Response to PSR Consultation CP21/10 on APP Scams

APP scams
Payment Systems Regulator
12 Endeavour Square
London E20 1JN

Submitted by: Bob Lyddon, Director of Lyddon Consulting Services Ltd
(www.lyddonconsulting.com)

Date: 10th January 2022

Introduction

What is Lyddon Consulting?
A specialist consultancy in payments and electronic banking. We have recently acted as advisor regarding the UK payments landscape to a trade body representing UK Payment Institutions and to a major payments communications cooperative reviewing their UK market positioning.

Why this evidence is being submitted:
A solution to Authorised Push Payments Fraud (APPF) is a sine qua non for the future of financial services. We have attempted to lobby for change in the past, raising doubts about both the timing and likely efficacy of the Confirmation of Payee service (CoP) and of the Contingent Reimbursement Model code (CRM).

We have been proved right in our qualms: neither has solved the problem. APPF has gone on far too long and cost customers far too much money.

Now that we have left the EU, the UK can make the legal changes necessary to put the liability where it should always have been: with the banks. The liability needs to be brought onto a par with the situation where a bank allows a cheque to be paid into an account with a different name than the name on the cheque's payee line. We have specified the changes needed. This will cost the banks many hundreds of millions of pounds – once. This is better than it costing customers hundreds of millions of pounds - per annum.

Contact details
Lyddon Consulting Services Ltd
6 The Glebe
Wells-next-the-Sea NR23 1AZ

07939 – 132341

bob@lyddonconsulting.com

Introduction

We consider the proposals in the consultation and all the questions to be irrelevant as they accept the validity of the status quo on several levels, including the payment data that runs though the UK's clearing systems, the Sort Code and Account Number qualifying as a "Unique Identifier", New Payments Architecture being constructed as a like-for-like as regards the payment data running through it, Confirmation of Payee, and the Contingent Reimbursement Code.

The APP Scams problem will not be solved by continuing down this pathway. The pathway to solving the APP Scams problem is laid out below. This was already submitted, virtually verbatim, to the Treasury Select Committee call on the Future of Finance in January 2021, to no avail.

Summary

Authorised Push Payment Fraud (APPF) must be eliminated. If this is not done, other industry initiatives will exacerbate the problem, because these initiatives are to be realised through the main channel for APPF: the Faster Payments system.

The Faster Payments system contains a serious technical design flaw, which interacts with the terms of the 2017 Payment Services Regulations and the Funds Transfer Regulation (both being EU legal instruments which the UK now needs to and can alter to suit its own needs).

Together they put customers into a position of extreme risk that the Confirmation of Payee service (CoP) and the Contingent Reimbursement Model code (CRM) have not solved. CoP and CRM are by definition solutions (*sic*) that tinker around the edges: CoP is an "overlay service" in the terminology used by Pay.UK, and CRM is a further step removed as the main contingency upon which the customer's reimbursement depends is that they have used CoP.

APPF needs to be solved in the core of the payments process, and not on the periphery. The New Payments Architecture project (NPA) offers an opportunity to do this. The project needs to be re-scoped to eliminate APPF as a Day 1 deliverable.

APPF can be eliminated firstly by the 2017 Payment Services Regulations being amended so that the payee name is included in the list of the data in its Article 43.2 required for a payment contract to be entered into. Once the payee name is within the scope of the payment as authorised by the payer, all the protections for defective execution are available to the payer, against their own bank (or PSP).

Secondly the Funds Transfer Regulation needs to be replaced such as to limit the derogation in its Article 5.1 to the data specified in its Article 4.1.c. All UK payments would then have to include the payer and payee names. This would also fulfil the requirements of Financial Action Taskforce Recommendation 16 - of which the Funds Transfer Regulation falls short - and thereby strengthen the UK's defences against Financial Crime generally.

These changes will withdraw the current permission to banks to process payments based only on the Sort Code and Account Number. If the banks between them contrive in future to pay a different payee from the one named by the payer, they will be liable to make the payer good.

The New Payments Architecture project is going to cost hundreds of millions of pounds anyway. It would be ludicrous to spend so much and fail to eliminate APPF, which is the main customer detriment in UK payments and possibly in UK financial services as a whole.

Problem statement

The elimination of Authorised Push Payment Fraud is long overdue, and it is a blindspot in the middle of many industry initiatives:

- Open Banking: the standard payment type deriving from the activities of a Payment Initiation Service Provider (or PISP) is a Faster Payment, the payment outcome in which APPF is most prevalent;
- New Payments Architecture (NPA): within NPA, Faster Payments becomes the nodal retail payment system, through which others (BACS, cheques) will clear and settle. Unless APPF simply cannot happen by the time NPA is rolled out, NPA can only serve to increase APPF;
- Adoption of the ISO20022 XML data standard: the proposed standard UK credit transfer message begins as a like-for-like replacement for the messages in different formats (SWIFT MT, Standard-18, ISO8583) used by the UK's payment systems now. The stated pathway is later to include richer data. However, the existing flaw in Faster Payments is not eliminated: that the payee name is not processed by the payee's bank. That will remain the loophole permitting APPF unless plans are altered. The proposed ISO20022 standard UK credit transfer message must include the payee name and NPA rules must demand that it be validated against the name on the account identifiable through the Sort Code and Account number;[1]
- Possible adoption of IBAN: if IBAN is adopted as part of the adoption of ISO20022 XML, it must be excluded that UK payments can be completed with the IBAN-only as the payer and payee information.[2]

It will be expensive for the banks to close the APPF loophole, but it will be expensive to implement NPA and its sister project called RTGS Renewal.[3]

The crux point is why the actors in UK payments should expend the time and effort on NPA and RTGS Renewal and fail to eliminate the main detriment to customers in the UK's current payment set-up.

Failure of Confirmation of Payee and the Contingent Reimbursement Model

The APPF problem has gone on for far too long, it costs customers far too much money, and it has not been properly diagnosed. The supposed solutions – CoP and CRM – may have mitigated it to a degree, and there will be much argument as to the degree, but APPF has not been eliminated.

These "solutions" operate around the payment service itself. In other words they do not alter the core of the payment process and the legal and operational premises on which it is based.

CoP is labelled by Pay.UK as an "overlay service", and this indicates its relationship to the core of the payment process: it works on top of it, or, more specifically in this case, before it. It purports to confirm that the payee name inserted by a customer into an eBanking service correlates to the name associated with the account at the payee's bank.

[1] ISO20022 XML is a data standard for which SWIFT (Society for Worldwide Interbank Financial Telecommunication, a Brussels-based co-operative) is the registration agent. Its main current deployments is as the data standard for the Single Euro Payments Area

[2] IBAN is another ISO standard for the International Bank Account Number

[3] RTGS Renewal applies to CHAPS – the "Clearing House Automated Payment System" that is the UK's Real-Time Gross Settlement system for high-value/systemically-important payments run by the Bank of England - and RTGS Renewal foresees the replacement of SWIFT MT messages with ISO20022 XML

However, the service to the payer is not deployed identically at each bank. For example, a different algorithm may be applied depending upon whether the payee is a business or a person.

The possible response in the CoP specifications of a "Partial match" may not be part of a bank's offering. Aside from that, not all UK banks are live on the service. As regards proof of what happened, not all banks offer their customers a log of all their usages of CoP and the outcomes, that the customer can store themselves and have as evidence to be used in the case of a dispute: only the bank has this audit log.

CRM, under which customers can supposedly be compensated if they have been victims of APPF, requires a customer to use CoP where it is available and to take the most risk-averse posture towards continuing with their payment: the customer should not go ahead unless they get an unequivocal positive match.

Customer is put in an impossible position

This puts the customer in an impossible position. It is simply not a viable option to eschew proceeding with the payment in every case where CoP does not furnish an unequivocal positive match.

This state of affairs has been brought about firstly by the banks withdrawing effective access to other methods of payment than Faster Payments, and secondly by banks promoting the usage of eBanking services in which a Faster Payment is the default (and sometimes the only) method of making a payment.[4]

eBanking services generally do not allow BACS as a channel for customers to make electronic credit transfers; this option was withdrawn thanks to the first EU Payment Services Directive 64 of 2007).[5] eBanking services generally do not allow CHAPS as a channel for customers to make electronic credit transfers; banks try to reserve this channel for large, urgent payments where they charge the customer £20-30. Payees – especially consumer payees – do not have the facility to accept a card payment. Sending cash in the post is not a realistic option. The only lower-risk alternative for the payer is to post a cheque and this is the payer's best option for avoiding APPF: the payee bank must reimburse if they allow the cheque to be credited to an account that does not correlate to the name on the cheque's payee line. This is the gold-standard of payer protection against "conversion": other parties conniving to conduit the money into their account when it is not meant for them.

Having said that, readers will make up their own mind whether sending cheques in the post is a realistic alternative for the payee, given firstly the timelags between the cheque being posted and the funds becoming available on the payee's account, and secondly the reduced availability of bank branches through which to pay cheques in.

Banks have made app-based pay-in of cheques available, but readers will have their own view as to whether that is an adequate replacement for branch counters and is equally accessible to all types of customer.

[4] eBanking – an umbrella term to denote various remote-banking services operating over the public internet, and accessible by the customer using a PC, laptop, mobile phone, or mobile device

[5] BACS standards for Bankers' Automated Clearing System and it is the UK's Automated Clearing House, handling a large volume of credit transfer and direct debit payments to a timeframe where a payment input on a Monday settles on the Wednesday i.e. on D+2

This brings us to a third action by the banks to discourage the usage of cheques: the withdrawal of the cheque guarantee function on their cards such that a payee releasing goods or services against the cheque – rather than against the cleared funds from a cheque – is open to credit risk. Admittedly the guarantee only operated up to a given amount. Nevertheless the cheque guarantee function was one of the supports to the viability of cheques as a payment option. The supports have been progressively eroded.

Readers may consider that the banks have trained customers to stop using cheques – over an extensive period and using a variety of means – but without delivering a replacement product that ensures the achievement of a core and critical performance criterion: that the bank should pay the payee that the payer tells them to pay.

If one concatenates the flaws in the CoP service with…

- the needs and obligations of customers to make payments in a timely fashion
- the banks' policies of weaning customers off the usage of cheques
- the lack of alternative credit transfer offerings that do not contain the loophole

…it is inevitable that significant numbers of customers will go ahead with making their payments as Faster Payments but in a way that invalidates their rights under the CRM. Indeed it could be argued that CoP lays more obligations on the customer without equipping them to make informed choices, and that it therefore has the primary effects of invalidating CRM cover and furnishing the banks with incontrovertible proof for their denial of liability.

Finding a solution to APPF

So what is the solution?

The first step is a proper diagnosis, and it is that APPF derives from the coincidence of the construction of the Faster Payments service with wording in the 2017 Payment Services Regulations – the UK's transposition of the EU's second Payment Services Directive 2366 of 2015 – and the EU Funds Transfer Regulation 847 of 2015.

Diagnosis – technical construction of Faster Payments

To begin with the construction of Faster Payments, it uses the ISO8583 message standard. It is vital to appreciate the meaning of this factor: ISO8583 is the message standard for the Cards business. This points to the system's heritage.

Vocalink's technical solution for the construction of Faster Payments was not a new-build, but a basing on the existing processing of debit card payments: the only payment process in existence in the UK at the time which both worked in near-real-time (NRT) and involved a query-and-response exchange between the parties in the payment chain. In a debit card payment these parties are the payer's bank (the cardholder's card-issuing bank), the payee (through their merchant acquirer), and the switches in between. In other words the debit card process involved an exchange of messages in both directions in NRT, and could be classified as an appropriate rail on which to carry the message exchanges under Faster Payments.

As Faster Payments had to be built to a date extrapolated, inter alia, from the Cruikshank Report, there was not enough time to invent a new and task-specific solution. Instead Faster Payments was constructed using several pieces of pre-existing systems – mainly of the debit card system, but also of the BACS system (e.g. the Sort Code table).

The major banks – Vocalink's shareholders at the time – accepted the proposed solution.

The solution left an understandable loophole because a debit card payment is a "pull payment" whilst a Faster Payment is a "push payment". With a debit card payment the initiating party is the payee, and the payee uses the transaction – in the same way as a cheque – to pull money from the payer's account into their account.

The payee under a debit card payment uses an acquirer to route what is a "request for confirmation of payment" through to the cardholder's card issuer, the settlement of the payment following some days later. The cardholder is identified with the 16-characater number, not their name, in a "cardholder present" situation. This "request for confirmation of payment" need contain neither the name of the payee (who is the initiator of the message through their terminal) nor the name of the payer. Even if the payee's name was mentioned, the card issuer cannot process that name because the card issuer has no relationship with the payee: it is the payer, not the payee, who has the account in their books over which the transaction will be processed.

A Faster Payment, though, is a "push payment": the payer initiates the transaction and orders their bank to push funds through to the payee's bank for credit to the payee. The payee name is included in the payment order but there is no step in the process for the payee's bank to verify the payee name: it is a step that is simply not present in the process of which Faster Payments is, in effect, a clone.

The result of cloning a "pull payment" service to produce a "push payment" one in this way has been the loophole that the payee name is not processed at the payee's bank. This is valid in the case of a "pull payment" but misplaced in the case of a "push payment".

Impact of EU legal instruments in conjunction with the technical flaw

This is the operational problem deriving from the technical construction of Faster Payments. The loophole enabling APPF is expanded by the legal roles and responsibilities allocated to the actors in the payment chain by 2017 Payment Services Regulations, the UK transposition of EU legislation that was aimed at a quite specific purpose. This in turn interacts with existing UK case law that the Sort Code and Account Number of a payee are held to be the "unique identifier" of a payee account.

The prime purpose of the EU legislation was to enable a feature of the Single Euro Payments Area (SEPA Area), namely that "payment accounts" could be identified with a "unique identifier" alone, and where IBAN meets the definition of a valid "unique identifier".

Payments in Euro with both endpoints in the SEPA Area should, under the EU's vision, be completable only with the IBANs of the payer and payee, and not needing name, address or any other identifying data. This approach is reinforced by the EU Funds Transfer Regulation 847 of 2015 on payer and payee information to accompany funds transfers.

One might ask why APPF has not become prevalent in the SEPA Area, if the above is the case. The answers to that are:

1. SEPA's counterpart service to Faster Payments has only existed since 2017;
2. the low amount limit (EUR15,000) compared to that of Faster Payments (£250,000);
3. the convoluted pathway for clearing and settling a SEPA payment, leading to the designated timeframe not being adhered to (see Appendix 1).

The SEPA INST service (Instant SEPA payment) is the counterpart SEPA service to Faster Payments. SEPA INST has only existed since November 2017. The SEPA governing body (the European Payments Council) issued its initial rulebook for the service in November 2016 for rollout a year later.

It is a clone of the "core and basic" SEPA Credit Transfer, launched in 2008. Both services are "push payments".

SEPA's system for clearing and settling payments is distributed over many market actors: Faster Payments clearing and settlement is centralised. The UK has never had the flow-restricting problem of convoluted clearing and settlement arrangements that SEPA INST faces. Moreover the Faster Payments system went live in 2008. It is well-embedded. The maximum payment has been steadily raised, not least in order to satisfy the requirement of the Bank of England to move payments off CHAPS that it does not deem to be "systemically important".

The result has been the perfect arena for fraudsters: a real-time system carrying large amounts, to which almost all UK payment service providers are connected, with a fatal operational flaw, and a legal underpinning that absolves the banks from blame.

Case law construing Sort Code and Account Number as "unique identifier"
The legal underpinning starts with existing case law establishing a customer's Sort Code and Account Number as the "unique identifier" for their payment account. When a UK bank requires the customer to complete a payment template for a credit transfer in an eBanking service, the mandatory information (a sine qua non for carrying out the payment) includes the payee name, amount, Sort Code and Account Number.

The payer's bank, though, is entitled to carry out the payment with the amount, Sort Code and Account Number alone, either not passing on the payee name, or passing it on in the knowledge that the payee bank (identified by the Sort Code) is under no obligation to validate that the payee name in the payment matches the payee name on the account in its books.

The main reasons for failure – and return of the payment – are that the Account Number does not exist at the Sort Code, that the account has been closed, and that the account is blocked/frozen. There is a no return message that the name in the payment and the name on the account do not match.

If there were, there would be no need for Confirmation of Payee, and APPF would be subject to the same legal terms as the conversion of a cheque: it would be the payee bank's fault if they failed to return the payment and instead credited an account named differently to the payee stated in the payment. The payee bank would then have to reimburse the payer's bank, who would have to make good the payer's account.

Clauses in 2017 Payment Services Regulations that combine to place the liability on the customer
The clauses in current legislation that underpin this state of affairs are copied below from the 2017 Payment Services Regulations.

In each case we have:

- the page number
- the subject
- the Article reference
- our interpretation of the meaning

They are listed at first seriatim, and afterwards brought together as what the problem is.

P15 – Definition of unique identifier
"unique identifier" means a combination of letters, numbers or symbols specified to the payment service user by the payment service provider and to be provided by the payment service user in relation to a payment transaction in order to identify unambiguously one or both of—
(a) another payment service user who is a party to the payment transaction;
(b) the other payment service user's payment account;

Meaning: the UK Sort Code and Account Number are a "unique identifier".

P42 - Information required prior to the conclusion of a single payment service contract
43. (1) A payment service provider must provide or make available to the payment service user the information specified in paragraph (2) in relation to the service, whether by supplying a copy of the draft single payment service contract or supplying a copy of the draft payment order or otherwise, either—
(a) before the payment service user is bound by the single payment service contract; or
(b) immediately after the execution of the payment transaction, where the contract is concluded at the payment service user's request using a means of distance communication which does not enable provision of such information in accordance with sub-paragraph (a).
(2) The information referred to in paragraph (1) is—
(a) the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly initiated or executed;
(b) the maximum time in which the payment service will be executed;
(c) the charges payable by the payment service user to the user's payment service provider and, where applicable, a breakdown of such charges;
(d) where applicable, the actual or reference exchange rate to be applied to the payment transaction; and
(e) such of the information specified in Schedule 4 (prior general information for framework contracts) as is relevant to the single payment service contract in question.

Meaning: 43.2 does not include the payee name so it is not part of the payment contract. This holds true even if the payer's bank specifies it as mandatory information to be supplied by the payer for the payment to be carried out.

P51 - Consent and withdrawal of consent
67. (1) A payment transaction is to be regarded as having been authorised by the payer for the purposes of this Part only if the payer has given its consent to—
(a) the execution of the payment transaction; or
(b) the execution of a series of payment transactions of which that payment transaction forms part.

Meaning: the consent is given for the payment as defined by the information laid out in 43.2, and not including the payee name even if the payer's bank requires it as mandatory information.

P55 - Notification and rectification of unauthorised or incorrectly executed payment transactions
74. (1) A payment service user is entitled to redress under regulation 76, 91, 92, 93 or 94 (liability for unauthorised transactions, non-execution or defective or late execution of transactions, or charges and interest), only if it notifies the payment service provider without undue delay, and in any event no later than 13 months after the debit date, on becoming aware of any unauthorised or incorrectly executed payment transaction.

Meaning: notwithstanding the bank's demand for the payee name, its exclusion from the contract as per 43.2 declassifies an APPF payment as being unauthorised or incorrectly executed if the payment does not go to the named payee.

P55 - Evidence on authentication and execution of payment transactions
75. (1) Where a payment service user—
(a) denies having authorised an executed payment transaction; or
(b) claims that a payment transaction has not been correctly executed,
it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the payment service provider's accounts and not affected by a technical breakdown or some other deficiency in the service provided by the payment service provider.

Meaning: similarly to the case of 74. (1), this protection is denied to the payer because of the exclusion of the payee name from the payment contract.

75. (4) If a payment service provider, including a payment initiation service provider where appropriate, claims that a payer acted fraudulently or failed with intent or gross negligence to comply with regulation 72, the payment service provider must provide supporting evidence to the payer.

Meaning: this protection is similarly denied to the payer, namely the onus of proof being on the bank to demonstrate that the "acted fraudulently or failed with intent or gross negligence to comply…".

P56 - Payment service provider's liability for unauthorised payment transactions
76. (1) Subject to regulations 74 and 75, where an executed payment transaction was not authorised in accordance with regulation 67 (consent and withdrawal of consent), the payment service provider must—
(a) refund the amount of the unauthorised payment transaction to the payer; and
(b) where applicable, restore the debited payment account to the state it would have been in had the unauthorised payment transaction not taken place.
(2) The payment service provider must provide a refund under paragraph (1)(a) as soon as practicable, and in any event no later than the end of the business day following the day on which it becomes aware of the unauthorised transaction.

Meaning: this protection is similarly denied to the payer, because the payment does not count as "unauthorised".

P61 under "Liability" - Incorrect unique identifiers
90. (1) Where a payment order is executed in accordance with the unique identifier, the payment order is deemed to have been correctly executed by each payment service provider involved in executing the payment order with respect to the payee specified by the unique identifier.
(2) Where the unique identifier provided by the payment service user is incorrect, the payment service provider is not liable under regulation 91 or 92 for non-execution or defective execution of the payment transaction, but the payment service provider—
(a) must make reasonable efforts to recover the funds involved in the payment transaction; and
(b) may, if agreed in the framework contract, charge the payment service user for any such recovery.

Meaning: this clause acts in support of the banks' defence that the Sort Code and Account Number are the determining data as to where liability lies: if the payer supplied a Sort Code and Account Number that validly identify an account in the payee bank's books, then neither the payer bank nor the payee bank are liable.

90. (5) Where the payment service user provides information additional to that specified in regulation 43(2)(a) (information required prior to the conclusion of a single payment service contract) or paragraph 2(b) of Schedule 4 (prior general information for framework contracts), the payment service provider is liable only for the execution of payment transactions in accordance with the unique identifier provided by the payment service user.

Meaning: the payee name ranks as such "additional information" and this clause discounts that as having relevance, because liability is judged only on the Sort Code and Account Number.

P62 - Non-execution or defective or late execution of payment transactions initiated by the payer
91. (1) This regulation applies where a payment order is initiated directly by the payer.
(2) The payer's payment service provider is liable to the payer for the correct execution of the payment transaction unless it can prove to the payer and, where relevant, to the payee's payment service provider, that the payee's payment service provider received the amount of the payment transaction in accordance with regulation 86(1) to (3) (payment transactions to a payment account).

Meaning: the payer's bank is not liable for defective execution if it made payment to the bank identified by the Sort Code, and then the payee bank did have an account at that Sort Code with the stated Account Number.

P65 - Authentication
100. (1) A payment service provider must apply strong customer authentication where a payment service user—
(a) accesses its payment account online, whether directly or through an account information service provider;
(b) initiates an electronic payment transaction; or
(c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

Meaning: the evidence of authorisation derives from the application of so-called Strong Customer Authentication, the governing rules for which are the Regulatory Technical Standards as issued by the European Banking Authority.

Summary of Meaning of clauses in 2017 PSRs
The banks request the payee name as mandatory information and this data is transmitted from the payer's bank to the payee's bank. Nevertheless 2017 Payment Services Regulations offer the banks complete repudiation of liability for the case where the payee name does not match the name at the payee bank that is associated with the Sort Code and Account Number. The payment counts as "authorised" and as correctly executed when measured by what is in the payment contract.

As a result none of the protections and remedies for defective authorisation or execution are available to the payer.

Purpose of these clauses in terms of support for the Single Euro Payments Area project
This state of affairs has been brought about by the application of EU Directives and Regulations whose main aim was to underpin the construction of the Single Euro Payments Area.

A key element to be underpinned in the Single Euro Payments Area was the permission to transact a payment in euro:

1. between two payment accounts within the SEPA Area using only IBANs as the unique identifiers for the two accounts; and
2. where there cannot be intermediary "payment service providers" (PSPs); and
3. intermediaries (if any) are SEPA Clearing and Settlement Mechanism (CSMs) which are not "obliged entities" and therefore do not have responsibilities under legislation aimed at combatting Financial Crime.

Please refer to Appendix 1 for greater detail on the SEPA Clearing and Settlement Framework within which the CSMs sit, and a comparison with the Faster Payments model.

In the Faster Payments model there can be more PSPs in the payment chain than the payer's PSP and the payee's PSP; in the SEPA model there can be more CSMs. The only PSPs involved in a SEPA payment chain are Account-Servicing PSPs: they hold either the payer's account or the payee's.

This fact means that in a SEPA payment there are no intermediary PSPs who have a responsibility under the Funds Transfer Regulation (which derives from the global Financial Action Taskforce Recommendation 16) to check the presence of payer and payee data, and to screen the payment. Only the payer's bank and the payee's bank have these responsibilities, and we must now examine how Financial Action Taskforce Recommendation 16 has been enacted as the Funds Transfer Regulation in order not to block the IBAN-only tenet of SEPA.

Tie-in with the EU Funds Transfer Regulation 847 of 2015 in undermining the customer's legal position, and in generally failing to combat Financial Crime
The EU's Payment Services Directives (of the second of which the 2017 Payment Services Regulations are the derivative) and the Funds Transfer Regulation are designed to service the SEPA construction, but in doing so they have contributed to APPF, and failed - on an EU-wide basis - to adequately enact a globally-agreed measure to combat Money Laundering and the Financing of Terrorism: Financial Action Taskforce Recommendation 16.[6]

The clauses in the 2017 Payment Services Regulations quoted above deliberately marry up with EU Funds Transfer Regulation 847 of 2015.

The EU's second Payment Services Directive and its Funds Transfer Regulation (FTR) were originally meant to be one piece of legislation called "European Payments Regulatory Package". FTR is meant to create transparency and traceability of the actors in the payment chain for the purposes of combatting Money Laundering and the financing of terrorism.

[6] Financial Action Taskforce (FATF) is the global body, based in Paris, established after 9/11 attacks to put in place global frameworks for Anti-Money Laundering and Countering the Financing of Terrorism – or AML/CFT for short

FTR is the supposed enactment of the Financial Action Taskforce Recommendation 16, whose full text is:
"Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.

Countries should ensure that financial institutions monitor wire transfers for the purpose of detecting those which lack required originator and/or beneficiary information, and take appropriate measures.

Countries should ensure that, in the context of processing wire transfers, financial institutions take freezing action and should prohibit conducting transactions with designated persons and entities, as per the obligations set out in the relevant United Nations Security Council resolutions, such as resolution 1267 (1999) and its successor resolutions, and resolution 1373(2001), relating to the prevention and suppression of terrorism and terrorist financing."

Please note that there is nothing in the Recommendation that differentiates between domestic and cross-border "wire transfers", which means electronic funds transfers and includes credit transfers.

FTR's Article 4 defines the requirements for **"Information accompanying transfers of funds"** and these are in line with the Recommendation:

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.
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.
3) By way of derogation from point (b) of paragraph 1 and point (b) of paragraph 2, in the case of a transfer not made from or to a payment account, the payment service provider of the payer shall ensure that the transfer of funds is accompanied by a unique transaction identifier rather than the payment account number(s).

The above is the umbrella definition but then there is an important derogation (i.e. relaxation) in Article 5 regarding *"***Transfers of funds within the Union"**:

1) By way of derogation from Article 4(1) and (2), where all payment service providers involved in the payment chain are established in the Union, transfers of funds shall be accompanied by at least the payment account number of both the payer and the payee or, where Article 4(3) applies, the unique transaction identifier, without prejudice to the information requirements laid down in Regulation (EU) No 260/2012, where applicable.

This major relaxation of the FATF Recommendation is only explicable in two ways:

- That it eliminates conflict with the construction of SEPA that SEPA payments can be made with IBAN-only;
- That it betokens a view that Money Laundering and Terrorist Financing pertain to cross-border funds transfers, crossing an EU border, or to ones neither in euro nor a Member State currency but which are within the EU.

This second explanation is discernible in the EU's tolerance of the very weak regimes for AML/CFT in Member States such as Malta and Cyprus, in parallel with the EU's constructing a process to identify High-Risk Third Countries – non-EU countries that the EU considers to have very weak regimes for AML/CFT. The presumption that EU countries – and payments flowing between them – are Persil-white from an AML/CFT perspective should not be accepted.

For example, two terrorists who were able to open payment accounts at different PSPs within the EU could send SEPA payments to one another in the certain knowledge that nothing in the payment data could divulge that the payment had terrorist purposes: the payment can be completed with their respective IBANs and the amount, and nothing else. This certainly underpins the Freedom of Movement of Capital within the EU, but leaves a gap regarding Financial Crime.

As a result of the derogation in FTR Article 5, any payment in euro or a Member State currency, where both the payer's and the payee's PSP are within the EU, need only carry the payment account numbers or "unique identifiers" of the payer and payee. It would be assumed not to apply to payments in USD, JPY etc. because of the presumed need to have intermediary PSPs in the payment chain as correspondents located in the USA, Japan and so on.

FTR takes the position that the payee name need not even be passed along the payment chain, and it applies to Faster Payments as a Member State currency payment with both endpoints within the EU, even if the UK is not in the EU any longer.

Recommendation 16 was meant to aid the detection of Financial Crime. FTR allows a major weakening of its efficacy. This should be enough in itself for the UK to re-enact legislation adopting Recommendation 16 and correctly. This might have an impact on APPF if the fraudsters are identified by the screening of the payee name. However, the greater weakness is that the wording of FTR as applied to credit transfers in the UK has become a further plank underpinning of the banks' legal position: the payee name need not even be passed along, let alone screened and processed.

This strengthens the banks in their positioning in firstly denying any liability for APPF, then failing to ensure there is a robust plan to eliminate it, then participating in the non-solutions CoP and CRM, and continuing to run such lax Know-Your-Customer processes as to open accounts for the fraudsters committing APPF.

Recommendations

The legal basis for the banks' positioning needs to be removed.

Firstly the 2017 Payment Services Regulations need to be amended so that the payee name is included in the list of data in its Article 43.2. This causes the payee name to be included in the payment contract as authorised by the customer. The permission to banks to process based only on the Sort Code and Account Number is thereby withdrawn.

Secondly FTR needs to be replaced such as to limit the derogation in Article 5.1 to the data specified in 4.1.c. In other words all UK payments need to include the payer and payee names.

Thirdly the ISO20022 standard UK credit transfer message must carry the payee name and the rules of NPA must lay an obligation on the payee bank to verify the name in the credit transfer message against the name on the account. This must be the arrangement as of Day 1 of NPA.

If the banks between them then contrive to pay a different payee from the one named by the payer, they are liable to make the payer good. Once the payee name is within the scope of the payment as authorised by the payer, all the other protections for defective authorisation and execution are available to the payer, against their own bank (or PSP). If that bank believes it was the payee's bank that was at fault, they can make a loss-sharing agreement amongst themselves without that affecting the payer's rights.

Anticipated pushback and conclusion

The banks will counter that this will cost them hundreds of millions of pounds, and it certainly will.

Nevertheless it is the banks that originally accepted Vocalink's flawed technical solution for the construction of Faster Payments and who have pursued business policies in their own interests to sideline cheques, to elevate the Faster Payments system to their channel-of-choice for receiving and processing domestic payments for UK customers, and in due course to make it the nodal system for all other systems under NPA.

Those other systems will then become NPA "overlay services" sitting on top of Faster Payments, in the same way CoP is an "overlay service" now.

Serving these interests and following this routemap will continue to cost UK customers hundreds of millions of pounds but PER ANNUM.

Faster Payments is not fit-for-purpose and the current specifications for NPA do not resolve it; rather they entrench the problem by making Faster Payments the nodal system in NPA.

Instead the prime purpose of NPA should be re-set to being the elimination of APPF. The inclusion of the payee name in the payment contract and the necessity of its being checked at the payee bank should be Day 1 deliverables of NPA. On the same Day 1 CoP can be retired along with CRM; customers will have an incontestable right to compensation, failing which they will have their normal avenue of redress to the Financial Ombudsman. CoP and CRM will no longer be needed.

The APPF problem can be solved and the banks will solve it – once they are faced with potential pay-outs of hundreds of millions of pounds per annum. A positive business case for checking the payee name will magically appear, even if it costs £100 million per bank, because of the enormous savings in future customer compensation payments.

Appendix 1 – structure of clearing and settlement arrangements in the Single Euro Payments Area

There are two SEPA credit transfer services:

- The "core and basic" SEPA Credit Transfer payment was launched in 2008 with a target service level of D+1, where D is the day on which the payment was initiated. D+1 became the obligatory maximum as from 1st January 2012 under the terms of the first EU Payment Services Directive 64 of 2007;
- The SEPA INST service (Instant SEPA payment) - the counterpart SEPA service to Faster Payments - was launched in November 2017 with a maximum payment amount of EUR15,000 (Faster Payments - £250,000.

The wording governing the execution timeframe for the "core and basic" SEPA Credit Transfer is that "the amount of the payment transaction is credited to the payee's payment service provider's account at the latest by the end of the next business day". The service was not instant or same-day, and indeed can take nearly two days.

The SEPA INST service has an execution timeframe of 10 seconds.

It is obligatory for the thousands of financial institutions in the SEPA Area to be reachable – i.e. all of them can send a payment that reaches any other within the execution timeframe.

However this has to be done within the so-called SEPA Clearing and Settlement Framework, which is a part of the "layered market model" that the European Payments Council designed for SEPA (and which is integral to the UK's NPA project as well).

Originally it was hoped that 3 or 4 pan-European organisations would emerge, with high scale and each with thousands of member banks, to handle clearing and settlement. These were referred to as P-EACHes – Pan-European Automated Clearing Houses.

Instead we have fruit salad of national, trans-national and pan-European clearing systems (such as STET, Iberpay, and EBA STEP2 to name but three). These go under the name of SEPA Clearing and Settlement Mechanisms (CSMs).

Each payment service provider (PSP) must be directly connected to at least one such SEPA Clearing and Settlement Mechanism, and then these CSMs connect to one another under a concept called "interoperability". This is for the case that a member of one CSM sends a payment to a PSP that is a member of a different CSM. The CSMs have had to construct pathways between one another to get such payments to their destination.

This "interoperability" has worked satisfactorily for the "core and basic" SEPA Credit Transfer with a D+1 execution timeframe, but it has not worked optimally for payments with 10-second execution timeframe, and especially when query, rejection and return messages are needed.

There are ongoing discussions about using the ECB's TIPS system (TARGET2 Instant Payment System) as the universal clearing and settlement system for SEPA INST, instead of using the same model as for the SEPA D+1 service.

It is important also to recognise, for the purposes of comparison to Faster Payments, that there cannot be an "intermediary payment service provider" in the Single Euro Payments Area between the two PSPs where the payer account and payee account are held. The payer's PSP must transmit the payment directly into a CSM, and not through another PSP.

If the payee's PSP does not belong to the same CSM, the CSMs find a route through "interoperability" described earlier. These CSMs do not count as "intermediary PSPs" or, to use old world terminology, correspondent banks.

There are possibilities for smaller PSPs to be sponsored into a SEPA CSM by larger PSPs, but they still count as members and are directly addressable. That means that their message traffic is routed directly between themselves and the CSM. It does not pass through their sponsor and the sponsor has no visibility of it. The sponsor's role is limited to standing in for the PSP's ability to settle – the credit risk. The sponsor is not regarded as – and is not technically – part of the payment chain for the purposes of screening for fraud, AML/CFT, or sanctions.

The sponsor could anyway not take any relevant actions regarding the traffic even if the traffic was routed through them or made visible to them: a payment with IBAN-only as the payer and payee information is not screenable for fraud, AML/CFT, or sanctions.

The UK sponsorship model is different, with very few Directly Connected Participants and the numerical majority of PSPs connected indirectly. The payment traffic then goes through the sponsoring PSP or (under the Faster Payments model called Directly Connected Non-Settling Participant) it is copied to the sponsoring PSP. The sponsor is regarded as – and technically is – part of the payment chain. The sponsor is in a position to screen the payment for fraud, AML/CFT, or sanctions, the sponsor is an "obliged entity" and indeed UK sponsor banks do see this as their responsibility.[7]

In the Faster Payments model there can be more PSPs in the payment chain; in the SEPA model there can be more CSMs. A critical point derives from that: CSMs are not "obliged entities" and have no AML/CFT obligations. Only the PSPs have that responsibility and in a SEPA payment the only PSPs in the payment chain are both Account-Servicing PSPs: they hold either the payer's account or the payee's.

This fact means that in a SEPA payment there are no intermediary PSPs who have a responsibility under the Funds Transfer Regulation to check the presence of payer and payee data, and to screen the payment. Only the payer's bank and the payee's bank have these responsibilities.

As described above, these responsibilities are considerably diminished for certain payments with both endpoints within the EU. The respective legislation is meant to enable SEPA, while having the effect of turning a blind eye to AML/CFT failings as long as they do not cross an EU border, but it has caught Faster Payments in its net and contributed to the opening of the gates to APPF.

BL/10.1.22

[7] The subject has been extensively discussed and recently in an industry working group coordinated by Pay.UK called "Liability under Indirect Access Models"