Lyddon
CONSULTING

+44 (0) 7979 132 341
enquiries @lyddonconsulting.com
www.lyddonconsulting.com

2nd February 2023

**Open letter to Project Financial Crime**
**c/o The Payments Association**

Dear Sirs,

It is laudable that The Payments Association should undertake to improve the environment for fighting financial crime within the Fintech industry, but priority should be given to the elimination of certain practices commonly used by the Fintech industry, which have created opportunities for financial crime.

The Fintech industry has crafted these practices for the sake of customer convenience in both accessing and using services, in a manner that is at odds with what should prevail were AML/CFT compliance to be seen as a minimum level to be exceeded, and not as an arena where competitive advantage can be gained by seeking out, creating and exploiting supposed ambiguities in the requirements.

The practices have the effect of short-cutting the Customer Due Diligence (CDD) process, enabling the usage of IBANs where no account exists at the Payment Service Provider (PSP) to whom the IBAN is identifiable, and preventing transparency over how many PSPs are involved in individual payment chains.

The practices are used cumulatively. Not all Fintechs use all or any of them, but it is common for a Fintech to use more than one, and then of course the divergence of that Fintech from the true path of AML/CFT compliance is exacerbated.

A cleansing can be initiated by the adoption of three measures as a priority for Project Financial Crime to deliver. Then a solid basis will exist for the other matters that appear to be within the project's scope to be addressed. Adoption of these measures will demonstrate the Fintech industry's commitment to a full and proper implementation of AML/CFT regulations from the ground up:

1. Limitation of the scope of the 'reliance' that can be placed on Trusted Third Parties;
2. IBANs used by an account-holder must be identifiable to the PSP that acts as Account-Servicing Institution (ASI) for the account-holder, which means the ASI that has performed either ordinary CDD or Enhanced Due Diligence (EDD) on the account-holder;
3. Nesting must be made visible in payment messages by the identification of all Intermediary PSPs acting in the payment chain.

It follows from point (3), as will be further explained below, that:

1. Fintechs – which are Financial Institutions or FIs – cannot continue to use SWIFT Corporate Access;
2. The ISO20022 XML UK credit transfer message, contemplated by the Bank of England and Pay.UK for usage in RTGS Renewal and New Payments Architecture respectively for FI-to-Customer payments, is likely to prove inadequate;
3. The ISO20022 XML FI-to-FI credit transfer message needs to be developed to the same level as the FI-to-Customer message.

**Limitation of the scope of the 'reliance' that can be placed on Trusted Third Parties (TTPs)**

Fintechs routinely ask for the existing bank account details of their prospective customers, as if the existence of an account at a bank can be relied upon as proof that the customer is a good actor solely on the basis that the respective bank is an 'obliged entity'. The Fintech considers itself then justified in shortcutting ordinary CDD and not installing any triggers for carrying out EDD, let alone actually carrying out any EDD. Indeed this 'reliance' may be sufficient for the Fintech to pretend that its service merits only Simplified Due Diligence.

The bank where the account is held has no business relationship with the Fintech. There is no correspondence between the Fintech and the bank regarding the customer. The Fintech has no idea what CDD the bank went through, whether it threw up any 'red flags', whether EDD was carried out and so on.

The result is that bad actors, who have managed to obtain a bank account and slipped through the net at that bank FI, can proliferate their business with multiple Fintech FIs on the basis of a CDD weakness at the bank FI.

This facilitates Authorized Push Payment Fraud: the scammers move the stolen funds through this chain of accounts and then into the ether.

It should be obvious that AML/CFT regulations limit the manner and degree to which one 'obliged entity' can place reliance on the CDD work of another, but obviously not explicitly enough. There is thus a need for repetition of and subsequent adherence to the limitations, including but not only the following:

1. TTPs must in all cases also be 'obliged entities' themselves;
2. There must be a contractual relationship between the TTP and the FI using that TTP;
3. The contract must list the CDD tasks that the TTP is going to carry out for the FI and to what level;
4. The contract must specify the input data that the TTP will receive from the FI in respect of each individual customer case, for the TTP then to perform its tasks;
5. The contract must specify the output data that the TTP will send back to the FI;
6. The FI must document the business processes for the compilation of the input data, the analysis of the output data, and the flow chart for the making of the decision to go ahead, to reject, to invoke EDD and so on in each individual customer case;
7. The FI remains responsible for the decision to go ahead.

**IBANs used by account-holders must be identifiable to the PSP that acts as Account-Servicing Institution (ASI) for them, which means the ASI that has performed either ordinary Customer Due Diligence or Enhanced Due Diligence on them**

Fintechs routinely give out IBANs without their having registered for a domestic bank routing code (like a UK Sort Code) or a SWIFT BIC, two prerequisites for IBAN issuance.

This is because they have engaged with another FI, which does have a domestic routing code and a BIC, and the capacity to issue IBANs. This second FI breaks off a series of IBANs identifiable to itself, and passes them to the first FI. The first FI then issues those IBANs to its customers, upon whom it has done whatever level of CDD. The arrangement between that FI and the user of the IBAN may be ineligible to have an IBAN on its own: it may not amount to an account relationship, there may be no 'payment account' in the legal sense, and the CDD may have been Simplified Due Diligence, possibly based on the provision of the details of an existing bank account with the concomitant pitfalls as described earlier.

Nevertheless, the customer is equipped with an IBAN and can access all the benefits that entails, such as being accounted a good market actor and able to access numerous payment schemes.

The FI to whom the IBAN is identifiable, however, has no relationship with the IBAN's user, may not even know what entity is using it, and has no CDD file on the user.

This is a nonsense and rests on a misconstruing of what an IBAN is.

An IBAN is not a routing code. It has the effect of a warranty issued by one FI, acting as ASI, to the other actors in a payment chain that the ASI accepts the responsibilities allocated to it under applicable AML/CFT regulations. These comprise both the CDD or, as the circumstances demanded, EDD prior to the opening of the account for which the IBAN is a Unique Identifier (within the meaning of the EU Payment Services Directive), and the responsibilities laid on it for example by Funds Transfer Regulation 847/2015 for the handling of every payment.

There cannot be any difference between the FI to which the IBAN, thanks to its composition, is identifiable, and the ASI – the FI that has carried out CDD/EDD on the IBAN's user.

Ipso facto, no FI should issue an IBAN unless it has performed at least ordinary CDD on the entity to which the IBAN has been issued, and EDD as the circumstances demand.

Ipso facto, no IBAN can be associated with an arrangement that merits only Simplified Due Diligence.

Knowing that a customer has an IBAN already cannot be used, as per the previous section, to shortcut the CDD process for setting up an account at another FI – and then issuing another IBAN on that account as well. That fallacy leads to a chain of accounts that facilitates Authorised Push Payment Fraud.

**Nesting must be made visible in payment messages by the identification of all Intermediary PSPs acting in the payment chain**

Nesting is where one Fintech uses another Fintech as its main PSP. Nesting may have several layers until eventually there is a PSP that has direct access to payment schemes and systems. For each payment, then, there is a Payer's PSP, and one or more Intermediary PSPs, prior to the payment running through a payment system. On the payee side as well there may be several Intermediary PSPs relaying the payment before it finally reaches the Payee's PSP.

This arrangement is enabled by 'virtual' IBANs as described above; in that case the IBAN is normally identifiable to the Intermediary PSP that is the payment scheme member, and the IBAN has then been passed on – possibly several times – to the FI that has the relationship with the payer or payee.

AML/CFT demands transparency, and nesting interdicts it.

In order that transparency be delivered, all the FIs in a payment chain must be visible in the payment messages sent down that payment chain. Multi-level nesting would certainly challenge the payment messages used for CHAPS now (SWIFT MT), for BACS (Standard18), Faster Payments (ISO8583) and SWIFTFin payments (SWIFT MT), and may not even be feasible using current versions of ISO20022 (SEPA and in due course all of CHAPS, BACS, Faster Payments and SWIFT payments).

The current situation negates the responsibilities of Intermediary PSPs under Funds Transfer Regulation 2015/847 to check the presence of payer and payee information: if the Intermediary PSPs are invisible, it is impossible for financial regulators to verify their compliance.

The standard to be aimed at is that all Intermediary PSPs must be identified in the payment message.

Ipso facto, if there is not space in the payment message to include all Intermediary PSPs, then that payment message format cannot be used.

Ipso facto, if a payment scheme does not offer messaging in which all Intermediary PSPs can be identified, then nesting arrangements need to be collapsed down to a point where the maximum number of levels is what can be accommodated in the scheme's payment messages.

This issue is likely to prove problematical in the case of the launch version of the ISO20022 XML UK credit transfer message, contemplated by the Bank of England and Pay.UK for usage in RTGS Renewal and New Payments Architecture respectively for FI-to-Customer payments. The content of this message is a like-for-like with what exists now. Given the threat to financial stability posed by financial crime, there can be no delay to a v2 or v3 for the incorporation of the identification of all Intermediary PSPs: this must be a Day 1 deliverable.

A further twist is that the issue affects FI-to-FI payments as much as FI-to-Customer payments: the work to identify all Intermediary PSPs needs to be replicated across the ISO20022 messages for both types of payment. Plans for RTGS Renewal and New Payments Architecture need to be re-visited accordingly, or else Fintechs can simply forego their access to the respective UK payment systems until compliance is achieved.

However, it is perfectly possible that a barrier will be reached in this area, in the sense that there could be objections in principle to ISO20022 messages accommodating a three- or four-layer nesting, even if it is technically feasible to develop and deploy any new fields required. Payment scheme managers and/or other FIs and/or financial regulators may decide it is unacceptable to them and presents too much risk. A two-layer nesting might easily be the limit of the payment ecosystem's appetite: a payment scheme member has FI clients who in turn act for other FIs who have business and personal customers. Were that to occur, nestings with 3+ layers would not be able to make payments, and the Fintechs involved would have to either seek a more direct access path to payment systems or close down.

**Usage by Fintechs of SWIFT Corporate Access (SCORE)**

It also flows from the above point that Fintechs – which are Financial Institutions or FIs – cannot continue to use SWIFT Corporate Access or SCORE: FI-to-FI payments are in that case transacted using messages destined for FI-to-Customer payments. At the latest by the end of the SWIFT migration window for ISO20022 – as that seems to be the ubiquitous future message format – the proper distinction must be restored between Customer payments and FI payments.

Fintechs have been mistakenly allowed to become SWIFT members through SCORE, which is contemplated for corporates and not for FIs. Of course the rationale is that it is cheaper and quicker to join SCORE than it is to set up as a proper FI: it is a shortcut to SWIFT membership which SWIFT itself should arguably not have countenanced.

The AML/CFT problems arise through the consequent misuse of Customer messages instead of FI messages - misusing MT1nn series messages where MT2nn series messages ought to be used.

In a 2-layer example of nesting, a Fintech uses an Intermediary PSP (CurrencyCloud being a prominent one acting in this role), not necessarily to settle individual payments but to fund the 'nostro' accounts from which the Fintech settles such payments.

The Fintech might have accepted £pound from its customers for payments to be settled to beneficiaries in Thailand in Thai baht. The Fintech sells £pound to the Intermediary PSP and asks that the countervalue be sent by the Intermediary PSP to the Fintech's 'nostro' account at an FI in Thailand.

Being a payment from one FI to the 'nostro' account of another FI, the SWIFT MT202 should be used.

However, because the Intermediary PSP has joined SWIFT via SCORE, it is precluded from sending MT2nn series messages. Instead it has to send an MT103, and this creates problems such as:

1. Other Intermediary PSPs will see the MT103 and ask what customer payment is behind it, where there isn't just one, or even one at all when the payment's purpose is to increase the balance on the Thai baht 'nostro' account;
2. Other Intermediary PSPs might suspect that there is an MT202 COV running down a different route, without the supporting customer information being visible in the MT103;
3. Either way, other Intermediary PSPs may well divert the payment into an enquiry queue and raise an enquiry back down the payment chain, which at the very least causes delay.

Fintechs should migrate off SCORE and onto the normal SWIFT membership model for an FI, at the latest by the end of the SWIFT ISO20022 migration window. They should use the messages within the ISO20022 book designed for usage between FIs (which will predominantly be the 'pacs' series) for FI-to-FI payments, and 'pain' series messages for FI-to-Customer payments.

All messages will need to identify all Intermediary PSPs, as per the previous section.

**Conclusions**

These are basic problems with the practices adopted by the Fintech industry and which amount to constructive non-compliance with applicable AML/CFT regulations. They enable Authorised Push Payment Fraud. They interdict transparency. They enable bad actors to obtain accounts, IBANs and access to payment schemes. They do not so much exploit ambiguities in the wording of AML/CFT regulations as create and exploit ambiguities which do not exist, and thereby open the door to bad actors.

Whatever scope is adopted for The Payments Association's Project Financial Crime, the project will have little substantive effect if these problems are not eliminated.

I do not underestimate the size of threat to the Fintech industry that the measures outlined above represent. You must know as well as I do that the business models of many Fintech firms hinge on the usage of the related practices. The preferred course would be that the firms shut down if they cannot adhere to these measures and, if that substantially reduces the Fintech universe, there will be a concomitant benefit to wider society in terms of alleviating financial crime, a major and growing scourge that I am sure your Association is as dedicated to eliminating as your Association's members.

Yours faithfully,

R.J.Lyddon