Paym Account Name Verification Service

In its draft strategy report, the Payments Strategy Forum expresses a desire to increase trust in the payment system, with the aim of increasing security and reducing financial crime. The strategy also calls for co-ordinated campaigns to give businesses and consumers the tools to help them reduce the threat of becoming victims of fraud.

This response is concerned with two areas outlined in the strategy – payment assurance for consumers, and account name assurance for direct debit originators.

The draft strategy identifies that Paym provides payment assurance for consumer to consumer payments across its registered base, but also that it is limited in its scope and therefore capability to provide assurance across all payment types. Paym is used today for person to person and person to business payments, and is in effect an overlay service over the Faster Payments and LINK schemes.

The draft strategy points towards a future where Open Banking APIs will be used to deliver functionality that enables consumers, either directly or via PSPs, to confirm the identity of the account they are attempting to pay to, and to receive feedback on the status of the payment. This same technology can be offered to Direct Debit originators to determine the ownership of any account being presented in a new mandate.

This approach depends upon individual banks' abilities to develop both the Open Banking API functionality, and make the data on their own systems available through it. Additionally, they will need to connect out to other organisation's systems to access their versions of the same data.

Consultation Question 4 asks if there is a case for transitional solutions whilst this functionality and connectivity is put in place. Our response talks to that point.

Paym enables consumers to make payments using a phone number as a personal identifier for the payee, rather than a bank account and sortcode. The customer is advised of the name of the account they are attempting to pay to, and through either Faster Payments or LINK scheme, the payments are made instantly by the participants in those schemes.

The core asset of the Paym system is its database linking phone number, or other proxies, to bank account details. The data is stored securely in a high performance, high availability environment hosted by VocaLink accessed via an API published to participants using JSON. There are currently 10 bank and building society groups involved in Paym, reaching a possible 97% of UK current accounts. Additionally many of these organisation are either able to or are in the process of building facilities to offer PSPs access to Paym on a white-labelled basis.

Challenges/Dependencies for building an Open Banking API solution for Account Name Verification, vs an evolved Centrally hosted solution:

- **Banks will need to build a customer interface to offer the name verification service** – this is true whether the information is sourced through open banking APIs between PSPs or through an API to a centrally hosted platform.

- **Banks will need to build connectivity to other organisations in order to utilise their Open Banking APIs** – Bank A might have made available its data to other banks, but the other banks' customers won't be able to access that data until the other banks can connect to Bank A.

- **Banks will need to identify which other organisation owns the details for the account number being paid to,** for example using functionality similar to the sortcode databases operated by the payment schemes.

- **Banks will need to determine if an account number has been the subject of an account switch**, and act accordingly to determine the account owner's name.

  Where a customer is attempting to make a payment to an account which has switched, their bank will need to identify this situation and either attempt to find the ultimate destination to determine the account name, or else decline to offer the verification service. Declining to offer account name verification on switched accounts would place account switchers at a disadvantage detracting from the utility of the Current Account Switching Service (CASS) which is not in the interests of end customers.

  Any Open Banking based solution will need to determine how to solve this problem, particularly in the case of customers who have switched multiple times.

- **Banks will need to comply with the provisions of the Data Protection Act,** and ensure that their data is used in a manner consistent with that compliance when it is used by other banks.

Roadmap to a distributed solution

An evolving Central solution doesn't hinder development of Open Banking based solutions

Example:

- Bank A makes its data available through an Open banking API.
- Bank B uses a Central solution

In this scenario, for any organisation to make a payment to either Bank A or B, they must first determine which organisation hosts the account, taking into account the impacts of the CASS.

To achieve a fully distributed Open Banking API solution, a number of changes to the way that current account switch data is handled would be required. Today, account switch information, particularly directing or redirection of payments, is handled at the payment system level, after the point at which a customer has authorised a payment. The absolute view of which customers have switched and where they have gone to exists in databases outside of the banks. This ensures that no single bank can see market sensitive information about what their former customers have done after leaving them, or which other banks are winning or losing in the account switching market. Placing these databases within the banks' systems would enable banks to determine the final destination of any intended payment, but would at the same time give them access to this sensitive, competitive information.

Alternatively, account name verification queries could be directed toward an evolving central infrastructure which would resolve them before responding back with the correct organisation to talk to. This method would support organisations which choose to host their account data on a central depository, or make it available through Open Banking APIs.

Because of the complexity described above, and the need to solve problems which are currently already addressed, it should be apparent that a migration to a fully distributed solution is neither quick nor easy to solve. In the meantime customers will continue to make misdirected payments, either as a result of mis-keying data, or as a result of fraud actions. In addition, businesses collecting direct debits will be left with a complex system in order to validate the claimed ownership of a debit account during the set-up process.

MPSCo believes that rather than leaving this gap open or partially open until all Banks are able to address these points through Open Banking APIs, the customer-centric approach would be to commission the functionality to be delivered as early as possible.

In particular, MPSCo believes that its existing infrastructure can be adapted in order to

- fulfil the consumer and business requirements for account name verification,
- in a cost effective manner, in the immediate future.
- Integrate the data created by CASS with the sortcode lookup database,
- in a highly secure, low latency environment
- whilst constructing a model which would support Open Banking API deployments as they become available.

-oo0oo-