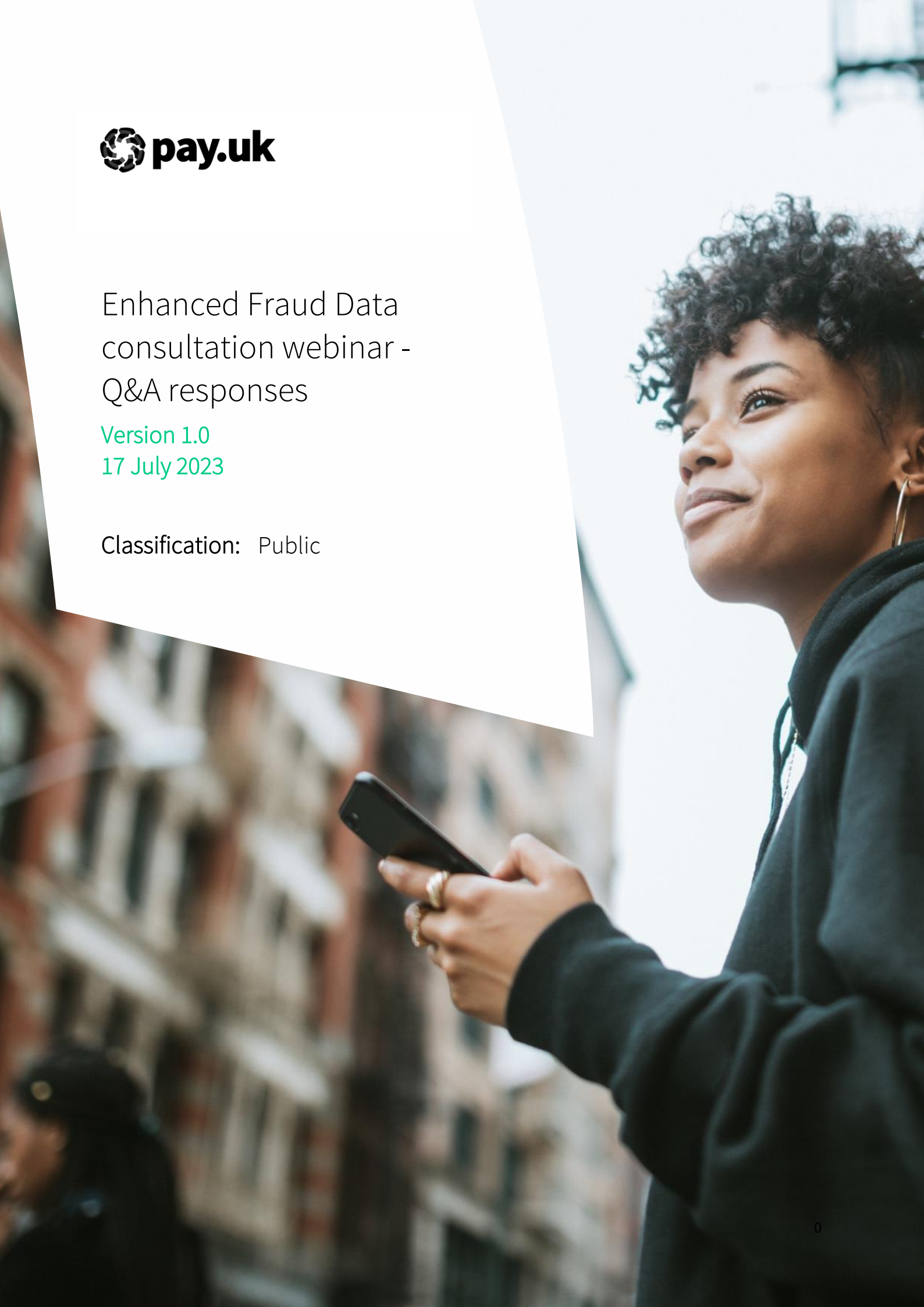


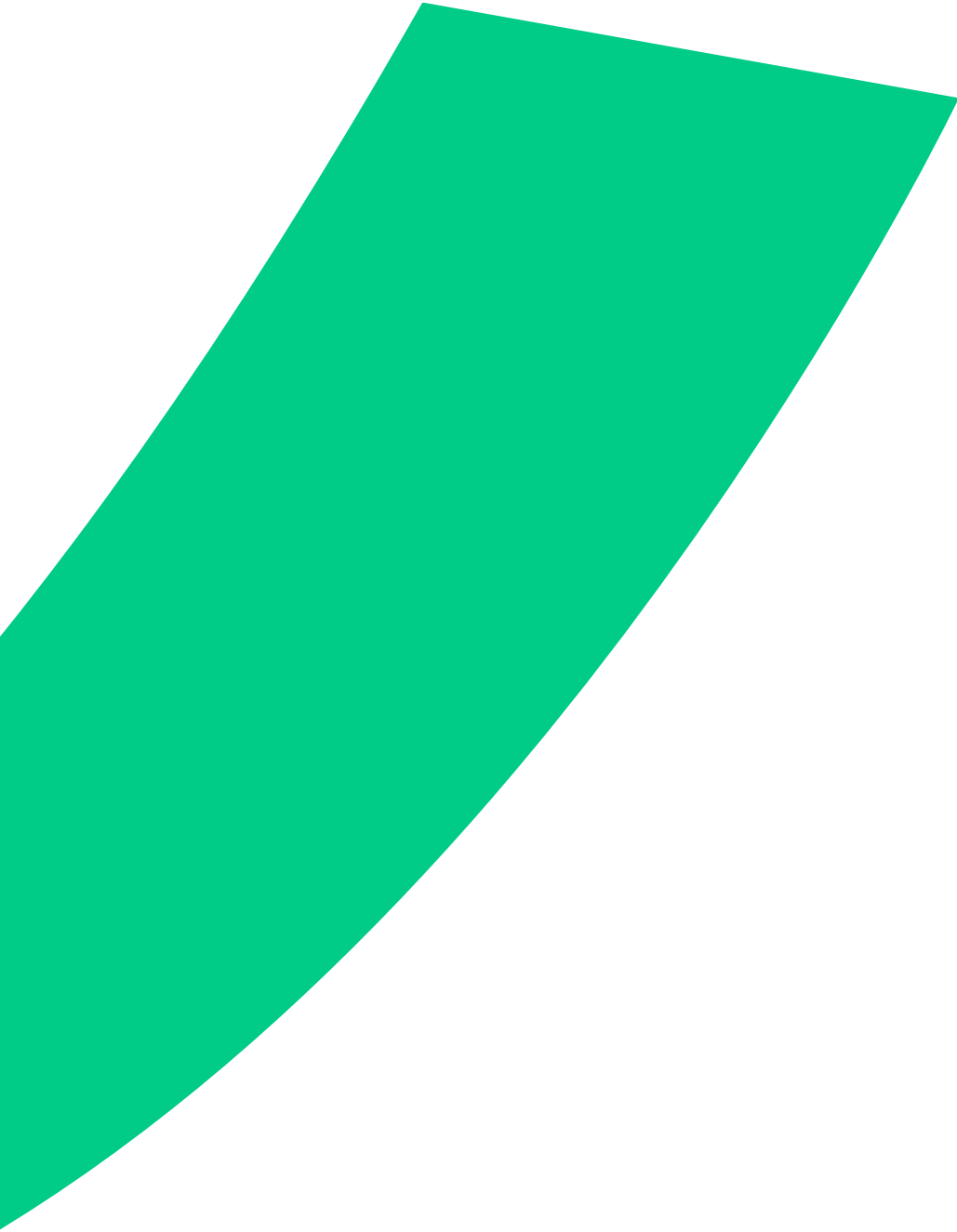


Enhanced Fraud Data consultation webinar - Q&A responses

Version 1.0
17 July 2023

Classification: Public





1 Enhanced Fraud Data (EFD) standards

Addressing fraud across payment systems is a critical priority. Working with key players including the Payment Systems Regulator (PSR) and UK Finance (UKF), we are taking a leading role in the industry-wide two-year strategy to tackle and prevent fraud and scams, covering action by all stakeholders that can affect the customer journey, keeping in mind that most fraud is initiated outside the payment system.

As part of addressing the main challenges around Authorised Push Payment (APP) fraud, we have worked with UKF to agree a common approach to industry engagement. As part of this, we have developed an Enhanced Fraud Data (EFD) messaging standard, capable of carrying data in a pre-agreed, structured format. This means that the data could be used more quickly and easily by economic crime (EC) specialists to facilitate informed detection of potential fraud, for both sending and receiving organisations. To help maximise the chances of identifying APP fraud, the EFD messaging standard is specifically designed for a pre-payment initiation message exchange, carrying data points between the sending and receiving financial institutions.

Standardisation of Data

Standardisation of data is a solution that can address some of the existing challenges around data exchange. If all parties agree how the information being sent should be structured and defined, it ensures that a sender and receiver will have the data in exactly the same format.

Industry Webinar

As part of our continued collaboration with the wider payments industry to mitigate payment fraud, we invited a range of industry representatives to share their views, via a webinar, on the first iteration of technical collateral for our EFD standard.

This webinar provided us with the opportunity to explain the work we have done to date, introduce our proposed next steps, and gather industry input and feedback.

The webinar was aimed at specific roles and functions within the industry, including those:

- a) Involved with tackling economic crime
- b) With an interest in ISO 20022 and open banking standards
- c) Working in data architecture
- d) Working in risk and legal in payments businesses
- e) Those with an interest in payments innovation, focusing on tackling industry challenges.

2 Webinar - Questions and Answers

We recorded the questions received from industry representatives at the webinar and have answered these below.

Ref	Question	Pay.UK Response
1	Did you say there would be separate guides for sender and receiver?	No, just one guide covering both.
2	10 mandatory fields out of 22 for sending and 5 out of 12 for receiving. Is that correct?	Yes, that is correct.
3	What are the chances the Payment Service Providers (PSPs) will populate the optional fields?	Still to be determined as this will be subject to data availability.
4	Did the account types identified include prepaid accounts, e-commerce, merchant acquiring, or other e-money accounts?	Yes, they were all included.
5	Will this data "check" be able to be used outside of a payment flow or by third parties who are not banks? Accountancy platforms, etc?	Outside payment flow, meaning to check when a payment is associated either pre or post - yes. Non-banks - no.
6	With the service aiming to take place in real time, are there any parameters for how best to deal with potential out of hours requests? Or is it at the bank's discretion?	The service should be available 24/7, with the exception of individual participants having outages or planned maintenance/update windows.
7	Do you feel the Payment Systems Regulator (PSR) will legislate smaller PSPs to sign up? And when do you think the EFD will reach critical mass? i.e. 2023 or further out?	The PSR has no immediate plans to mandate the EFD service, although pressure will continue on the regulator and government, if APP fraud is not brought under control. Ideally smaller firms would participate for more effective fraud prevention coverage.
8	Where can we find the list of mandatory fields?	Within the EFD standard area of Standards Source there are two documents - EFD_Request_V01.pdf and EFD_Response_V01.pdf. These define the fields used in EFD. Day one proposed mandatory fields have column "Mult" value equal to "[1..1]".
9	Are all banks and building societies going to sign up to this standard or is it a choice?	A choice for now. See Question 7, above.
10	Can you explain in a bit more in detail, how this new standard will help detecting money laundering and APP scams (If it is within the scope of the discussion)?	<p>The EFD service will deliver an (Application Programming Interface) API that enables bi-lateral sharing of data between customers for two primary business use cases:</p> <ol style="list-style-type: none"> 1. Upon setting up a new beneficiary; and/or 2. Risk based scenarios i.e. on subsequent occasions when economic crime is suspected, as fitting to the risk appetite of the customer. <p>The proof of concept demonstrated that a small number of data points, regarding the receiving customer, could have prevented fraudulent payments being made. Post day one, we will monitor the effectiveness of the data being shared and enhance the standard if deemed beneficial.</p>
11	Did you say that a receiver can initiate a message request following an inbound payment or is it always the sender who initiates this?	Yes, that is correct. All customers can act as requesters and responders, should they choose to do so.
12	What is the intended timeline for delivery of a live service?	Q1 2024.
13	Will there be a time frame requirement prior to the payment for the messages to be exchanged between the sender or receiving?	It is at your discretion as to whether you do this and EFD check for every payment, or just when setting up the beneficiary. Different institutions have different risk appetites.
14	Where does the EFD messaging fit in the chain alongside Confirmation of Payee (CoP) and the payment being instructed?	We would see this as complimenting CoP. It is at your discretion as to whether you do an EFD check for every payment or just when setting up the beneficiary. Different institutions have different risk appetites.
15	How early in transactions are checks implemented? Is it prior to payments or as payments are made. Or after payments have gone through and suspicion has arisen?	This is at your discretion. See Question 15, above.

16	Does the flow allow for the responding PSPs to communicate their own risk view with the payload?	No, as this introduces liability.
17	With the data standard, how can we introduce demographic data or information, such as the household risk. For instance, the entire patterns of customer behaviour and not just the individual account held by the bank?	For consideration post day one.
18	If the originating PSP is the payee PSP, how can the EFD exchange be a pre-payment initiation? How would the payee PSP know that a payment was about to be initiated?	It is the payer that requests and EFD checks, typically to check where a payment is being made to.
19	What role, if any, is envisaged for open banking Third Party Providers (TPPs) in this work? As described, it seems to involve only the payer's and payee's account servicing PSPs (Account Servicing Payment Service Providers).	For day 1, PSD2 TPPs are currently out of scope of EFD.
20	Are we able to provide scores derived from bureau data and patterns, that can be returned via the messaging framework and used by the payment initiator? For example, a mule propensity score (generated at point of origination and frequently refreshed)?	EFD is not a scoring service.
21	Have mortgage accounts and other loan accounts been included in the analysis?	Yes, we have discussed this with mortgage/loan account holding PSPs and how EFD can be applied accordingly.
22	If I am a Payment Initiation Service Provider (PISP) using open banking APIs to initiate a payment, is the expectation I use this API or should the sending bank I am instructing to initiate a payment perform the EFD check (or both)?	The sending bank would be expected to initiate the check i.e. the holder of the funds.
23	Could you provide more information on the account reference (both for debtor and creditor)? Could it be used to provide secondary reference data?	This is not mandatory. Assigned by the debtor/creditor i.e. trans ID/payment reference.
24	Can the EFD request be sent by the PSP receiving a payment to assess whether it wants to accept or return the payment?	Yes, that is correct. See Question 11, above.
25	Do you anticipate any blockers in relation to sharing data between parties and General Data Protection Regulation (GDPR)?	Not at present but completion of the core Data Protection Impact Assessment (DPIA) and Information Commissioner's Officer (ICO) impact assessment/guidance will confirm this. Estimate to complete: July 23.
26	Are any of the data points that will be shared, under the purview of GDPR? And if so, what remediations can we as a PSP take (beyond updating terms and conditions (T&Cs) with our partners/customers)?	The core DPIA and ICO guidance will confirm.
27	I'm assuming that this solution would also be used for areas such as an unsecured loan pay-out to a recipient bank account, to then reduce the risks of impersonation fraud/Non-Intelligent Terminal Protocol (NITP)?	EFD can be used where you have a sort code and account number. There is no restriction on the type of account.
28	Based on your discussions with the ICO, on what basis is the sharing of PII deemed ok?	To be confirmed once draft DPIA is shared.
29	Is there anything to stop the use of the data in areas that are not related to APP? For instance, verifying bank details that are being used to setup direct debits?	Yes, our T&Cs and operations guide i.e. rules. Verifying bank details to set up a Direct Debit is acceptable, as this will help prevent fraud but using bank details for marketing purposes would not be acceptable.
30	Post consultation and as we move into privacy/legal governance and downstream internal solutions builds, how does Pay.UK anticipate future discussions on the standard as these become clearer?	We will agree a frequency of the EFD standards review with UKF.
31	Will this be mandated to the CMA 9 initially?	We would not expect any mandate to be so limited as the coverage needs to incorporate all sizes of participants to be effective in fraud prevention.
32	Will there be a developer's portal / test environment to connect to and send sample requests? When will that be available?	Yes, technical accreditation will be required for onboarding.
33	What if the two parties have a different view on whether the payment should proceed based on their risk engines coming to different conclusions?	It is up to the sending party.
34	How does the "pre-transaction only rule", fit with the receiving bank sending an EFD request?	It is not pre-transaction only, but risk based. See Question 10, above.

3 Next steps

Our work on standardising additional data will continue this year. This work will seek to understand how we can create additional opportunities for using the enhanced data we have consulted on more broadly, through our standards work for the New Payments Architecture (NPA).

Data exchange is absolutely key to enabling improved detection of suspect payments. Creating a data standard, specifically to tackle APP fraud, can help play a key role in this fight.

We would like to thank all industry representatives for their input to our webinar and look forward to building on these relationships further, as we develop our standards work.

For further information, please contact efd@wearepay.uk.

2023 © Copyright in this document lies with Pay.UK Limited. All rights reserved.

The copyright in this document is owned by Pay.UK Limited. All material, concepts and ideas detailed in this document are confidential to Pay.UK. This document shall not be used, disclosed or copied in whole or in part for any purposes unless specifically approved by Pay.UK.