

IBOS ASSOCIATION

Payer Information

Overview of industry initiatives on acceptable Payer Information

7th May 2008

Bob Lyddon

Background

In 2007 the payments industry struggled with how to adopt – or not – Option F in Field 50a of MT101 and MT103, as they were rolled out in SWIFT's 2007 Standards Release Guide. Option F introduced new ways of identifying the payer in these messages.

Then, in response to the operational problems caused by Option F and its contents in many cases not being accepted further down the payment chain, a number of new Status and Rejection codes were introduced in SWIFT's 2008 Standards Release Guide.

Payer Information, amongst other things, were the subject of the Wolfsberg Group recommendations which will feed in turn into SWIFT's 2009 Standards Release Guide: the introduction of MT202/205 "COV" copying over the major details of a payment message into its cover.

Difficulty

The Payer Information issue is being driven by factors that are to some extent at odds with one another:

- (a) FATF – ensuring that any payment can be traced back to the Payer
- (b) Enabling "Workers' Remittances": high-scale migration and value-of-money differentials mean an increasing flow of regular, low-value payments from USA/EU in particular to other parts of the world. The payment industry's objective – supported by banking regulators and thus also by governments - is to capture these flows within a FATF-compliant banking system and not to let them flow through arrangements like Hawala, or through systems where AML and anti-terrorism requirements cannot be as rigorously enforced as in mainstream banks.

US regulators have already started to criticize m-payments on this latter point. However, "Workers' Remittances" will not flow through high-cost circuits, they will find another way.

It is worth mentioning that, from latest November 2009, there should be no distinction within the EU of the compliance environment within a mainstream bank compared to a non-bank payments company. To comply with Payment Services Directive the latter have to become "Payment Institutions" or cease trading. Both a "PI" and a mainstream bank are forms of Payment Service Provider ("PSP") and the core provisions of PSD on transparency, liability, timings etc apply equally to all PSPs.

However, this is of course somewhat undermined by the last-minute negotiations on PSD which exempt both (a) "electronic money institutions", and (b) companies with small payment volumes, from the necessity of complying with PSD.

Source Documents

We have the following documents acting as sources for this paper:

- (a) Payment Services Directive
- (b) EU Reg 1781 on Cross-Border Payments
- (c) EPC's "Interim Measures" on usage of IBAN+BIC
- (d) SWIFT SRG 2007 – Option F in 50A in 101 and 103
- (e) IBOS' analysis and proposals around Option F and the comparison by IBOS Office of Option F with the Party Identification options in ISO20022
- (f) SWIFT SRG 2008
- (g) SWIFT SRG 2009 proposal regarding Wolfsberg Group

The horns of the dilemma

At the same time the payment industry wants to attract worker remittances into the mainstream, while being wary of the compliance issues raised in that business.

Banks did adopt Option F when SWIFT put it onto the network. The ability to process messages that use Option F is thus mandatory – and banks are reluctant to ever reject an MT103. If there are issues with it, they hold it and ask the sending bank for further instructions.

This is different from the banks adopting it into their customer channels such that a payer might choose to identify himself with data that can only be supplied using Option F. Option F contains several possibilities that would only apply for a payer who had no account, so the question that presents itself to a bank is why bother? Especially if all our payer customers have accounts and we do not accept over-the-counter money transfer instructions.

Payer-coming-off-the-street is immediately a "red flag" situation for FATF, whilst also being a major source of payments for worker remittances and also comprising payments that the regulators want to see flowing through the mainstream.

This tension is unresolved. Alternative channels like mobile device tend to be quick, simple and STP, and to appear cheap. The mainstream channels can only be STP if FATF issues are solved in a harmonized manner and on a global basis, and so will not necessarily be either quick or cheap. While the tension is unresolved, it is hard to see how these payments can be **attracted** into the mainstream. Within the EU they will be **partially forced** into the mainstream by PSD, but – by their nature – these payments have a tendency to flow round such barriers in unanticipated ways, or else be driven into electronic money institutions.

New standards - how we got to where we are now

If we are looking for the source of (a) changes to payment messages to enable FATF compliance and (b) definition of new ways in which a remitter can be identified in payment messages, we have to recognize several tracks of work which have fed into one another.

EU/EPC

Within the EU we have to recognize the way of thinking followed by the European Payments Council in preparing for the SEPA environment, where very simple information is all that is needed for an intra-EU payment between two parties that hold payment accounts at PSPs.

This comes down to Name + IBAN + BIC, and was first defined as the sole valid information on the **payee**, in the EPC's "Interim Measures" of May 2005, namely that IBAN+BIC were the sole and essential data on the beneficiary account and routing for cross-border payments in EUR within the EU (and EEA).

“Interim Measures” also established the important principle that, where these were absent or incorrect (for payments within scope), banks were entitled to reject or return the payments in the normal course of business as from 1.1.2007.

In other words in the EU and thus in the SEPA environment – for cross-border payments and in due course for national ones as well – the rule is that inadequate payments are not “held in suspense pending receipt of further information”.

“Interim Measures” regarding beneficiary information can now be seen to be in alignment with the formal enactment of FATF on **payer** information in the EU, namely Regulation 1781/2006 of 15th November 2006.

Reg 1781 continues the distinction between what is acceptable within a given scope and outside it, and it does this by creating the definition of so-called “complete information”, as opposed to “simplified information”.

Article 4 defines “complete information” on the payer as:

- ⇒ Name
- ⇒ Address
- ⇒ Account number

The Address can be substituted with one of:

- ⇒ Date and place of birth
- ⇒ Customer identification number (i.e. the PSP’s unique ID for that customer)
- ⇒ National identification number

The Account number can be substituted with a unique identification number for the transaction itself.

Clearly some of these pieces of data point to a customer who has an account with the PSP, while others imply payer-coming-off-the-street.

Article 6 then states that, by way of derogation, the payer information on a payment within the EU need only consist of what is known as “simplified information”:

- ⇒ Account number **OR**
- ⇒ A unique identification number for the transaction

The payee’s PSP then has the right to ask for the complete information, and the PSP of the payer should supply this within 3 days of receiving that request (without the payee’s PSP holding up the payment, it is implied).

So this means that the payer information entered by the payer’s PSP can be as little as:

- ⇒ Where payer has an account: payer’s Account number
- ⇒ Payer-coming-off-the-street: unique identification number for the transaction

The payment need not contain the payer’s name, address or – for payer-coming-off-the-street – any other information at all.

However, we should look again at the IBOS banks’ responses on Option F to see if this is actually what has been implemented.

EBA and the SEPA Credit Transfer

EBA has worked to create a viable channel firstly for Credeuro (to which “Interim Measures” initially applied) and now for SCT.

SCT allows for more than the minimum “simplified” payer information – since the payee might not even recognize the payment if they only saw the minimum data.

This creates an inevitable problem, because there has not been harmonization in the way banks are treating payer information under Reg 1781:

- ⇒ Wanting more than the minimum, so insisting on Address, for example
- ⇒ Not having a process to complete the payment and then request extra information
- ⇒ Rejecting the payment even if it delivers the minimum
- ⇒ Rejecting and/or requesting more information but not using STEP2 for that, in other words not using the so-called R-messages that are part of the SCT scheme

ISO20022

ISO20022 has been the process for defining XML messages for payments and information, in response to corporate demand (TWIST, RosettaNet) and hand-in-hand with SWIFT’s strategy of firstly moving their traffic onto an IP network (SWIFTNet) and then migrating the messages from an MT format to XML (SWIFTMX).

The process has responded to the desire to have payer-coming-off-the-street using various forms of identification, and has also allowed the communication of, for example, Customer identification number, National identification number, and the unique identification number for the transaction.

So ISO20022 enables compliance with Reg 1781 in XML messages – and thus directly meets a requirement of the SEPA Credit Transfer.

The interbank messages are called ‘pacs’ = payment clearing & settlement. The data required in those messages is then factored back into the ‘pain’ messages = payment initiation.

The result is a long list of possible values for the data components “OrganisationIdentification” and “PrivateIdentification”.in pacs and pain.

SWIFT

Since SWIFT was and is an important player in ISO20022, it might be challenged that SWIFT is even identified separately here – but this is done so as to distinguish between SWIFT’s role in XML (which is seen as 100% aligned with ISO20022 and having its output as SWIFT MX) and SWIFT’s role in maintaining its own MT messages via its annual SRG or Standards Release Guide process.

The 2007 SRG – and proposals for the 2008 and 2009 SRGs – contain important changes to the MT payment and R-messages in three respects:

- (a) inclusion of an Option F for Field 50a that allows MT versions of a number values for data components that would rank as either “OrganisationIdentification” or “PrivateIdentification”.in ISO20022
- (b) Codes for MTn95 messages to act as Status Advices or Rejections of payment messages where payer information did not meet “regulatory reporting guidelines”
- (c) Copying over of main details of a payment message into its cover payment messages, in line with Wolfsberg Group recommendations

While point (c) is not about the capture of payer information at the originating PSP, it is about its transparency throughout the payment chain, and about traceability of the settlement to the payment itself.

Sounds good...a lot of excellent work: what's the problem?

The European industry has been implementing Reg 1781 to simplify while ensuring that there is a common measure of what is good enough: the fulfillment of that measure of "simplified information" is embedded in the adaptation of ISO20022 pacs that is the SEPA Credit Transfer, and so into the input criteria for the Euro Bankers Association STEP2 platform, the principle clearing and settlement mechanism for SEPA Credit Transfer.

ISO20022/SWIFT MX are aimed at enabling compliance of the mainstream payments business and gearing it up to receive payments-off-the-street.

Both workstreams are driven by Financial Action Taskforce ("FATF") and are aimed at ensuring that the payer/remitter can be traced back down the payment chain, and that each bank in the chain can fulfill its legal responsibilities.

That is where the similarity ends because the contents of the initiatives point to diametrically opposing outcomes.

Reg 1781 compliments related initiatives in moving towards a Yes/No environment in the EU/EEA. Yes = Compliant+STP. No = Rejected at point of initiation, or later if it slips through.

Option F, which is global including EU/EEA, introduces a raft of new ways of identifying the Payer, and it will be very hard to assure the Payer in advance that every link in the payment chain will be willing to accept that information as being good enough to pass the payment on, let alone in STP mode.

Instead there will be an unpredictable mix of:

- ⇒ Rejected at point of initiation
- ⇒ Rejected further down
- ⇒ Held further down pending supply of extra and satisfactory information
- ⇒ Paid on further down but with a request to supply extra and satisfactory information

The last response could be expected only where the bank involved is crediting an account in its books, and so could reverse the credit if the extra information is unsatisfactory or is not received at all. While the extra information is being sought, it will be interesting to see if banks credit the beneficiary "under reserve" or do not allow the beneficiary to draw on the funds (i.e. the bank credits the ledger balance and the interest-bearing balance, but not the available balance).

If the bank is in the middle of chain, the most likely case is to hold the payment pending supply of extra and satisfactory information. There is no certainty that this fate could not befall the same payment several times on its journey – or that it might not be rejected by a bank at the end of the chain, having already been held within the chain.

EU/EEA – towards a "direct" payments environment

Reg 1781 mirrors "Interim Measures" in defining IBAN as the key for all payments within the EU and EEA. This fits with the vision for a SEPA environment characterised by account-to-account **direct** payments, with all banks connected to infrastructures and thus not needing to employ intermediary banks.

The Euro Banking Association STEP2 platform for SEPA Credit Transfer is a signpost towards this environment.

This environment involves no serial or cover payments. There would be no intermediary PSPs passing on Payer Information that they could not validate. The Payer would always have a Payment Account at the sending PSP – who could always populate Name plus IBAN+BIC from

their database, because this is original KYC data taken from the customer at the time the account was opened.

The Payer would never be a person walking in off the street with cash or a draft (meaning also travelers cheques). The Payer would benefit from the protections offered by Payment Services Directive because their account would be held in a "Payment Service Provider", which could be a mainstream one or a "Payment Institution".

That is a simple environment with clarity upfront as to the success requirements, how these can be met, and with assurance that further players in the chain will accept the information and pay on. In fact the payment won't get as far as Rejection: the payer's bank won't accept the payment in the first place if requirements are not met.

Cover payments

The movement within the EU/EEA towards direct payments is a response, inter alia, to Regulator pressure to move away from cover payments (where the payment order is sent by the remitter bank to the beneficiary bank direct, but where settlement is arranged by separate messages).

On a global level cover payments should – under that view - be replaced by serial payments (where each bank in the chain moves the message and the settlement, and has responsibility for both).

We can categorise a "direct" payment as a "serial payment with no need for intermediaries": no need due to the nature of the payment, the currency etc.. However, any scenario in which a bank is making a payment in a non-functional currency (except EUR paid within the EU/EEA by a bank in a Euro-Out country) will require intermediaries, either acting in a "cover" loop or relaying the payment in a "serial" chain.

The "direct" payment model is the easiest scenario in which to control AML, Payer Information and FATF issues.

Cover payments are now held to be the most difficult to control. They are held to contain the risk that the settlement payment nefariously disguises what the payment is for.

An example:

- ⇒ SWIFT MT103 sent from Iranian-controlled account in Switzerland direct to Libyan-controlled account in Liechtenstein for USD5 mil
- ⇒ Swiss bank asks its New York bank via MT202 to pay USD5 mil to Liechtenstein bank's account at a second New York bank with reference "Cover our direct P/O", with no statement of who the remitter is or the payment reason

Under the serial payment model the Swiss bank should send an MT103 to its New York bank asking it to pay on to the second New York bank and the MT103 has to reveal the full details:

- ⇒ Remitter: Ministry of Defence on behalf of Revolutionary Guards:
- ⇒ Beneficiary: Quaddaffi Enterprises Tripoli:
- ⇒ Field 70 "Invoice #238282 FOB Tripoli MS Jamahirya dest Kharg 400 GPMG and spares"

The payment would be quarantined by the obligatory OFAC filter in the first New York bank's wire room and go no further.

Problems for intermediaries in serial payments

Operational issues can be expected to grow for banks who are part of a serial payment chain, handling payments on a pass-through basis where they cannot directly verify Payer Information from their own databases. Bank responses have included:

- ⇒ Holding up (in suspense or by a provisional credit) many more payments pending supply of corroborating data from the start of the chain
- ⇒ Rejecting payments
- ⇒ Withdrawing from acting as an intermediary bank in certain circumstances (e.g. for foreign currency payments into their country for non-account holders)
- ⇒ Closing their correspondent accounts so that the number of channels into the bank is sharply reduced, and focuses on direct clearing memberships

These experiences confirm that while cover payments may throw up OFAC issues, serial payments can cause extreme operational issues:

- ⇒ The bank cannot be sure of the criteria that will be applied by the banks sitting beyond the next agent in the chain
- ⇒ The bank will receive a large number of enquiries it cannot answer itself – but has to go back to the originating bank
- ⇒ Their direct client may be an agent for the originating bank
- ⇒ Big workload to track all outstanding enquiries and make sure they are closed off

This could simply become unmanageable for certain banks, causing them to withdraw as an intermediary - and resulting in the reduction of available payment routings.

This may even threaten the business case of certain banks who have so far built a specialization in payment intermediation, with a proposition that says “send it to me whatever it is and I’ll make sure it gets there”.

SWIFT codes to enable processing of these problems

SWIFT’s 2008 Standards Release now proposes the creation of new codes for Status advices and Rejections, to provide an automated and consistent way in which banks can advise one another of the fate of payment messages where Payer Information is inadequate for “reasons of regulatory reporting”.

We should overlook three points:

- ⇒ There is no guidebook for what data fulfills “regulatory reporting” at any particular bank in any particular country
- ⇒ SRG gives a code but does not then allow or force the bank sending the message to say what exactly was wrong or what exactly is needed to put it right
- ⇒ Banks do not have to “report” the identities of the payers to their authorities so it is “for regulatory reasons”, not “for regulatory reporting reasons”.

The important point is that these codes do not eliminate any problems: they simply allow banks that are experiencing the problem to explain it in SWIFT-speak.

The substance is that the new Status Advice codes mirror the “hold or execute, do not reject” rule for MT103. The data elements that the codes refer to closely parallel the ones that are defined in Reg 1781 as representing “complete information”.

However there is nothing in there that directly responds to inadequacies in what banks might populate under the new possibilities in Option F.

There are four Status Advice codes to go into Field 75 of a MTn95:

/48/ meaning we are holding it and want for further information on the account number or unique ID

/49/ meaning we are holding it and want for further information on the name and/or address

/50/ meaning we have executed it but want for further information on the account number or unique ID

/51/ meaning we have executed it but want for further information on the name and/or address

There are three proposed codes for a Rejection in relation to Payer **or** Beneficiary Information.

These codes would likewise go into Field 75 of a MTn95:

/RR01/ meaning we rejected it because specification of ordering customer's account or unique ID is missing/inadequate

/RR02/ meaning we rejected it because specification of ordering customer's name and/or address is missing/inadequate

/RR03/ meaning we rejected it because specification of beneficiary customer's name and/or address is missing/inadequate

Notice that there is no /RR04/ meaning we rejected it because specification of beneficiary customer's **account or unique ID** is missing/inadequate.

The Wolfsberg Group and transparency of cover payments

The push towards "serial" payments – including "direct" payments - can be traced back to 9/11 so it has been in train for 7 years. The "cover" payment model should be on its way out by now.

However, when measured against the problems outlined above with "serial" payments, a "cover" payment can be justified if it is termed as a "direct" payment **order**, with indirect delivery of value.

This applies to almost any scenario in which a bank is making a payment in a non-functional currency, and is so important to there being a range of payment routings between A and B (i.e. to there being consumer choice), that the rumours of its demise appear to have been exaggerated.

No better proof of its rehabilitation (unlike the Soviet model, this can happen before the subject's burial), SWIFT's 2009 SRG proposes a way of solving the issue of disguise.

2009 SWIFT Standards Release incorporates the recommendation on "Core Payments & Transparency" i.e. the outcome of the Wolfsberg Group's review. The recommendation is that the main contents of an MT103 need to be copied into a 202 or 205 cover payment.

The 202/205 would then be tagged as "202 COV" or "205 COV" respectively, a new type of 202/205.

These recommendations – or a variant of them – are very likely to be adopted and to become obligatory. The cost/effort of adoption by the industry will be huge, especially in adapting non-SWIFT based clearing systems like CHIPS and Fedwire to carry the requisite details in their own interbank messages.

However, in the rush towards "improvement" and "modernization", the industry risks going backwards in terms of speed and efficiency. The guiding principle of cover payments is not dissimulation but the trust that the receiver puts in the sender's undertaking to deliver good value to the receiver's SSI.

Receivers will categorise that undertaking dependent upon its source, most obviously into:

- (a) We pay away as soon as we get the 103 from that bank
- (b) We wait to see the cover from that bank

The timelag under (b) is currency and communication-channel dependent, with a rough baseline being:

- ⇒ Own currency: real-time through clearing membership
- ⇒ USD, GBP, EUR, CHF, JPY: real-time through 900/910, or 942, or proprietary system offered by the nostro correspondent, or RTN..
- ⇒ Others: MT950

202/205 COV disrupts this logic chain by introducing an element over which the receiver has no control, and upon which they cannot make an informed decision. It is not a credit decision. The receiver cannot take a view on the regulatory regime of the country of the currency being transferred, and will in all cases wait to see the cover before paying on.

Where is the industry going as a whole?

In terms of expenditure and investment, the lesson is simple: the industry continues to spend large amounts to keep every way of doing it alive.

Cover payments continue, direct payments continue, and so do serial payments. The industry introduces new rules for checking Payer Information, and new techniques for informing when these rules are broken – and at the same time greatly increases the number of ways in which the Payer Information can be configured, thus making its own problems ten times worse.

The SWIFT 2007 Standards Release established a whole raft of new ways in which a remitter can be identified in either MT101 Request for Transfer or MT103 Customer Payment, that is in ways other than by their Name and Account.

This was done to assist the initiation of payments by individuals with no Payment Account. That could be the unbanked, workers wishing to remit monies cross-border, or even a customer of one of the new “Payment Institutions” permitted in the EU by Payment Services Directive: PSD does not insist that all clients of PIs hold a Payment Account.

2007 SRG

SWIFT enacted this widening by the introduction of Option F in Field 50a in both the MT101 and MT103 messages, to sit alongside the existing options:

- ⇒ in SWIFT MT101, Option G (Account and BEI) and Option H (Account, and Name & Address)
- ⇒ in SWIFT MT103, Option A (Account and BIC/BEI) and Option K (Account, and Name & Address)

Option F is now allowed in both messages, and it is structured the same way in both. It consists of two elements, both of which must be present:

1. Party Identifier of one line, being either “Account” or “Code+Details”, the Code being 4 characters and the Details being up to 30
2. “Name + Address” of up to 8 lines, each line being in the form of a 1-character number that denotes the type of information that follows, then the information itself

Examples:

“Code+Details”:

ARNU (means “Alien Registration Number”), is then followed by /, then the ISO Country Code, then / and then the number

CUST (means “Customer Identification Number”), is then followed by /, then the ISO Country Code, then /, then the issuer of the number, then / and then the number

Examples:

“Name + Address”:

1/Name of ordering customer

2/Address line

3/Country and Town

6/Customer Identification Number

8/Additional information

Applicability of Option F to MT101

These changes do not sit so easily with the way that banks have made the MT101 message available to customers.

MT101 is used in corporate business to send an order through the electronic banking portal of one bank in order to debit an account at another. It has to contain the Name and Account details of the debit party, which is then the remitter under the resulting payment. The executing bank usually checks the details on the 101 that they match the details held in their own database on the account being debited.

It is never used in the context of a payment requested by a non-account holder. By definition the details that populate Option G or H must be present in the 101, so Option F adds nothing.

Account number as the core payer data in MT103, otherwise...

Regarding MT103, the introduction of Option F risks a blurring of what should be a hard-and-fast rule and which is an objective of Reg 1781, namely that the Payer Information should be Name and Account Number in all cases where the Payer holds a Payment Account.

Were Option F to be used for a remitter with a Payment Account, the details filled should be:

⇒ “Account”, up to 34 characters

⇒ “Name and Address”

In other words the same as are required under Option K – which makes Option F redundant.

By implication, then, Option F extends the functionality of MT103 only where the remitter has no Payment Account at the first SWIFT member entity in the chain.

That in turn could point to two situations:

- (a) the sender of the MT103 is the first link in the chain, does have a SWIFT BIC/BEI, and the remitter has no Payment Account there; or
- (b) the sender of the MT103 is the first SWIFT member entity in the chain, but is not the first Payment Service Provider in the chain,. The remitter is a customer (with no Payment Account) at a non-SWIFT-linked Payment Service Provider... which is in turn a customer of the sender of the MT103

From an EU/EEA perspective the Payment Services Directive (“PSD”) does not demand that all “Payment Institutions” obtain a BEI if not a BIC, but surely, at the very least, they would get a BEI even if it was managed by a Service Bureau.

A SWIFT payment originating at a “Payment Institution” entity with no BIC/BEIs, where the payment had been requested by a Payer with no Payment Account, would already be a Red Flag situation for many EU/EEA banks. It certainly runs counter to the environment that the PSD is aiming to create.

A SWIFT payment originating at a “Payment Institution” entity that did have a BIC/BEI and with the same Payer situation (no account) would hardly be regarded differently.

So there is a strong suspicion that any case where the remitter details use Option F but do not state the account number will be taken to mean “Remitter has no Payment Account” and will trigger as Red Flag, even worse where the originating institution has no BIC/BEI of its own.

If the originating institution is in the EU/EEA but is not linked to SWIFT, is it under any obligation to issue IBANs on its Payment Accounts? If not, then the population of “Account” when used as “Party Identifier” would not be recognizable to banks further down the chain as connected to:

- ⇒ the first sender of an MT103 over SWIFT
- ⇒ any particular bank

That being the case, the risk of the further banks in the chain concentrates on the first sender of an MT103 over SWIFT: those other banks will be reliant upon the “Account” details as supplied to that first bank as their own guarantee of traceability.

Acceptability of different options within Option F

Even if the payment was accepted with Option F at the start of the chain, there are variants within Option F that a bank further down the chain might have trouble in accepting as delivering traceability, even if the original PSP was quite happy with them.

If there are several PSPs in the chain, the ones further along may have no relationship with or knowledge of the payer’s PSP and its verification processes, and so will not place reliance on data that they cannot check themselves.

A business analyst from SWIFT’s Payments Standards Department who worked on Option F stated to the writer (at IPS 2008) that SWIFT did not know why several of these methods had been included, who asked for them, and whether the data that could be included in Option F was verifiable.

Specific troublesome elements would be:

- CUST (Customer Identification Number)
- DRLC (Driver’s License number)
- EMPL (Employer Number)

All of these require the quotation of the issuer of the number, as well as the ISO Country Code of the issuer, and the number itself. Is there a reliable database of all issuers of such numbers, with a consistent ID for the issuer?

CUST

As stated above, SWIFT’s field definition requires the quotation of the issuer of the number, as well as the ISO Country Code of the issuer, and the number itself.

Reg 1781 permits the quotation the Customer identification number, which is assumed to be the PSP’s unique ID for that customer.

SWIFT could have defined CUST as requiring the BIC of the PSP and then the number itself, with the following results:

- (a) the BIC contains the ISO code
- (b) would not accommodate non-SWIFT PSPs

Since it is not stated as a hard-and-fast rule by SWIFT that an instance of CUST can only be where the originating PSP issues it, SWIFT apparently envisage that the Customer ID could be issued by any organization – but then there is no discussion of a database of codes for Organisation IDs, or a test as to which organizations would be regarded further down the line as reliable sources of Customer IDs (UK Automobile Association? Silvermere Golf Club?)

It is also hard to see where a PSP can have a CUST for the payer but not have an account. If the payer has identified themselves such that they have been enrolled with the PSP, presumably with the expectation of repeat business or diverse business, why not have an account?

DRLC

Would a bank in France accept any or all of DVLA, DVLA Swansea, UK DVLA after DRLC/GB/ as indicating the official issuer of driving licenses for the UK?

It is quite possible that an operator might type “D/L” for driving licence somewhere in the character string, then the machines would see the “/” as a divider and not as part of a data element.

What if there were multiple issuing authorities in the same country e.g. separate DVLA for Wales, Scotland and Northern Ireland within GB?

What happens when the string is as follows (using a typical UK DRLC, slightly amended):
DRLC/GB/DVLA Swansea/LYTTO501907RJ7DD 62

Answer: “DD 62” risks being truncated because that string adds up to 35 characters, excluding the Code DRLC/. The SWIFT field definition specifies **4!a/30x** so there are only 30 spaces left for the elements in the Identifier.

EMPL

The meaning of EMPL is unclear. One must surely discount the explanation that this is an employer’s unique number for itself because the employer itself is the payer. Any reputable employer would have an account and be able to use Option K. It would be highly suspicious for an Employer to come into the bank and try to make cross-border payments offering cash or draft as value.

A UK bank would surely, in such a case, want to assure itself that the Employer had deducted income tax and Employee National Insurance at source, and paid over its own Employer National Insurance, before making cross-border wage payments.

All Party Identifiers must be a number unique to an individual entity - or it does not identify the Payer. Therefore EMPL must be meant to be a number issued by an employer to an employee.

Such a number will not be on an official database: it is on the employer’s database. The employer itself will have an official number, such as Company Number, and that is held on an official database (e.g. Companies House for England and Wales).

SWIFT call for the following data in this situation:

- ⇒ ISO Country Code
- ⇒ the issuer of the EMPL number
- ⇒ the number itself

There is an element missing.

For banks to use this number and verify it, they would need:

- ⇒ ISO Country Code
- ⇒ An ID for the Employer
- ⇒ The issuer of the Employer ID
- ⇒ The unique number issued by the Employer to identify the employee

Even with those details it is questionable whether banks further down the chain would regard the data as reliable.

On a practical level, what document, presented by the remitter at the bank, would have all those data elements – and in less than 30 characters? Would the first PSP definitely be prepared to rely on such a document at all? After all, it will have been issued by an employer, and each employer may use a different layout. Would banks only be prepared to accept it if the employer held an account with them, and the bank could check the employer's signatures on the document?

Would banks even in England, Scotland and Wales be geared up at their counters to access Companies House to verify the Employer ID while the customer is waiting?

Has SWIFT established a database of issuers of Employer IDs such that there is one version of the code for that authority for each geography?

How will banks cope when the relationship between the ISO Country Code and an issuing authority is not 1:1? For example, there is a separate issuer of company numbers in the UK (ISO Code GB) for Northern Ireland (the Companies Registry run by the Department of Enterprise, Trade and Investment). The relationship is 1:2.

Again, how is this to be achieved when there are only 30 spaces for Party Identifier?

Acceptability and STP

There is an air of unreality about the ability of originating PSPs to populate Option F in 50a using the new possibilities in such a way as to be certain that banks further down the chain will either process STP or will execute the payment at all. Populating details of the account would be acceptable – but that is not new.

On a detailed level – and notwithstanding the above – there can be problems even where the originating PSP does use the same data in Option F that it would have used for A or K (because the payer has an account).

Option A/K data but used in Option F will not necessarily present the same string of characters to another bank that meet their STP criteria.

STP is essential if we are looking at high volumes of low-value payments and they need to get to the destination quickly and without deductions.

The risks of acting as a primary PSP in the case payer-coming-off-the-street will then result in many possible permutations of Option F not being accepted.

How would the UK bank come to recognize a Belgian Alien Registration Card as a form of ARNU, let alone an EMPL/BE/EMPL's code/[issuer of EMPL's code]/[number] document, as legitimization to execute a payment for a person who had no Payment Account? Surely a bank would only deal in documents that were issued in their own country.

Would further banks down the chain accept data where the source of the payment and the country of issuance of the remitter details were different e.g. an Italian bank relaying a UK bank's payment that quotes an ARNU with ISO country code BE?

CUST, EMPL, DRLC all have their problems.

That leaves:

ARNU = Alien Registration Number

CCPT = Passport number = OK with ISO country code

IBEI = OK, checkable through SWIFT; would not be an off-the-street payment anyway

NIDN = National Identity Number

SOSE = Social Security Number

TXID = Tax Identification Number

The stance of a UK bank on NIDN, SOSE and TXID could be expected to be:

ARNU = OK if issued by UK

NIDN = OK if taken directly from an original ID Card issued by an EU member state

SOSE = No, not even UK National Insurance number as there are three in existence for each member of the UK population, and it is not accepted now as legitimate ID

TXID = No

Banks further down the chain would be comforted by the restrictive policies at the front end, but this introduces a wide disparity between (a) the range of possibilities on paper and (b) how much can be used in practice.

What's the way forward

So there is an air of unreality about Option F in 50a as regards the risks of acting as a primary or an intermediary PSP on a payment that is requested by a remitter coming off-the-street. It runs counter to the efforts within the EU/EEA to create an environment where certainty exists upfront:

Yes = Compliant+STP

No = order not accepted

Rejection = can only occur if the first PSP was under-educated at the point of receiving the order, and relays a non-compliant payment

The Option F environment looks like one where the first PSP is led to believe it can take in payments with a raft of different identifiers, but the payments get held up or rejected further along the chain.

The Reg 1781 environment is a much simpler one to operate, but even there we seem to be losing the basis that all remitters should have a Payment Account, at least within a Payment Institution.

A Payment Institution in the EU/EEA should have an IBEI at least, although that precludes it from issuing IBANs. This would enable it, nevertheless, to reach the following level to comply with Reg 1781:

Payments within EU/EEA (simplified information)

⇒ Unique identification number for the transaction

Payments outside EU/EEA (complete information)

⇒ Name

⇒ Customer identification number

⇒ Unique identification number for the transaction

The Payment Institution would in that case want to be sure that its payment messages all carried its own IBEI right down the chain so that the IBEI legitimised the source.

A Payment Institution without either a BIC or IBEI might find it difficult to assure its own customers that it could get their payments to the endpoint in all cases.

Even better if Payment Institutions had BICs and issued IBANs...but then the unbanked would be excluded.

Beyond the EU/EEA where IBAN+BIC are not yet accepted as a universal reference point,

These then should be the bases for the business, not Option F in 50a, and should enable – not obstruct – low-cost, STP services.

BL/7.5.08