with a bank in each one, or even – where they have 50 OpCos – to have relationships with 10 banks who each cover 5 countries.

That degree of multibanking brings with it:

- Different paperwork and AML/CFT compliance requirements
- Having to use different eBanking services, each with their own tokens and security set-ups
- Timezone, language issues etc.

The solution is to have Virtual Accounts that look to a trading counterparty like a local bank connection, so payments can be made and received through local low-value clearings, resident-to-resident, in local currency, and without the money crossing a national border.

The payments look towards trading counterparties as if a local bank is acting as ASI to the respective OpCo but the "account" established there is virtual, despite its having banking details constituted the same as a real account.

These are major drivers and remain so even where there is no Central Bank statistical reporting any longer and where measures like Payment Services Directive have reduced cross-border payment fees.

Virtual Accounts – account structure
Virtual Accounts are offered both by banks with their own networks of branches and subsidiaries, and by banks who supplement their own networks with partner banks. We use our putative SHAM bank as the test case because it has a few branches and subsidiaries of its own, and relies heavily on partner banks i.e. on banks that have no shareholding connection with SHAM.

The essence is that SSC maintains a set of "real" accounts – one per currency - with the bank at its main location e.g. SHAM London. The SSC's accounts will have numbering that is associated with the UK and with SHAM. The bank's ledger only reflects the balances on the SSC's accounts.

The OpCos get virtual accounts in every currency and country they need them. These accounts are numbered according to the conventions prevailing in the country of the account's domiciliation, and will be associated – however opaquely – with:

- The branch or subsidiary bank in that country of the main bank SHAM; or
- The partner bank in that country of the main bank.

Payments in and out of the virtual accounts go in and out in local currency, through local clearings and never cross-border.

The Virtual Account is actually a dedicated sub-account of a nostro account of SHAM London, held at its branch or subsidiary, or at the partner. Payments are debited and receipts credited to this OpCo-specific sub-account of SHAM's nostro. The OpCo's name is visible in the title of the dedicated sub-account.

SHAM's nostro account is not "swept" to the SHAM London. Instead and three or four times a day every entry on the nostro account and its sub-accounts is copied over to a database at SHAM London:

- The balance of receipts and payments increases or reduces the balance on the SSC's account at the main bank;
- Every debit and credit on the virtual account is passed across the SSC's account in the same currency;
- Each entry is also reflected in a statement of each virtual account;
- This statement of the virtual account is produced by the main bank for information only because it does not reflect a claim by/on the OpCo on/by the bank;
- However it is a precise replica of the entries over the virtual account of the same OpCo at the local bank, and so the SSC can use it to post up and reconcile the intercompany accounts it runs between itself and each OpCo;
- The SSC's processing ends up by identifying the balances owed between the SSC and each OpCo, and these then become intercompany loans between the SSC and the OpCo, or else are taken over by an in-house bank that steps into the shoes of the SSC.

The SSC receives one set of statements for itself, on the "real" accounts: these reflect what is on SHAM's balance sheet.

The SSC also receives a stream of statements relating to the OpCos – one on each virtual account. These will be marked by SHAM with a banner with wording along the lines of "For information only – not a record of dealings between SHAM and the OpCo".

Both sets of statements are produced by the main bank and formatted in the same way for ease of processing, but the statements on the virtual accounts are positioned as not being a reflection of banking dealings between the SSC and SHAM, or indeed between any bank and either the SSC or the OpCos, but as dealings between the SSC and the OpCos.

The SSC receives no statements from the local banks.

This perfectly meets the customer's requirements:

- Easy reconciliation as all statements are sent in the same data format;
- Only one account balance per currency at the main bank and on the company's balance sheet;
- Assets and liabilities between SSC and OpCos are made completely transparent;
- No local accounts to manage;
- Billing only comes from the main bank;
- Bank mandates exist only at the main bank;
- The main bank has access to all the debits and credits over all the "real" and "virtual" accounts;
- Single point of customer service.

Virtual Accounts – account numbering

The account numbering must accord with the key representation being made in an OBO structure towards third-parties: that each OpCo has a local bank account.

The key determinant of the representation being made is what the customers put on their invoices, and this is taken to be local banking details and nothing else. A putative relationship between SHAM as main bank and BankAustria as SHAM's partner for Central and Eastern Europe, and with Svenska Handelsbanken doing the same for the Nordics would lead to the scenario set out below.

A putative OpCo called Welch Paper (Austria) GmbH, with its virtual account identifiable to BankAustria, will put on its invoices its own name and the Austrian virtual account details, which are unique to it, and are not the same as the details of SHAM's nostro at that same bank.

The invoice will give no indication of the existence of:

- SHAM, either in London or Austria
- The putative Welch Paper Payments (Europe) B.V., the SSC that has the real account and at SHAM London
- The bank details of the real account, either the UK sort code + account number version or the IBAN only or IBAN+BIC versions

This achieves the desired objectives of the scheme in countries where domestic payments can be transacted based on:

- BBAN-based bank details that are all numeric;
- IBAN-only where the IBAN layout for that country, after the initial two letters, consists entirely of numeric characters i.e. this applies to anywhere in the Eurozone.

The identity of the IBAN's issuing bank can then be made opaque to the counterparties of Welch Paper. It is opaque but not unobtainable: they would need a look-up table, and it would then be obvious from that look-up table who the Virtual Account partner was.

So Welch Paper subsidiaries could be issued with IBANs on their Virtual Accounts like:

Country	Example IBAN
Denmark	DK50 0040 0440 1162 43
Finland	FI21 1234 5600 0007 85
Austria	AT61 1904 3002 3457 3201
Czech Republic	CZ65 0800 0000 1920 0014 5399
Slovakia	SK31 1200 0000 1987 4263 7541
Hungary	HU42 1177 3016 1111 1018 0000 0000

It becomes more difficult if BIC has to be used as well as IBAN because the Welch Paper OpCos would not want the BICs to be showing on their invoices:

Country	BIC
Denmark	HANDDKKK
Finland	HANDFIHH
Austria	BKAUATWW
Czech Republic	BACXCCZPP
Slovakia	UNCRSKBX
Hungary	BACXHUHB

Then it becomes obvious who their ASI is supposed to be.

The naming of the Virtual Account must contain the respective OpCo, even if the naming is complex in the partner's books, such as "SHAM London ref Welch Paper Payments (Europe) BV ref Welch Paper (Austria) GmbH".

SHAM's ledger would show "BankAustria Vienna ref Welch Paper Payments (Europe) BV ref Welch Paper (Austria) GmbH" and a contra of "Welch Paper Payments (Europe) BV ref Welch Paper (Austria) GmbH".

Whatever the accounting and naming are inside the banks, Welch Paper (Austria) GmbH puts only its name on its invoice, together with its numeric Virtual Account details, IBAN only or BBAN+domestic routing code and never IBAN+BIC.

The vital point as regards the AML/CFT obligations of BankAustria in this case is that the name of the OpCo appears in its records and uniquely associated with the banking details: no other OpCo shares the banking details associated in BankAustria's books with "SHAM London ref Welch Paper Payments (Europe) BV ref Welch Paper (Austria) GmbH".

The details will be uniquely issued to the respective OpCo and be identifiable to that bank, even if a consumer or business customer will not know this straightaway but have to refer to a look-up table to identify which bank is being represented by the respective OpCo to be its ASI.

Bank details as they drive the payment routing

Virtual Accounts can be directly addressable in EUR in the SEPA Area because of IBAN. The first two letters of the IBAN show which country's conventions on IBAN formatting apply.

Then the payment can be routed through SEPA clearings based on the subset of the subsequent numeric digits that indicate which bank is the ASI. Tables in clearing systems act on these digits to ensure the payment reaches the ASI that the IBAN is identifiable to.

Outside the SEPA Area and/or for non-euro payments within the SEPA Area, it would ideally be possible to issue unique bank details for the OpCos which do not obviously identify the bank the account is supposed to be with, in the form of a BBAN and a Bank Routing Code.

In the UK the sort code is the Bank Routing Code, and the clearing system tables ensure the payment is routed there, at which point the bank associated with that sort code credits the payment to the account associated with the BBAN.

Whether it is IBAN-only for Euro payments within the SEPA Area, or BBAN+BRC elsewhere, neither the sending bank nor the clearing system performs a check as to the status of the beneficiary account: that is the sole responsibility of the receiving bank identified in the IBAN or the BRC.

If the account does not exist or is blocked or meets other set criteria, there are agreed routines for rejecting/returning payments. In this case the beneficiary account is open to receive payments.

The appearance given to the OpCos' trading counterparties in each country is that a local bank account is maintained in the OpCo's name and identifiable – albeit with reference to routing tables – to a specific ASI in that country.

So what's the problem?
The first problem lies in the payment messages, and within a structure where the main bank is our putative SHAM London branch, and the banks servicing the OBO parties are its non-UK branches and subsidiaries, and partner banks.

The Wolfsberg guidance infers that payments are made from and to the SSC's accounts towards clearing systems, other banks and trading counterparties, and that the SSC then in turn debits or credits the payments to OBO accounts.

This is not the actual configuration: instead the payments run – towards clearing systems, other banks and trading counterparties – out of and into OBO accounts established as Virtual Accounts, and the arrangements put in place between SHAM and its non-UK branches, subsidiaries and partners result in the money coming to reside in the real account of the SSC and the correct debit/credit entries being made by the SSC on internal accounts for the OBO parties.

The OBO accounts sit in front of the SSC accounts in the appearance given to third-parties, not behind them, as the Wolfsberg guidance infers.

As a result the OBO account is not the end of the payment chain, neither for a payment nor for a receipt: the end of the payment chain is the SSC's account.

The SSC's account is thus absent from payment messages and this is a breach of applicable AML/CFT regulations.

The second problem is in the degree of AML/CFT compliance work performed on the OpCos by both the main bank and by the local banks identifiable as acting as ASIs for the OpCos, given what the OpCos put on their invoices.

Please note again that the OpCos only put on their invoices the unique local bank account details formatted to local conventions, which in many cases will be a numeric IBAN.

There is no mention on the OpCos' invoices that the account is virtual, and there is no mention of the SSC or of the main bank.

It is taken as read that the Virtual Account IBANs/unique local bank details are formatted according to the rules of the country of incorporation of the Virtual Account holder, and can then be used in local payment traffic and without mentioning the SSC.

The existence of a "real" **in-country** account in the OpCo's name is thereby implied to other parties in the payment chain – and by extension is implied also to authorities over consumer protection, bank licensing and financial crime.

Those other direct and indirect parties to the payment have a right to assume that there is a Customer Due Diligence file on the Virtual Account holder, and held at the in-country bank that the IBAN/local bank details are identifiable to.

A file on the OpCo held at the main bank - i.e. at the SSC's bank – is not the same thing:

- The SSC's bank is in a different country
- The Virtual Account bank may not even be a branch of the SSC's bank. It could be:
    - A subsidiary and not necessarily a direct one of the main bank
    - An unrelated partner bank contracted by the main bank

Would there be a file on the OpCo even at the main bank? Why should there be when the OpCo has no asset or liability towards the main bank?

The prevailing practice appears to be that there is no Customer Due Diligence file on the OpCo:

- Either at the in-country branch, subsidiary or partner, because the OpCo has a Virtual Account and not a real one, and anyway its account is virtual and is a sub-account of a SHAM nostro;
- Or at the main bank, because the OpCo has no account at the main bank, real or virtual.

Operational set-up

The key point is that the OBO accounts sit in front of the SSC accounts in the appearance given to third-parties, not behind them, as the Wolfsberg guidance infers.

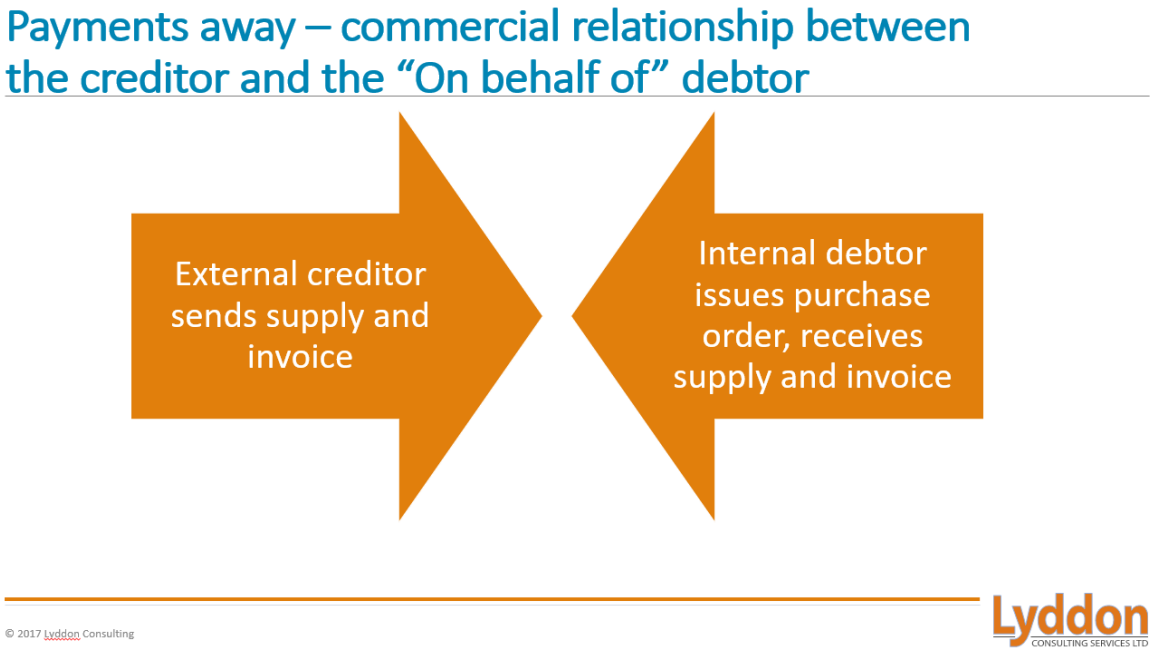
We can walk through the operational flows for both a payment away on behalf of an OpCo as a debtor, and a receipt on behalf of an OpCo as a creditor, and in six steps for each side:

1. Commercial relationship between the OpCo and its trading counterparty;
2. Bank details;
3. Message flow;
4. Which banks are involved;
5. What the payment chain is in substance;
6. What the payment chain is in appearance.

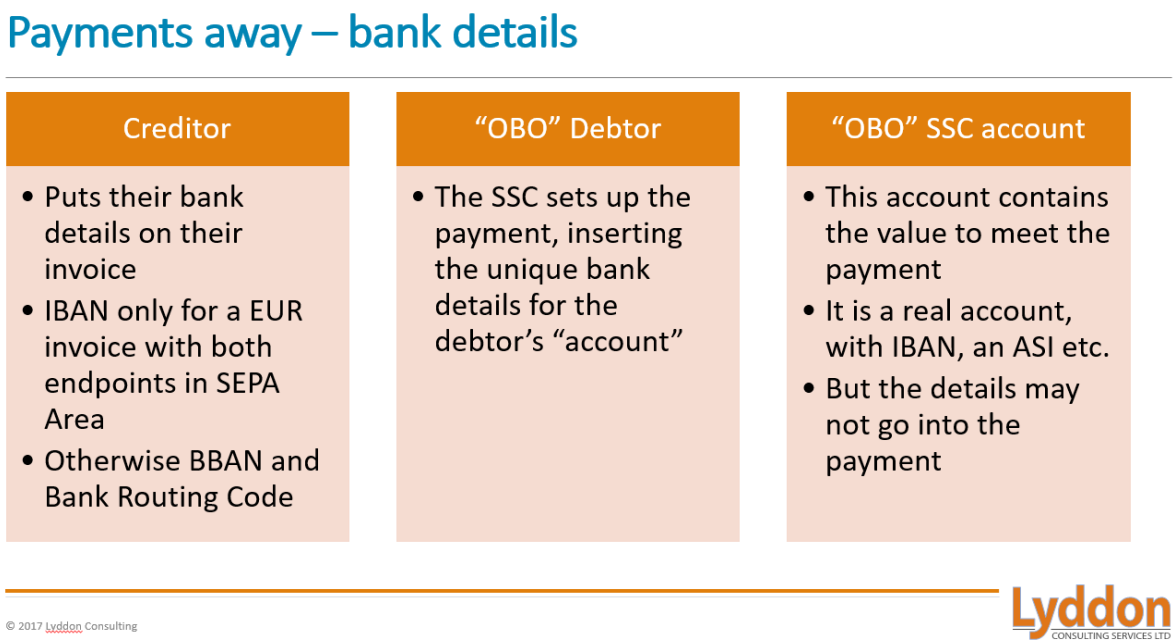
Payments away "on behalf of" an OpCo

The basis is a purchase of goods or services by the OpCo from a third-party creditor, the OpCo then becoming the "On behalf of" debtor.

The debtor issues a purchase order, the creditor supplies and invoices against it, and the "On behalf of" debtor receives and processes the supply and the invoice:

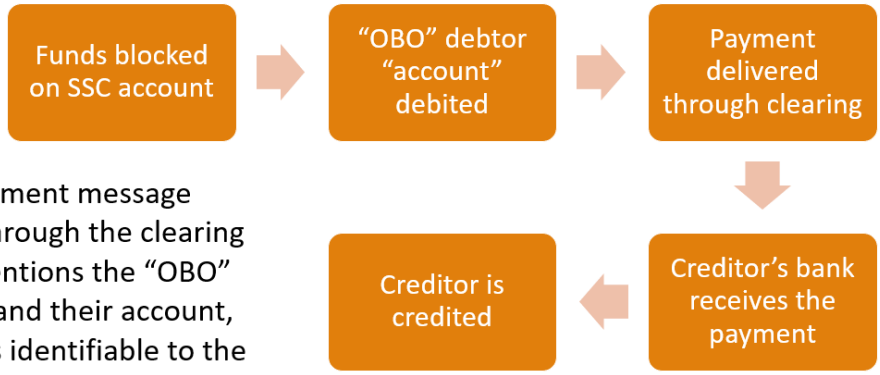


Then the payment has to be set up with the relevant banking details:



The flow of the payment is as follows, the key point being that the payment message does not mention the SSC or its bank details:

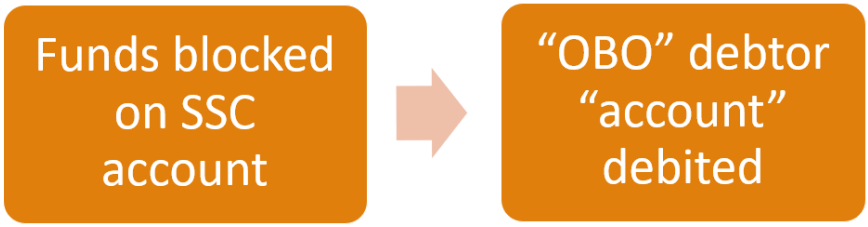
Payments away – flow



The payment message going through the clearing only mentions the "OBO" debtor and their account, which is identifiable to the bank that delivers the payment into the clearing

In the multi-country set-up for multinationals, the SSC's bank and the ASI identifiable from the bank details of the "On behalf of" debtor are different, and in different countries. The "On behalf of" debtor's account is actually a sub-account of nostro of the SSC's bank:

Payments away – which banks are involved

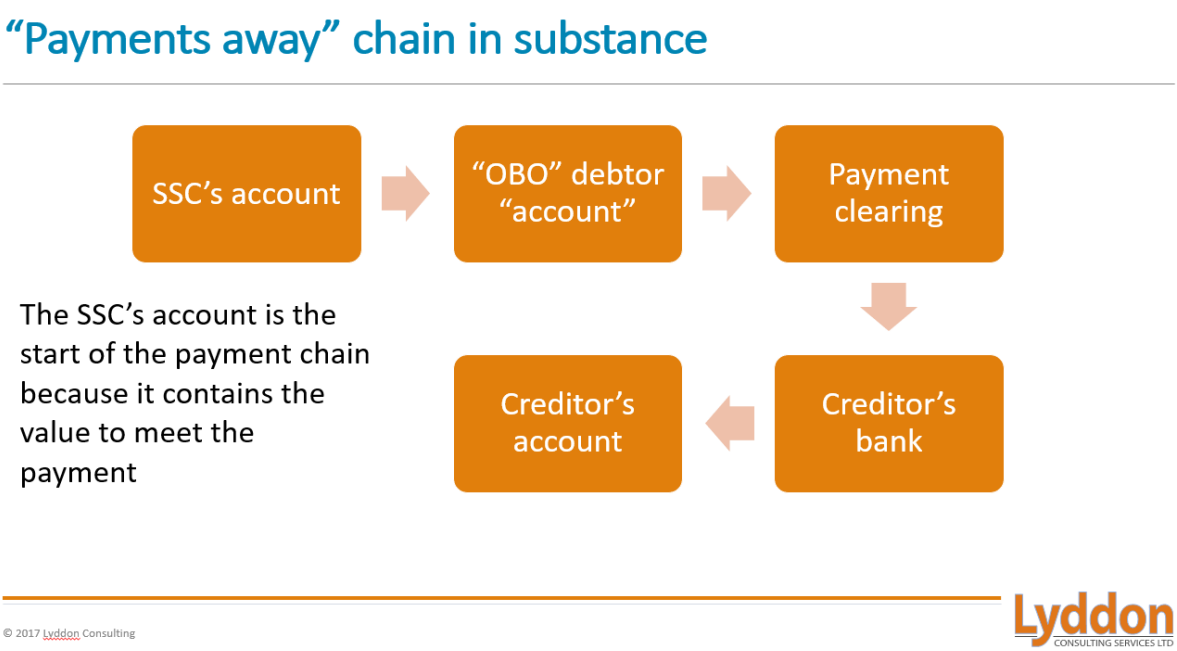


These could be different banks:

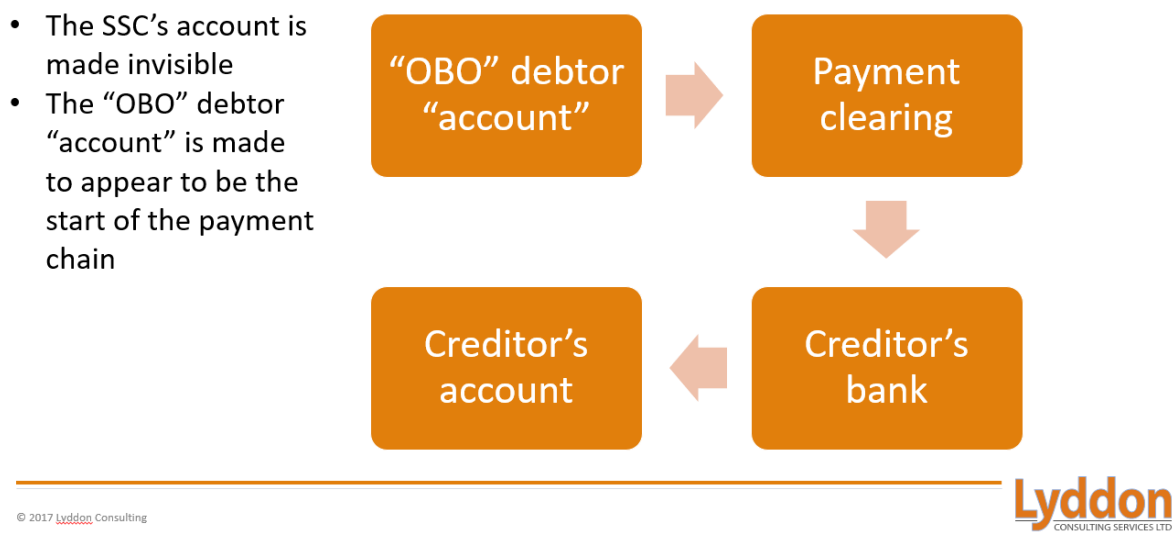
- The SSC's real account at one ASI
- The debtor's "account" at a different ASI, established as a sub-account of a nostro account of the first ASI

Length of the "Payments away" payment chain
The length of the payment chain is thus different in substance from the way it is made to appear in the payment message.

The substance is that the SSC's account is the start of the payment chain:



The payment message, however, infers that the "OBO" debtor "account" is the start of the payment chain:



Receipts "on behalf of" an OpCo

The basis is a sale of goods or services by the OpCo to a third-party debtor, the OpCo then becoming the "On behalf of" creditor. The debtor issues a purchase order, the "On behalf of" creditor supplies and invoices against it, and the debtor receives and processes the supply and the invoice:

Receipts – commercial relationship between the debtor and the "On behalf of" creditor

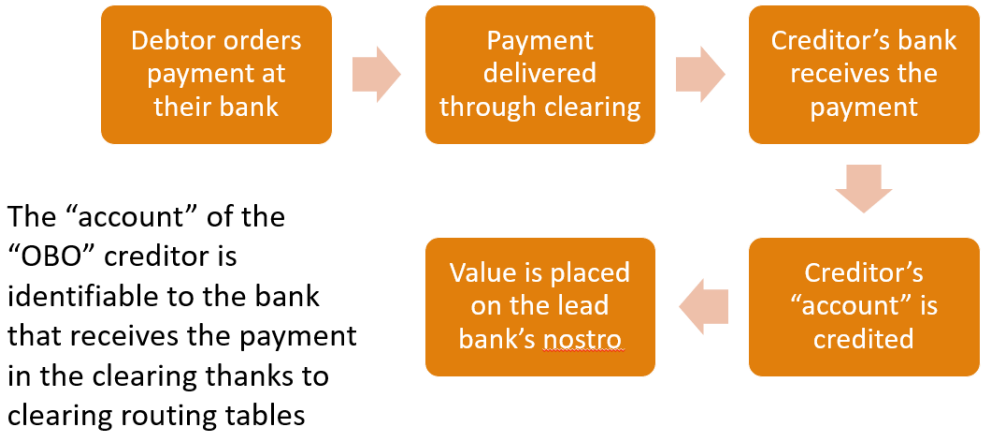
Then the payment has to be set up with the relevant banking details, noting that the "On behalf of" creditor puts only their own bank details on their invoice, not those of the SSC. If the debtor does not even have the SSC's bank details, they cannot include them in the payment, even where the payment message is in ISO20022 with specific fields for the Ultimate Creditor:

Receipts – bank details

"OBO" Creditor	"OBO" SSC account	Debtor's account
• Puts their bank details on their invoice • IBAN only for a EUR invoice with both endpoints in SEPA Area • Otherwise BBAN and Bank Routing Code	• Not visible on the invoice and therefore not on the payment message • The debtor cannot quote what they do not know	• At an ASI and associated with BBAN and Bank Routing Code, and, depending upon location, with IBAN and BIC

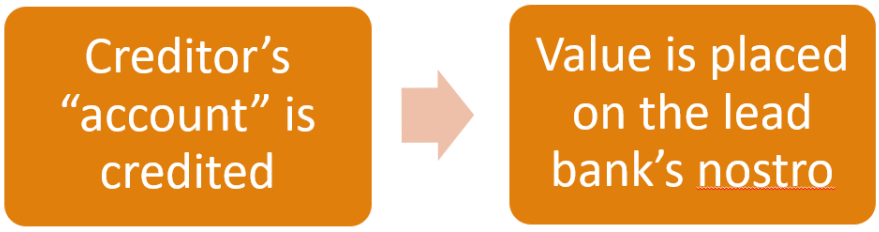
The flow of the payment is as follows, the key point being that the payment message does not mention the SSC or its bank details:

Receipts – flow



In the multi-country set-up for multinationals, the SSC's bank and the ASI identifiable from the bank details of the "On behalf of" creditor are different, and in different countries. The "On behalf of" creditor's account is actually a sub-account of nostro of the SSC's bank:

Receipts – which banks are involved

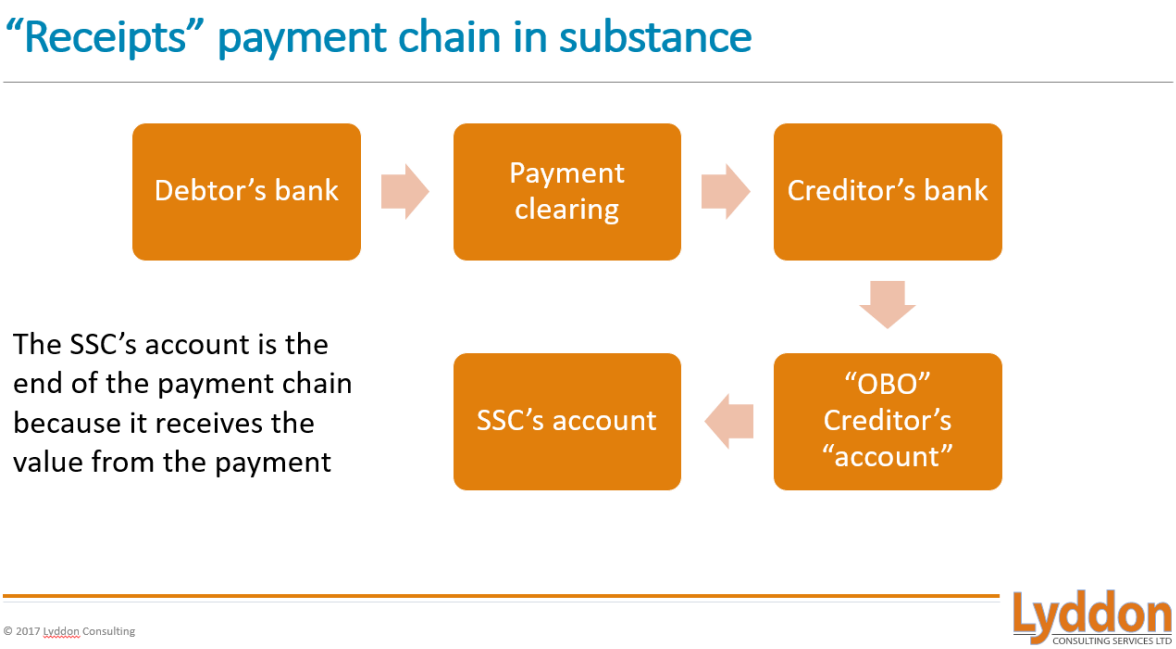


The "account" of the "OBO" creditor is a subaccount of a nostro account owned by ASI of the Shared Service Centre
The in-country ASI places the value onto that nostro and then replicates all the payments to the ASI of the Shared Service Centre, so that the SSC's real account can be posted up with them

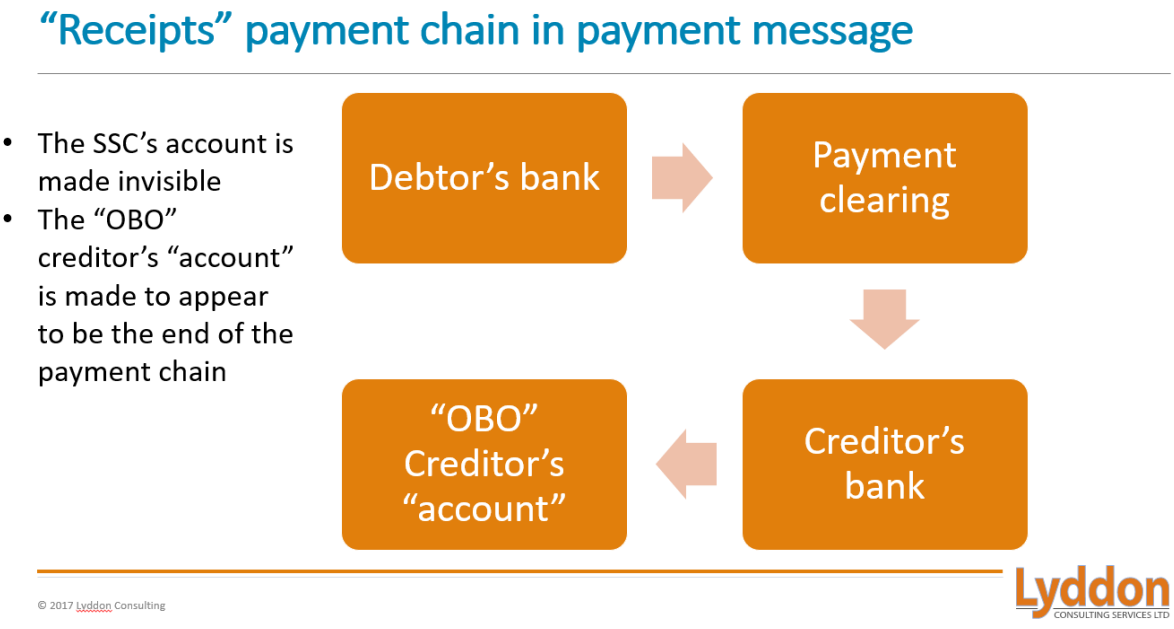
Length of the "Receipts" payment chain

The length of the payment chain is thus different in substance from the way it is made to appear in the payment message.

The substance is that the SSC's account is the end of the payment chain:



The payment message, however, infers that the "OBO" creditor's "account" is the end of the payment chain:



Conflict with EU Regulation 2015/847 on information accompanying transfers of funds
This EU Regulation is an enactment of FATF Recommendation 16 on wire transfers and the revised interpretative note for its implementation and so can be taken as a token for equivalent legislation in non-EU countries. At any rate it applies directly (without the need for transposition into Member State law) in the 28 EU Member States.

The implementation of OBO structures as described above conflicts with/is impacted by the contents of the Regulation in the ways laid out below.

Regulation contents	Conflict/Impact
Preamble (3) no discrimination or discrepancy between, on the one hand, national payments within a Member State and, on the other, cross-border payments between Member States	The Regulation applies equally to domestic payments and cross-border ones, and (see below) to all types of electronic payments, not just "wire transfers" in the sense of high-value payments. SEPA payments and local low-value transfers are within scope.
Preamble (9): It is therefore appropriate, in order to ensure the transmission of information throughout the payment chain, to provide for a system imposing the obligation on payment service providers to accompany transfers of funds with information on the payer and the payee	It has to be "information throughout the payment chain", so the payer and payee are the entities right at each end, and not any entity in between. OBO structures represent that the OBO party, not the SSC, is at the end of the payment chain, and this is incorrect and therefore non-compliant.
Preamble (15): Payment service providers should ensure that the information on the payer and the payee is not missing or incomplete	On the contrary, the payment service providers in OBO structures work individually and in concert to ensure that the information on the SSC – whether it be the payer or payee – is missing, and this is non-compliant.
Preamble (18) and enacted in Art 5: In view of the Union legislative acts in respect of payment services, namely Regulation (EC) No 924/2009 of the European Parliament and of the Council (1), Regulation (EU) No 260/2012 of the European Parliament and of the Council (2) and Directive 2007/64/EC, it should be sufficient to provide that only simplified information accompany transfers of funds within the Union, such as the payment account number(s) or a unique transaction identifier	This is the provision that enables all electronic transfers within the in-scope area to be made using IBAN-only, whether indeed the payment is in Euro or not. The area in which this provision applies is the SEPA Area, not just the EU.
Preamble (21): As regards transfers of funds from a single payer to several payees that are to be sent in batch files containing individual transfers from the Union to outside the Union, provision should be made for such individual transfers to carry only the payment account number of the payer or the unique transaction identifier, as well as complete information on the payee, provided that the batch file contains complete information on the payer that is verified for accuracy and complete information on the payee that is fully traceable	The SSC's payments away will normally be made in batch files. The SSC's identification will be in the batch header, but the OBO payments contained within the batch file will "carry only the payment account number of the payer" meaning the OBO debtor. There is a conflict in that the batch header infers the payer is the SSC – which indeed it is – but the individual payments suppress the identity of the SSC as the payer and construe that the OBO debtor is the payer. The batch file contents are therefore non-compliant because they do not identify the payer.

Regulation contents	Conflict/Impact
Preamble (22): In order to check whether the required information on the payer and the payee accompanies transfers of funds, and to help identify suspicious transactions, the payment service provider of the payee and the intermediary payment service provider should have effective procedures in place in order to detect whether information on the payer and the payee is missing or incomplete. Those procedures should include *ex-post* monitoring or real-time monitoring where appropriate. Competent authorities should ensure that payment service providers include the required transaction information with the wire transfer or related message throughout the payment chain	On the contrary the intermediary payment service provider is working to the lead bank of the SSC as its in-country branch or partner bank, and the essence of the scheme is that this intermediary payment service provider ensures that the information on the payer – the SSC – is missing. This is non-compliant.
Art 3 – Definitions - (3) 'payer' means a person that holds a payment account and allows a transfer of funds from that payment account, or, where there is no payment account, that gives a transfer of funds order	Only the SSC holds a payment account: the transfer of funds under a payment away comes from their account and the SSC gives the transfer of funds order. The OBO debtor "accounts" are not payment accounts, so the identification of the OBO debtor as the payer and not the SSC is non-compliant.
Art 3 – Definitions - (4) 'payee' means a person that is the intended recipient of the transfer of funds	The SSC is the payee because it is the intended recipient of the transfer of funds: the value of the payment goes into their account. So the failure to identify the SSC as the payee on receipts is non-compliant. The non-compliance is not the fault of the bank sending the payment, because their client will not have been given the bank details of the SSC or even been told there is an SSC.
Art 3 – Definitions - (7) 'payment account' means a payment account as defined in point (14) of Article 4 of Directive 2007/64/EC: "Point (14) of Article 4 of Directive 2007/64/EC: 'payment account' means an account held in the name of one or more payment service users which is used for the execution of payment transactions."	See above: the SSC's accounts are payments accounts whereas those of the OBO parties are not. So the failure to identify the SSC is non-compliant.
Art 3 – Definitions - (8) 'funds' means funds as defined in point (15) of Article 4 of Directive 2007/64/EC: "Point (15) of Article 4 of Directive 2007/64/EC 'funds' means banknotes and coins, scriptural money and electronic money as defined in Article 1(3)(b) of Directive 2000/46/EC."	The SSC's account contains funds or an overdraft: scriptural money that is a liability or as asset of a financial institution. The OBO "accounts" do not contain "funds". It is therefore the SSC that is the payer/payee because it has the funds, and the failure to identify the SSC as such is non-compliant.
Art 3 – Definitions - (9) 'transfer of funds' means any transaction at least partially carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider	The SSC's account is the source or the destination of the "transfer of funds". So to identify the OBO debtor/creditor as the payer/payee is non-compliant.

Regulation contents	Conflict/Impact
Art 4 – information accompanying funds transfers - 1.The payment service provider of the payer shall ensure that transfers of funds are accompanied by the following information on the payer: (a) the name of the payer; (b) the payer's payment account number; and (c) the payer's address, official personal document number, customer identification number or date and place of birth	Points (a) and (c) will fall away where the transfer can be done with IBAN-only, and indeed many other national payments either (i) do not contain the name (ii) do not contain address or other details (iii) contain no checks around these details even if they are present (e.g. UK Faster Payments: there is no check that the name on the payment is the same as the name on the account). In addition, the points made above apply again: the payment service providers acting directly and as intermediary for the payer ensure the OBO debtor appears to be the payer, when actually the SSC is the payer, and this is non-compliant.
Art 4 – information accompanying funds transfers - 2.The payment service provider of the payer shall ensure that transfers of funds are accompanied by the following information on the payee: (a) the name of the payee; and (b) the payee's payment account number	The points made above apply again: the payment service providers acting directly and as intermediary for the payer ensure the OBO creditor appears to be the payee, when actually the SSC is the payee, and this is non-compliant.
Art 4 – information accompanying funds transfers - 4.Before transferring funds, the payment service provider of the payer shall verify the accuracy of the information referred to in paragraph 1 on the basis of documents, data or information obtained from a reliable and independent source	Where the payment service provider is the in-country subsidiary, branch or partner bank of the lead bank to the SSC, they will not have any papers on the OBO debtor to check against as they do not recognise it as an account-holder. There is no way then of carrying out this check and this is non-compliant.
Article 7 Detection of missing information on the payer or the payee - 1.The payment service provider of the payee shall implement effective procedures to detect whether the fields relating to the information on the payer and the payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using characters or inputs admissible in accordance with the conventions of that system	Where the payment service provider is the in-country branch, subsidiary or partner bank of the lead bank to the SSC, they will not carry out procedures to find out the SSC details are missing because that is the essence of the scheme, and the result is non-compliance.
Article 7 Detection of missing information on the payer or the payee - 3.In the case of transfers of funds exceeding EUR 1 000, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked, before crediting the payee's payment account or making the funds available to the payee, the payment service provider of the payee shall verify the accuracy of the information on the payee referred to in paragraph 2 of this Article on the basis of documents, data or information obtained from a reliable and independent source, without prejudice to the requirements laid down in Articles 69 and 70 of Directive 2007/64/EC	Where the payment service provider is the in-country branch, subsidiary or partner bank of the lead bank to the SSC, they will not have any papers on the OBO creditor to check against because they do not recognise it as an account-holder, so they will not perform this check. This is not compliant with this regulation and having no CDD file is non-compliant with AML/CFT regulations.

Regulation contents	Conflict/Impact
Article 8 Transfers of funds with missing or incomplete information on the payer or the payee - 1.The payment service provider of the payee shall implement effective risk-based procedures, including procedures based on the risk-sensitive basis referred to in Article 13 of Directive (EU) 2015/849, for determining whether to execute, reject or suspend a transfer of funds lacking the required complete payer and payee information and for taking the appropriate follow-up action	Where the payment service provider is the in-country branch, subsidiary or partner bank of the lead bank to the SSC, they will not carry out these procedures because it is the essence of the scheme that the SSC details as payer/payee are missing, and this is non-compliant.
Article 12 Transfers of funds with missing information on the payer or the payee - 1.The intermediary payment service provider shall establish effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds lacking the required payer and payee information and for taking the appropriate follow up action. 5.6.2015 L 141/11 Official Journal of the European Union EN Where the intermediary payment service provider becomes aware, when receiving transfers of funds, that the information referred to in Article 4(1) or (2), Article 5(1) or Article 6 is missing or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system as referred to in Article 7(1) it shall reject the transfer or ask for the required information on the payer and the payee before or after the transmission of the transfer of funds, on a risk-sensitive basis	An intermediary payment service provider that is the in-country branch, subsidiary or partner bank of the lead bank to the SSC will not do this because it is the essence of the scheme that information on the SSC is missing, and this is non-compliant.

Virtual Account compliance - when is an account not an account?

The question that derives from the non-compliance of the payment messages themselves is what the requisite burden of AML/CFT compliance is on the bank that has issued the virtual account banking details. The structure as described depends upon the bank denying that it is an ASI for the OpCo to which it has issued unique banking details identifiable to itself. This is a clear case of “you cannot have your cake and eat it”.

An Account Servicing Institution Relationship exists when a financial institution issues bank details that uniquely associate a legal person with an account that is in the financial institution’s General Ledger. The financial institution must then have a Customer Due Diligence file on the legal person, compliant with applicable AML/CFT regulations.

It cannot be grounds for denying the existence of an ASI relationship when the line on the Balance Sheet into which the General Ledger account rolls up is inconsistent with the kind of legal person involved - i.e. an ASI relationship does not cease to exist where the “account” is supposedly opened for a corporate entity but it rolls up into the Balance Sheet under “Due to/from other financial institutions” i.e. where the “account” is a sub-account of a nostro.

The first key point is the appearance given to the putative "Man on the Clapham Omnibus" – that these unique bank details are issued to the legal person to use for their day-to-day business, just as they would use a real account. It cannot be a defence for the bank to claim that they issued the details as if they were some kind of internal memorandum account, not realising they would be used towards third-parties.

The second key point is identifiability of the financial institution: the bank details – whether by alpha or by numeric characters – identify the financial institution where the account is domiciled. That financial institution is therefore the Account Servicing Institution for the account and for the legal person associated with the account in its own records.

There cannot be any wiggle room between cases (A) and (B):

A. The financial institution **is** an Account Servicing Institution and issues unique bank details that are (i) identifiable to itself and (ii) associated with the legal person, that it knows will be used by that legal person in their dealings with third-parties. As an Account Servicing Institution, the financial institution must have a Customer Due Diligence file;
B. Alternatively the financial institution **is not** the legal person's ASI, it has no need to have a Customer Due Diligence file, and so it must not issue unique bank details that are (i) identifiable to itself and (ii) useable by a legal person in their dealings with third-parties.

That these are the two black-and-white alternatives is an obvious fact that has so far not been confirmed by Wolfsberg Group, and this is a missing piece in their guidance.

If the intermediary payment service providers – SHAM's branches, subsidiaries and partners - believe they **are not** acting as an ASI for an OpCo, they should not issue unique bank details for that legal person that are associated with an account in their General Ledger. If this is the situation, then the SSC is the payer and payee and should be identified in payment messages as such since the SSC is the end of the payment chain.

If the intermediary payment service providers believe they **are** acting as an ASI for an OpCo – which is inferred by their issuing unique bank details – they should have a Customer Due Diligence file. In this situation the OpCo is the payer or payee and they are the end of the payment chain.

As it is, the payment messages in the structure infer that the OpCo is the end of payment chain – but the bank associated with the OpCo's bank details does not regard the OpCo as a customer and has no Customer Due Diligence file on the OpCo: this is an instance of non-compliance with AML/CFT regulations.

Since the SSC is the only entity on whom a Customer Due Diligence file exists, and at the main bank, it must be the payer/payee. By the same token the institution that has the SSC's accounts - SHAM London in our example – must be the Account With Institution/Beneficiary Institution and must appear as such in all payment messages, with its customer the SSC identified as payer/payee. The absence of payer/payee details of the SSC and the invisibility of SHAM London in the payment messages is an instance of non-compliance with EU Regulation 2015/847 and, by extension, with FTAF Recommendation 16.

Where could this go wrong for the financial institutions involved?

There are clear risks for the financial institutions working together in these structures, in that the AML/CFT procedures may not pick up indicators of financial crime:

1. There would be no 'wet' signature mandate on the OpCos anywhere, so directors, principals and signatories of the OpCos would not be listed out and no identification checks would be carried out on them;
2. PEPs could be involved at the OpCo level (either global PEPS or national level ones) who are not involved at the SSC or parent level. German OpCos in particular have a tendency to take prominent local individuals onto their boards. Such PEPs would not be listed out, or have identification checks made on them;
3. There could be minority interests in OpCos that are not identified;
4. Major customers and major suppliers of each OpCo would not be identified;
5. No KYB would be performed on the OpCo when viewed in isolation from the group;
6. No financial information would be obtained on the OpCo individually.

The AML/CFT checks required by legislation would not be carried out: a process and bureaucratic issue, which does not mean that there is not then a major legal or financial problem.

PEPs, directors, principals, signatories might then actually have unspent criminal convictions, have been bankrupt, or be currently involved in money laundering or in the financing of terrorism.

Likewise customers, suppliers and third-party minority owners – or individuals associated with them – could have in the past been or indeed could currently be involved in money laundering or in the financing of terrorism, or otherwise have negative information against them.

There could also be breaches of company law. The collections made by the OpCo into its virtual account, the balance on which crystallises itself as a liability of the main bank towards the SSC, would cease to be a "Cash in [local] banks" asset of the OpCo and turn into a "Due from [foreign] related companies" asset.

Being a claim on a foreign party and not on an account in a local bank, the asset becomes more difficult to attach for a trustee-in-bankruptcy of the OpCo. If staff and local creditors of OpCo can then not be paid out, the trustee-in-bankruptcy may be able to prosecute the local bank for "capital stripping": participating in a scheme that moved the OpCo's money across a national border to the detriment of the ability of the OpCo to meet its local obligations.

The local bank has taken on the role of the ASI of the respective OpCo in the eyes of third-parties in the outside world, but, if it has not done complete AML/CFT as if this were a "real" account, it has a legal exposure.

Even in a basic situation where the OpCo has supplied defective goods and their customer is unable to get redress by direct communication with the OpCo, the customer could go to legal or consumer protection authorities in their own country. It would not be inconceivable that those authorities would ask questions of the ASI that it would only be able to answer if it had an up-to-date CDD file and a relationship manager.

What happens then to the ASI? Is it an acceptable answer to say that they have an indemnity from SHAM? Would the indemnity fully cover the possible penalties?

Does SHAM have an exposure in front of its own regulators as well? Its position would appear to be more secure than that of its partner banks.

It must surely have crossed the minds of these partner banks that SHAM only does complete AML/CFT on the holder of the "real" account and not on any of the holders of the accounts that SHAM puts up to them for "virtual" accounts.

The Virtual Account partners will find it difficult to explain their position to their local supervisors if, for example, the account holder has defrauded local counterparties, whose money was paid in using the invoice details provided… and then there is no AML/CFT file.

Conclusion on Virtual Accounts for OBO parties
Virtual Accounts perfectly meets the needs of major multinationals that have fully centralised their Finance function into an SSC.

Even for euro payments in the SEPA Area, commercial reality still requires the existence of local accounts.

The holding of "real" local accounts within any bank's network (of branches, subsidiaries or partners, or a mixture of all three) submits the bank and the multinational to the ever-increasing burden of AML/CFT compliance as a generality, and to the decrease in the efficiency that can be applied at the banking location charged with Global Relationship Management:

- A Global Relationship Manager would normally be able to commit foreign branches of the same bank that he/she is an officer of, as regards credit lines and to the principle of opening a bank account;
- But committing a foreign branch to a consistent process and to a harmonised set of account-opening papers may not be possible, because banking regulation for opening accounts will always impact a foreign branch of the bank at two levels:
    1. The regulations imposed on the whole bank by the parent-level supervisors;
    2. Rules and guidelines imposed by local supervisors and applying just to that one branch;
- On top of that, global banks are following a trend towards converting overseas branches to subsidiaries, where then the local rules take precedence over the parent-level ones;
- A bank owning foreign subsidiaries will structure their shareholdings to meet varying criteria. This will result in the subsidiary having a close or distant relationship to the banking entity in which the Global Relationship Management for a particular customer will be carried out, necessitating inter-unit processes to be designed that assume as their baseline that the units are not related in any meaningful way;
- Lastly, because the pace of expansion of global banks has stalled, they are even exiting some markets and switching to the usage of partner banks with whom no shareholding relationship exists at any level.

These trends increase the workload associated with holding distributed, "real" accounts, and equally-and-oppositely increase the attraction of Virtual Accounts, an offering that depends upon the view that AML/CFT compliance only has to be performed on the SSC and at the banking location of the main bank where the SSC's "real" accounts are held.

Were the view to be that AML/CFT compliance has also to be carried out on the OpCos at every location where Virtual Accounts exist, then the advantages of Virtual Accounts sharply reduce.

The view on AML/CFT that enables Virtual Accounts appears highly aggressive, and depends not on the opinion of the main bank because they will not be in the front line if and when things go wrong.

The view – and so the service – depends on the opinion of the partner banks (be they branches, subsidiaries or third-party partners) of the main bank, namely that they can issue unique bank details without being classed as an ASI for AML/CFT purposes.

These partner banks associate the unique number with the OpCo in their own books, by naming a putative account "SHAM London ref Welch Paper Payments (Europe) BV ref Welch Paper (Austria) GmbH". The fact that Welch Paper (Austria) GmbH is written into the account name and that the bank knows that only this name and the unique number associated with it will be put on the OpCo's invoices are the proof that the bank is acting as an ASI for the OpCo.

Overall conclusion
Wolfsberg Group's Payment Transparency standards only partially address payments away under OBO structures establishing for multinationals.

They do not address receipts under the same structures.

Nor do the standards confirm an obvious truth: that a bank does identify itself as an ASI when it issues unique bank details relating a party that it names in its own books. That the party's name might be held within complex naming on a bank nostro account is no defence when it is clear that the party claims the account as their own by putting the unique details on their invoices.

The Payment Transparency standards thus need to be comprehensively re-visited to eliminate these gaps.

BL/4.6.18