Faster Payments QIAT

Proposer: Dwolla, Inc.

February 21, 2017

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Proposal</td>
<td>2</td>
</tr>
<tr>
<td>Q&amp;A Response</td>
<td>167</td>
</tr>
<tr>
<td>Draft QIAT Assessment</td>
<td>199</td>
</tr>
<tr>
<td>(Includes proposer comment in Appendix A &amp; B)</td>
<td>213</td>
</tr>
<tr>
<td>Task Force comments</td>
<td>218</td>
</tr>
<tr>
<td>Proposer response to Task Force comments</td>
<td>228</td>
</tr>
<tr>
<td>Final QIAT Assessment</td>
<td>239</td>
</tr>
</tbody>
</table>
Faster Payments Task Force Proposal

*Dwolla FPS*

April 29, 2016

Submitted by: Contributors\(^1\) at [Dwolla, Inc.](https://www.dwolla.com)\(^2\)

---

\(^1\) Name of contributors can be found on the last page this submission

\(^2\) https://www.dwolla.com/
Proposal Template

Executive Summary

Provide a high-level description of what the solution does from end to end. In providing the description, proposers should highlight the main improvements the solution achieves over existing payment systems; that is, they should define the gaps in the current payment systems that the solution intends to address and what features of the solution address these gaps.

Please also include the definition of the solution’s baseline features, and a description of the direction of the payment flow (for example, whether, the payment is “pushed” by the payer to the payee, the payee’s provider “pulls” the payment out of the payer’s account, or both).

System Improvements

Problems with today’s legacy payment systems in the United States are well-documented\(^3\). In 2015, the Fed released two years of research and industry feedback, identifying many of these weaknesses and, more importantly, five desired outcomes of an improved payment system.

The proposers of this Solution\(^4\) agree strongly with the Fed’s findings and offer the following improvements outlined in their submission.

**Speed:** “A ubiquitous, safe, faster electronic solution(s) for making a broad variety of business and personal payments, supported by a flexible and cost-effective means for payment clearing and settlement groups to settle their positions rapidly and with finality.”

- The comprehensive electronic Payment System offers availability of Good Funds (Credit Push Model) within one minute of Initiation, 24/7/365.
- Solution demonstrates proven interoperability with the U.S. payment and financial systems, third-party platforms, and non-bank services.
- The scalable and automated Solution streamlines existing processes and reduces overhead costs, such as batch processing and manual return processes associated with older systems.

---

\(^3\) Federal Reserve Consultation Paper, “Payment System Improvement”

\(^4\) The brandless payment system proposed within this paper will using existing, adapted, and improved applications and processes of Dwolla’s current Network, Platform, Services, and Immediate Funds Transfer System (also referred to as “System”)
- Allows all Participants (including the Unbanked) secure, flexible, and regulated access to the Solution, accommodating nearly any use case, transaction type, device, channel, and platform.
- Subject to applicable regulation and/or rules, payments are final and Irrevocable.
- Timely, Deferred Net Settlement capabilities reduce system risk and implementation costs.

**Security:** “U.S. Payment System security that remains very strong, with public confidence that remains high, and protections and incident response that keeps pace with the rapidly evolving and expanding threat environment.”

- The System delivers a distributed, highly-available solution which seeks to remove single points of failure, minimize and isolate adverse changes, and follows an Immutable API Pattern.
- Pervasive use of cryptography allows for the integrity and confidentiality of messages and data in transit and at rest.
- Advanced Threat Modeling delivers a system with a “security by design” approach.
- The infrastructure provides a network with fraud information sharing and analytics.
- Mitigation or elimination of common problems inside the System (e.g., insufficient funds, account standing, and more) introduces greater confidence to the market.
- The absence of Primary Account Numbers (PANs), bank account numbers, and minimal usage of Personally Identifiable Information (PII) while transacting significantly reduces the exposure traditionally associated with existing systems.

**Efficiency:** “Greater proportion of payments originated and received electronically to reduce the average end-to-end (societal) costs of payment transactions and enable innovative payment services that deliver improved value to consumers and businesses.”

- Solution allows End Users to proactively or retroactively Enroll (upon first receipt of payment or payment request), reducing friction and increasing adoption.
- Conditional authorizations and API access enable both easy integrations and straight-through processing.
- Solution complements future standards (e.g. ISO 20022) while providing the flexibility of JSON for API-savvy integrators.
- Increased access to the System for Value-Added Services increases competition for and innovation to End Users.

**International:** “Better choices for U.S. Consumers and businesses to send and receive convenient, cost-effective and timely cross-border payments.”
ISO 20022 provides a global financial service messaging format that is proven and in use by foreign countries and multinational companies (see Executive Summary, “Assumptions section”).

The flexible structure offered by ISO 20022 allows for payment messaging changes (e.g., International Regulation) to be addressed within the standard as opposed to complex customization.

Interoperability exists with the leading implementations across Europe and APAC payment systems since ISO 20022 is already in use abroad.

Solution complements existing cross-border settlement services through FI means.

Collaboration: “Needed payment system improvements are collectively identified and embraced by a broad array of payment participants, with material progress in implementing them.”

Solution satisfies a majority of the Effectiveness Criteria, a framework of desired attributes for an improved payment system as ratified by the Faster Payments Task Force (“FPTF” or “TF”), a market-led initiative with over 500+ members.

Directory and governance structures reflect international best practices for faster payment systems and have received buy-in from numerous domestic organizations and initiatives (e.g. the Remittance Coalition’s B2B Directory).

Solution offers incentives for participation as well as fair and inclusive representation.

About Dwolla

Dwolla is a purely digital payment network and platform for modern bank transfers. The company was founded on a very simple principle: “Build the ideal way to move money.” Since launching in 2010, the firm has introduced technology that 1) increases distribution and utilization of the underlying bank transfer system, and 2) reduces inefficiencies and/or replaced fixed costs associated with today’s existing payment systems.

Today the company offers a comprehensive bank transfer solution, acting as:

1) Service Provider: The technical, operational, and administrative products, services, and FI relationships needed to support and broker access to the existing payment system to move money between a network of End Users. These include, but are not limited to: identity verification, bank validation, fraud mitigation, information security, and risk analysis.

---

2) **Network and Platform (i.e. “services” or “application” layer):** A branded or white label bank transfer network and API allow individuals and third-parties to create accounts, receive status notifications, and initiate the sending, receiving, and requesting of funds between Entities.

3) **Immediate Funds Transfer System:** FiSync is Dwolla’s real-time communication and interoperability protocol for financial institutions. The immediate funds transfer system delivers Good Funds to End Users via a Credit Push Model 24/7/365 using Deferred Net Settlement through the Automated Clearing House (ACH). The FiSync network and its relationship with the Network and Platform is currently used by financial institutions with a range in assets from $2B to $70B in assets.

**The Proposed System**

The brandless Solution proposed within this paper will use existing, adapted, and improved applications and processes of Dwolla’s current Network, Platform, Services, and Immediate Funds Transfer System to posit a comprehensive real-time transfer infrastructure and Faster Payment System (FPS) that provides 24/7/365 immediate availability of Good Funds that are, subject to applicable regulation and/or rules, final and Irrevocable.

Beyond satisfying the core criteria and desired outcomes, the unique benefits of the proposed FPS design over similar systems are the following:

- **Access and innovation:** The proposed Solution offers greater capacity for and more modern means of engaging with Third-Party Services (TPS) and Regulated Non-Bank Account Providers (RNAPs).
- **Usability and multiple use cases:** Agnostic to use case, channel, or device, the proposed FPS enables a wide range of payment types, such as Pre-Authorizations of future payments with fixed or variable amounts, and use cases.
- **On-boarding upon first use:** Proactive enrollment within the FPS is not necessary to receive funds or fulfill payment requests. Proposed registration process allows End Users to claim funds or fulfill requests sent to their email or short message service (SMS)-enabled phone on first use.
- **Deters fragmentation:** Allows End-users to authenticate and authorize payments and applications at a preferred FI or RNAP, regardless of Scheme or Operator.
- **Data Protection:** The protection of data in transit and at rest is enabled through the use of strong standards-based cryptographic solutions ensuring message integrity through digital signatures and confidentiality through Public/Private Key Pairs and the required use of Transport Layer Security (TLS) and symmetric key cryptography for data at rest.
Data protection follows leading practices such as Authenticated Encryption and Forward Secrecy.

**Participation in the FPS**

**Faster Payments System Regulator**

As the Entity (or Entities) tasked to represent the Public Policy Objectives of the System, the FPS Regulator offers leadership, enforcement, and oversight of the FPS Infrastructure, its Members, Providers, and—to a lesser extent—the End Users. The objectives are achieved through the FPS Operating Rules and Guidelines, which may include but are not limited to:

- Standardization
- Rulemaking
- Settlement arrangements and permissions
- Risk tolerance
- Change management
- Pricing baseline of core features
- Ensuring predictability and usability

*See “Executive Summary: Assumptions section” for more information.*

**Scheme Owners**

Depository Institutions (DIs) may run their own FPS Operator (or “Operator”) and Infrastructure to facilitate and authorize Clearing and Settlement between Members and other Operators. Called a Scheme, it represents the financial, legal, and regulatory relationships and obligations of an FPS Operator and its owners.

A Scheme Owner, also referred to as a “Scheme Company,” and its Infrastructure are beholden to the FPS Regulator and its Operating Rules and Guidelines. This ensures the integrity, scalability, interoperability and proper governance of the FPS as a whole.

The Company and its Member owners are responsible for defining and delivering standardized rules, services, and pricing (i.e. Scheme Requirements) not provided or enforced by the FPS.
Regulator and its FPS Operating Rules and Guidelines; this may include, but not be limited to: legal structure, bylaws, board of directors, settlement permissions, collateralization, risk management programs, etc. In order to operate the Company, Members are also expected to fund and incorporate the Scheme.

Members

DIs are eligible for membership with a FPS Scheme. Known as Members, DIs provide direct FPS access to their banking customers and/or broker access to the FPS Infrastructure to Providers, such as RNAPs (e.g. money transmitters, agency relationship, or non-Member FIs) and TPSs. Members that broker access to RNAPs are referred to as Sponsoring Members.

The primary responsibility of a Member is to ensure the necessary technical, regulatory, and administrative operations and requirements (as determined by the FPS Regulator or Scheme Requirements) are met in order to securely and responsibly originate and receive Payment Orders to and from the Operator. Services provided to help meet these Scheme Requirements may include, but are not limited to: token management and identity verification, risk analysis and system fraud reporting, clearing and liquidity monitoring systems, and other components. These services may be provided by the Member or a FI Service Provider.

The model positions banks and credit unions as custodians of the FPS, creating economic incentives for their participation.

Providers

In its current state, Dwolla’s robust API wrapper for ACH allows businesses, governments, and Consumers flexible, robust, and secure access to the nation’s bank transfer infrastructure. When placed at a FI, a similar “application layer” allows Providers to securely maximize the availability, value, and utilization of an FPS to End Users. The following section briefly outlines the Provider roles in an FPS.

Facilitated by a Platform Service Layer at a Member, a FPS API encapsulates the core features and capabilities of the FPS, delivering tiered and standardized methods of access that programmaticallly ensure the integrity, consistency, and scalability of the System for its Participants. More importantly, it allows Participants to improve existing products and services, maximize efficiencies of backend payment operations, or create new business lines. This allows

---

6 Payment System Rules may be used to explain the collective considerations and responsibilities provided by Scheme Requirements and FPS Operating Rules and Guidelines.

7 Platform access is a critical component of the proposed Solution. Companies like Stripe, Dwolla, and Braintree are highly effective at spurring competition, innovation, and value-added services with this model. Other FPSs around the world are moving toward more open and inclusive access to accommodate latent demand of their Systems.

8 IMPORTANT NOTE: The proposers of this solution use a definition for Providers that differs from than the Template and Federal Reserve Glossary

Participants to safely build FPS benefits into any device, channel, platform, or backend process, increasing FPS distribution, adoption, and value to the End User.

Providers are Participants or Entities that directly deliver, facilitate, and/or enable access of the FPS to End Users via the Provider's products, services, or APIs. This may include the Initiation and Receipt experiences associated with the transfer, request, return, or Pre-Authorization of funds between two or more parties. The degree to which Providers are able to leverage and engage with the FPS depends on the relationship and scopes provided by their Access Provider (i.e. a Member, Sponsoring Member or RNAP), FPS Operating Rules and Guidelines, and Scheme Requirements. Providers do not move funds at a Member, but provide the Authentication, Authorization, and payment information needed to create an eligible Payment Order for a Member or Sponsoring Member to execute a transaction, request, or return with the FPS. API access to baseline features of the FPS may be brokered (i.e. monetized).

Members

If a Member delivers faster payment services to End Users via products, channels, or services, then it is also a Provider. These services may include, but are not limited to: real-time payroll, online bill pay, or peer to peer (P2P) transfers.

To the extent that a Member offers FPS API access or services to TPS, it is an Access Provider. To the extent that a Member offers FPS API access or services to RNAPs, it is a Sponsoring Member.
Regulated Non-Bank Account Provider (RNAP)

RNAPs must be sponsored by Members and approved by Scheme Owners for the additional authorization granted to them within the Scheme, e.g. the ability to represent FPS Accounts (funds held at Sponsoring Member) in the Directory or broker FPS access to Third-Party Services. To be eligible, RNAPs must meet and maintain the relevant Scheme Requirements set forth by the FPS Regulator in the Operating Rules and Guidelines, including, but not limited to: security protections, identity verification, capital requirements, risk management systems, and agency agreements.

RNAP are also eligible to initiate Credit Transfers, Credit Requests, Returns, and Pre-Authorizations on behalf of an End User.

Examples of eligible systems today may include, but are not limited to: PayPal, Dwolla, Western Union, Square, or FI recipients’ Fed services through banking organizations (e.g. bankers’ banks).

Third-Party Services (TPS)

TPS are able to initiate Credit Transfers, Credit Requests, Returns, and Pre-Authorizations on behalf of an End User. These include, but are not limited to: non-account holding providers of technology, software, network services, processing services, mobile wallets, equipment, security services, program managers, etc. TPS Providers receive access to the FPS via Members or RNAPs (i.e. Access Providers).

Some current examples of eligible TPS may be Uber, FreshBooks, and others.

<table>
<thead>
<tr>
<th></th>
<th>Member FI</th>
<th>RNAP / Non-Member FI</th>
<th>Third-Party Service (TPS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to Directory</td>
<td>Direct</td>
<td>Indirect, access through Sponsoring Member</td>
<td>Indirect, access through Access Provider</td>
</tr>
<tr>
<td>Create and Manage FPS Accounts</td>
<td>Yes</td>
<td>Yes, funds held at Sponsoring Member</td>
<td>No</td>
</tr>
<tr>
<td>Access to Operator</td>
<td>Direct</td>
<td>Indirect, access through Sponsoring Member</td>
<td>Indirect, access through Access Provider</td>
</tr>
<tr>
<td>Access to Fraud Sharing Services</td>
<td>Direct</td>
<td>Indirect, access through Sponsoring Member</td>
<td>Indirect, access through Access Provider</td>
</tr>
<tr>
<td>Ownership of funds and accounts</td>
<td>Direct</td>
<td>Yes, access through Sponsoring Member</td>
<td>No</td>
</tr>
<tr>
<td>Ability to broker access to TPS</td>
<td>Yes</td>
<td>Yes</td>
<td>No, End Users only</td>
</tr>
<tr>
<td>Ability to Initiate on End User behalf</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**End Users**

An Entity that uses a payment Solution, payment network, or payment service for the purpose of sending or receiving payments, such as a business, government, or a consumer.

**Infrastructure**

The FPS Infrastructure facilitates Clearing, Settlement, and fraud sharing between its Members. Components of the Scheme are created and operated by a Scheme Owner. These are

1) Operator
2) Fraud Sharing Service

The Infrastructure also calls for the formation of a Directory, or a universal or federated framework for enrolling and identifying FPS Accounts. The custodian of this Component may be an Operator(s), independent party or parties, or a regulatory Entity or Entities.
“Operator” role

In its current capacity, FiSync acts as a clearinghouse and settlement instructor between its networked banks, much like an Operator would. This section briefly outlines how FiSync, as a communication and interoperability protocol, will serve as an Operator inside the proposed FPS.​

Clearinghouse and Ledger

The Members in the network are able to ensure Good Funds via the maintaining of an Operational Account for the purpose of processing real-time transfers. An Operational Account for a specific FI should be FDIC or NCUA- insured, interest-bearing, and hold funds on behalf of the customers of the FPS. When interacting with the Operator, the Member credits and debits the Operational Account to facilitate payments across the network.

Members execute intra-bank transfers between the FPS Account and Operational Account on behalf of Providers (as instructed by a Payment Order). Once complete, the Member translates the Payment Order into a standardized Payment Message and forwards to the Operator. In addition to facilitating the clearing and routing of messages between Members, the Operator’s ledger maintains the series of debits, credits, liabilities, and receivables within and across Members of the Scheme. The ledger tracks payment instructions, monitors risk, rebalances assets between Member FIs, and facilitates risk management within the Operator Network.

Central Bank Settlement

The Operator uses the ledger to facilitate Deferred Net Settlement with Fed-supported rails on behalf of its Members at coordinated times across the network. The process executes the outstanding obligations across participating Member FIs and other Operators. At the time of settlement, the obligations are aggregated into a single debit or credit entry for each participating entity. The inter-bank settlement is facilitated via the Operator’s use of Fed-supported rails.

Fraud Sharing Service

The Operator separately maintains a Fraud Sharing Service to collect and distribute additional data, with minimal personally identifiable information required (e.g. no taxpayer identification number, social security number, date of birth, or physical address information). This data allows the Fraud Sharing Service to conduct analysis across the platform in order to improve

---

9 Currently, FiSync allows participating FIs to leverage the Automated Clearing House (ACH) to reconcile Operational Accounts. The proposed Solution anticipates leveraging other existing Fed-supported rails (e.g. FedWire, NSS, Same-Day ACH), and the Proposers of this Submissions encourage improvements to these rails that drive down overall costs, decrease systemic risk, and drive efficiency. The Fed has not committed to provide any services to the Proposer.
decision-making. In its provision of the Fraud Sharing Service, the Operator defines several messages of potential high risk activity. As the Solution matures, the Operator refines and increases this type of messaging as a result of internal research and Scheme Owner feedback about the usefulness and quality of the data received.

Standardized messages and protocols allow for fraud sharing across multiple Operators.

Directory

The efficiency, accessibility, predictability, and usability benefits of national directories are internationally well-documented, and domestic efforts to create a federated Directory are already underway. The Directory\(^\text{10}\) proposed in this Solution offers a functional expansion of Dwolla’s current directory platform and a vision for how it exists within the proposed Solution. The Directory (or federation of Directories) serves as a secure, standalone repository and facilitates enrollment, lookup, authentication, authorization, and payment preference management of End Users. The main benefits of this Directory include:

- Deters fragmentation by allowing End-users to authenticate and authorize payments and applications at a preferred Financial Institution or Regulated Non-bank Account Provider, regardless of the Operator of the participating FI or RNAP.
- Enables anyone to send or receive payments with an email or phone number, reducing the circulation of sensitive PII.
- Allows a first-time user of the Solution to enroll and send/claim funds in one concurrent and predictable user flow, eliminating the need to proactively enroll in the FPS and increasing adoption of the Solution by the End User.
- Allows storage of Payment Preferences, associating an email and/or SMS with numerous Member Providers.
- Functions as the authenticated system of record for Components while containing minimal identity data elements necessary for signing requests and messages.

\(^{10}\) See Directory assumption in Executive Summary, “Proposal Assumptions”.
**USE CASE COVERAGE**

**Supported Use Case Coverage Summary**

In the table below, identify (by entering a “Y” or and “N”) which use cases the solution intends to support for payments within the United States and a description of the specific type of payments the solution supports (example provided in the table below). Also indicate for each use case whether the solution offers cross-border functionality. Blanks will be assumed as “N”.

<table>
<thead>
<tr>
<th>Use case</th>
<th>Support (Y/N)</th>
<th>Cross-border (Y/N)</th>
<th>Examples of payments supported</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business to Business (B2B)</strong></td>
<td>Y</td>
<td>Y</td>
<td>The solution supports transactions across various entities, including: commercial, nonprofit, and government. B2B eCommerce involves interactions and transactions between a company and its trading partners: suppliers, collaborators, subsidiaries, contractors, and large institutional customers.</td>
<td>The solution encompasses fund transfers for all sizes of business and organizations.</td>
</tr>
<tr>
<td><strong>Business to Person (B2P)</strong></td>
<td>Y</td>
<td>Y</td>
<td>Businesses are able to pay individuals for items such as benefits, marketplace transactions, blogging, and other on-demand services.</td>
<td></td>
</tr>
<tr>
<td><strong>Person to Business (P2B)</strong></td>
<td>Y</td>
<td>Y</td>
<td>Support for a wide range of one-time, recurring, and scheduled payments across many uses cases, including: crowdfunding, expense management, investment platforms, and online invoicing.</td>
<td></td>
</tr>
<tr>
<td><strong>Person to Person (P2P)</strong></td>
<td>Y</td>
<td>Y</td>
<td>An authorized user can send money to any other End User, email address, or phone. This is ideal for custom P2P solutions or fundraising platforms that provide the ability to hold funds for their End Users, but do not want to hold funds themselves.</td>
<td></td>
</tr>
</tbody>
</table>
Cross-border Use Case Coverage (If Applicable)

As designed, the FPS is agnostic to use case, currency, and location, making cross-border settlement an additional business objective subject to inclusion by Scheme Owners. The vendor or protocol for such services will benefit from the value propositions offered by an improved FPS.

For those use cases supporting cross-border, provide the jurisdictions and systems with which the solution interoperates in the table below.

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Non-US Corridor(s) and Systems</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business to Business (B2B)</td>
<td>International</td>
<td></td>
</tr>
<tr>
<td>Business to Person (B2P)</td>
<td>International</td>
<td></td>
</tr>
<tr>
<td>Person to Business (P2B)</td>
<td>International</td>
<td></td>
</tr>
<tr>
<td>Person to Person (P2P)</td>
<td>International</td>
<td></td>
</tr>
</tbody>
</table>
Proposal Assumptions (Optional)

Proposers may choose to provide a list of assumptions used in the creation of their proposal. Assumptions should be limited to those that are unique to the proposal and cannot be adequately addressed elsewhere in the document. The QIAT will take into account any assumptions listed in making their assessment of the proposal.

For example, as noted in the “Practical and Conceptual Considerations” section of the Faster Payments Effectiveness Criteria, many of the criteria require the solution proposer to describe various elements of the payment system rules for the proposed solution. In a multi-operator environment, it is possible that a single entity will be given rule-making authority by multiple operators that desire a standardized ruleset. Solution proposers planning to pursue such an approach may list this rule-making authority as an assumption. However, it should be noted that for the purposes of meeting the Effectiveness Criteria related to “Legal Framework”, proposers should coordinate with either the designated rule maker or articulate preferences for rules when preparing their solution proposal, even though rules may not be finalized until later.

Messaging Standards: Clear resolution between domestic and international messaging standards is missing. The proposed Solution demonstrates its technical capacity for handling the messaging standards of the future. Consequently, this Proposal assumes an agreed upon version of an inevitable ISO 20022 messaging standard, unless otherwise noted.

Note: Dwolla has chosen to reference ISO 20022 as it appears to be the imminent standard for adoption; however, the Proposers note the following shortcomings:

- Detailed standard reference material is not readily available or easily accessible.
- It is widely flexible, customizable, and open for interpretation and divergent uses.
- Implementation resources are currently limited or emerging.
- Business process mapping and modeling is a non-technical but required prerequisite for a successful implementation.
- The standard requires translation, serialization, and/or encapsulation for web services (JSON).

Beyond the format identified, the Proposal remains flexible and can be extended to any messaging standard.

Changes to the Submission Template: New systems and ideas don’t always play nicely with legacy processes, products, or lexicons. To better accommodate the Solution description, we needed to take liberties in augmenting the submission template.
The Directory: Following the precedent of numerous other Faster Payments Systems around the world, the Proposers call for the creation of a universal or federated Directory. While a decentralized approach is possible, we believe a universal or federated model offers simplified experiences to End Users, reduces touchpoints for interoperability (enhanced in a multi-operator environment), deters fragmentation of services, increases system efficiency, and streamlines system-wide maintenance.

Governance: The Solution’s governance arrangement assumes the FPS Regulator to have the power and oversight to establish, maintain, and enforce its Public Policy Objectives within a FPS Operating Rules and Guidelines, which outline the obligations and standards required for FPS Participants. Dwolla recommends that the Fed continues to be an active leader in encouraging faster payments innovation and acts as the FPS Regulator.

OFAC: Existing provisions for the reliance of ODFIs and RDFIs (Payer Member and Payee Member in the FPS Scheme) on one another for OFAC compliance in domestic ACH transactions will translate to domestic FPS transactions.
Part A: Detailed End-to-End Payments Flow Description

Part A is composed of three sub-sections:

- Section 1 focuses on the broad solution, looking across the eight stages of the payment lifecycle.
- Section 2 focuses on the details of the solution by describing the solution’s supported use cases across the eight stages of the payment lifecycle.
- Section 3 provides a summary table detailing whether the Effectiveness Criteria are addressed by each supported use case.

Part A, Section 1: Solution Description

In this section, the proposer should describe what the solution does at each of the eight stages of the end-to-end payments process (lifecycle stages). These eight stages compose the numbered sub-sections, below. For some solutions, the stages of the lifecycle may not occur as separate steps – they may occur simultaneously. The steps also may not occur in the order presented below (for example, receipt may be before or after settlement). Proposers may therefore choose to combine some steps in their description, instead of addressing all eight stages separately, or to re-order the sub-sections below as required to best describe their solution.

1. Initiation
2. Authentication
3. Payer Authorization
4. Approval by the Payer’s Provider
5. Clearing
6. Receipt
7. Settlement
8. Reconciliation

Proposers should include flow diagrams of the messaging and payment flows and the roles of stakeholders (End Users, technology providers, processors, including the proposer(s) of

---

11 Definitions of some of the terms used below are either defined in the Effectiveness Criteria or in the Glossary of Terms.
the solution) through the eight lifecycle stages of the solution. In completing this section, proposers should refer to the Effectiveness Criteria that relate to each of the eight stages (as noted in the instructions for each sub-section).

Any additional description or materials to support the explanation of the solution may be provided as an optional Appendix.

1. Initiation

Describe how and when End Users can initiate and/or receive payments, and to which accounts payments can be initiated and received. Indicate whether there are any prerequisites or limitations to initiating or receiving a payment (e.g., enrollment,) and, if applicable, how those prerequisites are met. Include whether the solution provides the ability to make multi-currency and/or cross-border payments, and describe the process for foreign currency conversion. Indicate for each use case, the channels, devices and platforms through which End Users can access and use the solution (e.g., remote with a mobile device, online, etc.). Describe any consumer protections; for example, whether and at what point there would be disclosure of End-User fees.

In this sub-section the proposer should also describe the capability and steps required for contextual data to be transferred or associated with the payment. Also describe any security features associated with initiation, including protecting sensitive information. Proposers should include flow diagrams of the messaging and payment flows through the end-to-end payment process of their solution in this section.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to initiation: U.1 (Accessibility); U.2 (Usability); U.3 (Predictability); U.4 (Contextual data capability); U.5 (Cross-border functionality); U.6 (Applicability to multiple use cases); E.4 (Payment format standards); S.7 (Security controls); S.9 (End User data protection).

Access, Consumer Protections, Limitations, and Use Cases

Who can access?

A wide range of Providers facilitates real-time payments via either direct or indirect relationships with an Access Provider (i.e. Member or RNAP). As stewards of the payment experience, Credit Transfers, Credit Requests, Pre-Authorizations, and Returns can be initiated by any of the following Providers:

- In-network FIs
- In-network RNAPs
- In-network TPSs
Note: In a multi-operator environment Providers that Initiate transactions outside the originator or receiver are considered to be Out-of-Network and are facilitated between Operators.

Limitations on Providers and Accounts

With a Solution that allows the Providers to be stewards of the End-User experience, the FPS Regulator, Scheme Owners, and Members determine the products, accounts, and limitations they deem eligible for a real-time payments inclusion—many of which can be made immutable through the access and services offered by the Member at the Platform Services Layer. The Solution is adaptable and flexible to expand to various products, but transactional accounts are the most widely supported across the ecosystem.

Technology Platforms, Use Cases, and User Types

The Solution enables secure, programmatic, and robust access through its use of APIs. This allows seamless integration with any Internet-connected device, channel, or platform, and accelerates adoption via consumer choice and competition for Value-Added Services. The lifecycle stages are the same for all use cases: business to business, business to person, person to business, and/or person to person. To insure simplicity and ease of integration, few data fields vary between personal and business use cases. The data fields that vary are:

Organization Payer or Payee:

- **Directory Name** - the organization’s name
- **Directory Type** - the account type designation of commercial, nonprofit, or government
- **Transaction Contextual Data** - leveraged for business-centric items, including: invoice, claims, or order numbers
- **Transaction Limit** (optional) - Transaction limits per account type may or may not be enforced by the FPS Operating Rules and Guidelines, Scheme Owners, or Members.

Personal Payer or Payee:

- **Directory Name** - the individual’s name
- **Directory Type** - the account type designation of personal
- **Transaction Contextual Data** - leveraged for personal items, including: comments or reason
- **Transaction Limit** (optional) - Transaction limits per account type may or may not be enforced by the FPS Operating Rules and Guidelines, Scheme Owners, or Members.
In addition to these differences, Providers and/or Members may enforce additional enrollment and Authentication practices or requirements based on their particular use case, risk threshold, etc. A Provider may also choose additional security measures based on the customer type, such as personal identification number (PIN) or two-factor authentication. While separate from the Directory and Operator, Providers may also opt to collect additional information for business entities, such as authorized representative information. The stewardship model allows Members and Providers customization options to strengthen the relationship with their customers.

As an agnostic real-time payments platform, the Providers remain best-positioned to understand their customers and how the Solution can adapt to their evolving payment needs. By providing that level of personalization, the Solution inherently supports various use cases across the network.

The capability of supporting all use cases, beyond the variations listed above, is instilled throughout the Platform and not exclusive to Initiation. This robust Platform is flexible to expand to different markets and bring success to all stakeholders.

**Messaging Standards**

Payment information and instructions flow through the Solution as a) Payment Orders, b) Payment Messages, and c) Payment Receipts. The technical means and formatting for a Payment Order and Receipt are reserved for Members, while a strict standardized format is used for Payments Messages with the Operator.

**Proprietary standards**

Because Payment Message inputs to and outputs from the Operator are standardized, Members have more flexibility over how they broker access to Providers. The degree to which a Member aligns their proprietary means of access (e.g. JSON) to the Payment Message standard is determined by the Member and/or Scheme and translated by the Member.
The customization of FPS access to Providers by Members allows for:

- differentiation in FPS Access during the first and last mile of a payment.
- more effective and efficient integrations at the Provider
- improved compatibility and flexibility between the Member’s technological capabilities and its Platform Services Layer

**Securing translation**

Any translation between formats are the responsibility of the Member, but will likely have additional security requirements to ensure system integrity. This is further discussed in Part C, Section 1: Security.

**Component Standards**

Payment Messages are comprised of verifiable, signed, and standardized collection of data exchanged between a Member an Operator for interbank or Inter-operator Clearing. The Standard chosen (e.g. ISO 20022) is identified, governed, and enforced by the FPS Regulator. A similar standardized approach is taken in the messaging protocols and format chosen for interaction with the Fraud Sharing Service and Directory. The selection of standardization for these FPS infrastructure components allows for strong interoperability within and out-of-network Members.

**Contextual Data**

Contextual data is exchanged via a metadata attribute on a Payment Order, Payment Message, and Payment Receipt. The contextual data parameter allows Members and Providers to expand the information shared with each payment, without adaptations to the Operator’s offerings.

Schemes will be enabled to collaborate with Members and Providers to develop agreed upon standards for the contextual data parameter. An example of this may include “InvoiceNumber” being an explicit attribute in the metadata that each Member or Provider is able to understand and interpret consistently. With agreed upon standards, the contextual data can be leveraged to increase collaboration across Members, Providers, and End Users.

**Consumer Protection**

**Transaction protection**

In conjunction with consumer protection, the stewardship model provides transactional protection for all participating Providers and End Users. Acting as stewards of the network, the Members and Sponsoring Members are granted Approval authority of the Credit Transfer, but
Providers are required to enforce boundaries determined, at a minimum, by the FPS Operating Rules and Guidelines and existing applicable regulations.

- **Payer’s Member or Sponsoring Member** - Credit Push structure allows the Member to authorize all send transfers.
- **Payee’s Member or Sponsoring Member** - These Members have the authority to allow or deny any incoming payment.
- **Operator** - Scheme Owners may enforce high-level restrictions to minimize liquidity risk across the network.

The Solution is agnostic and does not dictate enhanced limitations, but the Operator facilitates messaging between Members and Providers to enhance collaboration. Message facilitation leverages statuses and reasons for communication purposes to promote a great customer experience.

An example of the facilitation is as follows:

- The Payer’s Member initiates a $250,000 payment to a Payee
- The Payee’s Member enforces a $200,000 per transaction limit
- The Payee’s Member returns a message (facilitated by the Operator) to the Payer’s provider, including the following:
  - **Status** - Rejected
  - **Reason** - Amount exceeds Payee’s receiver limits

Members may enforce any additional limitations determined necessary to protect organizational liquidity risk, customer financial position, and overall risk mitigation.

Examples of additional limitations may include, but are not limited to:

- Lower individual transaction amount
- Daily aggregate transaction amount
- Daily transaction count

**Disclosures**

Products, services, and experiences made possible by Providers span many Use Cases and Entities (e.g. business, nonprofit, and government entities). Fee structures may differ across Providers depending on the services rendered, and Providers are responsible for the communication related to consumer protection.
The Proposers of the Solution suggest several items be designated in the FPS Operating Rules and Guidelines on Consumer Protection, including:

- Disclosure of transaction fees
- Disclosure of interest charges
- Distribution of confirmation notifications
- Disclosure of any other items necessary to keep consumers informed about their account and transaction history

A Provider’s ability and responsibility to disclose this information is essential to Consumer adoption. Because the Platform Services Layer is a Software as a Service (SaaS) model established between the Provider and Operator at the Member, any direct consumer fees will be assessed at the discretion of the Providers but be heavily influenced by the Member. Pricing of core features will be determined by the FPS Regulator and Scheme Operators while pricing of Value-Added Services remain at the discretion of the Member and Provider. The Solution provides dynamic touch points and controls to support a wide range of Governance-enforced requirements around End-User protections (e.g. Pre-Authorization flows).

**Applicability of existing laws**

The Solution is designed to allow each Member and Provider to comply with its own relevant legal obligations, whether such obligations are based on the Provider's entity type (e.g. depository versus non-depository institution) or the Provider's activities (e.g. provision of remittance services versus issuing credit). Due to the anticipated Provider types and their use of the Solution to effect fund transfers, the Solution expects that such Providers would continue to be subject to a wide range of federal and state laws and regulations, including, but not limited to: OFAC, BSA/AML, Reg GG, Reg E, Reg Z, Consumer Financial Protection Act, UDAAP, E-Sign, FCRA, UCC, and GLBA. In addition, the use of any Fed-supported rails system would require compliance with any applicable rules or regulations for such rails (i.e., the NACHA rules, Operating Circulars, etc.).

**Onboarding a new End User**

The Directory and Enrollment

End Users are able to access the FPS by enrolling with a Member or RNAP.

All requirements for onboarding an End User are owned and completed by Entities eligible for Enrollment (i.e. Members and RNAPs). End-user Registration, Authentication, and

---

12 Existing Member and Provider account opening processes remain unchanged by the creation of the FPS. A Member or Provider can allow transaction accounts at their institutions access to the FPS at their discretion.
Authorization are functions of the Member and RNAP to effectively manage their customer relationships.

There are four main functions of the Directory throughout the lifecycle:

*Enrollment (i.e. Registration)*: The End-User registration process allows an End User to send, receive, pre-authorize, return, and request payments via the FPS. To ensure authentication, authorization, and overall integrity of the FPS, registration is required and must be conducted at a Member or RNAP. This process can be done proactively by the End User signing up at their Member or can be retroactively completed by fulfilling a first-time request or receipt of payment.

To facilitate first-time use (and unify multi-operator fragmentation), a *Member and RNAP List*, which contains the name and Authentication Portal URL, is populated and maintained by the Member or RNAP via a Directory endpoint. The list is used to assist End Users in selecting their preferred Member or RNAP, and routing them to their Member or RNAP’s respective Authentication Portal URL.

To enroll, Providers must authenticate the End User. Likewise, the End User must Authorize FPS and/or Member or RNAP (e.g., via a Terms of Service) and provide a Destination ID (e.g., email address and/or phone number) to associate with the End User’s account(s). Payment preferences (e.g., in case an End User has multiple banks connected to an email address or phone number) may also be indicated during this process or managed later via the Provider’s interface.

*User Directory ID (UDID)*: The Directory associates a Destination ID (e.g., an email address or phone number) with the routing number of a Member and/or RNAP, along with other bank-level information, to create a UDID. Upon enrollment this is sent back to the Member or RNAP where it is associated with the End User’s corresponding account.

After enrollment Providers will use a supplied Destination ID to look up the corresponding UDID found at the End User’s preferred Provider.

*Multi-operator*: End Users authenticate and authorize payments and applications via the Authentication Portal URL maintained by the Member and RNAP at the Directory. Independent of Scheme Owner or Member, the Directory (plus strong messaging and protocol standards between Operators) serves as a powerful and secure way to enable FPS access and all but eliminate the threat of fragmentation in a FPS.

*Managing Payment Preferences*: The Directory allows End Users to associate multiple Providers and Provider Accounts with one or more Destination IDs. To manage an End User’s Default Account Preferences, Providers are relayed read/write access through their Access Providers to the Preference endpoint of the Directory. Upon receiving a signed
message that the End User has requested an update to their preferences (e.g., via a Provider’s “Manage Payments” tab in their interface), the Directory updates the preference in real-time.

Directory Enrollment

To start leveraging the real-time payments network, a new End User must complete the following requirements, as established by the FPS Operating Rules and Guidelines:

- Participant authenticates with the Provider
- Participant authorizes Provider and Operator to provide FPS services

*These requirements are detailed in Part A, Section 1: “Initiate”.*

Enrollment flows

**Adding an End-User to the Directory**

Once an End User is Authenticated and Authorized, the Provider/Member then populates the Directory with minimal identifiable information. The primary objective of the Directory is to allow Members and Providers to locate individuals or entities for a streamlined payment process.

The Member sends the following information to the Directory:

- *Name* - Individual or Organization name
- *Type* - Personal or Commercial
  - *Sub-type (Commercial only)* - Commercial, Nonprofit, or Government
- **Email** - Email address as a reference point for payment delivery
- **Phone** - Phone number as a reference point for payment delivery
- **Operator ID** - This ID is leveraged for interoperability with other Operator networks.
- **Routing Number** - The number used to determine Member or RNAP location for payment routing
- **Preference** - Field set by the Member or RNAP to indicate a preferred account by the End User

The primary objective is to allow End Users to send payments to others with as little information as possible while additional information resides in the Directory. With the Directory, an End User can send to another Consumer’s bank account with limited information (e.g. email address or phone number). The Member POSTs to a Directory hosted API endpoint, a process discussed in more detail in the Integration Timeline.

**Enrolling a New Payee at First Receipt of Credit Transfer or Request**

If a Payer’s Member does not find the Payee during a Credit Transfer or Credit Request attempt, the Payer’s Provider begins the Enrollment process. This transition may look like the following:

1. Payer logs in to a Member and initiates a Credit Transfer or Request.
2. Payer’s Member checks the Directory, but no Payee is found.
3. Payer’s Member continues with the transfer.
   - Transfer is created with a Pending status.
4. Payer’s Member engages the Payee via a notification and communication to Destination ID provided by Payer.
○ Payee clicks link in communication.
○ Payee is taken to comprehensive list of all eligible Members/Providers.

NOTE: The list is populated by Directory endpoint.

5. After selecting a preferred Member or RNAP, the Payee is redirected to an Authentication Portal provided by that Member or RNAP to Directory.

NOTE: Transfer ID needs to be securely delivered to the Member or RNAP, a recommended solution is outlined in Part A, Section 1: Authorization - "Pre-Authorization".

6. Payee’s Member or RNAP adds the Payee to the Directory.

7. Payee’s Member or RNAP retrieves from and completes the transfer with the Operator.

Populating the Fraud Sharing Service with End User information

The Operator maintains an additional database with regards to End Users and their transactions for the sole purpose of analyzing network activity to provide actionable intelligence to its Members. This information should require minimal PII but still give Members deeper insight into their Participants’ activity, so that fast and reliable decisions can be made about whether or not to block or delay a transaction due to potential fraud.

Separate from the Operator database, which is discussed later, this Fraud Sharing Service stores information reported by Members regarding their End Users and transactions.

The Fraud Sharing Service also requires information at the time of Enrollment. Upon initial registration of an End User the Fraud Sharing Service receives:

- **UDID** - Unique Directory ID from the Directory
- **Relationship open date** - The date the End User opened their account with the Member
The Provider POSTs to a Fraud Sharing Service-hosted API endpoint, which is discussed in more detail in the Part B, Section 3: “Integration Timeline”.

The Data Retention Schedule is set by the FPS Regulator as part of the FPS Operating Rules and Guidelines.

**Detailed End-to-End Payment Flows**

An enrolled End User can initiate a transfer or request via various platforms, devices, and channels. While each variation begins in a slightly different manner depending on the interface or instrument, each kickstarts a Credit Push Model focused on establishing Good Funds in the Payer’s account later in the payment lifecycle. Alternatives for starting the payment process are all conducted from an eligible Provider on the network or interoperable Operator solution, including:

- Payer initiated credit transfer to:
  - Known Payee
  - Unknown Payee

- Payee initiated credit request to:
  - Known Payer
  - Unknown Payer

- Returns

Each of these processes are described in detail below.
A Payer initiates payment to another enrolled End User by the following process:

1. Payer Authenticates with a Provider and initiates a Payment Order to the End User’s Member or RNAP, specifying:
   - Payee (e.g. email address or phone number)
   - Amount
   - Contextual Data
   - Session Data for Fraud Sharing Service Input

2. Payer's Member retrieves the Payee information from the Directory.

3. Payer's Member checks Payer and Payee information against the Fraud Sharing Service, providing:
   - Information sent to Fraud Sharing Service:
     - Payer UDID - known by Payer’s Provider and Member from Enrollment
     - Payee UDID - from the previous Directory response
   - Fraud Sharing Service returns:
     - Payer and Payee fraud information

4. Payer's Member approves and executes the intra-bank transfer from Payer Account to Operational Account
   - The following transfer occurs:
     - Debit to the Payer’s Account
     - Credit to the Operational Account
○ Payer’s Member authorizes, approves, and executes the transfer (i.e. Credit Push)
○ Funds available in the Operational Account (i.e. Good Funds)

5. Payer's Member sends an approved Payment Message to the Operator, including:
   ○ Information sent to Operator:
     ■ **Payer UDID**
     ■ **Payee UDID**
     ■ **Operator ID** - Operator of the Payee (for interoperability with multi-operator)
     ■ **Routing Number** - To determine which Member to engage
     ■ **Amount**
     ■ **Contextual Data**
     ■ **Payer Status** - Approved
     ■ **Payer Confirmation ID** - Identifier for reconciliation purposes
   ○ Information received from Operator:
     ■ **Transfer ID** - Identifier to reference

6. Payer's Member sends transfer information to Fraud Sharing Service
   ○ Information sent to Fraud Sharing Service:
     ■ **Payer UDID**
     ■ **Payee UDID**
     ■ **Transfer ID**

7. Operator sends Payee Member the transfer received Webhook notification
   ○ Payee Member is identified by Routing Number (from step #5) and/or Operator ID in the instance of an inter-Operator transfer
   ○ Identifier sent to the Payee’s Member
   ○ Payee’s Member is then able to retrieve the following from the Operator:
     ■ **Transfer ID**
     ■ **Payer UDID**
     ■ **Payee UDID**
     ■ **Amount**
8. Payee’s Member retrieves the Payer information from the Directory using the Payer’s UDID.

9. Payee’s Member checks Payer and Payee (optional) against the Fraud Sharing Service

10. Payee’s Member executes the following intra-bank transfer:
    ○ Debit from the Operational Account
    ○ Credit to the Payee’s FPS Account

11. Payee’s Member updates status and notifies Payee’s Provider of the received payment approval and completion.
    ○ The Provider subsequently notifies the Payee.

12. Payee’s Member sends approved transfer information to Operator, including:
    ○ *Transfer ID*
    ○ *Payee Status - Approved*
    ○ *Payee Confirmation ID*

13. Operator notifies Payer’s Member of Transaction Complete (Payment Finality)

14. Notification is sent to the Payer via Provider

Initiate Credit Transfer to Unknown Payee

There are two events where a Payer sends a Credit Transfer that becomes a Pending Payment:

1. The Payee is not located in the Directory.
2. The Payee’s Provider, Member, or other Scheme has an approval process.

In either circumstance, the Payment Message is updated once the payment is claimed by the Payee or approved by the Provider.

If a payment is pending, the Payer’s Provider notifies the Payer that funds have been transferred from their Account, but are pending approval from the Payee’s Member. The “Payment Finality” section in Clearing, which is determined by the Transaction Complete message, describes reclaim periods on cancellations.

If the Payee is not in the Directory, the Payer’s Provider conducts the “Enrolling a new Payee” flow as described in the “Initiate” section.
In the event that a Member does not find the End User during a Credit Transfer attempt, the sender’s Provider will kickstart the Enrollment process. This flow may look like the following:

1. Payer Authenticates to a Provider and initiates a Credit Transfer Payment Order.
2. Payer's Member checks the Directory, but no End User is found.
3. Payer's Member checks Payer against the Fraud Sharing Service.
4. Payer's Member approves and executes an intra-bank transfer.
5. Payer's Member sends the Credit Transfer (with Pending status) to the Operator.
6. Payer's Member adds the transfer information to the Fraud Sharing Service.
7. Payer's Member sends a notification to engage the new Payee.
8. Payee selects a preferred Member or RNAP to receive the payment.
   - Payee clicks link in communication.
   - Payee is taken to comprehensive list of all eligible Members or RNAP.
     
     **NOTE:** List is populated by Directory endpoint.
   - Payee is taken to Authentication Portal of preferred Member or RNAP.
     
     **NOTE:** Authentication Portal URL is associated with Directory Routing Number.
   - Transfer ID needs to be securely delivered to the Member or RNAP, a recommended solution is outlined is in Part A, Section 1: Authorization - "Pre-Authorization".
9. Payee’s Member adds the Payee to the Directory.
10. Payee’s Member retrieves the transfer information.
11. Payee’s Member retrieves the Payer information from the Directory.
12. Payee’s Member checks the Payer and Payee against the Fraud Sharing Service.
13. Payee’s Member approves and executes an intra-bank transfer.
14. Notification is sent to the Payee via Provider.
15. Payee transfer approved message is sent to the Operator.
16. Operator notifies Payer’s Member of Transaction Complete.
17. Notification is sent to the the Payer.

Initiate Credit Request to Known Payer

A Credit Transfer can also be initiated at a Payee’s request (e.g. requests for payment of membership fees, e-invoicing, or splitting the cost of a meal with friends). This request is the means by which a Payee specifies payment information for a Payer to fulfill. The payment is fulfilled via the same Good Funds, Credit Push Model described in the previous section, with the same benefits as a Payer-initiated payment.

The request initiation and fulfillment process is as follows:

1. Payee authenticates to a Provider and initiates a Credit Request Payment Order, specifying:
   - Payer *(e.g. email address or phone number)*
   - Amount
   - Contextual Data
2. Payee’s Member retrieves the Payer information from the Directory.
   - Information is retrieved by email address or phone number.
3. Payee’s Member sends approved Payment Message to the Operator:
○ Information sent:
  ■ Payer UDID
  ■ Payee UDID
  ■ Operator ID - Operator of the Payee (for interoperability)
  ■ Routing Number - To determine which Member to engage
  ■ Amount
  ■ Contextual Data

○ Information received:
  ■ Transfer ID - Identifier to reference

4. Operator sends Payer's Member the Credit Request Payment Message, including:
  ○ Transfer ID
  ○ Payer UDID
  ○ Payee UDID
  ○ Amount
  ○ Contextual Data

5. Payer's Member retrieves the Payee information from the Directory using the Payee’s UDID.

6. Payer’s Provider notifies the Payer.

7. Payer Authenticates to fulfill a payment.
  ○ The “Payer-Initiated Payment” flow begins

While the overall exchange between the Payee and Payer remains the same, there are slight variations to the process depending on the Payer’s characteristics.

Payer is not in the Directory

If the Payer is not enrolled in the Directory, the Provider engages the new customer via a notification (e.g. email or SMS). If the Payer has a banking relationship with the affiliated FI, the Provider redirects the Payer to their respective Provider.

Payer is in the Directory, but out-of-network

A Payer may also be a customer of a Provider on another Operator’s network. If this occurs, the flow remains the same as above, but the Operator delivers a message to the secondary Operator to complete the request.
Initiate Credit Request to Unknown Payer

The request initiation and fulfillment process is as follows:

1. Payee authenticates a Provider and initiates a Credit Request Payment Order, specifying:
   - Payer (e.g. email address or phone number)
   - Amount
   - Contextual Data

2. Payee’s Member checks the Directory, but no Payer is found.

3. Payee’s Member sends Credit Transfer Payment Message to the Operator, including:
   - Information sent:
     - Payee UDID
     - Operator ID - Operator of the Payee (for interoperability)
     - Amount
     - Contextual Data
   - Information received:
     - Transfer ID - identifier to reference

4. Payee’s Member engages the Payer via communication to Destination ID provided by Payee.
   - Payer clicks link in communication.

5. Payer is taken to comprehensive list of all eligible Members and RNAPs.

   NOTE: List is populated by Directory endpoint
○ Payer is taken to Authentication Portal of preferred Member or RNAP.

*NOTE: Authentication Portal URL is associated with Directory Routing Number.*

*NOTE: Transfer ID is securely appended to the URL for effective processing.*

6. Payer's Member adds the Payer to the Directory.

7. Payer's Member retrieves the Payee information from the Directory.

8. Payer's Member retrieves the transfer information from the Operator.

9. Payer fulfills the transfer request.

**Initiate Payment Return to Known End User**

Using messaging and status changes, the Solution automates a Hold Harmless process analogous to existing processes today and familiar to FIs. The End User bears the liability for an authorized payment in the Credit Push system. To mitigate errors, processes should be codified in the FPS Operating Rules and Guidelines and implemented technically.

If the End User wants to reverse a transfer due to a mistake (e.g. incorrect amount or recipient), the system allows the transfer to be automatically reversed as long as the transaction is not in a completed state. If the transfer is already complete, the system sends a request for reversal, rather than a mandate. The Member that received the payment can decide to automatically return the funds or complete a manual review to determine whether or not to do so, in accordance with applicable regulation. This decision is at the discretion of the Member and could include, for example, a consideration of whether the funds are still available in the receiving account, and the total amount of the transfer. If the transfer has already completed, returning the funds is at the sole discretion of the receiving Member, in accordance with applicable regulation.

**Payer requesting a Return**

The Payer is able to request a return from the Payee for any reason. References to the original transaction are facilitated via contextual data sent in Step 1 of the “Initiate Credit Request: Known Payer” transaction outlined above. The Scheme Owner is responsible for the structure of the messaging in contextual data.

**Payee initiated a Return**

The Payee is able to initiate a return to the Payer for any reason. A Payee’s Provider can initiate a return via the “Initiate Credit Transfer: Known Payee” transaction outlined above. References
to the original transaction are facilitated via contextual data. The Scheme Owner is responsible for the structure of the messaging in contextual data.
2. Authentication

Describe how the identity of an End User and provider would be authenticated. Describe any security features associated with authentication, including protecting sensitive information.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to authentication: U.2 (Usability); U.3 (Predictability); S.7 (Security controls); S.9 (End-User data protection); S.10 (End-User/provider authentication).

In the Solution proposed, there are two events that require varying types and levels of End-User Authentication:

1. **Participant Authentication**: Verification and validation of End-User eligibility by a Member or RNAP required to provide the End User access to the FPS. This is completed during End-User Enrollment by RNAP or Member.

2. **Provider or Application Authentication**: On-behalf of an End User, a Provider requests Authentication from the End-user’s Member or RNAP.

In addition, the System has Authentication measures between the Components of the FPS. This is referred to as Component Authentication.

**End-User Authentication**

**Participant Authentication**

Participant Authentication occurs when the Provider\(^\text{13}\) enrolls an End-User Account into the FPS. This may include a Third-Party Service (by way of an Access Provider), Member, or RNAP. In each instance the End User is subject to the Authentication requirements of its Member or RNAP. All participating entities are subject to authentication standards identified by the FPS Regulator. Minimum Authentication requirements may include items such as password composition or multi-factor authentication.

**Provider or Application Authentication**

The Platform Services Layer allows Providers to programmatically request access and permissions to an End User’s FPS-enabled Account at a Member or RNAP. The authentication

\(^{13}\) Depending on the business type or payment needs, the Provider may need to conduct reasonable Authentication practices and capture identifiable information for each of its End Users independent of the Authentication practices and information capture required by the Member or RNAP during Enrollment. The instances in which this duplicative data is required are determined by the FPS Regulator and FPS Operating Rules and Guidelines, and potentially by the Scheme, Member, or RNAP. End Users’ sensitive information remains with the Provider and is not disclosed across the entities of the network.
and programmatic scopes (i.e. authorizations) allow for a safe, secure, and market-tested way for innovators to unlock a wide range of experiences, convenience, and Value-Added Services for End Users.

The level of Authentication required from a Provider is informed by the FPS Operating Rules and Guidelines, but additional mechanisms may be enforced by a Member’s business or risk models (e.g. multi-factor authentication).

There are several ways the System can be designed and improved to facilitate this process for the Provider.

**Authentication by Technology Vendor**

Today, Providers are able to integrate the necessary security mechanisms for their customers and have multiple vendors and options to verify the End User’s bank account. An FPS enhances these third-party approaches to Authentication by speeding up verification deposits or introducing efficiency and coverage for bank verification services with the Directory. The absence of this currently necessitates using screen-scraping services which require high-value data and powerful login credentials for the simple task of proving account ownership. Using the Directory service, Public Keys, and Member validation, an authenticated user can prove account ownership via a simple API endpoint.

**Authentication by Member or RNAP Authentication**

This type of Authentication provides Members the opportunity to Authenticate their own End Users, ensuring their safety requirements are met (e.g. MFA), brand experiences are enforced, and End-User authentication remains a primary and trusted function of the Member.

As discussed in “Initiate Credit Transfer to Unknown Payee” section, the Directory facilitates enrollment of new End Users with their preferred Member or RNAP. A Member and RNAP provides the Directory with a dedicated Authentication Portal associated with its Routing Number via a URL reference. This is also used to facilitate Application Authentication and Authorization requests by Providers, allowing Member or RNAP to Authenticate their End User. This is further discussed and outlined in the “Payer Authorization” section.

**Component Authentication**

With sensitive information exchanged across the network, secure messaging is critical to the integrity of the FPS.
Provider to Member Authentication

- Provider requires a Directory entry facilitated by the Access Provider; Directory updates are authorized to the Members only.
- Providers retrieve their Private Key as well as an API secret to participate with the Member components. The Directory allows for the validation of message signing as Provider and Member Public keys are available.

Member to FPS Components Authentication

The information below describes how a Member securely authenticates and interacts with the Directory, Operator, and Fraud Sharing Service:

- Strong Authentication and Signing through the use of Public Key Cryptography as provided by the Directory service. The Directory and Members exchange information across a secure channel with signed messages using their respective Private Keys and validated by the available Public Keys within the Directory.
  - The Private Key is part of a key pair; Private is stored by the Member and the Directory publishes the Public Key. The Directory also makes available a series of Public Keys used for signing and retains the Private Keys in a strictly controlled repository.
  - The Directory acts in the role of a lightweight Public Key Infrastructure and allows for generation, management, and revocation of key pairs.

- The API secret (along with the requisite key) allows Members to authenticate and audit actions.

- A secure channel is established by the required use of TLS across Components. Certificate management aligns with required standards to ensure the channel is protected from downgrade attacks, impersonation or man-in-the-middle attacks, certificate authority compromises, etc.

The Member is required to have independent configurations with each Component. The Directory, Operator, and Fraud Sharing Service grants independent key and secret information that is not consumable by other Components.

Members create an account at the Component by completing the following:

- Visiting a web portal
- Verifying their organization
Once successfully created, the Member is provided:

- Public Key
- Private Key
- API Secret

The configuration must occur at each of the Components: the Directory, Operator, and Fraud Sharing Service. All GET and POST interactions require the appropriate security measures to ensure integrity of the interactions.

**Protecting Sensitive Information**

Information *not* shared across entities includes:

- Address
- SSN, Tax IDs, or EIN
- Account numbers, status, and type
- Username and password
- Security questions and answers

**Benefits**

The isolation of information sharing and security controls benefits the entire ecosystem. The benefits for each entity are outlined below:

*End User*

- No additional credentials needed to send and receive funds.
- Minimal financial information footprint reduces risk of exposure.

*Member/Provider*

- Can enforce existing and proprietary security control best practices.
- Updates do not require downstream system updates.
- Avoids sharing sensitive information.

*Platform (Operator, Directory, and Fraud Sharing Service)*

- Provides a secure experience with marginal data sharing across systems.
- Avoids costs of maintaining personal information in multiple systems.
3. Payer Authorization

Detail how and when payments would be authorized by the payer. If the solution allows Pre-Authorization, detail the process for establishing Pre-Authorization, and the process and timeframes within which a payer can revoke Pre-Authorization or change relevant parameters for Pre-Authorization.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to payer authorization: U.2 (Usability); U.3 (Predictability); S.2 (Payer authorization); S.7 (Security controls); S.9 (End-User data protection).

There are three types of End-User Authorizations in the proposed Solution:

1. **Participant Authorization**: End-User approval of FPS Enrollment with a Member or RNAP is completed during Enrollment.

2. **Provider or Application Authorization**: Approval of a Provider’s request for FPS permissions by the End User at its RNAP or Member.

3. **Transaction Authorization**: The explicit instructions given by the Payer to the Payee to transfer funds on a one-time or recurring basis, including: timing, amount, Payee, source of funds and other conditions.

**Participant Authorization**

Participant Authorization occurs at the Member or RNAP enrolling an End-User Account into the FPS. All Members and RNAPs are subject to adherence to Authorization standards identified by the FPS Regulator.

*The rest of this section is focused on the Authorization of a Payment. For more on Participant Authorization see Part A, Section 1: Initiation - “Enrollment in the Directory”.*

**Provider of Application Authorization**

*Note: This step follows Authentication of a Payer’s Member or RNAP Account.*

Granting Authorizations to a Provider offers convenience and control to the End User. The explicitness of an End-User interaction with an Authorization process is set by their Member and informed by the Member’s Scheme.
**Transaction Authorization or Pre-authorization**

**Transaction Authorization**

Transactions without established Pre-Authorization require End User Authorization before execution. While the FPS does not require any explicit authorization features, Scheme Owners may specify that Members and Providers collect additional information (e.g. two-factor authentication). All transaction authorizations are completed in five seconds or less.

Members and Providers may also establish additional criteria based on their security practices and customer needs.

**Pre-Authorization for payments**

For future and recurring payments, Payers may provide Authorization to a Provider to initiate a Credit Transfer without an explicit authorization for each individual payment. To permit this behavior, the Payer can provide a Pre-Authorization for payments to be initiated on their behalf. Payment Pre-Authorizations can be created and revoked. Pre-Authorization or revocations are completed within five seconds of the Payer’s approval.

A Pre-Authorization can occur at two entities within the System:

- *Payer’s Member* - A Member can obtain Pre-Authorization directly from their End Users (e.g. monthly bill pay providers).

- *Providers* - Authorized Providers can capture Payer Pre-Authorizations on behalf of the End User (e.g. internet subscriptions) at the End-user’s Member or RNAP.
Pre-Authorization: Participant to Third-Party

In this example the utility company uses a platform or suite provided by its Third-Party Service to access and leverage the FPS capabilities.

1. Payer Initiates Payment Order to a utility company through a Third-Party Service.
   
   **NOTE - Third-party has no affiliation with the End User’s Member or Provider.**

2. Third-Party Service requests the “Member and RNAP list” from an Access Provider.
   
   **NOTE - The Third-party does have a relationship with a participating Member.**

3. Access Provider retrieves Member and RNAP List from the Directory.
   
   ○ List includes:
     
     - Member or RNAP name
     - URL destinations of respective Authentication Portals

4. Member and RNAP List is returned to the Third-Party Service.

5. The Third-Party Service displays the list to the Payer and allows them to search and select their preferred Member or RNAP.

6. Payer is redirected to the associated Member or RNAP Authentication Portal and authenticates
○ The Pre-Authorization Request is securely transmitted with the redirect, via the following:
  ■ HTTP Headers denoting source and component information
  ■ JSON Web Token (JWT) as a POST Parameter
  ■ The JWT is assembled using the chosen elements from the Member and RNAP list including Pre-Authorization information.
  ■ The JWT is signed using the Member or RNAP’s Public Key from the Directory and encrypted using the destination Member or RNAP’s Public Key (either directly or via an exchange and one-time symmetric key).

7. The Payer’s Member or RNAP interprets and displays the Pre-Authorization information.
○ Interpretation of the secure message is conducted as follows:
  ■ The JWT is queued and, after successful authentication, is decrypted and then decoded to validated via its digital signature and interpret the embedded Pre-Authorization information.
○ A Pre-authorization Message includes:
  ■ Auth ID - identifier to reference the existing authorization
  ■ Status - designated as “Approved” when fully authorized
  ■ Payer UDID - The Unique Directory ID of the person who is providing authorization for the payments (if available)
  ■ Payee UDID - The Unique Directory ID of the person who requested the payment
  ■ One or more of the following Conditions
    ● Start Date - date of first payment
    ● End Date - date of last payment
    ● Recurrence - one-time or recurring
    ● Amount - amount of transaction
    ● Amount maximum - maximum amount the Payer will authorize
    ● Payment frequency - how often the payment is executed (e.g. monthly)

8. Payer’s Member or Sponsoring Member looks up the Payee information (via the Directory).
9. Payer’s Member or Sponsoring Member reviews the Payee via the Fraud Sharing Service.

10. Payer’s Member or Sponsoring Member completes the Payer Pre-Authorization and sends Pre-Authorization Message to the Operator.
   - Includes Auth ID
   - Updates the status to “Approved”

11. Operator notifies the Payer that Pre-Authorization is received.

12. The Payee’s Member notifies the Payee that Pre-Authorization is received.

**Executing a Pre-Authorization**

When the Conditions of a Pre-authorization are met (e.g. the Authorization is for the 1st of each month, and today’s date is May 1), it is the Provider’s responsibility to initiate the Credit Request of the Pre-Authorization.

1. Third-Party Service sends standard Credit Request with Auth ID to its Member or RNAP.
2. The Payee’s Member retrieves the Payer from the Directory.
3. Member sends Credit Request Payment Message with Auth ID to Operator.
4. The Operator notifies the Payer’s Member of the requested payment.
5. The Payer’s Member retrieves the Payee from the Directory.
6. Payer's Member cross-references Auth ID with Authorizations granted by Payer.
   - *Success* - Credit Transfer is initiated to Payee member
   - *Failure* - Payer's Member provides Reason (e.g. Insufficient Funds)
Revoking Pre-Authorizations

Any location where a Pre-Authorization can be granted requires an interface to allow revoking those permissions. Providers and Members supporting Pre-Authorizations must allow their customers the ability to revoke at any time after the authorization is granted. The communication is necessary to the enablement and revocation process and should be conducted as follows:

1. Payer logs in to a participating Member, Provider, or Third-Party Service.
2. Payer selects the Pre-Authorization to revoke.
3. A notification is sent to both Payer and Payee of the revocation of Pre-Authorization.
4. Approval by the Payer’s Member

Detail the process for approval of the payer’s Member (depository institution or regulated non-bank account provider), including how long approval will take from the point of completion of payment initiation, and the point at which the payment becomes final and irrevocable. Describe the consumer protections around payer approval and the assurance of Good Funds. Also describe any security features associated with approval, including protecting sensitive information, and detecting and limiting unauthorized, fraudulent or erroneous payments.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to approval by the payer’s provider: S.3 (Payment finality); S.7 (Security controls); S.9 (End-User data protection); F.1 (Fast approval); F.5 (Prompt visibility of payment status).

Upon receiving a Payment Order from the Provider, an initial Approval process is undergone by the Payer’s Member or Sponsoring Member. The FPS expects Approval to be completed within two seconds.

While the Approval requirements for a Payer’s Member are informed by Scheme Requirements and the FPS Regulator, the following risk factors are just a few examples of the many considerations taken by a Member:

- Payer’s Account Status
- Payer’s Member assesses Fraud Risk
- Payer’s Member assesses its current cash position

Following a successful assessment of these or other considerations, the final step of Approval is the intra-bank transfer that occurs between the Payer’s Account and the Operational Account.

Real-time decisioning on the Payer’s Account

Account Status

An internal assessment made by a Payer’s Member may include, but not be limited to:

- **Account Status** - An assessment on the eligibility of the Payer Account (e.g. a current hold on Account, existing suspicious activity, account closed, etc.)
- **Balance Check** - Verification that current holdings cover Credit Transfer Amount
• *Pre-Authorization* - In the event that a Credit Request contains a Auth ID, the Member is expected to cross reference the conditions and parameters’ permissions by the initial Pre-Authorization scope provided by the End User.

In the event that a Payer does not satisfy eligibility requirements a Status is sent to the Provider to notify Payer of the cause and potentially include instructions to complete (e.g. additional multi-factor authentication).

**Fraud Risk**

Relative to Payer’s Member’s own fraud capabilities, the Directory and Fraud Sharing Service offers a powerful new tool in combating payment fraud.

**The Directory**

As a facilitation point of Payer and Payee information, the Directory:

- Allows the Payer’s Member to identify Payee’s Account Information
- Provides the capability to retrieve Fraud Sharing information about both End Users
- Relies on a UDID model that reduces risk associated with the circulation of PII and PAN
- Enables effective routing by the Operator to the Payee’s Member

**Fraud Sharing Service**

The Fraud Sharing Service does not make decisions about End Users on behalf of the Members or their partnering Providers, since those entities are in the best position to know their End Users. The goal of the Fraud Sharing Service is to improve decision-making by providing data that Members or Providers would not otherwise have.

While the initial End-User information is populated at Enrollment, Members have the ability to query the End-User UDID and populate transaction information to help overall risk detection.

The initial Messaging scopes may include:

**Input to Fraud Sharing Service from Payer's Member:**

- Payer UDID
- Payee UDID (if available)
- IP address of the End User’s session, if applicable
- Browser type and version
- OS type and version
- Device type

**Outputs from Fraud Sharing Service to Payer's Member**
- Abnormal transaction volume (number or percent increase) from an IP address or range
- Payer or Payee has generated X exceptions (request for return, reported unauthorized payments) over the past 60 days
- Abnormal transaction volume from a geographic area
- Abnormal transaction volume from a third party service provider
- Payer and Payee names differ, yet share identification attributes (IP, device ID, etc.)

Examples of fraud analysis potentially conducted with this data can be found in Criteria S.6.

As the Solution matures, Scheme Owners will refine and increase this type of messaging as a result of research and Member feedback about the usefulness and quality of the data received.

Overall Cash Position

In evaluating the risk associated with an Approval, a Payer’s Member may need to contemplate its overall liquidity prior to completing the Intra-bank transfer and assure the availability of Good Funds.

Risk thresholds and ratios may be determined by the FPS Regulator, Scheme Requirements, or the Member.

Completing Payer Approval

Initiate and complete the intra-bank transfer

Based on the Payment Order and aforementioned risk assessments, the Member or Sponsoring Member is responsible for executing the intra-bank transfer from the Payer’s Account to a designated Operational Account inside the financial institution. The transfer is structured as follows:

- Debit to the Payer’s Account
- Credit to the Operational Account

Consumer protection

In addition to the ability to control the experience and notifications, the FPS better positions itself to protect End Users.

Removing sensitive information
The Payer’s personal information is not required by the Solution to facilitate a payment. The information below is limited to the data elements required to efficiently complete a transaction:

- Payer’s UDID
- Operator ID
- Routing Number
- Amount
- Contextual Data (leveraging metadata)\textsuperscript{14}

Unauthorized, fraudulent, or erroneous payments

A Credit Push payment system, combined with Authentication and Authorization by the Payer and Payer’s Provider, reduces the amount of unauthorized or fraudulent payments.

- First-party fraud: By requiring multiple steps to authorize a payment, the likelihood is reduced of an End User falsely reporting their transaction as fraud. The multiple steps allow a Provider to document key indicators of the interaction which can be used as evidence that the transaction was indeed initiated and authorized by the End User.

- Second- and third-party fraud: Additional factors create more barriers for a party other than the End User to compromise an account. Properly implemented MFA can alert an End User to an attempt to initiate an unauthorized transaction, which can be stopped at that point.

While no platform is 100% safe, the below fraudulent and erroneous activity is possible:

- Account takeover - The Payer’s Provider account profile is compromised.

- Fraudulent payment requests - Payment requests are positioned as a known Payee and result in a payment to another party.

- Erroneous payments - Payer accidentally sends a payment to wrong Payee (e.g. payment is sent to a Yahoo! email, rather than Gmail email).

While the scenarios range in severity, each results in payment to an incorrect Payee. Three basic mechanisms are available for mitigation:

- Cancel a payment - Unclaimed funds sent to an unauthorized Payee can be canceled and returned directly to the Payer.

\textsuperscript{14} It is possible that a Provider chooses to disclose personal information in the metadata of the transaction. While it remains a capability of the network, including PII in the metadata is strongly discouraged since the information is available to the Payer, Payee, and their Providers.
• **Request a Return** - Claimed funds sent to an authorized Payee can be reclaimed via an additional Return transaction request via a “Payer requesting a return” outlined in the Initiate section.

• **Issue a Return** - Claimed funds received by an authorized Payee can be reclaimed via a “Payee initiated a return” outlined in the Initiate section.

For additional information on disputes and erroneous payment, see section E.7.1.
5. Clearing

Detail the process for the exchange of relevant payment information between a payer’s and a payee’s Members (depository institution or regulated non-bank account provider), including payment format (message) standards utilized, the necessary communication processes, and how long the clearing process will take from the point of completion of payment initiation. Also describe any security features associated with approval, including protecting sensitive information.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to clearing: E.4 (Payment format standards); S.7 (Security controls); S.9 (End-User data protection); F.2 (Fast clearing).

Payment Messages Cleared by the Operator

The FPS Operators support four types of Payment Messages:

- Credit Transfers
- Credit Requests
- Returns
- Pre-Authentications

These Payment Messages and their respective data have been discussed in previous sections.

Clearing Participants

As previously explained, Clearing is predicated on a Good Funds model where funds are debited from Payer’s Account and credited to the Payer Member’s Operational Account. After completion of this action, Clearing between Members begins.
Payer Member Clearing

The exchange of Payment Message to the Payee Member is facilitated by the Operator. Only relevant information is shared across the network, allowing each Provider to mitigate the circulation of sensitive PAN and PII.

To facilitate payment, the Payer’s Member sends the Operator the following Payment Message, including the following:

- **Payer UDID**
- **Payee UDID**
- **Operator ID**
- **Routing Number**
- **Amount**
- **Contextual Data**
- **Payer Confirmation ID** - Identifier created by the Payer’s Member for reconciliation
- **Payer Status** - “Completed” or “Pending” depending on whether the Payee is Enrolled in FPS
- **Payer Reason** - Populated when Status is not “Completed”
- **Auth ID** - If applicable

Leveraging appropriate security mechanisms and messaging, the Payer’s Member POSTs to a predefined Operator-hosted API endpoint to submit an initiated and approved transfer.

Operator Clearing facilitation
The Operator is the primary facilitator of clearing information between the Payer and Payee Members. The Operator is expected to complete the following within two seconds:

1. Capture the Payment Message via the POST sent by the Payer’s Member as described above.
2. Record the transaction information to be used in the Deferred Net Settlement and Reconciliation process.
3. Notify the Payee Member via a Webhook Notification of the received payment.

Payee Member Clearing

The Payee’s Provider has the opportunity to approve the reception of funds. The Operator’s Webhook notification provides the appropriate information to allow a Payee’s Provider to callback to the Operator to retrieve the entirety of information. The Operator provides the following information for the Payee’s Provider about the received payment:

- **Transfer ID** - created and assigned by the Operator
- **Date** - date assigned by the Operator
- **Payer UDID**
- **Payee UDID**
- **Amount**
- **Metadata**
- **Payer Status**
- **Payer Reason**
- **Auth ID** - If applicable

*The Payee’s Member has the opportunity to conduct an approval process. The approval process is discussed further in the “Payee’s Member Approval” section in the “Receipt” stage.*

Payment Finality and Irrevocability

Subject to applicable regulation and/or rules, payments are considered final and Irrevocable once the Payer's Member has received the “Transaction Complete” message from the Operator. This is preceded by the Payee Member’s own Approval of the transaction. From the payment initiation

---

15 The Payee Member Approval process may be run similarly to Payer's Member Approval, including, but not limited to: an assessment of the Payee’s Account Status, Payee/Payer Fraud Risk, industry, or account type.
to the final step, there are a series of revocable steps that are subject to the discretion of the Providers in handling End User interactions.

If a Payee is not identified in the Directory an engagement process is initiated by the Payer’s Provider or Member. While the Payment remains unclaimed, it can be cancelled. The transfer can also incorporate a reclaim period allowing automatic reclamation of funds after a specified duration (e.g. 30 days).

Payment Finality is distinguished as the “Transaction Complete” message from the Operator to the Member. Upon the entire transaction completion, all disputes are resolved via the return process as discussed in E.7.1.

Security Features Associated with Clearing Process

When exchanging information with the Operator, the Member establishes a secure channel by signing and encrypting all messages with a key and secret exchanged between the two parties at setup.

- TLS is required for communication between components with mutual authentication provided by both digital certificates and Public/Private key pairs.
- Signing of messages ensures the Integrity of messages while TLS and optional data element encryption within the message provide Confidentiality.
6. Receipt

Describe how the approach would enable availability of funds (and contextual data, as appropriate) to the payee and the time this will take from the completion of payment initiation. Detail when and how the approach will make the payment status visible to the payer and payee (for example, visibility to the payer and payee that the payment has been approved, visibility to the payer and payee that the funds have been received in the payee’s account for use, etc.). Describe any security features associated with approval, including protecting sensitive information and mechanisms to block funds availability if an unauthorized, fraudulent, or erroneous payment is reasonably identified by the payer’s provider (depository institution or regulated non-bank account provider) prior to payment finality.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to receipt: U.1 (Accessibility); U.2 (Usability); U.3 (Predictability); U.6 (Applicability to multiple use cases); S.5 (Handling disputed payments); S.7 (Security controls); S.9 (End-User data protection); F.3 (Fast availability of Good Funds to payee); F.5 (Prompt visibility of payment status).

Payee Provider’s approval

When the Payment Message exchanges are complete between both Members, the Payee’s Member must approve or reject the transfer. The Payee Provider is expected to provide an approval response once accepted.

The first step in the Payee Member approval process is to ensure the Payee’s account is able to receive the specified payment. This include validation of the following:

- Payee is authenticated and authorized.
- Payee’s account is in “good standing” and active.
- Payment meets the Payee Provider’s criteria, which may include, but not be limited to:
  - Payer is an acceptable payment source.
  - The payment is within Provider limits.
  - The payment is in a Payee Provider’s supported currency.

Executing the transfer

Once completing an assessment of the acceptability of the funds, the Payee’s Member can complete the intra-bank transfer and inform the Payee. An intra-bank transfer is utilized to
conduct real-time messaging to Providers (and ultimately to the End User), leveraging the Member’s statuses and notifications capabilities. Based on the directive of the message provided by the Operator, the Payee’s Member conducts the following to complete the transfer to the End User’s account:

- Debit to the Operational Account
- Credit to the Payee’s Account

All notifications and statuses are maintained by the Member and shared with the Provider, specifically the following to inform the customer of the received transfer:

- Update status on all online banking avenues
- Notify the Payee
- Complete bank entry for the credit into the Payee’s account

Once the Payee’s Member has accepted and transferred funds, the Operator is owed an update. The Payee’s Provider updates the Operator via a POST to an API endpoint with the following information:

- Transfer ID
- Payee Confirmation ID - identifier created by the Payee’s Member for reconciliation
- Payee Status - “Completed” or “Rejected” depending on whether funds were accepted
- Payee Reason - Populated when Status is not “Completed”

The “Payee Status” and “Payee Reason” can be leveraged in the event that the Payee does not want to accept the funds. For example, if the transfer amount is above the Payee Provider’s transaction limit, the following may be returned:

- Payee Status - Rejected
- Payee Reason - Transaction exceeds the Payee’s limit

Notifications

The Operator notifies the Payer’s Member that the transfer has been received by the Payee via a Webhook made available through the Platform Services Layer at the Sponsoring Member. From the information included in the Webhook, the Payer’s Member is able to retrieve the full transaction detail from the Operator for reconciliation purposes.

The following notifications should be sent by email or SMS to reference the completed transaction:

- Payer’s Provider notifies the Payer.
● Payee’s Provider notifies the Payee.

Once all notifications are sent, activity is complete until the Deferred Net Settlement.
7. Settlement

Describe the approach or model for funds settlement between the providers to the approach, and the time it takes from the completion of payment initiation to the settlement of the payment. Describe whether the settlement will take place in central bank money or commercial bank money. Detail how the solution will manage settlement risks that may arise from a lag between funds availability to the payee and settlement between providers, or from settlement in commercial bank money.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to settlement: S.4 (Settlement approach); S.7 (Security controls); S.9 (End-User data protection); F.4 (Fast settlement among depository institutions and regulated non-bank account providers).

Aside from clearing Payment Messages, the FPS Operator tracks receivables and liabilities of its Members and instructs settlement of multilateral net positions with the Central Bank via Fed-supported rails. As an instructor of settlement (acts as protocol to initiate settlement), the Operator is technically agnostic to a settlement mechanism; therefore, the decisioning regarding settlement mechanism (i.e. new vs. existing) is a risk-, regulatory, cost-based decision that demands further discussion. For the sake of this section, the Proposers highlight a Deferred Net Settlement based on the existing mechanisms for Central Bank settlement.

Facilitating a Deferred Net Settlement

With multiple Operational Accounts, the network needs to Rebalance to ensure each participating Member avoids liquidity concerns.

The visual representation below depicts the Rebalance process for Operational Accounts across Members:
Both a receivable and a liability are recorded at the time Finality is determined. Below are the interactions and real-time transfers occurring throughout a settlement period:

- Debit to Payer’s Account
- Credit to Payer Member’s Operational Account
- Debit to Payee Member’s Operational Account
- Credit to Payee’s Account

To facilitate an effective rebalance, the transactional information recorded at the Operator accounts for an outstanding obligation, in this order:

1. Debit, or liability, from the Payer Member’s Operational Account
2. Credit, or receivable, to the Payee Member’s Operational Account

At coordinated times across the network (or ad hoc in the event of extraordinary circumstances), settlement on behalf of Members is executed to address the outstanding obligations across Members and other Operators. At the time of settlement, the obligations are aggregated into a single debit or credit entry for each participating entity. The inter-bank settlement is facilitated via the Operator’s use of Fed-supported rails (e.g. National Settlement Services (NSS)).
Operating windows

The settlement is conducted across multiple financial institutions and is initiated via a final and irrevocable settlement service operated by the Federal Reserve Banks. The FI rebalance is conducted every two hours leveraging the extended processing window offered by the Federal Reserve starting at 9:00 PM ET and closing at 5:30 PM ET each business day. The optional extended period is leveraged to reduce risk exposure associated with a Deferred Net Settlement solution.

Liquidity risk exposure

Regulatory enforcement

The FPS Regulator informs the risk requirements of its Participants, such as capitalization requirements and ratios; however, Scheme Companies may enforce additional precautions or services on their Members as they see fit (e.g. overdraft policies, collateralization, etc.).

System

Rebalancing every two hours reduces the risk associated with a Deferred Net Settlement solution, while lowering direct costs associated with Settlement. If a Member raises a liquidity concern, the Solution can conduct an ad hoc settlement, leveraging the same funding tools on an as-needed basis.

Participating FIs may introduce internal mechanisms to protect themselves from liquidity. Since the network is monitored at the Operator level, liabilities and receivables are settled on a regular basis. However, if an FI has ongoing concerns about the Operational Account and negative balance scenarios, internal safeguards such as optional contingency-funded accounts may be leveraged.
8. Reconciliation

Describe the solution’s mechanisms to create and record information to facilitate post-transaction evaluation, the processes and timeframes for handling unauthorized, fraudulent, erroneous, or otherwise disputed payments, and the allocation of liability among, and substantive liability limits for, all parties involved in the payment. Describe how consumer protections are built into the reconciliation processes. Also describe any security features associated with reconciliation, including protecting sensitive information.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to reconciliation: U.3 (Predictability); E.7 (Exceptions and investigations process); S.5 (Handling disputed payments); S.6 (Fraud information sharing); S.7 (Security controls); S.9 (End-User data protection).

Real-time transfers are facilitated throughout the day since the Solution is available 24/7/365. At the time of transfer, the Operator collects all the information required to facilitate reconciliation. Members and other Operators have the ability to access reconciliation information via a GET to a reconciliation endpoint with the following information:

- **Start Date** - date and time for the start of the Member reconciliation period, in UTC
- **End Date** - date and time for the end of the Member reconciliation period, in UTC

Since the request is signed and encrypted using the provided key and secret, the Operator ensures only the appropriate information is returned to each Member. Information included in this exchange includes:

- **Date**
Each Member is expected to provide a reconciliation endpoint to allow the Operator to complete a network reconciliation. The Member makes an endpoint available to allow the Operator to retrieve information via a GET request.

**Protecting sensitive information**

Delivering End-User information only to the required Provider or Member is a great benefit of the new payments Solution. Customers do not have to be concerned that their PII is constantly exchanged across a network and subject to security threats, such as interception.

The reconciliation process reinforces this limited data sharing for the protection of End Users and participants by providing access to only the information needed to complete a reconciliation process. Members maintain their customer information and leverage the reconciliation information to supplement the already-received transaction information.

The summary below provides detail on where information can be located:

- **Transaction information** - accessible at the Operator
- **Provider’s customer information** - owned and stored at the Member/Provider
- **Other Provider’s customer information** - accessible via the Directory

*See S.7.1 reference to Public Key cryptography and data encryption.*

**Handling reconciliation discrepancies**

The Solution provides a confirmation-based System, but it is possible that discrepancies arise. There are two possible scenarios of reconciliation discrepancies:

- **Member has a transfer the Operator has not recorded** - The Operator has no record of the transfer and the Member may have recorded a transfer that never cleared the System.
this instance, there was no response from the reciprocating party (e.g. Payee Status is empty).

- **Operator has a transaction that the Member does not have** - The Operator has a record of the transfer, but the Member does not or never received it (e.g. Payee Member never recorded the transfer).

Scheme Owners can further define timeliness and other operating rules relative to resolving reconciliation discrepancies.
Part A, Section 2: Use Case Description

In this section, the proposer should describe what the solution does at each stage of the end-to-end payments process for each use case that the solution supports (business to business; business to person; person to business and/or person to person, as indicated in the table “Supported use case coverage summary”, above). Proposers should include flow diagrams of the messaging and payment flows and the roles of stakeholders (End Users, technology providers, processors, including the proposer(s) for the solution) through the eight stages of the end-to-end payment process of their solution. The description and diagrams should be specific to each supported use case and should highlight all processes and features that are unique to the use case being described. For example, the solution may be designed to enable contextual data capability for business-to-business payments, but not for person-to-person payments. The business-to-business use case description should, therefore, include all the additional processes and features related to enabling contextual data capability.

The Platform provides a robust solution for all Payers and Payees. While there are slight differences in the use cases, nothing disrupts or changes the payment flows described in the previous sections. These minor differences are identified in the “Initiation” section, but the stewardship model enables Members and Providers to be in the best position to manage their End Users’ on-going payment needs.

Below is a summary of the various use cases and technology platforms:

- Use cases
  - There are minimal use case differences across the Platform, identified in the Initiation section.
  - Members and Providers can adapt the customer experience based on account type.
  - Metadata can be leveraged to distinguish different information based on account type.

- Technology Platforms
  - The FPS is technologically agnostic.
  - All platforms available to End Users are extensible for faster payments.
  - Solution accounts for the ability for Members and Providers to extend the network to all customer touchpoints.
Part A, Section 3: Use Case by Effectiveness Criteria

For each use case that the solution supports (business to business; business to person; person to business and/or person to person, as indicated in the table “Supported use case coverage summary”, above), complete the following table. For each criterion relevant to the lifecycle stage, enter a “Y” if the use case addresses the Effectiveness Criteria (at least to a “somewhat effective level”) or an “N” if it does not (blanks will be assumed as “N”). For example, the solution may be designed to enable contextual data capability for business-to-business payments (U.4, Contextual data capability criterion), but not for person-to-person payments. Proposers should enter a “Y” for any functionality that will be in place at the date of implementation or for which there is a credible plan to implement the enhancement at a future date (as described in Part B, sub-section 1 “Implementation Timeline”).

For solutions where lifecycle stages occur simultaneously, the proposer should enter a “Y” or an “N” based on the criterion listed (rather than focusing on the categorization by lifecycle stage). The table is intended to be a summary of the description in Part A, Section 2.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>U.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.6</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>E.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Authentication</td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.10</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Payer Authorization</td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Approval by the Payer's Provider</td>
<td>S.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Clearing</td>
<td>E.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Receipt</td>
<td>U.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>U.6</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Settlement</td>
<td>S.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>F.4</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>U.3</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>E.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.5</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.6</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.7</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>S.9</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
Part B: Business Considerations

In this part, the proposer should describe important business considerations to demonstrate the feasibility for the solution. Proposers may detail their qualifications or past experience in implementing faster payments in the subsections below if they view it will support the description.

1. Implementation Timeline

Specify the projected timeline and explain the credible plan for developing, testing and achieving initial implementation of the solution, including all key milestones and project phases to reach ubiquity (as defined in the glossary). The level of detail in the credible plan and timeline will assist in demonstrating the feasibility of the solution. The description should clearly indicate the use cases, functionality (e.g., cross-border, domestic, contextual data capability, etc.), whether the solution will be newly built and/or interface/interoperate with existing solutions, and features that will be ready at initial implementation and those that will be added in subsequent phases. The description should also indicate key dependencies (e.g., stakeholders or other external factors) and possible risks to the projected timeline.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to implementation timeline: U.1 (Accessibility); U.2 (Usability); U.3 (Predictability); E.3 (Implementation timeline); E.5 (Comprehensiveness).

When its charter is complete, the Federal Reserve Faster Payments Task Force will have successfully:

- Defined the desired attributes of an improved Payment System (i.e. Effectiveness Criteria)
- Assessed Faster Payment Proposals per the Effectiveness Criteria and market-endorsed process (i.e. QIAT and TF review)
- Identified gaps and provide a credible foundation for next steps (i.e. the Final Paper)

External market forces, other Faster Payment initiatives, and secure and low-cost cloud-based technology all combine to offer unprecedented urgency and confidence for a rapid deployment of Faster Payments in the United States. The following sections outline an open-ended yet aggressive three-year approach to capitalize on this momentum.
Timeline

General Dependencies and Possible Risks

Ambiguity exists on the following items:

- Regulatory oversight and the responsibilities of an FPS have yet to be defined.
- Without clear regulatory oversight or guidance, the path to ratifying FPS Operating Rules and Guidelines is unclear.
- ISO 20022 standard adoption timeline is undefined.

Phases

Due to the uncertainty outlined above, Proposers offer quarterly and annual snapshots of phases and milestones not tied to specific dates. This approach provides a flexible outlook on the Solution’s three-year plan to reach domestic Ubiquity.

Phase 1: Coordination

<table>
<thead>
<tr>
<th>Scheme Formation</th>
<th>Structure, bylaws, multi-operator considerations</th>
<th>Initial Membership LOI period</th>
<th>Incorporation, Membership fees due, Approval by FPS Regulator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>Consultation paper and response period</td>
<td>RFP issued, if necessary</td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td></td>
<td></td>
<td>Review, Approval by FPS Regulator</td>
</tr>
<tr>
<td>Year 1 - Q1</td>
<td>Year 1 - Q2</td>
<td>Year 1 - Q3</td>
<td>Year 1 - Q4</td>
</tr>
</tbody>
</table>

Scheme Formation

While Schemes may be formed at any time, Phase 1 provides a snapshot of the potential timeline for incorporation and creation of a Scheme by its Members. The Scheme Owner is responsible for the operation and strategic development of its FPS Infrastructure.

A formal review, audit, and stress testing of the Scheme and its systems will be conducted by the FPS Regulator and funded by applying Scheme Owner to ensure integrity and compliance of the FPS.

Directory

During Phase 1, a consultation paper will be issued for the services outlined in this proposal. This document will outline in more detail and depth the functions and points of interoperability needed for the services, and will invite comment from industry leaders. The consultation paper
and its responses will serve as the baseline for a Scheme Owner’s in-house build or for an RFP of the services.

**Governance**

While oversight and logistics are within the purview of the FPS Regulator and FPS Guidelines and Operating Rules, Proposer suggests a 90-day review process of Scheme applications and infrastructure plans. Monthly check-ins with stakeholders by Scheme Owners will ensure a smooth process.

**Phase 2 - Development, Testing, and Proof of Concept**

From a functionality standpoint, each use case and technological avenue will be delivered in the order outlined below. As discussed in “Part A, Section 1 - Solution Description” differences in use cases are minimal and will not impact the overall design and development of the components.

Since the development phase focuses on creating a Proof of Concept, minimal dependencies are expected aside from interactions with technical vendors (e.g. hosting providers). Each of these dependencies will be managed from a project perspective and do not pose considerable or unique risk to the implementation.

The Proof of Concept will be demonstrated via the effective implementation of a single pilot Member. The pilot integration will be leveraged to demonstrate effectiveness with the following success criteria:

- Stress-tested to show availability during periods of high-demand
- FPS core capabilities enabled for Provider
- Precise daily reconciliations occur without fail

In addition to the features delivered as part of Phase 2, the pilot Member and subsequent integrators will have the following available:

- Accessible API documentation that includes:
  - API endpoint reference
  - Code examples
  - Guides and resource articles including best practices
- If applicable, updates to supported client libraries
- API/developer support channels available
<table>
<thead>
<tr>
<th>Scheme Infrastructure</th>
<th>RFP awarded, development, proof of concept</th>
<th>Governance Review, Member Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory</td>
<td>RFP awarded, development, proof of concept</td>
<td>Governance Review, Member Approval</td>
</tr>
<tr>
<td>Member / Providers</td>
<td>Proof of concept</td>
<td>Governance Review, Member Approval</td>
</tr>
<tr>
<td>Governance</td>
<td></td>
<td>Governance Review</td>
</tr>
</tbody>
</table>

**Scheme Infrastructure**

**Operator**

Acting as payment message clearinghouse, ledger, and settlement instructor for Members of an FPS Scheme, the Operator interactions require the following:

**Online portal** - the following web-based portal is used for development and testing:

- *Member admission* - allows a Member to participate with the Operator

**API endpoints** - the following API endpoints are used by integrators for development, testing, and documentation:

- *Payer transfer approved* - allows a Payer’s Member to share transfer information with a Payee’s Member
- *Payee transfer approved* - allows a Payee’s Member to approve a transfer
- *Payer pre-auth complete* - allows a Payer’s Member to approve a Pre-Authorization
- *Retrieve a Payment Message* - allows either Member to retrieve a Payment Message
- *Retrieve Reconciliation information* - allows Payer’s and Payee’s Member to reconcile transactions

**Webhook notifications** - the following notifications are used by integrators for development, testing, and documentation:

- *Payee transfer received* - notifies the Payee’s Member that a transfer requires approval
- *Payer pre-auth received* - notifies the Payee’s Member that a Pre-Authorization has been approved
- *Payer transaction complete* - notifies the Payer’s Member that a transaction was completed (Payment Finality)

Infrastructure-related items (e.g., database and server configuration) are also required.

**Fraud Sharing Service**

The Fraud Sharing Service consists of several interactions that require the following:

*Online portal* - a web-based portal is used for development and testing:

- *Member admission* - allows a Member to leverage the Fraud Sharing Service

*API endpoints* - the following API endpoints are used by integrators for development, testing, and documentation:

- *Add an End User* - allows a Member to add an End User
- *Retrieve an End User* - allows a Member to retrieve End User information
- *Add transfer information* - allows a Member to add transfer information

Infrastructure-related items (e.g., database and server configuration) are also required.

**Directory**

The Directory consists of several interactions that require the following:

*Online portal* - the following web-based portal is used for development and testing:

- *Member admission* - allows a Member to leverage the Directory

*API endpoints* - the following API endpoints are used by integrators for development, testing, and documentation:

- *Add an End User* - allows a Member to add End User
- *Update an End User preferred account* - allows a Member to specify an End User’s preferred account
- *Retrieve an End User* - allows a Member to retrieve End User information
- *Retrieve Member and RNAP List* - allows a Member to retrieve a list of Members and RNAPs and corresponding Authentication Portal URLs

Infrastructure-related items (e.g., database and server configuration) are also required.

**Governance Review, Member Approval**

While oversight and logistics are within the purview of the FPS Regulator and FPS Guidelines and Operating Rules, Proposer suggests a 90-day review process of Operator, Fraud Sharing

Phase 3 - Member Integration and Testing

The final phase will focus on the integration of Members. Members will have the ability to integrate, test, and provide feedback. From a build perspective, the components should be available and ready for implementation.

<table>
<thead>
<tr>
<th>Scheme Infrastructure</th>
<th>Integration and testing</th>
<th>Audit</th>
<th>Live</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Directory</td>
<td>Integration and testing</td>
<td>Audit</td>
<td>Live</td>
</tr>
<tr>
<td>Member / Providers</td>
<td>Integration and testing</td>
<td>Audit</td>
<td>Credit/Request</td>
</tr>
<tr>
<td>RNAP</td>
<td>Integration and testing</td>
<td>Credit/Request</td>
<td></td>
</tr>
<tr>
<td>TPS</td>
<td>Integration and testing</td>
<td>Credit/Request</td>
<td></td>
</tr>
</tbody>
</table>

**Integration and Testing**

Throughout Phase 3 support is given to Members and Providers in various levels of the integration, including:

- Integrating and testing Member to System Components
- Integrating and testing Providers to Members

Support provides relationship-based services such as:

- Integration by the Member (discussed in Part B.3—Integration Effort)
- Integration consulting
- Resolving support items arising from Member feedback

**Audit and Examination by Scheme, Governance**

While oversight and logistics are within the purview of the FPS Regulator and FPS Guidelines and Operating Rules, Proposer suggests a 90-day review process by Scheme Owners, prior to submitting for examination by FPS Regulator. Monthly check-ins with stakeholders by Members will ensure a smooth process.
Value Proposition and Competition

For each use case supported by the solution, describe the value proposition to each stakeholder in the solution (End Users, technology providers, processors, the proposer(s) of the solution) through each of the eight stages of the payment lifecycle (as discussed in Part A). Consider why stakeholders will adopt the solution. NOTE: If the value proposition discussion includes fees in the system, describe the nature of what type of fees might be charged to and received by different stakeholders such as whether they are one-time, recurring, per item, ad valorem, any floors/caps, per item + ad valorem and provide any related system constraints. Do not provide any proprietary cost or pricing information.

Describe how the solution will enable access to new entrants (competition) into the broader ecosystem of the proposed solution (e.g., to provide base-level features or Value-Added Services).

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to pricing model and competition: U.3 (Predictability); E.1 (Enables competition); E.2 (Capability to enable Value-Added Services).

Proposer note: Dwolla was designed to enable communication agnostically between nodes (i.e. Accounts) on the Network. This gives Accounts a full range of features and capabilities to anyone in the Network.

To manage risk, accommodate regulatory requirements, and facilitate other considerations, limitations are applied to a Node as the End User establishes their relationship with Network (e.g. businesses are required to provide EINs, have different daily limits, and are evaluated for high-risk industries). This scoped approach to its Account structure allows Dwolla (i.e. the System) and Dwolla-enabled applications (i.e. Providers) to programmatically minimize and maximize capabilities on an Account level, creating a dynamic, scalable, and feature-rich Network that is both regulated and use case-agnostic.

Applied to national system, this approach allows Scheme Owners, Providers, and Participants the flexibility to apply programmatic parameters downstream from an Operator to an End User (e.g. limits, authentication requirements, miscellaneous scopes, etc.), and enable limitless Value-Added Services and experiences.
Competition and Value-Added Services

A high-degree of competition for Value-Added Services is best achieved through wide access to core FPS capabilities and services. The Solution’s Platform Services Layer provides a simple and modern means to build FPS value propositions into new or existing applications or business processes.

A wide range of new products, services, and markets that offer monetizable value for End Users is created by the ability to Initiate enrollment into the FPS and then Initiate credits, requests, and returns to, from, and between End Users.

New value, new business models

In an FPS world, traditional forms of economic incentives may not be applicable to certain Use Cases. For example, while ad valorem pricing had been successful in bringing near ubiquitous acceptance of Card networks among business and consumers, it’s now seen as a fixed cost-center and loss leader for new P2P applications which must offer free services to meet consumer expectations around P2P. A dynamic network that offers robust capabilities, elegant End-User experiences, and a brandless Platform is best positioned to accommodate the business models, consumer expectations, and market forces of the future.

Costs and incentive mapping

As directed by the template, this Proposal “does not provide any proprietary costs or pricing information”; however, the Submission does outline generic business relationships and expenditures, such as Operating and Maintenance Costs.

Scheme Owners

Potential Implementation and Maintenance Costs

As noted by the Federal Reserve Bank Of Boston in its paper, Cost and benefits of the UK FPS:\textsuperscript{16}

\begin{quote}
“Operating costs of a new service with frontier technology may be lower than operating costs of existing networks…. By comparison, the annual cost of operating the FedACH was $116.3 million in 2013, almost 38 percent of the seven-year cost of the U.K. FPS. This $116.3 million cost does not include the cost of the EPN, which comprises approximately half of ACH traffic.”
\end{quote}

\textsuperscript{16} Federal Reserve Bank of Boston, “Costs and Benefits of Building Faster Payment Systems: The U.K. Experience and Implications for the United States”.
We generally agree—the secure exchange of real-time data over information systems has a marginal cost of essentially $.00, significantly reducing the overhead and exposure associated with maintaining traditional systems for Scheme Owners.

Initial costs may include, but not be limited to the following items:

- Legal and compliance costs
- Third-party audits of compliance, security, and general operations
- Development and Integration efforts related to the RFP for creation of Operator, Fraud Sharing Service, and Directory services, and their respective interfaces.
- Capital reserves for operations or liquidity events, as determined by FPS Governance and FPS Rules and Operating Guidelines
- On-going support costs related to infrastructure, system updates, and more

System Value Propositions and Incentives

The large and highly complex banking population of the United States makes economic incentives for Scheme Ownership hard to qualify and the return value of an FPS hard to quantify. However, that has not slowed down activity in payments. A new reality is facing stakeholders, including:

- **Unprecedented developments**: FPS programs and standardization efforts by institutional stakeholders, such as The Clearing House’s Faster Payments Initiative, NACHA’s processing window expansion to enable Same-Day ACH, and the Federal Reserve’s Faster Payments Task Force have reached critical mass and buy-in over the past few years.

- **New entrants**: Cultural sentiment following the 2008 financial crisis, dramatically lower costs of infrastructure technology, and ubiquity of Internet-connected devices created a new market for nimble FinTech companies to directly or indirectly marginalize institutional services with more attractive products and services. (e.g. Blockchain, Apple Pay, Dwolla, Stripe)

- **Speed of business, life**: Advances in information technology have created new requests and heightened expectations for an underlying bank transfer system, creating pent-up demand and opportunity for Faster Payments among Participants.
• **Diversification of services:** Institutional Stakeholders continue to invest heavily in Value-Added Services to supplement the direct and indirect costs of an uncertain regulatory banking environment.

Membership in a Scheme not only provides assured relevancy and stability in a greater real-time economy, but a voice (and vote) in the creation of Scheme Requirements, potential profit sharing, pricing, and general operation of the Scheme itself\(^{17}\). Furthermore, the implicit benefits of direct access to the Directory, Fraud Sharing Service, and Operator are greatest felt by those closest to it.

Scheme Owners are incentivized to lower costs, threats, and inefficiencies of its System Component. This provides Members greater profit margins from brokered access to the FPS or their own products and services provided to their customers.

**Members**

**Potential Operating and Maintenance Costs**

ROI approaches for the formation of a Scheme and Scheme Infrastructure are reserved for the Scheme Owner or Company, but it is likely that FIs would pay a Membership or Connection fee to become a Member of the Scheme.\(^{18}\)

**System Value Propositions and Economic Incentives**

The Proposers anticipate Members recoup these costs directly by brokering and/or providing baseline access or additional value to other Participants in the system.

The technical, operational, and regulatory work required to run ACH deterred broader, more consumer-facing Third-Party Platforms. A Good Funds model with real-time availability, status updates, and other benefits provides FIs an opportunity to build new products, upgrade old services, or cater to markets previously deemed impossible to reach.

---

\(^{17}\) In a multi-operator environment, specialization of Schemes and/or additional Scheme services or products may provide a wide range of additional economic incentives depending on the business model of its Member.

\(^{18}\) It is also strongly recommended that these fees be oriented towards long-term recompense (ten years minimum) rather than short-term profits to aid ubiquity and incentivize Value-Added Services (e.g. connection fee relative to an FI’s Asset holdings, anticipated transaction volume in System, etc.).
Example: Monetizing above baseline features

End-User notifications are typically reserved for payment notifications. In Dwolla’s API, these are facilitated through Webhooks. An FI Member could offer enhanced Webhook capabilities to a customer to enable features or experiences deemed valuable to their End Users. For example, End Users could authorize utility companies to stream money out of their connected Member based on current energy consumption. Webhooks could allow smart thermostats to display not only temperature, but also the household utility costs in real-time.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Value proposition</th>
<th>Potential economic incentive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiation</td>
<td>Initiation can be done via any device, platform, or channel</td>
<td>Members create specialized products, services, or experiences to create business value to customers, create new lines of business, or better cater to the un- and underbanked.</td>
</tr>
<tr>
<td></td>
<td>The API-capable FPS enables seamless, dedicated, and secure baseline capabilities to potential Providers</td>
<td>FIs broker availability of core baseline capabilities via Platform Services Layer; The highly automated and self-scaling, benefits of an FPS reduce traditional overhead at FIs (e.g. manual processes) while increasing net-new revenue opportunities for Providers and Provider Business Models; Market created for additional FI services that enhance or support FPS capabilities to Participants.</td>
</tr>
<tr>
<td></td>
<td>Transport Encryption and Digital Signing</td>
<td>Messages in transit are better protected with current and strong cryptographic protections including TLS and Digital Signing to enable confidentiality and integrity of messages.</td>
</tr>
<tr>
<td>Payer</td>
<td>Ability to configure account settings for End Users to raise or lower requirements for certain activities, account types, etc.</td>
<td>Capacity to better customize or price products and services specific to certain markets or profiles.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Ability to endorse Pre-Authorization for future payments with variable or fixed amounts, accommodating multiple recurring consumer use cases (e.g.</td>
<td>Enables an expansive number of use cases and transactional styles, increasing opportunities for utilization, productization, and</td>
</tr>
<tr>
<td><strong>paying utilities or rent</strong> and business models (e.g. pay at pump, connect FPS to Uber)</td>
<td>ultimately driving down overall FPS costs.</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td><strong>End User establishes and manages all Payment Authorizations associated with FI Member via FI-controlled user interface.</strong></td>
<td>Centralizing management of FPS Authorizations ensures a consistent touchpoint between FIs and End Users.</td>
<td></td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td><strong>Authentification</strong> Centralizes Authentication at Member FI or RNAP via the Authentication Portal; Allows Member or RNAP to enforce additional Authentication requirements above Stakeholder requirements (e.g. Multi-Factor Authentication).</td>
<td></td>
</tr>
<tr>
<td>Authentication Portal presents potential marketing touchpoint for Members, RNAPs; Assures System integrity through standardized Authentication requirements;</td>
<td>Mitigates risk with information security exposures and associated costs;</td>
<td></td>
</tr>
<tr>
<td>Abstraction process replaces PANs and mitigates PII of End Users.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud Sharing Service securely distributes minimal information to help monitor FPS Account activity.</td>
<td>Provides session data and activity to Members to better monitor Accounts and make shared intelligence actionable.</td>
<td></td>
</tr>
<tr>
<td><strong>Approval by the Payer's / Payee's Provider</strong></td>
<td><strong>Approval by the Payer's / Payee's Provider</strong> Model ensures that transaction decisioning remains with the Member; Fraud Sharing Service provides enhanced data for fraud analysis on accounts and transactions.</td>
<td></td>
</tr>
<tr>
<td>Control remains with the financial institution; Reduce dollar losses due to fraud, as system-wide data could assist in identifying account takeovers. Reduce staff time spent on customer issues identifying fraud prior to occurrence. Provide a better customer experience by being able to identify potentially fraudulent receivers prior to authorizing a payment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Clearing</strong></td>
<td><strong>Clearing</strong> Two second Clearing of Credit Transfers, Requests, Returns, and Pre-authorizations; Does not send/receive bank account numbers; Standardized messages assure interoperability with sending/receiving</td>
<td></td>
</tr>
<tr>
<td>Confirmation of Good Funds.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Receipt</strong></td>
<td>Robust and real-time status updates, messaging, and protocols provide detailed updates and reconciliation data.</td>
<td>Reduces operational, administrative, and support processes at FI; Package core features and baseline requirements as Value-Added Services for Providers (e.g. monthly statements for End Users of Providers).</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Settlement</strong></td>
<td>Advanced ledger and rebalance system for interbank transfers and later settlement; Deferred Net Settlement with existing Fed systems. The Ledger’s Multilateral Netting and Deferred Net Settlement processes reduce complexity and number of settlement entries to the Central Bank.</td>
<td>Existing account structure and interoperability with Fed-supported rails lowers Initial Implementation costs for FPS; Reduction in processing costs.</td>
</tr>
<tr>
<td><strong>Reconciliation</strong></td>
<td>The Reconciliation propagates the neutralized data encapsulated by network, providing access only to information needed to complete a reconciliation process. Pull-based systems allow members to reconcile at any time and as often as required.</td>
<td>Reduces threats associated with the distribution of PII and PAN; Reduces the overhead of set and fixed processes.</td>
</tr>
</tbody>
</table>

Providers

Potential Operating and Maintenance Costs

API documentation for the FPS is openly available but FPS connectivity is brokered and enabled by Members of the Scheme. This access and other FPS-related products or services are priced and differentiated by the Access Provider, and will likely be heavily influenced by market forces.

Third-Party Services vs. Regulated Non-Bank Account Providers

The FPS API delivers the services, protocols, and experiences needed to access the baseline capabilities of the FPS. While API access may be attractive to many Entities and TPS that want a
light-touch, modern, and predictable interface to the FPS, more complex Providers (e.g. RNAPs) may need additional control, capabilities, and privileges within the Scheme.

These additional privileges may carry higher thresholds (e.g. costs, security, capitalization, licenses, etc.) to be met by RNAPs. These requirements are informed by the FPS Guidelines and Operating Rules and Scheme Requirements, and may include, but not be limited to: sponsorship by a Member, robust identity verification, risk mitigation processes, fraud sharing capabilities, and more.

<table>
<thead>
<tr>
<th>TPS</th>
<th>RNAP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Directory</strong></td>
<td>Indirect access, handled by Access Provider</td>
</tr>
<tr>
<td><strong>Funds ownership</strong></td>
<td>Holdings reflected by TPS are held at Access Provider’s Member or Sponsoring Member</td>
</tr>
<tr>
<td><strong>Broker Access to TPS</strong></td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

System Value Propositions and Economic Incentives

Programmatically accessible and agnostic to device, channel, and platform, a modern bank transfer system offers Providers unprecedented opportunities to bring faster, affordable, and secure payments to a wide range of customers, use cases, and devices. By designing for non-bank inclusion at the onset, the Solution brings FinTech—which itself brought innovation and competition by providing more, and often cheaper, alternatives for payments—into clearer and more definable regulatory scope. This boosts transparency, innovation, and security as well as creates a level playing field between different Providers.

**Example: Capturing the Unbanked**

According to the [FDIC’s Report on the Unbanked and Underbanked population](https://www2.fdic.gov/research Vaults/2013/2013-FDIC-Report-on-Unbanked-and-Underbanked-Households.pdf), thirty-three percent of the nation’s households were unbanked, under-represented, or invisible participants in the nation’s banking, representing one of the largest underserved markets in the country. With FPS in place, new products and services from Providers are better positioned to deliver

---

innovative and attractive features (e.g. real-time payroll or free P2P transfer to entice insured account eligibility).

<table>
<thead>
<tr>
<th>Stage</th>
<th>Value Proposition of Lifecycle</th>
<th>Economic Incentive for Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enrollment</strong></td>
<td>RNAPs: Enroll and represent FPS Accounts, set Payment Preference; TPS: eligible to initiate enrollment</td>
<td>RNAPs: Pricing based on enrollment number or degree of access to Third-Party services; Capture and enable FPS services for End Users invisible to traditional banking system.</td>
</tr>
<tr>
<td></td>
<td>Enrollment takes just seconds to complete and can be completed proactively at Member Provider or on first receipt of payment or request—facilitated through a standardized, secure and familiar communication (e.g. Access Provider).</td>
<td>Reduced friction and increased conversion to FPS increases value and viability to End User.</td>
</tr>
<tr>
<td></td>
<td>Allows unbanked to Register via Third-Party Service (via their FI Member) and RNAPs</td>
<td>Allows RNAPs and TPSs to create attractive products or services for un- or underbanked with business models that are more profitable or sustainable.</td>
</tr>
<tr>
<td></td>
<td>Ensures Confidentiality and Integrity of communications.</td>
<td>The Directory facilitates a lightweight Public Key Infrastructure allowing for signing of messages and enabling a required secure channel across Components.</td>
</tr>
<tr>
<td></td>
<td>Delivers and utilizes Unique Directory ID, not PANs</td>
<td>Security measures have both a direct and indirect economic incentive.</td>
</tr>
<tr>
<td><strong>Initiation</strong></td>
<td>Designed to enable and account for API access. To the extent available, an FPS API allows Providers to Initiate Credit Transfers, Requests, Returns, and Pre-authorizations.</td>
<td>Accommodates a wide range of Use Cases, Payment types, and latent demand, enabling near limitless revenue opportunities commensurate to the value-added service or experience provided.</td>
</tr>
<tr>
<td><strong>API</strong></td>
<td><strong>Better positioned to accommodate latent demand of new business models.</strong></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Allows basic services and payments to be integrated into any device, platform, or channel.</td>
<td>Ability to embed standardized metadata and authorizations for STP processing; increasing efficiency and automation.</td>
<td></td>
</tr>
<tr>
<td>Allows Providers to create specialized products, services, or experiences to amplify business value to customers, market or internal processes.</td>
<td>Payment preferences allow End User to automate payment routing to preferred destination.</td>
<td></td>
</tr>
<tr>
<td>Allows for pending payments to Non-Registered FPS End Users.</td>
<td>Available end-to-end status notifications for up-to-the-second transparency of End-User payments.</td>
<td></td>
</tr>
<tr>
<td>Capacity to append contextual data before and after Initiation.</td>
<td>Ability to automate most operations and administrative requirements associated with normal bank transfer processes.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ability to package and sell efficiencies to End Users or TSP (if RNAP).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Payer Authorization</strong></th>
<th>Enables an expansive number of use cases and transactional styles and types, increases opportunities for utilization, and ultimately drives down overall FPS costs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables tiered access and permissions to FPS Accounts</td>
<td>Enables an expansive number of use cases and transactional styles and types, increases opportunities for utilization, and ultimately drives down overall FPS costs.</td>
</tr>
<tr>
<td>Ability to request and receive Pre-Authorization for future payments with a range of Conditions (e.g. recurrence, date, frequency, etc.)</td>
<td>Enables an expansive number of use cases and transactional styles and types, increases opportunities for utilization, and ultimately drives down overall FPS costs.</td>
</tr>
<tr>
<td>Pre-Authorizations have Conditions (e.g. date, amount range, frequency) which allow for programmatic, self-fulfilling Pre-Authorizations with greater control and narrower scopes.</td>
<td>Enables an expansive number of use cases and transactional styles and types, increases opportunities for utilization, and ultimately drives down overall FPS costs.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>TPS: Authentication of Payment conducted at trusted FI Member or sponsored RNAP</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>RNAPs: Easy to accommodate multiple forms of Authentication (e.g. two-factor authentication)</td>
</tr>
<tr>
<td><strong>Approval by the Payer's / Payee's Provider</strong></td>
<td>Creates confidence in 24/7/365 availability and Good Funds to End Users.</td>
</tr>
<tr>
<td></td>
<td>Fraud Sharing Service ensures system wide identification of possible fraud and fraud trends. Veracity of payment information helps further reduce Fraud.</td>
</tr>
<tr>
<td><strong>Clearing</strong></td>
<td>Immediate availability of Good Funds 24/7/365 in two seconds or less</td>
</tr>
<tr>
<td><strong>Settlement</strong></td>
<td>Final, and irrevocable where eligible by law</td>
</tr>
<tr>
<td><strong>Reconciliation</strong></td>
<td>Standardization in messaging and protocols allow better automation of traditionally manual processes.</td>
</tr>
<tr>
<td></td>
<td>Reconciliation propagates the neutralized data encapsulated by network, providing access only to information needed to complete a reconciliation process.</td>
</tr>
</tbody>
</table>

**End User**

**Potential Operating and Maintenance Cost**

End Users access the core features and benefits of the FPS through Providers’ products, services, instruments, etc. The extent to which an End User must pay depends on a variety of
circumstances but the market’s threshold and tolerance for such charges, use case of the payment, or the perceived monetary value experienced are likely to play significant roles.\textsuperscript{20}

System Value Propositions and Economic Incentives

As market drivers and consumers of the FPS, End Users benefit most from the advancements offered by an improved payment system. From reduced circulation of PII to the simplicity and ease of Enrollment, the baseline features of the FPS offer a secure, cost-effective payment system. These benefits are amplified by API access to Providers, offering End Users a diverse and competitive landscape of Value-Added Services.

Example: Selling convenience

A small publisher pays 100 freelance writers twice a month. Individually sending FPS payments is possible, but not efficient. The publisher pays a small fee for a Third-Party Service that allows its accounts payable office to submit hundreds of payments through a single endpoint in real-time.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Value Proposition of Lifecycle</th>
<th>Incentives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrollment</td>
<td>Enrollment takes just seconds to complete and can be completed proactively at trusted Provider or on first receipt of payment or request—facilitated through a standardized, secure and familiar communication that is platform, device, and channel agnostic.</td>
<td>Claiming and fulfilling funds requests carry their own social and economic incentives to an End User. Enrolling at the &quot;point of need&quot; with a range of potential provider, is a convenient and powerful call-to-action that unlocks the respective benefits of a FPS to an End User and accelerates ubiquity.</td>
</tr>
<tr>
<td></td>
<td>Allows multiple Accounts at multiple Members and RNAPs to be associated with a single Email or SMS; Ability to set and manage FPS Payment Preferences in real-time.</td>
<td>Availability of Value-Added Services and &quot;top of wallet&quot; hierarchy fosters competition and incentives for End Users by Providers.</td>
</tr>
<tr>
<td></td>
<td>Use email and SMS to send, receive, and request money</td>
<td>Reduction of direct and indirect costs associated with the circulation of today's payment credentials and instruments.</td>
</tr>
<tr>
<td></td>
<td>Allows un- or underbanked to Enroll with RNAPs or Members.</td>
<td>Benefit from user experiences, costs, or specialization needed to</td>
</tr>
</tbody>
</table>

\textsuperscript{20} Proposers strongly recommend to the FPS Regulatory and Scheme Members that Customers of FPS not be assessed fees for receiving payments and that costs associated with sending payments either be subsidized by other revenue opportunities or capped to a national limit.
<table>
<thead>
<tr>
<th><strong>Initiation</strong></th>
<th>Ability to send or request Credit Transfers, or grant Pre-authorizations for future payments with variable or fixed amounts.</th>
<th>Flexibility enables greater control, automation, and choice of payment.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Allows pending payments to unenrolled FPS End Users.</td>
<td>Mitigates anxiety associated with enrolling with new payment forms or systems.</td>
</tr>
<tr>
<td></td>
<td>Ability to embed standardized Contextual Data and authorizations for STP processing, increasing efficiency and automation</td>
<td>Improved efficiencies in information capabilities may provide $10-$40 billion in backend efficiencies(^21).</td>
</tr>
<tr>
<td>Platform enables FPS basic Services and Payments to be integrated into any device, platform, or channel. Allows Providers to create specialized products, services, or experiences to amplify business value to customers, markets, or internal processes. Payment Preferences allow End User to automate payment routing to preferred destination.</td>
<td>Allows Providers to sell specialized products, services, or experiences to amplify business value to customers, markets, or internal processes. Availability of services on instrument of choice minimizes direct and indirect costs associated with other payment types (e.g. walk time to cash a check, ATM fees, and more).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Easy to remember Destination IDs replace hard to remember routing and account numbers</td>
<td>Increase adoption and participation. Send and receive money with email or phone, reduce exposure and threats of PII.</td>
</tr>
<tr>
<td><strong>Payer Authorization</strong></td>
<td>Transparent End-User Authorization and Authorization Requests</td>
<td>Empowers End Users to make informed decisions on their payment relationships.</td>
</tr>
<tr>
<td></td>
<td>Ability to grant Pre-Authorization for future payments with variable or fixed amounts.</td>
<td>Flexibility enables greater utilization, control, automation, and choice of payment.</td>
</tr>
<tr>
<td></td>
<td>Authorization is easily revocable via Provider and/or Member or RNAP.</td>
<td>Empowers consumers with control over authorizations.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Authentication conducted at trusted FI Member or sponsored RNAP.</td>
<td>Improves confidence and visibility of trusted brand.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Easy to accommodate multiple forms of Authentication (e.g. two-factor authentication).</th>
<th>Deters fraud and account takeover.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval by the Payer's/Payee's Provider</td>
<td>Creates confidence in 24/7/365 availability. Available Fraud Sharing Service protects customers with access to real-time information across multiple Participants.</td>
<td>Fosters financial certainty and clarity. Empowers End Users to make financial decisions with more intelligence and confidence.</td>
</tr>
<tr>
<td>Receipt</td>
<td>Platform Webhooks enable Providers to supply robust status updates to End Users via any device, channel, or platform in real-time. Contextual data enables straight-through processing.</td>
<td>Real-time updates and balance status provides accurate overview of financial status; $10-$40 billion in potential efficiencies.</td>
</tr>
<tr>
<td>Settlement</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Reconciliation</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

22 Id.
Integration Effort

For each use case supported by the solution, describe the points of integration required for each stakeholder in the solution (End Users, technology providers, processors, the proposer(s) of the solution) for each of the eight stages of the payment lifecycle (as discussed in Part A). Proposers should include flow diagrams of the points of integration and the business relationships between the various stakeholders. For each stakeholder, identify the effort required on a relative order of magnitude basis (e.g., either temporally – days, weeks or years – and/or as compared to other common integration experiences in the payments industry such as, connecting to a new EFT service or supporting a new ACH file type). Discuss any explicit on-going efforts to maintain integration to the system.

Integration points must consider the payer’s depository institution or non-bank account provider (for origination and receipt on behalf of End Users), third-party service providers, merchants (e.g., PoS and eCommerce), billers, consumers, businesses, etc.

In completing this description, proposers should focus on the following Effectiveness Criteria as they relate to payment volume assumptions: U.1 (Accessibility); U.3 (Predictability); E.1 (Enables competition); E.2 (Capability to enable Value-Added Services); E.6 (Scalability and adaptability).

To the extent that Members manage and monetize access to the FPS, the proposed Scheme provides a fairly FI-centric System that streamlines and incentivizes Integration efforts for participants.

As with any integration, the size and scope of the effort will vary depending on the technological and experiential strengths of the Participant. The proposed Solution, which offers a mix of cloud-based technologies, points of interoperability with existing systems, and risk mitigating benefits, provides a secure and cost-effective approach to an FPS.
General Assumptions

**Compliance:** Requirements for participation in the FPS is governed by the FPS Regulator and outlined in the FPS Operating Rules and Guidelines. Any requirements not outlined by the FPS Regulator or existing legal requirements are drafted and enforced by the Scheme Requirements and, finally, its Members.

**Baseline security:** The integration points will meet or exceed a minimum level of security operation and configuration such that attack surfaces are minimal, current and approved versions of software are leveraged, and communication across points will require encryption and mutual authentication of data in transit.

**Technical expertise:** Each Member and Provider has technical expertise and experience with API integrations. While the ease of the integration allows for all levels of experience, the effort and timelines assume a moderate level of understanding. To assist in the sizing of this effort, the Proposers of this solution have outlined the capabilities needed by a Member to interact with the Operator.

**Organizational process:** The integration effort assumes the phases of the development lifecycle and only assumes a minimum amount of organizational process included in various areas such as Change Management.

**Core services:** A Member’s core services are already extendable to an API-based integration. If a Member’s core is not accessible, additional effort will be required from the Member or FI Services Provider.

**Integration Timeline:** There are several dependencies in developing a comprehensive integration effort for the proposed Solution. While the integration with the Operator effort can be based on our current implementations, integration with the Directory and Fraud Sharing Service is dependent on how the Scheme Owners.

Security between System Components

*See Part A, Section 1: Authentication - “Member to FPS Components Authentication”.*
Integration effort and requirements: Directory

The effort to integrate with the Directory varies depending on the sophistication of an FI’s core and/or online banking technology. To assist in the sizing of this effort, the Proposers of this solution have outlined the capabilities needed by a Member to interact with the Directory.

Admission to the Directory

The Member needs to create a Member at the Directory by following the steps outlined in the “Security between System Components” section. Additionally, the Member supplies the following information to the Directory:

- **Authentication Portal URL** - allows Members, Providers, and Third-Parties to redirect End Users to an established URL for authentication, transaction fulfillment, and Pre-Authorization
- **Routing Number**
- **Name of Member or RNAP, and/or name variations** - allows End-users find and select their FPS Account

Adding a new End User to the Directory

When an End User registers through a Member, the Member must send the End User information to the Directory via an API endpoint.

The Member POSTs the user’s information to the Directory API endpoint and may include:

- **Name**
- Type
- Email
- Phone
- Operator ID
- Routing Number
- Payment Preference

The Directory returns the following:

- UDID

**Designating a Preferred account in the Directory**

The Member has the ability to indicate a preferred routing number for the End User in the Directory. The Member POSTs the following information:

- UDID
- Payment Preference - TRUE

The Directory returns the following:

- UDID

The POST to the API endpoint is signed and encrypted using the key and secret provided by the Directory during setup.

**Retrieve End User**

The Members retrieve End-User information from the Directory using an API endpoint provided by the Directory. The Member makes a GET request to the Directory API endpoint specifying a UDID. The Directory returns End-User information for the specific UDID.

**Retrieve Member and RNAP List**

The Member has the ability to retrieve a full list of participating Members and RNAPs. The Member makes a GET request to the Directory API endpoint and the following is returned:

- Name of Member or RNAP
- Authentication Portal URL

The Member is then responsible for the display of the options and redirecting the End User.

---

23 The Directory determines if a UDID already exists or if a new user needs to be created by matching on email address and possibly other information. If there is already an existing UDID, the value is returned to the Member from the API endpoint. If the user does not exist in the Directory, a new record is created and a new UDID identifying the user is returned.
On-going maintenance considerations: Directory

The Member is responsible for updating the following information in a timely manner, as informed on FPS Operating Rules and Guidelines or Scheme Requirements.

- End-user payment preferences
- Authentication Portal URL
- Cryptographic key management (storage, rotation and monitoring)
- Certificate management

Non-technical efforts or business relationships: Directory

As custodian of the Directory, the FPS Regulator is charged with determining the requirements, standards, qualifications, and pricing model of the Component; however, these aspects are likely to be informed by the following:

**Industry Coalition**

Temporary workgroups help influence or determine messaging formats, End-User experiences, scope of work, access requirements, technical structure, and more.

**Advisory council**

This semi-permanent body represents industry and consults the FPS Regulator in the governance of the Directory.

**Member to Operator**
Integration effort and requirements: Operator

*The effort to integrate with the Operator varies depending on the sophistication of an FI’s core and/or online banking technology. To assist in the sizing of this effort, the Proposers of this solution have outlined the capabilities needed by a Member to interact with the Operator.*

**Admission with the Operator**

The Member needs to create a Member at the Operator by following the steps outlined in the “Security between System Components” in this section. Additionally, the Operator needs to collect the routing and account number of the Operational Account to be used for Settlement.

**Payer transfer approved**

The Payer’s Member sends a Payment Message to the operator through an API endpoint provided by the Operator. The Member POSTs the Payment Message to the Operator, formatted as an ISO-20022 message.

The Operator returns the Transfer ID and Status Code.

**Payee transfer received**

The Operator notifies the Payee’s Member of an incoming payment through a Webhook endpoint hosted by the Payee’s Member. The Operator POSTs the Transfer ID to the Payee’s Member, which the Member uses to retrieve the Payment Message in “Retrieve a Payment Message.”

**Payee transfer approved**

The Payee’s Member notifies the Operator that the Payee has approved the payment through an API endpoint provided by the Operator. The Payee’s Member POSTs the Transfer ID and any related data to the Operator API endpoint.

**Payer transaction complete**

The Operator notifies the Payer's Member that the payment was completed through a Webhook endpoint hosted by the Payer's Member. The Operator POSTs the Transfer ID to the Payer's Member through the Webhook endpoint.

**Retrieve a Payment Message**

Payer’s and Payee’s Member receiving Webhook notifications leverage an identifier to retrieve the Payment Message information. Members make a GET request to the Operator API endpoint specifying a Transfer ID. The Operator sends the full Payment Message.

**Payer Pre-auth complete**
When a Payer has granted a Pre-Authorization, their Member relays the Pre-Authorization Payment Order through the Operator to the Payee’s Member. The Payer’s Member POSTs the Pre-Authorization information (Auth ID) and subsequently a Webhook is sent to the Payee’s Member of the completion.

Retrieve reconciliation information

The Members retrieve reconciliation information from the Operator using an API endpoint provided by the Operator. The Member makes a GET request to the Operator API endpoint specifying a Start and End Date. The Operator returns a list of payments that were initiated by the Payer’s Member in the specified date range.

On-going maintenance considerations: Operator

As demonstrated in other nations with advanced digital national payment systems\textsuperscript{24}, the maintenance costs associated with supporting the Operator component are relatively low compared to the same costs of legacy systems. This is due in part to the high-level of automation and standardization of the System. However, on-going maintenance is critical for the Scheme Owners. This may include, but not be limited to:

- Component software updates/bug fixes
- Data storage optimization
- Log file collection, review, retention and storage
- Cryptographic key management (storage, rotation and monitoring)

Non-technical efforts or business relationships: Operator

**Scheme formation, admission**

As discussed throughout the Proposal, Schemes are owned and operated by its Members. The process for forming such an arrangement was detailed in the “Implementation Timeline” section but requirements and processes for joining a Scheme are relegated to the Scheme Owners.

The negotiation, qualification, and review processes for formation and admission may include, but not be limited to:

- Cost of membership
- Maintenance costs
- Capital requirements
- Operational capabilities

**Operational considerations**

Examples may include:

*Maintain an Operational Account*

Each Member FI is required to maintain an Operational Account for settlement. The Operational Account enables interbank settlement of funds between FIs. Each of these accounts are maintained for the purpose of leveraging the FPS to send and receive payments for the benefit of End Users. Routing and account number information is provided to the Operator at the time of the FI registration.

The effort required is equivalent to the creation of any commercial DDA account.

*Member Settlement*

A deferred net settlement occurs between the Operator and Providers. Since the settlement is a facilitation of debits and credits across Operational Accounts, no additional technical integration is necessary. A Provider may implement additional technological solutions to monitor the settlement activities, but this will occur within the organization's own internal practices.

Effort required on a relative order of magnitude basis: Operator

The framework for the proposed Solution is in place. One previous integration for the existing FiSync solution with a leading U.S. bank took between four to six months, but similar connections can potentially be completed in as little as three months with a team of six developers.
Member to Fraud Sharing Service

Integration effort and requirements: Fraud Sharing Service

**Admission with the Fraud Sharing Service**

The final integration point is gaining access to the Fraud Sharing Service. The Member creates a Member at the Fraud Sharing Service by following the steps outlined in the “Part B, Section 3: Security between System Components” section.

**Add an End User to the Fraud Sharing Service**

The Member adds End-User information from the Fraud Sharing Service via a POST to the Fraud Sharing Service API endpoint and may include:

- **UDID**
- **Relationship Open Date**
- **ZIP Code**
- **Industry Classification (business only)**

**Retrieving an End User from the Fraud Sharing Service**

Member is able to request information from the Fraud Sharing Service about a UDID using an API endpoint provided by the service. Member makes a GET request to the Fraud Sharing Service API endpoint specifying a UDID. For example, a Payee’s Member can make a request to the API endpoint to gather information about the Payer UDID, then make a second request to the endpoint to get information about the Payee UDID. The Payee’s Member can then use that
information to make a determination about the riskiness of the transaction and provide information about the risk to the Payee.

**Sending transaction information to the Fraud Sharing Service**

The Payer’s Member sends transaction information to the Fraud Sharing Service upon completion of the payment by POSTing the transaction information to an API endpoint provided by the Fraud Sharing Service.

**Connecting Fraud Sharing Service to existing Fraud Systems**

Fraud Sharing Service formats are standardized by the FPS Regulator to better support inter-Operator knowledge exchange, which makes connections with existing fraud systems straightforward.

**On-going maintenance considerations: Fraud Sharing Service**

As the Scheme Company monitors the performance of the Fraud Sharing Service, both internally and via feedback from Scheme Owners, additional messaging will be created to address new fraud trends as they arise. This requires a smaller effort to integrate this new messaging, both from a technical and non-technical standpoint.

**Non-technical efforts or business relationships: Fraud Sharing Service**

Once the fraud messaging data is consumed by existing fraud systems, analysis is needed over time as actual fraud is observed and compared against the messaging received in those cases. This will require additional procedural documentation and staff training to understand the underlying meaning of the messages received.

In the likely event that enforcement agencies will want to access Fraud Sharing Service data, proper procedures will need to be in place to accommodate such requests.

**Relationships**

Market forces would give existing fraud service and software providers incentive to implement Fraud Sharing Service messaging in their existing solutions, which may decrease integration effort and analysis time at individual institutions.

As a Component of the Scheme, the existence and maintenance of the Fraud Sharing Service is funded by its Members.

Additional business relationships at the Member may be solicited to improve an individual Member’s risk analysis or actionability of data provided by the Fraud Sharing Service.
Member to Platform Service Layer

**Proposers Note:** While the opportunity to broker access to Providers or build FI products on top of FPS core capabilities and services is a powerful incentive, the degree to which they want to facilitate access or offer capabilities is ultimately up to the Member.

Integration effort and requirements: Platform Service

To facilitate responsible and secure access to Providers, portions of an FPS API may be informed by Payment System Rules (e.g. ability to create and/or programmatically enforce via endpoints or other attributes). This allows for market differentiation of FPS services at the Member, while ensuring predictable End-User experiences, security requirements, and baseline compliance requirements are met by a Provider.

Additional Processing Services:

The extent to which a Member or RNAP wants to be an Access Provider relies on the range of core capabilities they wish to make available to other Providers, as well as the additional services they may need to provide relative to those capabilities. For example, a Member that wants to enable End Users of a Provider to pay another Entity may need to acquire a Bank Account Verification product in order to satisfy an FPS Requirement around KYC. Other examples of potential Value-Added Services include, but not be limited to:

- Sandbox environment
- Email or SMS vendor services
- KYC, OFAC, BSA Services
- Fraud and risk mitigation services
- Support (e.g. compliance, customer, or development)

The monetization approach of services is relegated to the Access Provider.

On-going maintenance considerations: Platform Services Layer

- Quality assurance
- Deprecating APIs, endpoints
- Change orders or controls issued by System Requirements or FI Services

Provider to Member
Integration effort and requirements: Provider

The Integration effort of a Provider varies depending on the endpoints or services required by the Provider’s business need and offered by the Access Provider (e.g. a Sandbox Environment may accelerate integration). Because we expect regulatory scopes similar to ACH to be placed on Providers, the following section outlines a slightly adapted approach to current service and access brokered by Dwolla to Providers.

Non-technical efforts or business relationships: Provider

Members and RNAPs (i.e. Access Providers) broker FPS access and services to Providers. The threshold beyond which certain services are formally required (e.g. identity verification) depends on numerous factors (e.g. type of business integration, FPS API endpoints, risk). The degree to which a Provider purchases these from an Access Provider is considered a business decision.

For example, the customer verification threshold for receiving payments may be lower than the threshold for sending payments. A Provider whose platform is used to pay freelancers may need a less formal arrangement with their Access Provider, even benefiting from an “off-the-shelf” contract or package of services. On the other hand, an RNAP that wants to represent customer accounts in the FPS, broker access to other Providers, and allow End Users to send/receive funds will likely have a more formal process of brokering, qualifying, and reviewing with an Access Provider. These may include, but not be limited to:

- Legal eligibility
- Regulatory and System compliance
- Financial practices (e.g. reconciliation, liquidity management)
- End-User communication touchpoints and standardization
- Dispute processes
- Fraud and risk mitigations

Effort required on a relative order of magnitude: Provider

Thanks to the encapsulation and standardization of core capabilities and services with in the FPS API, Providers in the proposed FPS have an unprecedented level of ease, security, and access to the nation’s bank transfer system. FPS operations at a Provider could take just a few days, from first contact to production.
Scalability and Adaptability\textsuperscript{25}

The following sub-section explores the Solution's attributes that enable a scalable and adaptable FPS. The distributed network helps enable Members to interact separately with the Directory, Operator, Fraud Sharing Service, and other Operators. The API design allows the Directory to connect users and the Fraud Sharing Service to monitor fraud while the Operator focuses on the streamlined exchange of payment information.

Leveraging a McKinsey study\textsuperscript{26}, five use cases may benefit from a faster payment solution. The group represents 12\% of the total payments market, outlined as follows:

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Transactions (in billions)</th>
<th>Value (in trillions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2B ad hoc low value</td>
<td>11.1</td>
<td>$30.50</td>
</tr>
<tr>
<td>B2P ad hoc high value</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>P2P transfers</td>
<td>4.3</td>
<td>$1.00</td>
</tr>
<tr>
<td>B2P ad hoc low value</td>
<td>3.2</td>
<td>$2.80</td>
</tr>
<tr>
<td>P2B ad hoc, remote</td>
<td>10.3</td>
<td>$0.50</td>
</tr>
<tr>
<td>TOTAL</td>
<td>28.9</td>
<td>$34.80</td>
</tr>
</tbody>
</table>

The adoption of real-time payments and conversion can be assumed to mimic adoption in the United Kingdom over the first several years of their FPS\textsuperscript{27}:

\textsuperscript{25} The Proposers have only provided high-level details about the scalability of its current Solution as they consider such information to be proprietary.

\textsuperscript{26} FPFS Faster Payment Roundtable - https://fedpaymentsimprovement.org/wp-content/uploads/faster_payments_roundtable.pdf

\textsuperscript{27} https://www.bostonfed.org/economic/current-policy-perspectives/2014/cpp1405.pdf
Incorporating a scalable infrastructure is essential to support growth of approximately 1.5 billion transactions in a six year period. While traditional infrastructure options (i.e. physical servers) may be able to accommodate this growth, the cost to maintain, scale, and secure would not be economical through this adoption period and in the long-term.

A solution adopting cloud computing services (e.g. Amazon Web Services) provides the proven flexibility, compliance, and technology needed to support the increasing demand and to scale horizontally. Cloud computing services are a proven solution to deliver a secure, reliable, scalable, and economical solution for the expansive adoption of a Faster Payments Solution. The flexibility of cloud computing not only equips the Solution well for the progressive growth over a six year period, but also maneuvers peak-time variations via auto-scaling options. Being able scale up easily during peak times such as the 1st month for tenants ensures a reliable, performant experience for End Users.

In addition, the stewardship-based model provides a great foundation for technical adaptability. With only identifiers exchanged (e.g. UDIDs, Transfer IDs, Auth IDs, etc) across the various subsystems, each can be upgraded with minimal impact to other entities.
**Part C: Self-Assessment Against Effectiveness Criteria**

This section should be used by proposers to assess how the solution meets each of the criteria outlined in the Effectiveness Criteria (considering all use cases supported by the solution). Proposers should include in their self-assessment any functionality that will be in place at the date of implementation or for which there is a credible plan to implement the enhancement at a future date (as described in Part B, sub-section 1 “Implementation Timeline”). For example, the Effectiveness Criteria specifically acknowledges that proposers may not have cross-border functionality at implementation but may have a credible plan to implement it at a later date.

Proposers should use the tables below to indicate their self-assessed rating on the Effectiveness Scale outlined for each criterion, as well as a detailed discussion of why the rating is justified and how the solution meets each criterion (e.g., U.1, U.2, etc.), including each consideration (e.g., U.1.1, U.1.2, etc.). Proposers may use the far-right column (“Proposal Page Number”) in the tables to cross-reference the section/page number for the relevant description provided in Part A or Part B, above.

Proposers should note that a number of the criteria have been written in a way that provides flexibility for a range of different approaches to address the criteria or for the solution to determine how certain terms and parameters are defined. Proposers should ensure their justification of how the solution meets each criterion includes a clear explanation of the approach taken in the solution, and how solution-determined terms and parameters are defined. For example, S.2.3 (Payer authorization criterion) requires the solution to enable the **payer** to revoke any Pre-Authorization of payments easily and timely. The proposer’s justification for S.2 should include how the revocation is “easy” for the payer and the time it takes (i.e., number of minutes, hours, or days) for the revocation to take effect. Similarly, E.6.2 (Scalability and adaptability criterion) requires the solution to demonstrate the capacity to handle projected volumes and values (determined by the solution), including heightened transaction volumes and values during peak times or periods of stress. The proposer’s justification for E.6 should include its assumptions for determining the heightened volumes and values and how they relate to normal periods (e.g., heightened volumes are equal to twice the projected volumes during normal periods).

Proposers should refer to the Effectiveness Criteria for an explanation of what Very Effective, Effective, Somewhat Effective and Not Effective mean for each criterion.
## Ubiquity

Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: accessibility, usability, predictability, contextual data capability, cross-border functionality, and applicability to multiple use cases.

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria Name</td>
<td>#</td>
<td>Consideration Name</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.1</td>
<td>Accessibility</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.2</td>
<td>Usability</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.3</td>
<td>Predictability</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.4</td>
<td>Contextual data capability</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.5</td>
<td>Cross-border functionality</td>
</tr>
<tr>
<td>Ubiquity</td>
<td>U.6</td>
<td>Applicability to multiple use cases</td>
</tr>
</tbody>
</table>

### Justification for U.1

#### U.1.1

At launch, the Solution’s Platform Services Layer will be able to send, request, return, and pre-authorize payments to, from, and between End Users via FIs, RNAPs, or TPSs (i.e. “all types of payment Accounts based in the United States (U.S.)”).

#### U.1.2

As demonstrated in technical and End-User workflows of section “Part A, Section 1: “ Initiation”, the Proposed Solution accommodates the delivery of payment to any eligible Payee. Below are a few important characteristics of the network that make this possible.

### Directory
Allows End Users to authenticate and authorize payments and applications at a preferred Financial Institution or Regulated Non-bank Account Provider, regardless of the Operator of the participating FI or RNAP.

Learn more about the Directory in Part A, Section 1: Initiation - “Directory and Enrollment”

Capacity for Overlay Services

Absent a mandate for FI participation in the FPS, the access and services provided and encapsulated by the Platform Services Layer allow Providers to facilitate a wide range of transactions, communications, and predictable experiences to an End User.

Inclusion of Regulated Non-Bank Account Providers (RNAPs)

Better positioned to create sustainable, attractive, and cost-effective services for the Unbanked or underserved, the role and capabilities of RNAPs support the distribution, adoption, and utilization among the underserved banking populations in the U.S.

These capabilities include:

- The capacity to send, request, and facilitate Payment Orders between customers
- Representation of FPS-enabled Accounts (with FI Member) on behalf of the End User
- Enrollment of End Users into the FPS

Inclusion of FIs

Although the Solution is designed to maintain and bolster FIs’ position as custodians of the bank transfer system, 100% participation at launch is unlikely. The access to FPS via RNAPs will create a compelling call to action for non-FI Members to join a Scheme or become an RNAP of FPS capabilities and services.

Destination IDs

While multiple Destination IDs could be incorporated at some point (e.g. Facebook Profile, website URL, etc.), the initial scope of the FPS proposes the ability to use Email addresses and SMS phone numbers as the primary identifiers for the Directory. Aside from successful international adoption of Email and SMS as payment identifiers, messaging channels, and on-boarding mechanisms, the logic of this choice was additionally bolstered based on the following:

Email: In 2016, there will be an estimated 232.5 million email users in the United States. Email is free and readily considered a dynamic, secure, and efficient form of communication with a $.00 marginal cost to operate.

SMS: According to Pew Research Group, 91% of adult Americans had a cell phone in 2013. A similar study by the group two years later showed that of all the features
available on smartphone, **texting was the most likely to be used (97%)**. SMS text messaging, while not as dynamic as email as a communication channel, benefits from a reduction in the personal hardware required (e.g. smartphone vs. legacy phone), friction, and simplicity.

*Experience:* Dwolla and other modern payment providers have had proven success in using email addresses and SMS-enabled phone numbers.

**U.1.3**

The Solution is dependent on two items to facilitate multi-currency payments:

- Ability of Provider or Member to approve and accept various currencies
- A settlement option to Rebalance other currencies

If Providers and Members have the ability to support different currencies, the Operator can facilitate via an optional “Currency Type” parameter included the Payment Message. The Solution continues to explore Multi-Currency options for inter-bank settlement processing.

**U.1.4**

**Addressing the Unbanked**

As discussed in U.1.2, the ability to create products and services tailored to this specific market segment is widely appreciated as a benefit to the overall economy [28].

**Addressing the Disconnected**

Not everyone in the United States has access to SMS or email. For these groups, we expect to see innovations and services created by RNAPs and TPSs to help enable sustainable and cost effective offline access to these End Users. A few examples include, but are not limited to:

- Printable vouchers for redemption at Authorized Providers, Members
- Reusable and reloadable prepaid cards that cannot expire or be overdrawn against

**U.1.5**

To recap Part B, where this information is provided in better detail, the Solution accounts for:

- **Immediate availability of baseline capabilities and services:** Able to initiate and facilitate Credit Transfers, Requests, Returns, and Pre-Authorizations to Members and Providers within three years of FPS Operating Rules and Guideline creation. The Directory

---

connects all participating Members and RNAPs, regardless of Operator, to enable authentication and authorization of a payment or application by an End-user.

- **Scheme formation and admission:** Member FIs receive greater control, specialization, and preference over the structure, pricing, and system requirements of a Scheme than Non-Member FIs.

- **API Access to Providers:** Access creates competition for Value-Added Services, innovation for Consumers, and lower costs for Schemes which benefit from adoption and utilization of the network.

- **System improvements as an incentive:** Numerous system improvements, like payment decisioning, Fraud Sharing Service, and transparency, provide qualitative and quantitative benefits for Participants.

- **Low-maintenance costs:** As demonstrated by the UK FPS’ ongoing operational costs,
  a highly automated system provides a technical and scalable approach to managing and reducing overhead.

- **Interoperability with existing systems:** Secure API approach to connecting System Components and Participants, along with interfacing with existing settlement systems, reduces upfront costs and integration efforts.

### Governance and Standardization

The FPS Regulator provides FPS Operating Rules and Guidelines and necessary standardizations that run horizontally (stretching across Operators) and vertically (through Schemes) to ensure Interoperability, End User predictability, and system liquidity. These may include, but not be

---

limited to: Payment Messages, communication protocols, security obligations, and Settlement requirements and arrangements.

**Points of interoperability**

Operators interface with each other through a standardized Payment Messaging format and an Operator Number provided during the Payee or Payer lookup at the Directory. Message and protocol standards also help govern the interactions between Fraud Sharing Services and the Directory.

**Multi-operator settlement**

In a multi-Operator environment, the participating Operators have agreed-upon Settlement procedures (e.g. the Payer's Operator always settles since there is an outstanding liability to the Payee's Operator) and standardized messages (e.g. ISO 20022). The necessary interactions are identified, governed, and enforced by the FPS Regulator.

**Economic Incentives**

Today’s real-time information technology and cloud-based systems significantly reduce or streamline the costs and inefficiencies associated with clearing and settling payments. A strong FPS, with thorough standardization and interoperability, could reasonably pave the way for multiple Operators and for-profit Schemes that wish to specialize or enable services specific to their Members’ business needs. A multi-Operator system may be better positioned to ensure competition and innovation at the very bottom of the payments stack than a Financial Market Utility.

**Justification for U.2**

**U.2.1**

As demonstrated by the Proposer’s own existing APIs and Software Development Kits (SDKs), the Platform Services Layer (i.e. “Application Layer”) allows Providers to programmatically enable or build core FPS capabilities and experiences into any internet-connected device, channel, and platform.

Additional governance rules and risk decisions at participating Members and RNAPs may inform Usability/instrument parameters.

**U.2.2**

The Solution securely abstracts the traditional PII associated with bank transfers, replacing it with a UDID and allowing End Users to initiate Credit Transfers and Requests with only an
email address or SMS-enabled phone number. The approach accounts for enrollment of End User on first engagement (e.g. a friend sending a payment to an unregistered email or a business requesting rent payment). This capacity for reactive Enrollment provides End Users convenience and an incentive to register and participate with the FPS.

See Part A, Section 1: Initiation - “Enrolling a New Payee at First Receipt of Credit Transfer or Request”.

U.2.3

The Operator provides FPS availability of Good Funds 24/7/365. Operator will push real-time transaction state updates (e.g. “Transaction Complete”) to the Member through Webhooks. This structure enables the Member or Provider to send timely notifications to the End User.

U.2.4

Combined with the FPS access and services made possible by the Platform Services Layer, Providers are capable of facilitating special considerations and interfaces for disabled users, the elderly, and individuals with limited English proficiency as deemed necessary by the collective requirements of the System and its stakeholders.

Justification for U.3:

U.3.1

The core features and services of an FPS are successfully delivered to Participants and End Users.

<table>
<thead>
<tr>
<th>Baseline of Core End-User Features</th>
<th>TPS</th>
<th>RNAPs</th>
<th>Member (as a Provider)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eligible instruments or interfaces</td>
<td>Any internet-connected platform, device, or channel; off-line methods possible&lt;sup&gt;30&lt;/sup&gt;</td>
<td>Any internet-connected platform, device, or channel; off-line methods possible</td>
<td>Any internet-connected platform, device, or channel; off-line methods possible</td>
</tr>
<tr>
<td>Enrollment</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<sup>30</sup> Offline transactions may be facilitated through Store Value providers (e.g. paper vouchers that Initiate payment upon Internet-enabled activation)
The proposed FPS Solution provides the technical capabilities (e.g. programatically-enforced access scopes) and existing legal framework for stakeholders to inform, enforce, and/or require numerous End-User experiences. It is the assumption of Proposer that FPS Regulator will inform and enforce the necessary Operating Rules and Guidelines needed to govern and sustain the proposed system and Public Policy Objectives, including its baseline features.

However, the proposers offer the following comments as suggestions to the FPS Regulator and Scheme Owners regarding Usability:

**Timing**

Notification at Initiation, irrevocability, and confirmation should be promptly communicated to the End User via their preferred Destination ID associated with their Provider.

**Acknowledgement of Costs**

Individual or packaged costs associated with FPS baseline of core features should be clearly documented and outlined for all Participants at a consistent point in the payment flow (e.g. Payment Authorization for single or recurring transactions).

**Costs of Core Capabilities and Services**
To encourage adoption and ultimately reduce FPS costs, Proposer strongly recommends that Members and Providers keep pricing:

- as low as possible to increase distribution, incentivize Value-Added Services, and broaden utilization, thereby decreasing the overall costs of the FPS Solution.
- attractive and consistent across End-User type and use case (e.g. free P2P payments or zero cost for receiving payments as an individual).
- low to provide margins that incentivize the creation of Value-Added Services; thus, helping drive competition and innovation.

**Participant and Provider Authentication**

Baseline requirements regarding Participant Authentication, which is done at the End User’s Member FI or RNAP, should be strong and encourage multiple factors of Authentication. Preference for level of Payment Authentication should be determined by the End User’s Member FI or RNAP.

**Pre-authorizations**

Standing Pre-Authorization, or the ability to interact with a Participant's account on an ongoing basis, should be easily revoked by the Participant at the Provider or their Member FI via a simple user interface (e.g. in Settings).

**U.3.3**

The FPS Operating Rules and Guidelines, as well as other standardized transaction data deemed necessary by the FPS Regulator, will ensure continuity in experience for End Users as they participate within the FPS.

**U.3.4**

The baseline features experienced by an End User (e.g. Enrollment, Initiation, Authorization, Authentication, Receipt, and Reconciliation) follow standardized messages, protocols, user flows, branding guidelines, and are delivered via the End User’s preferred Destination ID.

**U.3.5**

The suggested Error Resolution process follows processes familiar to existing FIs and customers within the U.S. and has been shown to work via real-world examples such as the UK's Faster Payments Initiative.\(^{31}\)

---

\(^{31}\) UK Faster Payments. “What happens if I have sent the wrong payment?”
http://www.fasterpayments.org.uk/consumers/what-happens-if-i-have-sent-payment-wrong-place
See E.7.1 for more detail about the Error Resolution process.

U.3.6

A unified term for Providers and End Users will undoubtedly assist in adoption, utilization, and reach, especially as branded applications and platforms interface and represent the FPS to End Users. Such decisions, however, are a powerful tool for fostering inclusion among key stakeholders. Rather than exclude these Participants from the process, the Proposers suggests that the FPS Regulator establish a special working group tasked with researching and identifying a brand strategy for naming the System.

The Proposers also submit the following suggestions:

- ACE - Advanced Clearing Exchange
- DATA: Digital Asset Transfer Architecture
- DARTS: Digital Asset Real-time System
- FiSync or Sync: (Financial Institution Synchronization)

Justification for U.4:

U.4.1

The Solution maintains information applicable to overall transaction processing and provides contextual guidance to enable an effective payment exchange between the Payer and Payee. Transactional elements necessary to process the payment, available to both Payer and Payee, include:

- **Date** - date and time the payment was initiated by the Payer
- **Transfer ID** - identifier generated by the Operator and referenced by Members and Providers
- **Payer UDID** - Directory identifier of the Payer sending the payment
- **Payee UDID** - Directory identifier of the Payee receiving a payment
- **Operator ID** - identifier to the Operator of the Payee
- **Routing Number** - number to identify the Payee’s Member
- **Amount** - the amount of the transaction
- **Payer Confirmation ID** - identifier from the Payer’s Provider as a confirmation of completed and approved transfer
- **Payer Status** - a status field leveraged to indicate whether a payment is complete, pending, or rejected

- **Payer Reason** - populated when a payment is not completed and provides a contextual reason to the Payee

- **Payee Confirmation ID** - identifier from the Payee’s Member as a confirmation of completed and approved transfer

- **Payee Status** - a status field leveraged to indicate whether a payment is complete, pending, or rejected

- **Payee Reason** - populated when a payment is not complete and provides a contextual reason to the Payer (e.g. “Receiver not able to accept payment greater than $10,000”)

- **Auth ID** - identifier noting that the transfer involved a Pre-Authorization

In addition to the above critical elements that ensure successful transaction processing, the Solution provides additional contextual data leveraging a metadata structure. As a name-value pair attribute, metadata is fully customizable and structured as follows:

Fields named and defined by the initiator, such as:

- **Individuals** - comment or reason for payment

- **Organizations** - invoice, claim, or order number

The corresponding value is populated by the initiator:

- **Individuals** - “Here’s my half for lunch!”

- **Organizations** - 123456

Contextual Data allows Payers and Payees to exchange information in order to understand the reasons behind a received or requested payment.

*See Part A, Section 1: Initiation - “Contextual Data” to learn more.*

**U.4.2**

As an Operator and facilitator of Payment Messages, the Solution is agnostic to the needs of business and personal software solutions. Instead, integrations with such products and services are facilitated by Members to and from Providers using either a ISO 20022 standard or JSON. This separation assures integrity and standardization of the FPS while accommodating the varying integration needs of a Provider.

*See Part A, Section 1: Initiation - “Payment Messages” to learn more.*
The Contextual Data metadata attribute allows Providers to expand the Solution to feed into various software solutions. Providers can leverage naming standards and formats predefined in software packages (e.g. naming standard recognizable by Quickbooks).

*See Part A, Section 1: Initiation - “Contextual Data” to learn more.*

U.4.3

In addition to the flexibility to interoperate with software solutions, the Contextual Data metadata-based Solution provides customizable capabilities. Members and Providers have the ability to collaborate with others across the network and create agreed-upon standards for passing Contextual Data elements.

An example of this includes a network of Members agreeing to include “InvoiceNumber” as an element within Contextual Data. Providers then understand that “InvoiceNumber” will be included and can be displayed to the End User. If Members agree to the usage of key elements, the capabilities of expansion and collaboration are extraordinary with customizable metadata.

**Justification for U.5:**

U.5.1, U.5.2, and U.5.5

The FPS is agnostic to use case, currency, and location. This makes cross-border settlement an additional business objective subject to inclusion by Scheme Owners. The vendor or protocol used for cross-border settlement will benefit from the value propositions (e.g. cost, timing, improved messaging formatting, etc.) offered by an improved FPS.

U.5.3

*See: U.3.2*

U.5.4

*See: U.1.3*

**Justification for U.6:**

The payment flows and lifecycle stages remain intact for all use cases: business to business, business to person, person to business, and person to person. The Solution supports all use cases elegantly, but does have slight variations depending on the use case. To insure simplicity and
ease of integration, there are few data fields that vary between personal and business use cases, including:

**Organization Payer or Payee**

- **Directory Name** - the organization’s name
- **Directory Type** - the account type designation is Commercial, Nonprofit, or Government
- **Transaction Contextual Data** - leveraged for business-centric items such as invoice, claims, or order numbers
- **Transaction Limit (optional)** - Transaction limits per account type may or may not be enforced by the FPS Operating Rules and Guidelines, Scheme Owners, or Members.

**Personal Payer or Payee**

- **Directory Name** - the individual’s name
- **Directory Type** - the account type designation is Personal
- **Transaction Metadata** - leveraged for personal items such as payment comment or reason
- **Transaction Limit (optional)** - Transaction limits per account type may or may not be enforced by the FPS Operating Rules and Guidelines, Scheme Owners, or Members.

*For more information on Use Cases, see Part A, Section 1: “Initiation”, specifically the “Technology Platforms, Use Cases, and User Types” sub-section.*
Efficiency

Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: enables competition, capability to enable Value-Added Services, implementation timeline, payment format standards, comprehensiveness, scalability and adaptability, and exceptions and investigations process.

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>#</strong></td>
<td><strong>Consideration Name</strong></td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.1</td>
<td>Enables competition</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.2</td>
<td>Capability to enable Value-Added Services</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.3</td>
<td>Implementation timeline</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.4</td>
<td>Payment format standards</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.5</td>
<td>Comprehensiveness</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.6</td>
<td>Scalability and adaptability</td>
</tr>
<tr>
<td>Efficiency</td>
<td>E.7</td>
<td>Exceptions and investigations process</td>
</tr>
</tbody>
</table>

Justification for E.1:

E.1.1

Scheme Owners are incentivized to lower costs, protect against threats, and continually identify and address inefficiencies of their System Components. This provides Members greater profit margins from brokered access to the FPS or their own products and services provided to its customers.
The Solution accounts for and enables dynamic access to the bank transfer system (e.g. balance check, credit transfers, requests, Pre-Authorizations). This readily available and modern means for accessing the value propositions of an improved payment system allows Providers to re-imagine and build a range of new products, services, and experiences deemed valuable to their market segments.

See Part B, Section 2: “Value Propositions” for more information.

E.1.2

The Directory easily allows End Users to claim and changes preferences by allowing End Users to:

- Associate an email address or SMS-enabled phone number with numerous Members and Providers
- Manage and update Payment Preference with Members and Providers
- Revoke Provider Authorizations

See Executive Summary: “Directory” and Part A, Section 1: Initiation - “On-boarding a New End User” for more information.

E.1.3

Baseline costs conveyed to End Users are subject to the Payment System Rules enforced by the FPS Regulator, Scheme Owner, and/or Member (see: Predictability U.3).

E.1.4

Access

Aside from their own products and services delivered to their customers, Members may also broker access to RNAPs or other FIs. RNAPs are then able to offer their own products, services, and brokerage access to Participants and/or Third-Party Services. An Platform Services Layer encapsulating the core features and services needed to engage with the FPS allows all participants simplified and automated access to the FPS value propositions, which reduces overhead and inefficiencies typically associated with the bank transfer system.

Market forces driven by access, competition, and new Value-Added Services reduce System costs, increase adoption, and allow for equitable access to a low-cost, real-time payments system.

System Requirements
The proposed FPS Solution provides the technical capabilities (e.g. programmatic­enforced access scopes) and existing legal framework for stakeholders to inform, enforce, and/or require the necessary Payment System Rules for its Participants. These specific thresholds and requirements to access the FPS and its services are reserved for the FPS Regulator; however, additional requirements may be relegated to Participants from Scheme Owners to Providers.

Justification for E.2:

E.2.1

See E.4

E.2.2

Access and capabilities are governed by the FPS Regulator and are outlined in the FPS Operating Rules and Guidelines; however, as relevant to the Solution, the Platform Services Layer allows for tiered access to and privileges of the FPS. This allows Stakeholders to programmatically remove, enforce, or reduce the scopes of a Provider based on their role, responsibility, or risk within the FPS. These programmatic scopes allow for a much wider range of safe participation by a wide range of providers. For example, a Member brokering access to a high-risk Third-Party Service may easily limit their daily transaction totals or require additional identity verification data from their End Users. This compartmentalization reduces otherwise burdensome requirements for certain Participants and End Users, fosters broader inclusion and participation, and mitigates risk and abuse of the FPS.

E.2.3

By definition, all Value-Added Services are completely optional and would be required to be disclosed during the required End-User Authorization of said service.

Justification for E.3:

E.3.1

The implementation timeline outlines a three-year plan for full rollout and integration. For example, assuming the Coordination Phase is started in the beginning 2017, the initial integration will be completed by 2019, and full Ubiquity by 2020.

**Justification for E.4:**

**E.4.1**

Payment information and instructions flow through the Solution as Payment Orders, Payment Messages, and Payment Receipts. The technical means and formatting for Payment Orders and Receipts are reserved for Members, while a strictly standardized format is used for Payments Messages with the Operator.

**Proprietary standards**

Payment Message inputs to and outputs from the Operator are standardized, so Members have more flexibility over how they broker access to Providers. The degree to which a Member aligns their proprietary means of access (e.g. JSON) to the Payment Message standard is determined by the Member and/or Scheme and translated by the Member.

The customization of FPS access to Providers by Members allows for:

- differentiation in FPS access during the first and last mile of a payment
- more effective and efficient integrations at the Provider
- improved compatibility and flexibility between the Member’s technological capabilities and its Platform Services Layer

Any translation between formats is the responsibility of the Member, but will likely have additional security requirements to ensure message integrity.

---

**Component Standards**

*Payment Messages, and FPS Infrastructure*

---

32 If differing or proprietary messaging formats are used to send Payment Orders, additional measures should be taken to ensure message integrity given the threat model of an advanced adversary. The details and enforcement of these measures included in Payment System Rules may include digital signatures, key message elements preserved and compared via hash validation, etc.
Payment Messages are comprised of verifiable, signed, and standardized collection of data exchanged between Member and Operator for interbank or Inter-Operator Clearing. The Standard chosen (e.g. ISO 20022) is identified, governed, and enforced by the FPS Regulator. A similar standardized approach will be taken to the messaging protocols and format chosen for interaction with the Fraud Sharing Service and the Directory. The selection of standardization for these FPS infrastructure Components allows for strong interoperability with in-network and out-of-network Members.

**Open Standards**

While Authentication and Authorization for FPS Participation (i.e. Enrollment) and Payments are provided by the RNAP or Member, OAuth 2.0 is strongly recommended as part of an FPS API. It offers an open standard with robust scopes and security, as well as an established record as the default authentication and authorization experience for the nearly all digital platforms (e.g. Google, Facebook, Twitter, etc.). The usage of OAuth 2.0 increases the predictability, transparency (i.e. permission request), and simplicity to the End User and flexibility to the Member or RNAP.

Enhancing OAuth 2.0 to deliver token encapsulation for confidentiality and integrity, along with the use of JWTs for self-contained and compact information exchange provides the necessary flexibility and security needed for the platform while building on the strong foundation provided by existing OAuth 2.0 implementations.

E.4.2

Initiatives by Swift and others in Europe[33] and The Fed and The Clearing House[34] in the U.S. are underway to standardize ISO 20022 standards. While the Proposer of the Solution believes ISO 20022 establishes readiness for greater cross-border interoperability, Schemes will represent the extent of their interest and involvement in standardizing cross-border settlement.

E.4.3

As a new System, the cost associated with building to the standards of an FPS Infrastructure is built into the costs of implementation; however, legacy systems and channels may require modernization. While the costs are incalculable at this stage, the short-term costs incurred could be initially offset by the degree to which existing systems, switches, and other services are used or how implementation costs are calculated during a Scheme’s formation. Initial costs could be further mitigated through strategic channel or use case rollouts at a Member.

---


E.4.4
Sourcing the industry for input, we expect the FPS Regulator to act as a fair steward for standards modernization.

E.4.5
The constitution and development process of a standards body is determined by the FPS Regulator and will be in line with its Public Policy Objectives.

Justification for E.5:

E.5.1
The robustness of the FPS Platform to deliver effective payments for various stakeholders, use cases, and technology platforms is described throughout this paper and in detail in the Part A, Section 1: “Initiation”. The effectiveness of the solution is based on the ability to deliver an enhanced payment experience within an experience that is most effective for End Users.

E.5.2
The Integration effort summarizes the technical design elements. The stewardship model and Scheme Ownership extend the ease of integration, security controls, and operations to the Providers closest to the End User via the following:

- **Usability** - The API design focuses on succinct endpoints and ease of integration across various Components.
- **Reliability** - The Solution is architected to be highly available by leveraging practices focused on maximizing uptime, including change/revision management, geographically distributed hosting facilities, and load-balancing (see S.8.1).
- **Performance** - Optimal performance is achieved with API design and cloud computing capabilities that enable capacity changes within minutes.
- **Information security protocols** - The Solution follows security practices (e.g. Authentication, Signing, API secrets, and secure channels) to ensure appropriate confidentiality and integrity is maintained across Components (see “Part A, Authentication: “Component Authentication””).
- **Operations & Compliance** - The FPS Regulator will develop and maintain the FPS Operating Rules and Guidelines, supplemented by the Scheme requirements (see G.1.1).
• *Risk Controls* - The Scheme will maintain a risk management program which will perform risk assessments and monitor a risk register (see G.1.4).

For more information, see the technical design described in the Part B, Business Considerations: “Integration Effort”.

**Justification for E.6:**

**E.6.1**

As demonstrated in U.6.1 “Applicability to multiple use cases”, the FPS and its Infrastructure provides an elegant blend of core capabilities, extensible architecture, and customization to its Participants. This model allows the FPS the flexibility to adapt or enhance core services without impacting other services. Examples include:

• *Programmatic Scopes* - Ability to configure account settings for Members, Providers, and End Users to raise or lower requirements for certain activities, account types, etc.

• *Pre-Authorization Conditions* - Support for additional or more complex conditions (e.g. geolocation, “if this, than that” triggers, etc.) enhances applicability and value to End Users.

• *Identifiable Information* - Currently the Directory maintains a subset of identifiable information. Over time if other forms of End User data are required (e.g. physical address) to identify an entity, this can easily be integrated without impacting the Operator’s ability to facilitate payments.

• *Contextual Data* - Leveraging metadata as a means to exchange Contextual Data. Agreed upon attributes can easily be added and deprecated from the metadata based on Provider agreement and adherence.

**E.6.2**

*Project Volumes/Values, Scalability, and Adaptability are discussed in “Part B: Business Considerations - Integration Effort”.*

**E.6.3**

The model provides a great foundation for technical adaptability. With only identifiers exchanged across the various subsystems and minimal interdependencies, each can be upgraded with minimal impact to the Directory, Operator, and Fraud Sharing Service. The benefits of enabling Providers and Members with own their customer experience, while focusing on the exchange points of the Operator, Directory, and Fraud Sharing Service are:
- **Technology-driven** - Providers and Members can expand technological solutions without impacting the capabilities of the Solution (e.g. platform additions, like mobile in-person, mobile not in-person, online, etc.)

- **Economics-driven** - Since Operator serves as a settlement instructor, it assists Economic stability. Its flexibility and agnosticism to settlement mechanism (e.g. Deferred Net Settlement vs. Real-time Gross Settlement) makes it a dynamic and responsive choice to accommodate new or existing settlement systems that reduce risk systemwide.

- **Regulatory-driven** - Allowing the Scheme Owners to define Scheme Requirements provides flexibility to adapting to ongoing Regulatory changes.

- **Customer-driven** - The Solution allows Members or Providers the ability to own the customer experience and enforce measures to protect the experience. In addition to End-User experience, the Solution can be adjusted to include the following examples:
  - Collect additional information to exchange in the Contextual Data parameter
  - Offer new products and accounts (e.g. introduce credit lines, treasury management solutions, asset management, P2P)
  - New authentication technologies (e.g. biometric recognition)
  - New Payer Authorization features, including:
    - Payment approval - additional authorization mechanisms such as a PIN entry
    - New Destination IDs - if acceptable, Directory could be equipped to handle additional unique identifiers (e.g. Facebook Profile)
    - Payment Conditions - more customizable Conditions or the addition of new scopes (e.g. geolocation, time of day, autonomous “if this, then that” payment triggers, etc.)
  - Additional Fraud Sharing Service capabilities - capacity for inputs to and outputs from the Fraud Sharing Service could be increased based on Member feedback

*For more information on use cases and payment flows, see the technical design described in the Part A, Section 1: Initiation.*
Justification for E.7:

E.7.1

The Solution automates, via messaging and status changes, a Hold Harmless process that is analogous to existing processes today and familiar to Members. With a Credit Push Model, an End User bears the liability for an authorized payment. However, in order to mitigate errors, processes may be codified in the FPS Operator Rules and Guidelines and technically implemented to streamline the process.

If the End User wants to reverse a transfer due to a mistake (e.g. incorrect amount or recipient), the system allows the transfer to be automatically reversed as long as the transaction is not in a completed state. If the transfer is already complete, the system sends a request for reversal, rather than a mandate. The Member that received the payment can decide to automatically return the funds or complete a manual review to determine whether or not to do so. This decision is at the discretion of the Member and could include, for example, a consideration of whether the funds are still available in the receiving account, and the total amount of the transfer. If the transfer has already completed, returning the funds is at the sole discretion of the receiving Member, in accordance with applicable regulation.

Status updates are passed via the network so the End User has visibility at all times to the state of their return request. The timeframes for these investigations laid out in the Rules are also integrated directly to the system, creating alerts for Members to insure timely resolution of exceptions.

In the event of an unauthorized payment being originated via a compromise of the End User’s credentials, the Member or Provider who managed those credentials limits a consumer’s liability as required by applicable regulation.

E.7.2

The Solution passes some information end-to-end in an encrypted fashion and thus will not have visibility to the underlying data. Data which the Solution has visibility to and stores (see “Appendix A”) will be maintained for, at a minimum, five years from the date that the Member of record for an End User notifies the Solution that they have ceased their relationship. This allows an authorized party to obtain any related information the Solution has on any End User with a transaction ID or UDID.

E.7.3
The Operator monitors exception data by Provider, Member, and End User. Acceptable standards of exceptions by a given party will be codified in the FPS Operating Rules and Guidelines, along with remediation steps to be taken should these standards be breached.

Further data will be aggregated to alert Members to anomalous network activity and potential fraud (see S.7).
Safety and Security

Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: risk management, payer authorization, payment finality, settlement approach, handling disputed payments, fraud information sharing, security controls, resiliency, End-User data protection, End-User/provider authentication, and participation requirements.

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
<th>Proposal Page Number</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>#</strong></td>
<td><strong>Consideration Name</strong></td>
<td><strong>VE</strong></td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.1</td>
<td>Risk management</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.2</td>
<td>Payer authorization</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.3</td>
<td>Payment finality</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.4</td>
<td>Settlement approach</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.5</td>
<td>Handling disputed payments</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.6</td>
<td>Fraud information sharing</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.7</td>
<td>Security controls</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.8</td>
<td>Resiliency</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.9</td>
<td>End-User data protection</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.10</td>
<td>End-User/provider authentication</td>
<td>X</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>S.11</td>
<td>Participation requirements</td>
<td>X</td>
</tr>
</tbody>
</table>
Justification for S.1:

S.1.1
In addition to technical staff, a Scheme Company maintains an in-house legal and regulatory compliance team that analyzes new legal and regulatory requirements as they are released, and addresses any findings with participants in the network. When Scheme Requirements Scheme Requirements demand changes or new additions, a formalized rule-making process will be followed, with proposals being published to Scheme Owners and a comment period to allow for consensus to change.

S.1.2
The Operator sets and manages multilateral net positions by Member based on individual Member risk, as measured by the Operator’s internal designation similar to bank supervisors’ CAMELS ratings. The ratings will be derived by analysis of a Member’s public examination report, third party assessments and actual settlement performance. A Member will have the ability to address their rating through a formal review process.

Analysis of volume by Member triggers settlements as volume begins to reach limit amounts. Settlement failures result in suspension of further transaction processing for the Member and any of its Providers, as well as potential additional mitigating factors once a successful settlement has occurred (e.g., lower float amounts, more frequent settlement windows, or in extreme cases, suspension from the network).

S.1.3
The Solution is designed in such a way that there is a minimum of human intervention required to process a payment, particularly for Member staff. An End User initiates and confirms a payment, and the Solution automatically completes all the actions required, except for final approval by the receiving Member.

See Part A, Section 1 for more information on the transaction lifecycle.

S.1.4
The Solution’s ability to deter fraud is primarily driven by the ability of Members to manage their End User’s authentication; as such, the Members may elect to incorporate multi-factor

---

authentication ("MFA") be a requirement to initiate payments via the Solution. The Credit Push Model offered by the Solution, along with MFA, works to reduce fraud from multiple angles:

- **First-party fraud:** By requiring multiple steps to authorize a payment, the likelihood is reduced of an End User falsely reporting their transaction as fraud. The multiple steps allow a Provider to document key indicators of the interaction which can be used as evidence that the transaction was indeed initiated and authorized by the End User.

- **Second- and third-party fraud:** Additional factors create more barriers for a party other than the End User to compromise an account. Properly implemented MFA can alert an End User to an attempt to initiate an unauthorized transaction, which can be stopped at that point.

In order to reduce erroneous payments, the FPS Operating Rules and Guidelines will identify standardized content and presentment requirements to insure End-User protections (e.g. fees presented with the relevant information prior to authorizing a transaction, a chance to confirm the information is correct prior to the transaction being initiated, etc.).

Further, it is recognized that a new system will require increased customer outreach and education to explain features of the Solution that may differ from existing functionality, particularly around finality of payments. As the Solution provider, the Scheme Company will work with Members to provide standardized content that can be used within the initial experience to highlight these important key differences.

S.1.5

To protect the integrity of services rendered by the FPS, the FPS Operating Rules and Guidelines will identify the circumstances and incentives for Participants. Additionally, Scheme Companies, Members, and Providers are able to endorse or require incentives. Examples of incentives may include but not be limited to: fees, suspension, discounts, and fines.

S.1.6

The Scheme Owner and its System Components follow examination practices similar to that of its FI participants, with independent examinations of key processes, such as information security. These practices will be codified in the FPS Operating Rules and Guidelines. As an Operator, the Scheme Company has an inherent business incentive to update services and maintain and increase service levels to its participants, lest they opt to receive their services from a different Operator.
Justification for S.2:

S.2.1

Authorization is handled via the bank’s own credentialing, which can be set at whichever risk threshold each organization desires. Further, debit pulls, as they exist in the current ACH system, cannot occur. An End User must proactively give access to a biller prior to them being able to debit an account.

The FPS will be built upon a Good Funds and Credit Push Models where the Payer’s Member grants authorization for each individual payment executed on the End User’s behalf. The transfer is not designated as complete and approved until the Payer’s Member completes the intra-bank transfer from the FPS Account to Operational Account.

In addition the Payer’s Member can grant Pre-Authorization for future payments. This is outlined in “Part A, Section 1: Payer Authorization” section.

S.2.2

Pre-Authorizations allow Providers to initiate Credit Push transfers on behalf of an End User. A Pre-Authorization Request Message is assembled by the Provider, facilitated by the Provider Authentication flow via the Directory and Authentication Portal, and is approved by the Payer at the Payer's Member or RNAP.

Pre-Authorization Request Message includes:

1. Auth ID - identifier to reference the existing authorization
2. Status - designated as “Approved” when fully authorized
3. Payer UDID - The Unique Directory ID of the person who is providing authorization for the payments (if available)
4. Payee UDID - The Unique Directory ID of the person who requested the payment
5. One or more of the following Conditions
   ○ Start Date - date of first payment
   ○ End Date - date of last payment
   ○ Recurrence - one-time or recurring
   ○ Amount - amount of transaction
   ○ Amount maximum - maximum amount the Payer will authorize
○ *Payment frequency* - how often the payment is executed (e.g. monthly)

All the information listed above should be visible to the Payer by both the entities below, but will display Payer and Payee names rather than UDIDs:

- The Payee Member or Provider requesting Pre-Authorization
- The Payer’s Member or RNAP granting the Pre-Authorization

When Conditions are met, the Payee submits a Credit Request with an appended Auth ID to the Payee Member, which is then forward to the Payer Member via the Operator.

To complete a transaction, a Payee initiates the Credit Request with the Auth ID. The Payee’s Member appends the Auth ID to the Payment Message. The Auth ID is received by the Payer’s Member and used to cross-reference the stored Conditions associated with that Auth ID at the Payer’s Member. If met and Approved by the Payer’s Member, the Payer Member Initiates a Credit Transfer on the behalf of its Payer.

*See Part A, Section 1: Authorization for more details.*

S.2.3

Any location a Pre-Authorization can be granted requires an interface to allow revoking of those permissions. Providers and Members supporting Pre-Authorizations must allow their customers the ability to revoke at any time after the authorization is granted.

*For additional information on all S.2 criteria relative to the intricacies of the Payer Authorization, see:*

- *Part A, Section 1: Solution Description - Payer Authorization*
- *Part A, Section 1: Solution Description - Approval by Payer’s Provider*

**Justification for S.3:**

S.3.1

Payments can be initiated on the Platform via nearly any channel, device, or platform; therefore, consistency in Payer Member’s approval is key to Credit Push in a Good Funds model.

Regardless of whether the payment is Initiated by the Payer, Pre-Authorized by the Payer, or Requested by the Payee, each action requires funds to be immediately debited from the Payer’s Account and credited to the Operational Account. The transfer occurs as an intra-bank transfer within the member FI and requires Good Funds to complete the transfer.

*For more on all S.3.1 criteria relative to the intricacies of a Good Funds transfers, see:*
S.3.2

Until the Payer’s Provider receives the final “Transaction complete” message, there are stages where the payment is revocable. For example, while the transfer is in a “Pending” state because the recipient is unknown to the Directory because the recipient is unknown to the Directory, the Payer is granted the ability to cancel the payment.

For more on Payment Finality, see Part A, Section 1: “Payer Authorization”.

S.3.3

Justification included in E.7, specifically E.7.1, S.5.5.

For more on Payment Finality, see Part A, Section 1: “Clearing”.

Justification for S.4:

S.4.1

To settle financial obligations across Member FIs, the Operator leverages a Deferred Net Settlement approach. The inter-bank settlement is facilitated via the Operator’s use of current Fed-supported rails. Rebalances across FIs are conducted every two hours during the hours of operation of the Federal Reserve Bank to reduce overall risk exposure.

For more on settlement procedures, see Part A, Section 1: “Settlement”.

S.4.2

The amount of risk associated with a Deferred Net Settlement solution is greatly reduced by rebalancing every two hours. If a Member raises a credit or liquidity risk concern, the Solution can conduct an ad hoc settlement by leveraging the same funding tools on an as-needed basis.

FPS Operating Rules and Guidelines will help offset settlement risk by setting caps, thresholds, or ratios during both operating and nonoperating business hours. Additionally, to the extent that they are not already provided by the FPS Regulator, the Scheme may also place thresholds or requirements on its Members to proactively address potential settlement risks (e.g. overdraft policies, pre-funded accounts, etc.) associated with their Scheme.
Participating FIs may introduce internal mechanisms to protect themselves from liquidity. Since the network will be monitored at the Operator level, liabilities and receivables will be settled on a regular basis. However, if an FI has ongoing concerns about the Operational Account and negative balance scenarios, optional internal safeguards (e.g. contingency funded accounts) may be leveraged. Internal risk mitigation measures can also be enforced by the Scheme on an as-needed basis.

*For more on settlement procedures, see Part A, Section 1: “Settlement”.*

S.4.3

With a centralized ledger at the Operator, net positions of the Operational Accounts at all participating Member FIs can be monitored in real-time. In the event that a Member becomes negatively impacted by transaction activity, the Operator can leverage ad hoc settlement (via the same Fed-supported rails) on an as-needed basis to help mitigate the risk. Providing real-time contingency settlement in conjunction with multiple standard settlement windows reduces the burden on any individual FI.

Each Member FI will maintain an Operational Account for settlement. Each Operational Account will be maintained for the purpose of sending and receiving End Users’ PFS payments.

*For more on settlement procedures, see Part A, Section 1: “Settlement”.*

**Justification for S.5:**

S.5.1

As highlighted in E.7.1, the Solution provides a standardized process to resolve payment exceptions (e.g. erroneous or unauthorized payments). The Solution enables each Member to make a final decision whether or not to post funds to their End User, by providing Members additional information (e.g. Fraud Sharing Service gives Payee’s Member reason to believe funds are coming from a compromised account).

S.5.2

The FPS Operating Rules and Guidelines specify the timeframes and processes required to handle a Consumer payment dispute. As highlighted in E.7.1, the Solution automates messaging between and within Members to insure mandated timeframes are met.
S.5.3

The FPS Operator Rules and Guidelines standardize a Hold Harmless Process for Participants within the FPS to allow Members to voluntarily return funds. If there is a legal requirement to return the funds, the Solution’s data fields and messaging allow Members to easily communicate with one another to settle the legal order, including the return of funds.

S.5.4

The FPS Operator Rules and Guidelines rely on a variety of factors that define potential parties to a transaction and determine liability. The foundation of these rules is that an End User bears ultimate responsibility for the accuracy of information submitted to a Member, with no guarantee that an erroneous payment can be returned. On the opposite end, the Member managing an End User’s credentials is the responsible party in the event that an End-User account is compromised. Members are also responsible for providing commercially-reasonable authentication standards for non-End User accounts.

S.5.5

The FPS Operator Rules and Guidelines referenced within this document are written with consumer protection in mind. The proposed dispute/exception process falls directly in line with current Reg. E requirements. Enhanced authentication should reduce unauthorized payments, and Consumer education will be required to highlight Payment Finality.

**Justification for S.6:**

S.6.1

Information sharing is required by default. The sensitivity of information requested by the Fraud Sharing Service is low enough that Participants are willing to share this information in return for aggregated data in return. In the event of a breach, this shared data cannot be used to compromise an identity or initiate a transaction.

The data shared back from network-wide analysis give Members real-time information about the status of an End User across the network. Larger institutions gain value by being able to validate whether threats are unique to or targeted at their institution, or whether the threats are seen across the network. Smaller institutions gain value through the scale of the network, giving them visibility to larger fraud schemes even if the only impact to their institution is from a single End User or payment.
S.6.2
The Fraud Sharing Service provides a list of all data stored within the Service, as well as a retention schedule for that data. The goal of this data collection is to conduct analysis and pass actionable intelligence back to Members. Guides explain how the data is used, as well as list and explain the standardized messaging passed back to Members. This standardized messaging is system agnostic and can feed fraud systems of Members, whether the systems are rules-based or machine learning algorithms.

Data provided to the Fraud Sharing Service will be analyzed by the Operator for the purpose of fraud monitoring only—this data will not be shared, sold, or used for any other purpose.

S.6.3
The Fraud Sharing Service is an integral part of each transaction. As transactions occur in real-time, the Fraud Sharing Service messaging provides information back to Member and/or Provider to assist in making a decision in near real-time.

UDIDs and transaction IDs associated with a Member or Provider can also be queried outside of the transaction lifecycle for internal report creation or analysis.

S.6.4
See Part B, Section 2: “Integration Effort”.

S.6.5
The FPS Operator Rules and Guidelines referenced here and in S.5.4 are written with consumer protection in mind. The proposed dispute/exception process aligns with current Regulation E processes. Enhanced authentication should reduce unauthorized payments, and Consumer education will be required to highlight Payment Finality.

S.6.6
The Scheme Company maintains a Fraud Sharing Service with regards to End Users and their transactions for the sole purpose of analyzing network activity to provide actionable intelligence to Members. This information requires minimal PII but still gives Providers deeper insight into their End Users’ activity, allowing fast and reliable decisions to be made about whether or not to block or delay a transaction due to potential fraud.

Separate from the Operator database, this Fraud Sharing Service stores information reported by Providers with regards to their End Users and their transactions. There are three stages in an
End-User lifecycle when a Member stores information with the Fraud Sharing Service. The data points below are an example of what may be provided in each stage and are not a complete list; further, they are fields only to be used for the Fraud Sharing Service. The stages are:

1. Initial End-User registration with the Solution
   a. End User’s relationship open date
   b. End User’s zip code

2. End User initiates a transaction
   a. IP address of the End User’s session, if applicable
   b. Other session data, such as:
      i. Browser type and version
      ii. OS type and version
      iii. Device type

3. End User updates information
   a. End User’s new zip code

The Fraud Sharing Service can compare this information across Members in the event multiple Members report an End User with the same information. If conflicting information is associated with a single End User, the Fraud Sharing Service is able to report that information back to a Member when a transaction is initiated using standardized messaging. For example, a new End User opens new accounts at multiple Providers with the same email address and begins receiving multiple payments immediately across the network. This type of activity is a red flag for suspicious or fraudulent activity and the Fraud Sharing Service could send back a risk message to each Provider sending and receiving payments related to this End User.

Abnormal volumes of activity initiated from any source (e.g. a single IP, geographic region, Provider, etc.) can be reported to Members involved in a transaction initiated from that source. Both large and small Providers can benefit from economies of scale and have visibility to a potential large-scale fraud issue, even if they were only directly involved with a single transaction.

The Fraud Sharing Service does not make decisions about End Users on behalf of the Members or their partnering Providers, since those entities are in the best position to know their End Users. The goal of the Fraud Sharing Service is to improve decision-making by providing data that Members or Providers would not otherwise have. In its provision of the Fraud Sharing Service, Scheme Company defines a number of messages of potential high-risk activity. As the Solution
matures, the Scheme Company will refine and increase this type of messaging, as a result of research and Member feedback as to the usefulness and quality of the data received.

S.6.7

While the Fraud Sharing Service provides messaging related solely to potential risk factors on a single account or transaction, its greatest value lies in data aggregation across the network, which is the primary goal behind its design.

See S.6.1 and Part A, Section 1: “Fraud Sharing Service”.

Justification for S.7:

S.7.1

The System is built with security by design. Controls are implemented according to best practices and identified threats. A threat model and associated risk frameworks (e.g. OWASP) drive architectural requirements.

Identity verification and access management

This is delivered via an authenticated session protected via Public Key cryptography as demonstrated by the Directory service identity stores. The Directory service functions as a Public Key Infrastructure (PKI) updated by participating FIs and referenced for data confidentiality and integrity assurance.

Data encryption

This is delivered in transit via required and pervasive Transport Layer Security (TLS). Data encryption is delivered at rest via a series of datastores configured with transparent encryption, segmented data sets, and the capability for entity-level encryption using the Directory service PKI.

The quality and integrity of data

This is founded on its integrity throughout the system. The Directory service PKI makes possible the pervasive use of digital signatures, which provide integrity of messages and transactions.

Data breach prevention and detection

This is an ongoing process of following required Information Security practices, monitoring continuously, using strong cryptography, and having a layered approach to the application. Continuous security monitoring, a well-defined Incident Response (IR) plan, a trained IR team, documented and available forensic baselines and rapid information sharing (e.g. early warning
Layered security controls

This may include, but not be limited to: strong edge protection, load-balanced services, continuous security monitoring, vulnerability management including support for responsible disclosure, routing penetration tests, etc. Leading practices may include, but not be limited to: hardened and minimal systems, configuration as code, Multi-Factor Authentication (MFA) for all administrative access and ubiquitous support for MFA solutions, a well-defined plan and trained Incident Response team, immutable architecture patterns, training and security embedded into all system development.

Components and controls

These are employed to align with NIST 800-53 and FedRamp frameworks; however, they are flexible enough to accommodate other leading and open components/standards where applicable. For example, the Authenticated Encryption scheme delivered by ChaCha20-Poly1305 is not a NIST standard; however, it is provably strong (i.e. an eStream Cipher Project Member), in wide use, and provides high-speed encryption for devices not able to leverage native process extensions for the AES algorithm.

S.7.2

The System is designed with operational controls and procedural components which deliver data management, physical controls, and operational, communication, network, and application security.

The system retains data

This is based on a defined retention schedule aligned with relevant and emerging regulatory guidelines. Transactional data is kept no longer than necessary while master data may be kept for an agreed-upon longer duration as defined by regulation and/or policy. Data disposal follows NIST guidelines (800-88) or is disposed in such a way that recovery or loss risks are mitigated.

Physical security

This aligns with NIST 800-53 and/or FedRAMP guidelines and expectations.

Operations security

This aligns with NIST 800-53 and/or FedRAMP guidelines and expectations.

Communications security

This aligns with NIST 800-53 and/or FedRAMP guidelines and expectations.
S.7.3
Managerial policies and cross-system oversight are managed and measured using consistent metrics, automated data collection, and thorough integration across the early warning service.

- The Solution is API-driven, therefore existing Risk Management processes input data made available to authorized parties.
- Enterprise-level Security Architectures are compatible with policies and procedures as they align with NIST 800-53 and/or FedRAMP guidelines and as they are mapped to relevant risk management frameworks (such as SOC).
- This freely available mapping proves adaptability with Enterprise Security Architectures (e.g. TOGAF).
- Policies and procedures have a set review and enhancement cadence. Compliance and improvements are defined by the frequency of the review process against event-driven (e.g. incident) changes. See: S.1.5 for more information.

Justification for S.8:
A failure-resistant system delivers high-availability through a distributed and auto-scaling environment, reduction of single points of failure, and the ability to automatically recover.

S.8.1
The System is designed with a high level of availability for Directory, Fraud Sharing Service, and Operator interfaces similar to any reliable utility (e.g. telephone network). Changes to the System are API-centric, using change-management techniques designed to maintain uptime during revisions. The API components are immutable so that versions are not deprecated rapidly. As API revisions grow, stable and supported versions are maintained. The architecture makes use of geographically distributed hosting facilities, load-balancing, multiple network paths and native DDoS protection.

S.8.2
The system follows leading practices and aligns with FedRamp/NIST 800-53 for the definition, implementation, and routine testing of Business Continuity Planning (BCP) and Disaster Recovery (DR) scenarios. BCP and DR scenarios include tabletop and full-scale events on a periodic basis.
A cyber-attack scenario is a separate and uniquely positioned test held on an annual basis and requiring active defense, system baselines, established behavioral patterns, change monitoring, and forensic incident response elements.

S.8.3

Resiliency is a function of System design and change management that minimizes and isolates adverse changes. Since the System is API-driven, any changes are delivered without immediate depreciation of existing and stable API endpoints via an immutable API architecture. The system follows a three-tiered landscape including testing, signoff, and production releases to minimize change-related risks. A testing and risk-based change process facilitated by a Change Advisory Board with rollback plans mitigates systemic risks.

S.8.4

The System requires demonstrated capabilities (e.g. controls) of hosting providers and operators either through the demonstration of an independent report (e.g. SOC), results of technical analysis, or independent auditing against FedRAMP/NIST 800-53.

Periodic testing and exercises are required to provide metrics which track and review resources and operating effectiveness of BCP and DR controls.

S.8.5

In addition to the testing covered in S.8.4, sanctioned testing of non-production landscape tiers may include but not be limited to: load testing, vulnerability scanning, penetration testing, or simulated abuse.

Justification for S.9:

S.9.1

End-User data protection is a shared responsibility of the Participants and the Infrastructure. A framework of controls and applicable cryptographic protections serve to protect End-User data in transit and at rest.

The system requires demonstrated capabilities (e.g. controls) of hosting vendors and Operators either through the demonstration of an independent report (e.g. SOC), results of technical analysis, or independent auditing against FedRAMP/NIST 800-53.

See S.7.1 reference to Public Key cryptography and data encryption.
S.9.2
The Directory service and a unique identifier (UDID) limits the need for sensitive information to be sent across networks and systems. Email and SMS-enabled phone number are the primary identifiers as mapped and maintained by the Directory. The Directory also binds the UDID with a requisite Public Key (e.g. large key pairs) for message signing and message encapsulation.

S.9.3
See S.9.2.

Justification for S.10:

S.10.1
The System relies on the the Directory to provide core identity information which is securely updated by participating FIs. Payment System Rules determine the level of authentication necessary, but additional authentication measures may be enforced based on each FI's respective risk appetite.

See Part A, Section 1: “Authentication” and “Authorization”.

System administration requires MFA for all staff.

S.10.2
Payment messages are authenticated by Public Key information provided by the Directory service. The combination of the UDID and Public Keys permit mutual signing and authentication. Monitoring and validation of messages ensures the integrity of payment messages (e.g. thwarts spoofing and manipulation). Identity information as provided by the Directory service ensures Payee uniqueness using UDID and a trusted destination.

S.10.3
The system aligns with End-User authentication requirements as outlined by FedRamp/NIST 800-53; a composite mapping will be made available.

S.10.4
See S.9.2 and S.10.1.

S.10.5
The System allows Members and RNAPs to determine the levels of authentication and control Directory information to facilitate required authentication sequences.

S.10.6

The API-driven System allows FIs to determine and advance authentication models accordingly. Administration of the Platform will continue to advance and strengthen MFA.

**Justification for S.11:**

S.11.1

The FPS Regulator will develop and maintain the FPS Operating Rules and Guidelines that inform the baseline eligibility requirements accessed by Providers. Additionally, Schemes may place additional requirements on their Providers to protect the integrity of the Scheme.

A formal dispute and appeal process, which is codified in the FPS Operating Rules and Guidelines, offers an escalation path for Providers with Access complaints.

S.11.2

The FPS Regulator will develop and maintain the FPS Operating Rules and Guidelines that inform the baseline eligibility requirements for Scheme formation and FI Membership. Within reason, Schemes may place additional requirements on their Members to protect the integrity of the Scheme.

A formal dispute and appeal process, which is codified in the FPS Operating Rules and Guidelines, offers an escalation path for FI with Scheme admission complaints.

S.11.3

The Scheme will maintain a risk management program. The risk management program will include performing risk assessments and monitoring a risk register. An annual self-assessment and third-party independent audit will be performed and the results made available to the public. The results of the third-party audit and any enforcement actions will be maintained by the company utilizing a risk scorecard. The risk scorecard will include common criteria and key metrics that members will align with and the results will be made available on the website.
Speed (Fast)

Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: fast approval, fast clearing, fast availability of Good Funds to payee, fast settlement among depository institutions and regulated non-bank account providers, and prompt visibility of payment status.

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>Consideration Name</strong></td>
<td>VE</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>Fast approval</td>
<td>X</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>Fast clearing</td>
<td>X</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>Fast availability of Good Funds to payee</td>
<td></td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>Fast settlement among depository institutions and regulated non-bank account providers</td>
<td>X</td>
</tr>
<tr>
<td>Speed (Fast)</td>
<td>Prompt visibility of payment status</td>
<td>X</td>
</tr>
</tbody>
</table>

**Justification for F.1:**

Upon receiving a Payment Order from a Provider, the Payer's Member or Sponsoring Member undergoes an initial Approval process. The FPS expects approval to be completed within two seconds.

While the Approval requirements for a Payer's Member are informed by Scheme Requirements and the FPS Regulator, the following risk factors are a few examples of many considerations taken by a Member:

- Payer’s Account Status
- Payer’s Member assesses Fraud Risk
- Payer’s Member assesses its current cash position
Following a successful assessment of these or other considerations, the final step of Approval is the intra-bank transfer that occurs between the Payer’s Account and the Operational Account. A Good Funds model is predicated on the transfer of funds into the Operational Account.

For more information, see the Part A, Section 1: “Approval by the Payer’s Member”.

**Justification for F.2:**

Following the intra-bank transfer, Clearing is the exchange of Payment Message to the Payee Member. Only relevant information is shared to across the network, allowing each Provider to mitigate the circulation of sensitive PAN and PII.

The Operator is the primary facilitator of clearing information between the Payer and Payee Members. The Operator is expected to complete the following within two seconds:

- Capture the Payment Message via the POST sent by the Payer’s Member (described above)
- Record the transaction information to be used in the Deferred Net Settlement and Reconciliation process
- Notify the Payee Member via a Webhook Notification of the received payment

This provides the exchange of information needed for the Payee’s Member to execute an approval decision.

For more on Clearing procedures, see Part A, Section 1: “Clearing”.

**Justification for F.3:**

A Payee’s Member is expected to approve or deny a payment within one minute. Factors to consider may include:

- Payee is authenticated and authorized.
- Payee’s account is in “good standing” and active.
- Payment meets the Payee Provider’s criteria, which may include, but not be limited to:
  - Payer is an acceptable payment source.
  - The payment is within Provider limits.
  - The payment is in a Payee Provider’s supported currency.

Similar to the Payer’s Member, the Payee’s Member executes the transfer to the Payee’s FPS Account. Funds are withdrawn from the Operational Account held within the Member FI and
credited to the Payee’s FPS Account. Funds are cleared and immediately available to withdraw after meeting the Payee acceptance criteria.

This off-setting transfer is made possible because of the Good Funds model.

*For more on Clearing procedures, see Part A, Section 1: “Receipt”.*

**Justification for F.4:**

F.4.1

The Settlement Approach described in Part A, Section 1: “Receipt” and S.4 details how Fed-support rails are leveraged to reduce the duration of outstanding obligations between participating FIs.

F.4.2

All settlement windows are defined based on the Fed-supported operational hours, rebalancing every two hours.

*See S.4.1 for more information.*

F.4.3

Rebalancing every two hours reduces the amount of risk associated with a Deferred Net Settlement solution. If a Member raises a credit or liquidity risk concern, the Solution can conduct an ad hoc settlement by leveraging the same funding tools on an as-needed basis.

*See S.4.3 for more information.*

**Justification for F.5:**

F.5.1

The status provided by the Payer and Payee Providers and facilitated by a Member is required to be displayed to the End User per the FPS Operating Rules and Guidelines and/or additional Scheme Requirements. The following statuses are to be available within five seconds:

- *Completed* - payment is completed by both Member FIs:
  - debited from Payer’s Account
  - credited to Payee’s Account
- *Pending* - payment is sent, but waiting to be claimed by the Payee:
- debited from the Payer’s Account

- Rejected - rejected by the Payee’s Provider (reason for rejection included):
  - debited from the Payer’s Account and
  - credited back to the Payer’s Account

Since funds are transferred immediately to or from End-User Accounts, End Users can leverage their existing account management at a Provider or Member for up-to-date statuses and account balances.

F.5.2

Payees can view statuses at any time, much like Payers. From a Payee’s perspective, funds are only credited to their account once the Payee Member has approved the incoming transaction. The appropriate Contextual Data is to be displayed to the End User for insight to the payment details.

*For more on Clearing procedures, see Part A, Section 1: “Clearing” and Part A, Section 1: “Receipt” sections.*
Legal Framework

Provide a self-assessed rating in the table below and then justify how the solution meets criteria for: legal framework, payment system rules, consumer protections, data privacy, and intellectual property.

<table>
<thead>
<tr>
<th>Criteria Name</th>
<th>#</th>
<th>Consideration Name</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Framework</td>
<td>L.1</td>
<td>Legal framework</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.2</td>
<td>Payment system rules</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.3</td>
<td>Consumer protections</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.4</td>
<td>Data privacy</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Legal Framework</td>
<td>L.5</td>
<td>Intellectual property</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

L.1.1

The Solution is designed to allow and require each Provider to comply with its own relevant legal obligations, whether such obligations are based on the Provider's entity type (e.g. depository versus non-depository institution) or the Provider's activities (e.g. provision of remittance services versus issuing credit). Given the anticipated Provider types that would use the Solution and their use of the Solution to effect funds transfers, it is expected that such Providers would continue to be subject to a wide range of existing federal and state laws and regulations, including, but not limited to: OFAC, BSA/AML, Reg GG, Reg E, Reg Z, Consumer Financial Protection Act, UDAAP, E-Sign, FCRA, UCC, GLBA, and state money transmitter and data breach notification rules. In addition, the use of any Fed-supported rails would require compliance with the Fed’s specific rules and regulations applicable to such rails.

L.1.2

There are no known gaps with respect to the proposed legal framework for the Solution.

L.1.3
As a utility offered to Providers, the Solution requires Members and Providers to enter into agreements with its End Users governing the End Users' use of the Members' and Providers' services, including any services enabled by the Solution. The Solution's Payment System Rules may require the addition of certain language in Members' and Providers' agreements with End Users.

L.1.4
The Solution supports compliance with relevant United States law by all End Users, Members, and Providers when sending and receiving payments because it operates within the existing framework of U.S. law. The Solution does not create new requirements or extinguish any End User's or Provider's obligation to comply with existing legal requirements. For example, the Solution will support compliance tied to:

- the collection and transfer of data by laws such as OFAC and BSA/AML by allowing the collection and transfer of data as required by Providers (e.g. for consumer identification program (CIP) purposes under BSA/AML rules), and, the Solution will not prevent Providers from collecting CIP data and, as necessary and legally permissible, transferring it to other participants;
- the collection and analysis of data by laws such as UIGEA by allowing Providers to flag inappropriate transactions or system users (e.g. the Solution will not prevent Providers from applying internal controls and policies over their use of the Solution); and
- the processing of transactions and management of errors and unauthorized transactions by laws such as Reg E by giving Providers the ability to track transaction progress and associated metadata (e.g. for the purposes of determining whether a transaction reported as unauthorized was actually unauthorized).

L.1.5
The Solution is designed to allow each Member and Provider to comply with its own relevant legal obligations, whether such obligations are based on the Provider's entity type (e.g. depository versus non-depository institution) or the Provider's activities (e.g. provision of remittance services versus issuing credit). Both the data collection fields and availability of transaction data are optimized to allow Providers to meet respective legal obligations.

Justification for L.2:

L.2.1
The Solutions describes key features of existing or proposed Payment System Rules governing the rights and obligations of all End Users, Providers, Members, Payers and Payees to enable the Solution to operate effectively and efficiently, including Payment System Rules addressing:

L.2.1.1
Authentication of all Entities, payments or messages connected to a payment
See Part A, Section 1: Initiation - “Message Standards”

L.2.1.2
Legal responsibility of Providers that provide Payment System access to End Users (see L.1);

L.2.1.3
Payment Order Initiation/Authorization and termination of Authorization (see Part A, Section 1: Initiation - “Access, Consumer Protections, Limitations, and Use Cases“ and “Contextual Data“)

L.2.1.4
Cancellation of a Payment (see S.3.2);

L.2.1.5
Delayed and failed payments;
See Part A, Section 1: Payer Authorization - “Unauthorized, fraudulent, or erroneous payments”
E.7.1 - Exceptions and investigations process

L.2.1.6
Payment Finality and Settlement
See Part A, Section 1: Clearing - “Payment Finality and Irrevocability”;

L.2.1.7
Timing of sending and receipt of a payment (see L.1);

L.2.1.8
Records as proof of payment for Payers and Payees (see L.1); and

L.2.1.9
Error Resolution for anticipated disputed payments among End Users, Providers, Payers and Payees (see S.5).
L.2.2
The Solution will follow the process set forth in G.1 and G.2 in developing and amending the Payment System Rules, including obtaining input from stakeholders.

L.2.3
The Solution will follow the process set forth in G.1 and G.2 in enforcing and monitoring the Payment System Rules.

L.2.4
The Solution should describe existing or proposed Payment System Rules for allocating legal responsibility to appropriate Entities to obtain valid Authorization from the Payer.

L.2.5
The Solution will rely on existing rules, as applicable, under Reg E, any rules and regulations established by the Fed for the Fed-supported rails used by the Solution, and UCC 4A, for the purpose of setting Payment System Rules related to error, unauthorized transaction, and dispute resolution.

Justification for L.3:

L.3.1
The Solution proposes to use the consumer protections set out in Reg E and any rules and regulations established by the Fed for the Fed-supported rails used by the Solution as the Legal Framework for allocating legal and financial responsibility for this criteria element.

L.3.2
The Payment System Rules for the Solution will align with the Error Resolution procedures set out in Reg E and any rules and regulations established by the Fed for the Fed-supported rails used by the Solution.

L.3.3
The Solution will not prevent participants from offering greater Consumer protections than those otherwise required under applicable law.
Justification for L.4:

L.4.1

A Member and Provider will be required to maintain a privacy policy and comply with such policy, as required by applicable law for the Entity type, activity, and jurisdiction in which the Member and Provider operates. Data shared with Member and Providers via the Solution may only be used for the purposes of processing a payment through the Solution, subject to express authorization by an End User to use data for other purposes. The Solution's own collection and use of data would be limited to those activities required to process transactions and related activities, such as fraud management.

L.4.2

A Member and Provider will be required to comply with any applicable data security requirements specific to its Entity type and activity (see S.7 through S.11).

L.4.3

The Solution describes in detail the nature and type of End-User data that is required for transaction processing, and the stewardship model allows for Members and Providers to tailor their implementation of the Solution to allow for collection of additional End-User data needed for security, legal compliance, fraud monitoring, and Authentication purposes (e.g., name, address, phone, email, bank account number, bank routing number, DOB, SSN, GUID, IP location, and third party account information (e.g. a non-bank ID if the Provider isn't an FI)).

L.4.4

Data collection will be restricted to processing transactions and related activities (e.g., fraud management), and End Users have the choice not to use the Solution if they object to that use. Use of Data beyond transaction processing and related activities will be strictly on an aggregated and anonymized basis, e.g. tracking stats, etc.

L.4.5

With respect to data breach notifications and procedures, the Solution will continue to require Members and Providers to comply with existing state and federal laws and regulations in the event of a data breach.

Justification for L.5:
L.5.1

The Proposers are confident that the Solution does not infringe upon third party intellectual property rights and would undertake an appropriate review when necessary. Some proprietary intellectual property owned by Dwolla is disclosed in this Proposal, including, without limitation, certain intellectual property covered by a pending United States patent.
Governance

Provide a self-assessed rating in the table below and then describe how the solution meets criteria for: effective governance and inclusive governance.

<table>
<thead>
<tr>
<th>Effectiveness Criteria</th>
<th>Effectiveness Criteria Self-Assessment (Check One)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria Name</strong></td>
<td><strong>Consideration Name</strong></td>
<td><strong>VE</strong></td>
</tr>
<tr>
<td>Governance</td>
<td>G.1</td>
<td>Effective governance</td>
</tr>
<tr>
<td>Governance</td>
<td>G.2</td>
<td>Inclusive governance</td>
</tr>
</tbody>
</table>

G.1.1

The FPS Regulator develops and maintains the FPS Operating Rules and Guidelines, as well as custodianship of the Directory.

The Solution's governance arrangement will be organized by an organization (“Scheme” or “the Company”) responsible for the operation and strategic development of faster payments. The company will be owned and operated by its Members. The Scheme will develop the Scheme Requirements to supplement the FPS Operating Rules and Guidelines.

G.1.2 and G.1.3

The Scheme will define and deliver standardized rules, services, and pricing (“Scheme Requirements) for its Members. The Scheme will be responsible for the Operator and Fraud Sharing Service activities. The rules will define the requirements for participants involved in delivering the solution. A comment period will be available for pending operating rules changes. The Scheme will provide periodic updates related to recommended guidance and considerations.

Transparency in the Scheme’s activities will be facilitated by a public facing website with current documentation and support including board members, committee structure, articles of association, meeting minutes, Member eligibility, member risk scorecards, etc.
G.1.4

The Scheme will maintain a risk management program. The risk management program will include performing risk assessments and monitoring a risk register. An annual self-assessment and third-party independent audit will be performed and the results made available to the public.

The Scheme will be responsible for Member eligibility which includes defining the requirements, establishing membership fees, and monitoring compliance with the operating rules. The Members will be responsible for the implementation and ongoing operating effectiveness of the operating rules. The Members will be responsible for conducting an annual self-assessment and performing a third-party independent audit. The results of the third-party audit and any enforcement actions will be maintained by the company utilizing a risk scorecard. The risk scorecard will include common criteria and key metrics that Members will align with and the results will be made available on the website.

RNAPs will be required to have a Sponsoring Member to be granted additional privileges within the Scheme. A Sponsoring Member will be responsible for monitoring the performance of RNAPs according to requirements set forth within the operating rules and guidelines and Scheme Requirements.

Justification for G.2:

G.2.1

The Scheme will be open to any financial institution that is able to meet the necessary technical requirements. The Scheme's board of directors will be comprised of independent representatives and member nominated representatives, including public policy and consumer groups.

G.2.2

A committee structure will support the board of directors’ initiatives.

G.2.3

The FPS Regulator will maintain the Directory based on input from an Advisory Council.

G.2.4

The Scheme will have a user group provide feedback for improvements to the Solution.

G.2.5
The Scheme Owner’s Requirements will define what constitutes a conflict of interest and will implement monitoring procedures to confirm expected relationships.
## Appendix A - Data Descriptions

<table>
<thead>
<tr>
<th>Component</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Directory</strong></td>
<td>User Directory ID (UDID)</td>
<td>An identifier assigned to each individual End User within the Directory</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>Individual or Organization name</td>
</tr>
<tr>
<td></td>
<td>Type</td>
<td>Personal or Commercial - Sub-type (Commercial only) - Commercial, Nonprofit, or Government</td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td>Email address as a reference point for payment delivery</td>
</tr>
<tr>
<td></td>
<td>Phone</td>
<td>Phone number as a reference point for payment delivery</td>
</tr>
<tr>
<td></td>
<td>Operator ID</td>
<td>This ID is leveraged for interoperability with other Operator networks.</td>
</tr>
<tr>
<td></td>
<td>Routing Number</td>
<td>The number used to determine Member or RNAP location for payment routing</td>
</tr>
<tr>
<td></td>
<td>Preference</td>
<td>Field set by the Member or RNAP to indicate a preferred account by the End User</td>
</tr>
<tr>
<td><strong>Fraud Sharing Service</strong></td>
<td>UDID</td>
<td>Directory identifier of the End User</td>
</tr>
<tr>
<td></td>
<td>Relationship Open Date</td>
<td>The date the End User opened their account with the Member</td>
</tr>
<tr>
<td></td>
<td>ZIP Code</td>
<td>The ZIP code of the End User’s physical address</td>
</tr>
<tr>
<td></td>
<td>Industry Classification</td>
<td>This classification represents the industry of operation of the business. (business only)</td>
</tr>
<tr>
<td></td>
<td>IP Address</td>
<td>Internet Protocol address assigned to the End User's device</td>
</tr>
<tr>
<td></td>
<td>Browser Type and Version</td>
<td>Browser type and version of the End User</td>
</tr>
<tr>
<td></td>
<td>OS Type and Version</td>
<td>Operating System type and version of the End User</td>
</tr>
<tr>
<td></td>
<td>Device Type</td>
<td>Device type of the End User</td>
</tr>
<tr>
<td><strong>Operator</strong></td>
<td>Date</td>
<td>Date and time the payment was initiated by the Payer</td>
</tr>
<tr>
<td></td>
<td>Transfer ID</td>
<td>Identifier generated by the Operator and referenced by Members and Providers</td>
</tr>
<tr>
<td></td>
<td>Payer UDID</td>
<td>Directory identifier of the Payer sending the payment</td>
</tr>
<tr>
<td></td>
<td>Payee UDID</td>
<td>Directory identifier of the Payee receiving a payment</td>
</tr>
<tr>
<td>Operator ID</td>
<td>Identifier to the Operator of the Payee</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Routing Number</td>
<td>Number to identify the Payee's Member</td>
<td></td>
</tr>
<tr>
<td>Amount</td>
<td>The amount of the transaction</td>
<td></td>
</tr>
<tr>
<td>Contextual Data</td>
<td>Customizable data structured as Metadata allowing Payers and Payees to exchange information in order to understand the reasons behind a received or requested payment</td>
<td></td>
</tr>
<tr>
<td>Payer Confirmation ID</td>
<td>Identifier from the Payer’s Provider as a confirmation of completed and approved transfer</td>
<td></td>
</tr>
<tr>
<td>Payer Status</td>
<td>A value leveraged to indicate whether a payment is complete, pending, or rejected</td>
<td></td>
</tr>
<tr>
<td>Payer Reason</td>
<td>Populated when a payment is not completed and provides a contextual reason to the Payee</td>
<td></td>
</tr>
<tr>
<td>Payee Confirmation ID</td>
<td>Identifier from the Payee’s Member as a confirmation of completed and approved transfer</td>
<td></td>
</tr>
<tr>
<td>Payee Status</td>
<td>A value leveraged to indicate whether a payment is complete, pending, or rejected</td>
<td></td>
</tr>
<tr>
<td>Payee Reason</td>
<td>Populated when a payment is not complete and provides a contextual reason to the Payer (e.g. “Receiver not able to accept payment greater than $10,000”)</td>
<td></td>
</tr>
<tr>
<td>Auth ID</td>
<td>Identifier noting that the transfer involved a Pre-Authorization</td>
<td></td>
</tr>
</tbody>
</table>
Definitions

Capitalized terms used but not otherwise defined in this Proposal will have the meanings set forth in the **Fed FPTF Glossary**

**Access Provider:** A Member or RNAP that provides Third-Party Services with indirect access to the FPS.

**Advanced Threat Modeling:** A process by which the security of a solution is analyzed through a structure of application decomposition and the application of threats and countermeasures such as Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Escalation of Privilege. The goals of a robust threat model are to improve security design, drive testing, and reduce cost.

**Application Programming Interface** (API): A set of routines, protocols, and tools for building software and applications that expresses a software component in terms of its operations, inputs, outputs, and underlying types, defining functionalities that are independent of their respective implementations, which allows definitions and implementations to vary without compromising the interface.

**Authenticated Encryption (AE) or Authenticated Encryption with Associated Data (AEAD):** Block cipher mode of operation which simultaneously provides confidentiality, integrity, and authenticity assurances on the data; decryption is combined in single step with integrity verification.

**Authentication Portal:** A URL or endpoint associated with a specific Member or RNAP that is presented to an End User for Authentication and Authorization purposes. The URL or endpoint is established and supported by the Member or RNAP, and is available via the Directory.

**Business Continuity Planning** (BCP): The process of creating systems of prevention and recovery to deal with potential threats to a company.

**Change Advisory Board** (CAB): Delivers support to a change-management team by approving requested changes and assisting in the assessment and prioritization of changes.

**Component Authentication:** The process of verifying the pedigree of FPS components (e.g. an API endpoint) through cryptographic validation.

---

**Conditions**: The parameters and requirements (e.g. timing, frequency, amount, etc.) approved by an End User during Pre-Authorization.

**Contextual Data**: Describes the reason for, or is otherwise related to the funds transfer, as appropriate to the use case. (also described as the Metadata included with a Payment Order, Payment Message, and Payment Receipt to or from the Operator)

**Credit Requests**: The FPS protocol for requesting Credit Transfers from a Payee’s Member to a Payer’s Member.

**Credit Transfers**: The FPS protocol for enabling the real-time availability of Good Funds 24/7/365 from a Payer’s Member to a Payee’s Member.

**Demand Deposit Accounts**[^dda]: Funds held in an account from which deposited funds can be withdrawn at any time without any advance notice to the depository institution. Demand deposits can be "demanded" by an account holder at any time. Many checking and savings accounts today are demand deposits and are accessible by the account holder through a variety of banking options, including teller, ATM and online banking.

**Deferred Net Settlement**[^dr]: A system that affects the settlement of obligations or transfers between or among counterparties on a net basis at some later time.

**Directory**: A secure, standalone repository to facilitate enrollment, lookup, Payment Preference management, and Authentication and Authorization for Providers of End-User Accounts held at a Member or RNAP.

**Disaster Recovery**[^dr]: A set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster..

**End-User Account**: Authorized Payer Account or Payee Account at Member or Sponsoring Member

**Enrollment (or Enroll)**: The registration of an End-User Account into the FPS

**eSTREAM**[^estream]: A project to "identify new stream ciphers suitable for widespread adoption,” organised by the EU ECRYPT network.

**Faster Payment System (FPS)**: The comprehensive policies, infrastructure, and relationships described in this paper that facilitate end-to-end faster payments across multiple Operators.

[^dr]: “Committee on Payment and Settlement Systems: A glossary of terms used in payments and settlement systems.” BIS. March 2003
**FPS Account:** FPS Account is a Payer Account or Payee Account at Member or Sponsoring Member. (also known as “FPS-enabled Account”)

**FPS API:** Brokered by Access Provider, the FPS Application Programming Interface (API) that encapsulates and delivers the services, processes, and protocols needed to securely and compliantly access baseline capabilities of the FPS.

**FPS Infrastructure:** Core technologies, processes, and components (i.e. Directory, Operator, and Fraud Sharing Service) required to facilitate Faster Payments. (Also referenced as “System Components” or “Infrastructure”)

**FPS Operating Rules and Guidelines:** Body of rules, standards, and governance instructions drafted by the FPS Regulator to regulate the participation, roles, and responsibilities of Schemes, Members, Providers, and End-User participation within an FPS. Helps ensure and sustain integrity, security, scalability, interoperability.

**FPS Regulator:** The Entity (or Entities) that represent the Public Policy Objectives of the System and provide leadership, oversight, and enforcement over the FPS Infrastructure, its Members and Providers, and—to a lesser extent—the End Users.

**FPS Rules and Guidelines:** Body of rules, standards, and governance instructions drafted by the FPS Regulator to regulate the participation, roles, and responsibilities of Schemes, Members, Providers, and End-User participation within an FPS. Helps ensure and sustain integrity, security, scalability, and interoperability.

**FedRamp**[^44]: A government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

**FI Service Provider:** Provides necessary technologies, products, and services exclusively to Financial Institutions (e.g. FIS, Jack Henry, Fiserv).

**Financial Market Utility**[^45]: Multilateral systems that provide the infrastructure for transferring, clearing, and settling payments, securities, and other financial transactions among financial institutions or between financial institutions and the system.

**FiSync:** Dwolla’s real-time ledger, messaging protocol and settlement instructor for real-time bank transfers.

**Forward Secrecy**[^46]: A property of secure communication protocols in which compromise of long-term keys does not compromise past session keys. (source: Wikipedia)

---

Fraud Sharing Service (or “Fraud Service”): Takes unique data from each Member and compares it across the FPS, then passes it back to the Member to improve their fraud decision-making.

Hold Harmless Process: The Hold Harmless process is an agreement between two Members where the Members agree to release each other from any legal claims involved with the voluntary return of funds.

Immutable API Pattern: Approach where new functionality is delivered through new API endpoints rather than a continuous change of existing endpoints.

Infrastructure: See “FPS Infrastructure”

JavaScript Object Notation⁷ (JSON): An open-standard format that uses human-readable text to transmit data objects consisting of attribute–value pairs.

JSON Web Token⁸ (JWT): A JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties.

Ledger’s Multilateral Netting⁹: An arrangement among three or more parties to net their obligations. The obligations covered by the arrangement may arise from financial contracts, transfers, or both. The multilateral netting of payment obligations normally takes place in the context of a multilateral net settlement system.

Members: Depository Institutions directly connected to an FPS Scheme that offer direct products or services to Third-Party Services, RNAPs, or End Users. “Member” may be used interchangeably with Sponsoring Members.

Metadata⁰: data that provides information about other data.

Non-Member FI: Financial Institutions that may not be a direct Member of a Scheme but wish to access and provide FPS access and services to their customers.

Originating Depository Financial Institution (ODFI): as defined in the “NACHA Operating Rules & Guidelines”

Operational Account: A designated, FDIC or NCUA-insured, and interest-bearing internal account at a Member for the purpose of holding and processing real-time transfers.

Operator: A payment message clearinghouse, ledger, and settlement instructor for Members of an FPS Scheme.

---

⁹ “Committee on Payment and Settlement Systems: A glossary of terms used in payments and settlement systems.” BIS. March 2003
**Participant Authentication:** Verification and validation of End-User eligibility by a Member or RNAP required to provide the End User access to the FPS. This is completed during End-User Enrollment by RNAP or Member.

**Participant Authorization:** End-User approval of FPS Enrollment with a Member or RNAP is completed during Enrollment.

**Payee Member:** The direct Member or indirect Sponsoring Member (in the case of a RNAP) that facilitates the necessary process associated with receiving Credit Transfer on behalf of an End User in an FPS.

**Payer Account:** An End User’s FPS-enabled account held at a Member or Sponsoring Member.

**Payer Member:** Payer Account is an End User’s FPS-enabled account held at a Member or Sponsoring Member.

**Payment Message:** A verifiable, signed, and standardized collection of data exchanged between a Member an Operator for interbank or Inter-operator Clearing.

**Payment Preference:** Preferred account identified and managed by the End User via a Member or RNAP.

**Pending Payment:** Pending Payment are Good Funds allocated and held in Payer Member’s Operational Account awaiting claim by an un-enrolled End User or approval by a Payee’s Scheme, Member/Sponsoring Member, or Provider.

**Platform Services Layer:** A secure application layer at a Member or RNAP that provides the necessary APIs and/or services to allow Providers access to or build overlay services on top of the FPS.

**Pre-Authorization:** Prior approval from an End User to Initiate future Credit Transfers.

**Primary Account Numbers**\(^5\) (PAN): The 14, 15 or 16 digit number that appears on the primary account holder’s credit card. (Source: Investopedia)

**Provider:** Participants or Entities that directly deliver, facilitate, and/or enable direct access of the FPS to an End Users through Initiation via a Member in the Scheme.

**Provider or Application Authentication:** On-behalf of an End User, a Provider requests Authentication from the End-user’s Member or RNAP.

**Provider or Application Authorization:** Approval of a Provider’s request for FPS permissions by the End User at its RNAP or Member.

---

**Public Key Infrastructure**: a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

**Public/Private Key Pairs**: Public/Private Key Pairs: Public-key cryptography, or asymmetric cryptography, is any cryptographic system that uses two kinds of keys: public keys that may be disseminated widely, while private keys are known only to the owner.

**Rebalance**: The act of settling financial obligations across participating FIs.

**Receiving Depository Financial Institution (RDFI)**: as defined in the “NACHA Operating Rules & Guidelines”

**Returns**: Returns are new transactions that transfer funds back to the Payer and are associated with a previously completed transaction.

**Scheme**: Represents the financial, legal, and regulatory relationships and obligations of an FPS Operator and its owners.

**Scheme Component**: A utility (e.g. National Directory, Fraud Sharing Service, Operator) that facilitates the critical processes, protocols, and standardization of the FPS.

**Scheme Requirements**: Rules, standards, and governance requirements NOT dictated by the FPS Regulator that are provided and enforced by Scheme Owners. These help regulate the participation, roles, and responsibilities of Members, Providers, and End User participation within an FPS Scheme. This may include, but not be limited to: legal structure, bylaws, board of directors, settlement authorizations, collateralization, risk management programs, etc. In order to operate the Company, Members are also expected to fund and incorporate the Scheme.

**Service Organization Control (SOC)**: Internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service.

**Software Development Kit (SDK)**: Is typically a set of software development tools that allows the creation of applications for a certain software package, software framework, hardware platform, computer system, video game console, operating system, or similar development platform.

**Solution**: A brandless solution proposed within this paper will using existing, adapted, and improved applications and processes of Dwolla’s current Network, Platform, Services, and Immediate Funds Transfer System (also referred to as “System”)

---

Sponsoring Member: A Member of an FPS Scheme that endorses and ensure FPS and Scheme Owner compliance to RNAPs.

System Component: See “FPS Infrastructure”

Third-Party Services (TPS): Entities eligible to Initiate Credit Transfers, Credit Requests, Returns on behalf of an End User are considered to be Third-Party Services. Third-Party Service Provider receive access to the FPS via Members or RNAPs.

Transaction Authorization: The explicit instructions given by the Payer to the Payee to transfer funds on a one-time or recurring basis, including: timing, amount, Payee, source of funds and other conditions.

Transport Layer Security (TLS): Provides communications security over the Internet.

Unbanked: Households without a depository account at an insured institution.

User Directory ID (UDID): An identifier assigned to each individual End User within the Directory.

Utility: A core component of the Infrastructure (i.e. Directory, Fraud Sharing Service, and Operator) that facilitates the critical processes, protocols, and standards of the FPS.

Value-Added Services: Any product, service, or experience that represents the opportunity for net-new revenue through the improvement or packaging of FPS above its core capabilities to an End User (e.g. MassPay, ACH to FPS migration tool, real-time payroll, Third-Party Service P2P, etc.).

Webhook: A method of augmenting or altering the behavior of a web page, or web application, with custom callbacks. These callbacks may be maintained, modified, and managed by third-party users and developers who may not necessarily be affiliated with the originating website or application.

---

Contributors

The proposal was submitted by the Dwolla team with contributions from the following individuals:

- Adam Steenhard
- Adrienne Sum
- Ben Milne
- Ben Schmitt - Secure Payments Task Force Member
- Brent Baker
- Jeremiah Wingett
- Jon Eichhorn
- Jordan Lampe - Faster Payments Task Force member and Steering Committee representative
- Nick Leeper
- Ryan Hodge
- Sara Blass
Faster Payments QIAT

PRELIMINARY ASSESSMENT

Proposer: Dwolla, Inc.

Summary Description of Solution:

Dwolla is a digital payment network and platform for real-time payments with immediate availability of good funds. The solution is an end-to-end Faster Payments System (FPS) comprising:

Federal Reserve as the FPS Regulator

An FPS “Scheme Owner/Operator” that operates the clearing and settlement infrastructure between members. The solution involves real-time clearing and deferred net settlement through the Federal Reserve’s National Settlement Service (NSS). To reduce overall risk exposure, funds are rebalanced across FIs every two hours during the FRB’s hours of operation

Depository institutions as member-owners of the FPS scheme. These members can: 1) serve as direct providers of faster payment services to end-users, 2) offer FPS access or services to a third-party service (e.g., Uber) as an access provider, and/or 3) offer FPS access or services to a regulated non-account provider (e.g., PayPal) as a “sponsoring member”

Providers that deliver, facilitate, or enable access to the FPS by end-users through products, services, or APIs

A directory or federation of directories serving as a secure, standalone repository that enables anyone to send and receive payments using just an email or phone number. Users may also store payment preferences in the directory

A Fraud Sharing Service, which the Operator maintains separately, to collect and distribute data and conduct analysis across the platform to spot high-risk activity

EXECUTIVE SUMMARY OF THE PROPOSAL

Major strengths

The solution facilitates payments to/from all types of accounts—checking, savings, checking, and others—across depository institutions, regulated non-bank account providers and third-party providers

The solution facilitates competition by allowing end-users to choose among providers, to use multiple provider accounts, to specify payment preferences in the directory, and to switch providers. Providers can develop value-added services by integrating with the solution using open, accessible standards through the solution’s Platform Services Layer.

The solution’s messaging format will help to ensure interoperability. ISO 20022 will be the format for payment messages to and from members and the operator; messaging between providers and members will be determined by the member and translated to ISO 20022. Schemes will be enabled to collaborate with Members and Providers to develop agreed upon standards for contextual data (attributes in the metadata).

The solution’s security controls meet all criteria for fraud information-sharing, security controls, and end-user data protection. The solution requires payer authorization to their member FI when initiating payments. Payers can pre-authorize payments and can revoke pre-authorization easily and quickly. The solution enables same-day settlement, mitigating the need to manage managing liquidity risks.

The solution meets the criteria for speed: Payments are expected to be approved and cleared within two seconds of payment initiation. The payee’s member institution is expected to approve or deny a payment within one minute. After the payee accepts the payment, funds will be immediately available for withdrawal. Payment statuses are available within five seconds.

Areas for improvement and enhancement
The solution itself does not control a consistent end user experience, nor does it articulate guidelines or requirements for Providers to ensure a consistent experience.

Throughout the proposal, the submission outlines how the Platform Service Layer (PSL), a secure application layer at a Member or RNAP that provides the necessary APIs and/or services to allow Providers access to or build overlay services on top of the FPS, delivers a technical framework for the delivery of dynamic access to third-parties and ubiquitous payments. This modern access is a cornerstone of the proposed FPS, as it is used to build and deliver End Users with valuable FPS services and products. As such, the technical framework also serves a critical role in facilitating End-User experiences that are both consistent and convenient.

While it’s true that the dynamic PSL will be greatly informed by the finalization of Payment System Rules (PSR) of the FPS Regulator and Scheme Owners, it is not lacking the technical means to ensure a consistent experience. In fact, because such FPS APIs and SDKs would be programmatically informed by the PSR, the PSL can strike the ideal balance between Predictability (e.g. disclosures, notifications, etc.) and Usability (e.g. frictionless payments, value-added services, etc.).

To clarify the Proposal’s capabilities and offer potential guideline/requirements suggestions, the Proposers have revisited this programmatic approach with more specificity, highlighting potential End-User experiences and real-world user flows as examples in its responses to U.2 and U.3. We look forward to additional comments and improvements made by the Task Force.

The solution’s implementation timeline does not address or include: 1) a plan for member adoption or for phasing in members over time, 2) an explanation of how implementation will be funded, 3) the hurdles to adoption that might arise, or 4) a partnership plan or list of potential providers/members.

These items are addressed in the Proposal and further clarified upon in the Proposers’ response to the assessment in E.3.

Defining standards for contextual data elements will require collective action or collaboration across participants, which may challenge adoption and scaling.

The Proposers agree with the above statement that collaboration will be a prerequisite for the successful implementation of any Solution. Throughout the submission, the proposers draw from best practices, the success of domestic and international work group efforts, and its own experience to highlight this challenge and posit a potential solution for further consideration. This method is elaborated upon further in our response to U.4 and E.4, and the Proposers look forward to further collaboration on this matter.

The solution’s rules include requirements and processes for resolving unauthorized, fraudulent, erroneous, or otherwise disputed payments but do not include timeframes or a process for cases in which the payee refuses to return the funds. The standard process is limited to a reversal process/request for return of funds and notifications of completion. This approach complies with Reg. E, but Reg. E only covers consumers.

There would be no differentiation in the process between government, commercial or consumer disputes. With the stated goal of settlement finality, returned payments will not be a routine occurrence as with existing systems such as card networks and ACH. The solution offers robust and layered levels of authentication of a user, along with meta-data and intelligence to improve sending and receiving banks’ decision making with regard to allowing a payment to be sent and received. Both the Payer FI or RNAP, and the Payee FI or RNAP all must explicitly approve a payment before the funds cannot be disputed.

More detail is required on the proposed risk management framework and legal framework, which are heavily dependent on Providers’ compliance, payment system rules and governance.

---

As noted by the QIAT, “Somewhat Effective” assessments were applied to the proposals of many Governance sections. Unlike other Criteria, Governance and PSRs transcend the individual systems, stakeholders, and use cases and are uniquely shared and uniformly applied in most cases. Given the uncertain nature of this proposal process and unknown details of other’s proposals, we believe the Task Force runs the risk of discrediting or disqualifying the initiative by assessing Governance similarly to other Criteria.

Given these constraints, it was important to Dwolla that we provided a framework approach to key aspects of the Proposal, including Governance. We refer to this in our responses as the “framework approach.” This approach is not prescriptive or unilaterally determined, instead it describes guidelines, relationship dynamics, rule sets, and technical capabilities that are compatible with the future determinations of the final paper. While our responses outline additional considerations for the QIAT, we believe this pragmatic, flexible, and approach to be the only route to a Very Effective solution for the market at this stage.

Use cases addressed

The Solution addresses all four major use cases (P2P, P2B, B2P, and B2B). It does not yet support cross-border payments, deferring the future plan for these to scheme owners.

Proposer’s overall ability to deliver proposed solution

Dwolla is an established payments solution provider that currently provides a bank transfer solution

The Solution uses existing, adapted and improved applications and processes of Dwolla’s current Network, Platform, Services and Immediate Funds Transfer System. Thus, the QIAT has high confidence in the ability to deliver the technical solution

Significant differences in proposer’s assessment and that of the QIAT including proposer responses

TBD based on proposer comments
ASSESSMENT

Ubiquity

U.1 Accessibility

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

Rationale:

The solution facilitates payments to/from all types of accounts—savings, checking, and others—across Depository Institutions, Regulated Non-bank Account Providers (RNAP) and third-party providers (U.1.1).

End Users can enroll with a Member depository institution or RNAP. First-time payees that are not part of the directory can also enroll; the Payer’s Member engages the payee via a notification to email or mobile phone, and the payee is then taken through the registration process in order to receive the transfer. This helps ensure that Entities’ payments can reach any and all Payees (U.1.2).

For multi-currency transactions, the solution supports any transfer, so long as end-points can accept the currency (U.1.3). However, the ability to handle multi-currency is dependent on providers, and interbank settlement processing for multi-currency is being explored. It is not clear how solution would ensure the same SLAs for a multi-currency offering.

The ability to send and receive payments from RNAPs and third parties supports the needs of the unbanked and underserved. (U.1.4). In addition, innovations for consumers without access to SMS or email include vouchers for redemption and prepaid cards.

While the Solution is technically feasible, the value proposition for individual Providers to participate and make the Solution available to end users is not clear (U.1.5). In addition, more detail is required on the plan for achieving interoperability across operators (U.1.6).

Questions back to proposer

U.1.2: How can a payee be reached if s/he does not bank at a member depository institution? The process for enrollment requires choosing a member FI or an RNAP that is part of the network.

A Payee does not need to have an existing account with a Member FI or eligible RNAP to receive funds. The on-boarding process illustrated in “Onboarding a new End User” (p23), “Initiate Credit Transfer to Unknown Payee” (p31), and “Enrolling a New Payee at First Receipt of Credit Transfer or Request” section (p26) provides Providers the necessary access, reference data, and technical flows to populate a user interface, facilitate the selection of an eligible on-boarding Provider, and ultimately enroll an unaffiliated End User with FPS-enabled institution.

1. Upon receipt of a payment via the Identifier (e.g. SMS or email address) that funds were directed to, the End User clicks link and is taken to the Payer Provider’s hosted Directory interface or portal.
2. End User acknowledges that he or she is unaffiliated with a FPS-enabled institution. Payer’s Provider populates list of eligible FIs and RNAPs capable of facilitating native online account origination.
3. End User selects from list of eligible FIs and RNAPs.
4. End User is taken to the registration or account origination process hosted on by the selected chosen FI or RNAP. The transition from Payer Provider to new Payee Provider carries with a secure, time-based JSON web-token (JWT) with the protected information needed to complete the transfer.
5. Newly selected Preferred Provider enrolls End User into and collects a UDID from the Directory (can be done simultaneous with Step 2).
6. Payee’s Provider uses newly acquired UDID and JSON webtoken to complete the transaction and claim the funds on behalf of End user.
NOTE: All RNAPs are required and expected to meet or exceed the requirements set by the PSR for FPS enrollment and usage. This may include but not limited to Know Your Customer, Anti-Money Laundering, Fraud and Risk Management, and other regulatory requirements. Furthermore, RNAPs must be sponsored and banked by a Member FI, ensuring proper collateralization and operational alignment.

A number of physical and other digital experiences could also exist (e.g. a non-digital experience, such as enrollment or cash out at a physical retail location, could be pursued so long as it aligned with PSR).

U.1.5: What are the economic incentives to get FIs and RNAPs to adopt and promote the system? How will Dwolla achieve minimum, viable endpoint utility at launch?

The Proposers outline the economic incentive for all stakeholders by relationship with each other and stage in payment in the “Costs and Incentive Mapping” section (starting on p76-88).

As highlighted by the Federal Reserve in its Strategies for Improving the U.S. Payment System Report, the traditional forms of revenue generating relationships between stakeholders (e.g. like membership fees, per transaction fees, etc.) and known reduction in operational costs provided by an improved system may offset direct investment costs and lost revenue within the first 10 years with a possible surplus of up to $1.8B in new revenue. The noted efficiency gains are demonstrated the Federal Reserve in its report on “Costs and Benefits of Building Faster Payment Systems: The U.K. Experience and Implications for the United States”.

The Proposers believe these net revenue estimates to be highly conservative, noting that previous systems provided End Users neither had the value proposition, technical access, or the capabilities of a modern payment system. Citing examples such as Stripe, Braintree, and its own experiences, as Dwolla, these new age providers have unlocked new products, services, and revenue that Proposers believe provide Stakeholder an incalculable number of profit-generating opportunities. For example, the “latent or adjacent demand” highlighted by the Federal Reserve, but not tallied in its estimates.

Competitively, RNAPs are admittedly better positioned to cater to the unregistered or unbanked users noted in the previous question and for a variety of reasons (e.g. business model, narrower regulatory scope, value from niche market providers, etc.). The lower barriers and ability to execute against niche use cases provide for faster and simpler account creation processes, allowing End Users to safely register for a service, claim funds, and enroll with the FPS in minutes. Furthermore, the capacity for specialization among RNAPs can prove extremely useful in creating different sets of value for different sets of End Users (e.g. payroll, invoicing, or procure-to-pay RNAPs), elevating the appeal and distribution of these services among specific use cases.

Absent a regulatory mandate for FI participation inside an FPS Scheme, the proposers believe this relationship between FIs and RNAPs (aside from other incentives highlighted in the proposal) fosters a competitive environment that will lead stakeholders to enroll in a FPS Scheme and promote their products and services aggressively.

U.1.6: Does the Solution include multiple operators or networks? How do payments from one operator/network reach a Payee in another operator/network?

Yes. Strong standardization among Operators, a dynamic web-based Directory, and the inclusion of an Operator ID as a core data element of each transaction provide End Users, Providers, and Operators a path to deliver and clear a payment out-of-network. Settlement across Operators occurs leveraging a net settlement of Operational Accounts. See also, “Payer is in the Directory, but out-of-network” (p34), “Multi-operator settlement” (p108), and “Adding an End User to the Directory” (p25).

---


Usability and Predictability

**Note: Due to the similarity the concerns expressed by the QIAT, the Proposers combined the their responses to Usability (U.2) and Predictability (U.3)**

### Usability U.2

<table>
<thead>
<tr>
<th>Level</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**

The solution enables a straightforward, simple end-user experience by allowing Providers to build FPS capabilities and experiences across devices and channels, thereby enabling initiation of payment with just an email or phone number (U.2.1-2). The FPS is available 24x7x365. The payee’s member FI is expected to approve or deny a payment within one minute. After the payee accepts the payment, funds are immediately available for withdrawal (U.2.3).

Providers use the solution’s Platform Services Layer to build end-user experiences; however, the solution itself does not articulate guidelines or requirements for usability. It therefore cannot be assured that the solution will be easy to use for users of all technological proficiencies or for the disabled, etc. (U.2.4).

### U.3 Predictability

<table>
<thead>
<tr>
<th>Level</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**

The solution’s baseline, core features are well-defined and the solution’s design ensures their delivery (U.3.1). The communication of baseline features in the payment experience is the responsibility of the FPS Regulator and Scheme owner, but the Proposer offers suggestions on authentication, timing, and acknowledgment of costs (U.3.2). The solution uses standard messaging and protocols between the FPS operator and providers, but leaves Providers to decide on the messaging standard and protocols used to deliver the end-user’s experience (U.3.3).

As mentioned, it is generally up to the member/provider to determine the end-user’s experience, so there is a trade-off between ease of integration for members and predictability for end-users (U.3.4). The solution relies on yet-to-be-defined FPS operating rules and guidelines to ensure consistency in the end-user’s experience. The error resolution process follows processes similar to the UK’s Faster Payments Service (U.3.5). The Solution is “brandless”; however, terms suggested to distinguish the Solution from other payment methods include Advanced Clearing Exchange (ACE), Digital Asset Transfer Architecture (DATA), Digital Asset Real-time System (DARTS), and FiSync or Sync (U.3.6).

**Response to Rationales of U.2 and U.3**

First described in “Participation in the FPS” (p7) and throughout the Proposal, the PSL programmatically delivers the technical flow and End User framework for most all End-User interactions through its use of APIs and SDKs. As informed by the PSR, these APIs and SDKs would deliver and enforce the usability and predictability requirements of the FPS, yet also provide Providers the necessary framework to develop fluid, branded, and convenient End-User experiences.

A common example of this programmatic approach is mentioned in E.4.1 (p119) and exemplified by OAuth 2.0. The open and standard protocol allows platforms to technically authenticate End Users and authorize permissions to third-party applications. To an End User, it provides a consistent and familiar flow that many are used across all industries, while branded elements help convey confidence.

---

and Provider-based hosting ensures safety. An example is using Facebook to sign and authorize third-party platforms, like the WSJ.

Step 1: Prompt
End User selects “Facebook” to register.

Step 2: Authenticate
End User is taken to Primary Provider’s platform to authenticate their identity.

Step 3: Authorization
Upon successful authentication, the primary platform relays the authorizations requests of the third-party transparently to the End-user for their approval. In this instance, the authorization request is for the End-user’s public profile information and the email.

Revocation:
Removing and managing authorizations follow a familiar format and is typically accessed through the Provider’s Account Settings.
The open protocol has been applied numerous times in finance and can be safely applied to FIs and RNAPs, such as Dwolla, to securely authorize permissions to third-party applications. In the example below, Dwolla presents a co-branded OAuth API to easily provide permissions to a third-party application (i.e. Dwolla Forms, a payment collection service from Dwolla) in a way that is predictable and secure.

**Step 1: Prompt**
End-users are taken to an Authentication Portal hosted by the selected Preferred Provider. Note the branding, but also the predictable and required elements of this interface. (e.g. Privacy, Legal, requesting Third-party, HTTPS, etc.)

**Optional:**
Aside from controlling branding and user interface, hosting the Authentication Portal also allows the Preferred Provider to enforce additional security requirements. In this case, a Dwolla End User attempting to authenticate is required to pass a multi-factor request.

**Step 3: Authorization**
Similar to the previous example, the Preferred Provider communicates the requested permissions of the Third-Party Platform.

**Revocation:**
End Users would be able to manage settings in a predictable manner through the Primary Provider.
An SDK and API approach can be applied programmatically or administratively to a range of experiences to help promote the Usability and Predictability of other End Users.

Questions back to proposer
U.2.4: How will the solution ensure a straightforward and simple end-user experience?

Aside from our response to the rationales of U.2 and U.3, a programmatic approach is well suited to create scalable and automated experiences that could be designed to complement the Accessibility recommendations provided by such groups as the W3C Web Accessibility Initiative (WAI) and other organizations that seek to foster inclusion of those that are disabled, elderly, or have low-English proficiency. Examples include, but are not limited to:

- Informing baseline Usability requirements for mobile experiences
- Text-to-speech availability
- Font sizing minimum
- Ensuring keyboard compatibility

Questions back to proposer
U.3.5: If a transaction is completed in error, and the payee does not return the funds, what recourse does the payer have?

The solution’s authentication and fraud service protects all entity types equally, as proposed herein. The hypothesis of the solution is that increased authentication and upfront notification will decrease unauthorized payments; further, the level of logging of device and behavior will better enable institutions to detect “friendly fraud”, or a customer falsely claiming they did not initiate a transaction. In order to comply with Reg. E, consumer accounts will still need to be made whole in the event of an unauthorized payment.

The payer would first need to dispute the payment; if the receiving bank had not made the funds available to the receiving customer, the receiving bank could, at their discretion return the funds. Otherwise, the funds would need to be recovered via outside means such as civil court. This is modeled after existing practices of other faster payments systems internationally, as well as current domestic practices with wire transfers. See Proposer’s response to S.5 for more information.

U.4 Contextual data capability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

Rationale
The solution enables contextual data capabilities using ISO20022 (U.4.1) and exchanges contextual data on payment orders, payment messages and payment receipts. Integrations of contextual data with interfacing businesses and personal finance systems can be through ISO20022 or JSON (U.4.2).

The approach to contextual data is flexible as the Solution is “metadata-based” and has customizable capabilities. Members and Providers collaborate across the network to create agreed-upon standards for passing Contextual Data elements such as agreeing to include an “Invoice Number” as an element within Contextual data (page 22). More detail is required on how the Solution will develop, scale and customize the standards, particularly for business payments.

Questions back to proposer
U.4.1: Please explain in more detail the concept of “customizable metadata.” How would “attributes be easily added and deprecated from the metadata based on provider agreement and adherence” (page 23)? How would business payments that require standardized fields be able to scale quickly in using this payment solution?

U.4.3: Would the operating rules and guidance provide standards for contextual data so that the data could be more easily integrated into common solutions?

The proposal outlines a solution that combines “Core” and “Optional” attributes to promote straight-through processing and customization.

“Core” attributes are required to ensure transfers facilitated by the Operator include the necessary information to process a payment. This includes items such as Date, Transfer ID, Amount, etc. The series of “Core” attributes are comprised of the data required for every use case supported by all Operators (enabling multi-operator transfers).

In order to facilitate efficiencies inside various use cases, the solution also identifies an “Optional” parameter delivered via a Metadata Object. The structure of the Metadata Object allows Schemes to accept parameters without impacting the straight-through processing provided by the “Core” elements. Throughout the proposal, the Metadata Object is referred to as “Contextual Data” providing the primary function of exchanging contextual data between End Users.

In addition to the contextual capabilities of the Metadata Object, the elegant design allows Scheme Owners to expand required elements for various use cases and—to the extent that these Metadata Objects are standardized—across Schemes. A couple potential examples include but are not limited to the following use cases:

<table>
<thead>
<tr>
<th>Business</th>
<th>Personal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Date</td>
</tr>
<tr>
<td>Transfer ID</td>
<td>Transfer ID</td>
</tr>
<tr>
<td>Payer UDID</td>
<td>Payer UDID</td>
</tr>
<tr>
<td>Payee UDID</td>
<td>Payee UDID</td>
</tr>
<tr>
<td>Operator ID</td>
<td>Operator ID</td>
</tr>
<tr>
<td>Routing Number</td>
<td>Routing Number</td>
</tr>
<tr>
<td>Amount</td>
<td>Amount</td>
</tr>
<tr>
<td>Payer Confirmation ID</td>
<td>Payer Confirmation ID</td>
</tr>
<tr>
<td>Payer Status</td>
<td>Payer Status</td>
</tr>
<tr>
<td>Payer Reason</td>
<td>Payer Reason</td>
</tr>
<tr>
<td>Payee Confirmation ID</td>
<td>Payee Confirmation ID</td>
</tr>
<tr>
<td>Payee Status</td>
<td>Payee Status</td>
</tr>
<tr>
<td>Payee Reason</td>
<td>Payee Reason</td>
</tr>
<tr>
<td>Auth ID</td>
<td>Auth ID</td>
</tr>
<tr>
<td><strong>Contextual Data</strong> (metadata)</td>
<td><strong>Contextual Data</strong> (metadata)</td>
</tr>
<tr>
<td>○ Invoice Number - 1234567A</td>
<td>○ Description - “Thanks for the coffee Jordan!”</td>
</tr>
<tr>
<td>○ Customer ID - 9876</td>
<td></td>
</tr>
<tr>
<td>○ Order Description - “Monthly payment for August 2016”</td>
<td></td>
</tr>
</tbody>
</table>

Within an individual Scheme, rules could set the standards for interpreting the Metadata Object. The sub-items, under the Contextual Data attribute, allow Scheme Owners to define standards on what attributes are required for a Business versus Personal End User. An example scenario could be a scheme that requires Payers to supply an invoice number in the Invoice Number attribute.

In defining these intra-Scheme standards, Scheme Owners should be explicit on which Contextual Data attributes are required by the sending and receiving the RNAP and FI rather than
arbitrary referential information. Below is an example of how an Invoice Number could be required for business transfers inside such a Scheme:

- **Payee Input** - Each Payee FI or RNAP is required to present an Invoice Number field and capture the information from the Payee.
- **Transfer Inclusion** - The Payee FI or RNAP is expected to include an “Invoice Number” sub-attribute within the metadata object on the Credit Request.
- **Payer Reference** - Each Payer FI or RNAP will display the Invoice Number to the Payer for contextual reference before the Payer authorizes the Credit Transfer.

The efficiency gains that are captured per use case would be informed heavily by the degree to which the Scheme Owners and/or PSR standardize the Metadata Object format and protocol for transactions across multiple Operators. Leveraging a messaging standard such as ISO20022, inter-Scheme transfers could enforce rules where Invoice Number is included in the “Max10Text” attribute of the PAIN message set. The FPS Operating Rules and Guidelines would provide an excellent medium for such clarity and a foundation for future use case expansion.

### U.5 Cross-border functionality

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**

The solution does not yet support cross-border payments. It defers the plan for later inclusion by “scheme owners” (depository institutions that “run their own FPS operator and infrastructure to facilitate and authorize clearing and settlement between members and other operators” - page 6).

**Questions back to proposer**

No questions

The proposed FPS is agnostic to use case, currency, and location. This proposer’s original cross-border strategy was designed to accommodate the current on-going domestic and international standardization initiatives and complement the business needs for a particular Scheme Owner. In light of the assessment, the proposer offers clarity on the following items identified by the QIAT:

**U.5.1**

Operators would facilitate and receive International payments on behalf of their participating Members. An agreed upon International Standard messaging format (e.g. ISO20022) would inform the necessary addressing and provide a convenient, effective, and timely cross border payment experience.

The security measures and precautions identified in S.1-S.11 apply to cross-border payments.

**U.5.2**

The adoption of international standards would be reliant on the collective acceptance of said standards by industry stakeholders and Fed-supported rails, but not on the technology framework of the proposed FPS. Message integrity, system security, format mapping, and risk management controls outlined in the document provide the submitters of this proposers confidence in the solutions capacity for adopting and supporting the interoperability needs of an approved standard and payment system rules.

**U.5.3**


The End-user experience of a cross-border transaction would mimic the guidelines and capabilities outlined in U.2 and U.3, including the satisfaction of regulatory consumer requirements (L.3). Those items unique to Cross-Border transactions (e.g. Exchange Rates, returns, etc.) would align with the spirit of transparency and ease of use of the system and further outlined in the PSR.

U.5.4

As noted in the proposal, the proposed FPS enables conversion through its delivery of a standardized message. The necessary logic for such conversion could be supplied as a utility by the Scheme or built/purchased by the Member FI.

U.5.5

The lack of an international standard for real-time cross-border settlement hinders our ability to provide a credible timeline; however, there has been a significant uptick in initiatives and programs to align with the many flavors of ISO 20022, both domestically13 and internationally14. We can look to such examples and industry collaborations and their timelines to create a framework for cross-border standardization and implementation. More specifically the “High-level implementation strategy for the Fedwire Funds Service and CHIPS”15:

Combined with ISO 20022 mapping and adoption efforts by NACHA and usage of an FPS, it’s with high confidence that industry stakeholders, regulators, Scheme Owners, and the Federal Reserve Board of Services would begin drafting rules, applying standards and testing service with the National Settlement Service (NSS) by the year 2018 (similar to FedWire timeline noted above) and subsequent rollout by 2020.

U.6 Applicability to multiple use cases

Very Effective Effective Somewhat Effective Not Effective Not Assessable

Rationale:
The solution supports all use cases and is extensible to future use cases. The design particularly supports targets consumer payments, such as P2P (person-to-person) payments.

Questions back to proposer

No questions

13 “NACHA Publishes ISO 20022 Mapping Guide” 20 April 2015
14 “First draft standard on ISO 20022 for real-time payments published” Finextra, 10 Aug 2015
15 “The Federal Reserve is making strides to adopt ISO® 20022 in the U.S.” FRB Services
Efficiency

E.1 Enables competition

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

Rationale:

The solution allows end users to choose among providers, to use multiple provider accounts, to specify payment preferences in the directory, and to switch providers (E.1.1-2). More clarity is needed about how “easily” end users can switch providers and specify payment preferences in the directory. Providers give end users advance disclosure of costs in accordance with the payment system rules (E.1.3). The Platform Services Layer enables all members, RNASs and Third Party Services access to the FPS to provide services as long as participation requirements are met (E.1.4).

Questions back to proposer

E.1.2: If an end user can associate multiple provider accounts with an alias in the directory, how do end users directly update the directory and how do end users send and receive money from and to different accounts?

End users update and manage the Directory information and primary preferences through an authorized FI or RNAP and their customer-facing interface (e.g. Online banking portal, mobile app, etc.). It is very possible that an End User has two different Preferred Providers, one for their Email and SMS. In such an instance, the End User uses the two interfaces provided by the Preferred Providers to send and receive money.

Standing relationships with other third-parties (e.g. invoicing software or trading account) is managed by the Directory and supported by the Preferred FI or RNAP. These relationships follow the payment flows discussed in Part A.

E.1.2: How would end-users be able to change their payment preferences in the directory? Would they have to go through their provider/member, or would they have direct access?

Authenticated and authorized FIs and RNAPs update and manage customer information at the request and with the authorization of their End User. The status information of an FI or RNAP in the Directory (e.g. Authentication Portal URL) is managed through secure API endpoints by the FI or RNAP. Introduced in the “Onboarding a New End-User” (p24-24) and “Adding an End User to the Directory” (p25), the Preference endpoint available to RNAPs and FIs allows authenticated End User’s to manage their default provider. To an End User, this may look like A) signing into your Provider, B) heading to settings, and C) “make Provider XYZ default FPS Provider for this Phone Number and/or Email”.

At this time, we see the Directory as a web-service, not as an End User interface.

E.1.3: How will rules and guidelines address requirements for disclosures to end-users?

As discussed in U.2 and U.3 the proposed FPS provides stakeholders a tool to programmatically inform, enforce, and constrain End-user experiences through the use of APIs and SDKs. These APIs and SDKs would be informed by the PSR and presented prior to a transaction.

E.2 Capability to enable value-added services

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

Rationale:

Providers integrate with the solution using open, accessible standards through the solution’s Platform Services Layer (E.2.1). The Platform Services Layer allows for tiered access to the
FPS, allowing for a broad range of safe participation by a wide variety of providers (E.2.2). For example, a Member brokering access to high-risk Third Party Services may limit daily transaction totals or require additional identity verification from end users. All value-added services are required to be disclosed as optional to customers (E.2.3).

**Questions back to proposer**

E.2.1: Please provide more details about the support provided for developers to leverage the open standards to create value-added services.

Under the proposed system, RNAPs and FIs are authorized to broker third-party development support and access to the FPS in much the same way Dwolla supports and provide access to third-party developers to the ACH system today via its APIs (p99). These may include, but not limited to:

- API and SDKs
- Compliance services (KYC, OFAC, AML, and more)
- Developer documentation (i.e. API documentation, guides, libraries, etc.) and sandbox environment
- InfoSec consultation
- Financial Intelligence and Fraud services and support
- Dashboard and Administrative tools for integrations
- Integration and dedicated customer support

RNAPs and FIs may build or license such services from Platform as a Service providers.

E.3 **Implementation timeline**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**

The proposal outlines a three-phased implementation plan that articulates activities and milestones over three years. It assumes a year for member integration and testing. However, the timelines does not address or include: 1) a plan for member adoption or for phasing in members over time, 2) an explanation of how implementation will be funded, 3) the hurdles to adoption that might arise, or 4) a partnership plan or list of potential providers/members.

**Questions back to proposer**

E.3.1: What is the plan for funding the solution? What type of FI will initially be targeted as members? Please provide further information regarding funding for implementation and partnership plans, or lists of potential providers/members.

1) “a plan for member adoption or for phasing in members over time”

The adoption and phasing plan is outlined in Part B, “Implementation Timeline” (p69) and “Integration Effort” (p89), specifically:

- System component and governance must be established prior to Member FI adoption.
- Upon the successful completion of a pilot period, the adoption and creation by Scheme (i.e. Member FIs) and its components may begin at any time.
- Assuming the successful completion of the required compliance reviews, governance audit, and stress tests by FPS Regulators, Scheme Owners are able to go live at any time.

2) “an explanation of how implementation will be funded”

---


17 Simulated environment and services used by developers to build and test prior to going live with an integration
Funding for the implementation of Scheme is provided by Member FIs and discussed in “Scheme Owners: Potential Implementation and Maintenance Costs” (p76)

3) “the hurdles to adaption that might arise”

As discussed in “General Assumptions” (p16, p90) and noted in Part B’s “Implementation Timeline”, many interdependencies exist outside the scope of the Task Force objectives, including:

- Regulatory oversight and the responsibilities of an FPS have yet to be defined.
- Without clear regulatory oversight or guidance, a path to ratifying FPS Operating Rules and Guidelines is unclear.
- ISO 20022 standard adoption timeline is undefined.
- No mandate or authority exists to compel participation in an FPS by stakeholders.

Additionally, other concerns not cited in the Proposal may affect Member adoption include:

- Technical capabilities of Member FIs
- Funding audits, stress tests, and other administrative requirements of the FPS Regulator

4) “a partnership plan or list of potential providers/members”

Schemes are developed at the behest of Member FIs. This aligns with current market trends (e.g. ClearXchange, Dwolla FiSync, and partnerships between The Clearing House and other core banking providers).

E.4 Payment format standards

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

Rationale:

ISO 20022 is the standardized format used for Payment Messages between Members and the Operator (E.4.1, E.4.5). The message format between Members and Providers is determined by the Member/Access Provider (e.g., JSON – JavaScript Object Notation or ISO messaging) and translated to ISO 20022. The solution does not yet support cross-border payments, but the message format enables cross border interoperability as ISO 20022 becomes an international standard (E.4.2).

More detail is needed on the Solution’s mechanism for updates to the message format in order to facilitate innovation and adaptability (E.4.4)

Questions back to proposer

E.4.1: Please elaborate on all of the messaging formats that the solution will be able to handle.

See “Proposal Assumptions” (p15), “Messaging Standards” (p20), and Criteria U.1.6 (p107), U.4.2 (p113).

E.4.3: What is the mechanism for updating the message format?

The messaging format between Members and [multiple] Operators and its evolution has benefits and consequences to the Scheme participants. While the infrastructure strives to provide API-based end points, which evolve but rarely deprecate required functionality, the path to a new format will require both approval and a rollout that does not break existing functionality.

An update request would follow a formal channel for submission with the relevant and required documentation as defined in G.1. Submission would initiate a workflow. The defined decision criteria via a matrix will define the path of the workflow and additional required actions, such as formal ISO proposals for message format changes or scheme notifications of new functionality and API endpoints to support the adaptations.
E.5 Comprehensive

**Very Effective**  Effective  Somewhat Effective  Not Effective  Not Assessable

**Rationale:**
The solution fully meets the sub-criteria: it enables all aspects of the end-to-end payment process (E.5.1), and its technical design supports all of its features (E.5.2).

Questions back to proposer
No questions

E.6 Scalability and adaptability

**Very Effective**  Effective  Somewhat Effective  Not Effective  Not Assessable

**Rationale:**
The technical design supports projected use cases (E.6.1) and has the capacity to handle projected volumes and values, based on adoption rates from the U.K. (E.6.2). Since the Solution enables Providers and Members to innovate around the customer experience and focuses on the exchange points of Operator, Directory and Fraud Sharing Service, changes can be made by the Operator, Providers, Members across the end-to-end payments process in response to technology, economics, regulations and customers (E.6.3).

Questions back to proposer
E.6.2: At the operator level, what is the transactions-per-second (TPS) capacity of the switch? Please provide further detail as to how the solution is expected to handle peak volumes and the lead time needed to scale up capacity.

As noted in the “Scalability and Adaptability” section (p101) the Operator is anticipating similar demand to the adoption in the United Kingdom. Leveraging cloud-computing services to scale all facets of the solution (outlined p102) to support the projected growth over a six-year period.

E.7 Exceptions and investigations process

**Effective**  Somewhat Effective  Not Effective  Not Assessable

**Rationale:**
The solution includes a mechanism to request a payment reversal and provides end-users with status updates on return requests (E.7.1). Timeframes for investigations are also integrated into the system, allowing members to receive alerts to ensure the timely resolution of disputes/exceptions. Additional tools are not mentioned. The operator monitors exceptions data to spot patterns and detect fraud. The Operator alerts Members when there is anomalous network activity. In addition the operating rules will define acceptable standards of exceptions by a given party (E.7.3).

The solution maintains exceptions data for a minimum of five years, but it does not address tools for post-transaction assessment or even for transaction trace-ability (E.7.2).

Questions back to proposer
E.7.1, E.7.2: Please provide further details about tools for handling exceptions within a reasonable timeframe and running post-transaction analyses.

Please see the response to S.5 in regards to handling exceptions.
Safety and Security

S.1 Risk management

Very Effective    Effective       Somewhat Effective    Not Effective    Not Assessable

Rationale:

More detail is needed on the Solution’s proposed risk management framework. The solution’s scheme owner will maintain a risk management framework that responds to changes such as the unexpected application of a law or regulation (S.1.1). Settlement risk is addressed by the Operator managing multilateral net positions by Member based on individual Member risk ratings. Analysis of volume by Member triggers settlements as volume reaches limit amounts. Settlement failures result in suspension of further transaction processing for the Member and its Providers and mitigating actions such as more frequent settlement windows or even suspension from the network (S.1.2). The risk of fraudulent or erroneous payments is addressed through a variety of prevention mechanisms, including multi-factor authentication to address fraud, and standardized content and presentment requirements to minimize the change of end user error (e.g., chance to confirm information is correct prior to transaction initiation) (S.1.4).

More information is needed on operational risks as well. Even if the human intervention needed to process a payment is minimal (as the proposal states on page 128), operational risk still exists (S.1.3). The proposal states that the FPS operating rules and guidelines will determine the incentives to providers and other participants to contain risk but provides no further detail (S.1.5).

Questions back to proposer

S.1.3: How is operational risk (beyond human error) considered in the foreseen framework?

As noted in S.7.1 (page 137), the risk management framework will provide guidance and controls based on the acquisition, implementation, delivery, support, monitoring and continual evaluation and improvement of the solution. The framework will be based on a selection of controls from known frameworks (such as COBIT, NIST, CIS, FedRAMP) with a preference for software, services and platforms which currently align with these control frameworks and provide existing capabilities in areas such as vendor management, DR/BCP, incident response, cost modeling/charging, etc.

The proposal has considered operational risk through the calibration and evolution of the framework which is based on the foundation provided by 1) the initial threat model (page 136) and 2) the continuous management of a risk register (page 141). The risk register will be updated no less than monthly with input from members, regulators and other parties to respond and adapt to changes and newly identified risks.

Operational risk will be managed through a combination of internal processes (such as access management, change management, Segregation of Duties via matrixed RBAC, etc.), leading security controls (such as MFA via Push Notifications, File Integrity and Process Monitoring against known and approved secure baselines, configuration as code using immutable architecture and dual-control for platform changes, routine vulnerability scanning and penetration testing, cryptographic key rotation and a bug bounty program to promote and control responsible disclosure of vulnerabilities).
S.2 Payer authorization

Very Effective   Effective   Somewhat Effective   Not Effective   Not Assessable

Rationale:
The solution requires payers to authorize to their member when initiating payments (S.2.1). Payers can pre-authorize payments based on a number of parameters (S.2.2) and can revoke pre-authorization easily and quickly (S.2.3).

Questions back to proposer
No questions

S.3 Payment finality

Very Effective   Effective   Somewhat Effective   Not Effective   Not Assessable

Rationale:
The solution requires the Payer's Depository Institution or Regulated Non-bank Account Provider to approve each payment following its initiation to assure that the payer's account has good funds (S.3.1). The payment is irrevocable once the payer’s provider receives the final “transaction complete” message (S.3.2). The Solution provides mechanisms and processes to protect or compensate the Payer in the event that the payment is disputed through a request for reversal, which gives the Payee the choice of automatically returning the funds or completing a manual review to determine whether or not to do so. In cases of fraud, the Member or Provider of the Payer limits a consumer’s liability as required by regulation (S.3.3).

Questions back to proposer
No questions

S.4 Settlement approach

Very Effective   Effective   Somewhat Effective   Not Effective   Not Assessable

Rationale:
Same-day settlement is performed using the Federal Reserve Banks’ National Settlement Service (NSS). To reduce overall risk exposure, funds are rebalanced across FIs every two hours during the FRB’s hours of operation (S.4.1-2). In addition, “If an FI has ongoing concerns about the operational account and negative balance scenarios, optional internal safeguards (e.g., contingency-funded accounts) may be leveraged” (page 133). Obligations are settled in central bank money (S.4.3).

Questions back to proposer
No questions

S.5 Handling disputed payments

Very Effective   Effective   Somewhat Effective   Not Effective   Not Assessable

Rationale:
The solution’s rules include requirements and processes for resolving unauthorized, fraudulent, erroneous, or otherwise disputed payments but do not include timeframes (S.5.1, S.5.3). The
standard process for resolving exceptions does not seem to go beyond a reversal process/request for return of funds (S.5.3), notifications of completion, and the use of a fraud information-sharing service. No process is described for cases in which the payee refuses to return the funds.

Ultimately, the end-user bears responsibility for the accuracy of the information submitted to a member, and there is no guarantee that an erroneous payment can be returned. Members are responsible if the end-user account is compromised. This approach may be adequate for consumer payments but will likely be challenged when applied to business payments (S.5.4-5). It is compliant with Reg. E, but Reg. E only covers consumers.

Questions back to proposer

S.5.1: If payments are irrevocable, but a dispute arises, what recourse do end-users—particularly payers—have after the request for funds? Please elaborate on the dispute procedure.

The solution’s authentication and fraud service protects all entity types equally, as proposed herein. The hypothesis of the solution is that increased authentication and upfront notification will decrease unauthorized payments; further, the level of logging of device and behavior will better enable institutions to detect “friendly fraud”, or a customer falsely claiming they did not initiate a transaction. In order to comply with Reg. E, consumer accounts will still need to be made whole in the event of an unauthorized payment.

The payer would first need to dispute the payment; if the receiving bank had not made the funds available to the receiving customer, the receiving bank could, at their discretion return the funds. Otherwise, the funds would need to be recovered via outside means such as civil court. This is modeled after existing practices of other faster payments systems internationally, as well as current domestic practices with wire transfers.

S.5.3: Please clarify the timing stipulated for returned transactions.

The timeframe for this to occur would be within the existing Reg E guidelines, which would be used for all entity types, not just consumers.

S.5.4: The proposal states that the solution is Reg. E-compliant, but how are business and government payers protected against losses from fraud or errors?

The solution’s authentication and fraud service protects all entity types equally, as proposed herein. The hypothesis of the solution is that increased authentication and upfront notification will decrease unauthorized payments; further, the level of logging of device and behavior will better enable institutions to detect “friendly fraud”, or a customer falsely claiming they did not initiate a transaction. In order to comply with Reg. E, consumer accounts will still need to be made whole in the event of an unauthorized payment.
The process would work as follows:

1. **Sender initiates payment**
2. **The Fraud Service provides Payer’s FI or RNAP with intelligence to assist in approving/denying the transfer**
3. **If approved, the Fraud Service then provides the Payee’s FI or RNAP with intelligence to assist in approving/denying the transfer**
4. **If approved, the funds settlement is final**
5. **Payer disputes payment via his or her Provider**
6. **Payer’s FI or RNAP flags the payment as disputed**
   a. Notification is sent to the Payee’s FI or RNAP bank
      i. If the Payee’s FI or RNAP has already approved the transfer, the Payee must voluntarily choose to return the funds (handled via API endpoints coded into Platform Services Layer)
         1. If the Payee chooses not to approve the reversal, the transfer dispute is marked as final, reversal not approved, with no further action required.
            a. The Sender will then need to seek 3rd-party recourse (small claims, collections, civil court, etc.) to recoup funds
         2. If the Payee chooses to approve the reversal, the transfer dispute is marked as final, reversal approved
      ii. If it has not been approved, the funds will be automatically returned with no further manual intervention required
         1. The transfer dispute will then be marked as final, automated reversal

There would be no differentiation in the process between government, commercial or consumer disputes. With the stated goal of settlement finality, returned payments will not be a routine occurrence as with existing systems such as card networks and ACH. The solution offers robust and layered levels of authentication of a user, along with meta-data and intelligence to improve sending and receiving banks’ decision making with regard to allowing a payment to be sent and received. Both the sending user, the sending bank, and the receiving bank all must explicitly approve a payment before the funds cannot be disputed.

1. The Proposers makes two main assertions in this regard:
   a. The solution provides levels of authentication beyond any current existing network, which should minimize the level of unauthorized payments.
   b. The speed of this solution, along with true settlement finality, will provide much greater macroeconomic benefits to users than the potential harm of irreversible payments.

### S.6 Fraud information sharing

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**

The solution meets all the criteria through its Fraud Sharing Service (S.6.6). The Solution requires information sharing in exchange for the aggregated, network-wide data analysis that gives Members real-time information about the status of an End User across the network (S.6.1, S.6.7). The Fraud Sharing Service provides guides with the list of data stored, retention schedule, and explanation of how data is used and how standardized messages are passed back to Members to feed fraud systems of Members (S.6.2, S.6.3).

**Questions back to proposer**

No questions
S.7 Security controls

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**
The solution meets all criteria across technical access components and controls (S.7.1), operational and procedural components and controls (S.7.2), and managerial policies and oversight (S.7.3).

**Questions back to proposer**
No questions

S.8 Resiliency

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**
While the approach to meet the solution’s “up-time” targets is clear, the targets themselves need to be specifically defined (S.8.1). The proposal addresses business continuity and disaster recovery plans through routine testing of scenarios (S.8.2). In addition, the system is API-driven with testing and risk-based change processes to mitigate systemic risk (S.8.3). Testing of business continuity and disaster recovery controls is supplemented by load testing, vulnerability scanning, penetration testing and simulated abuse (S.8.5).

More information is needed on the sufficiency of resources allocated to business continuity and resiliency (S.8.4).

**Questions back to proposer**

S.8.1: Please specifically define the solution’s up-time targets

*In order to provide a consistent, available network for real-time payments, the solution proposes a 99.99% up-time target.*

S.8.4: Please comment on the resources allocated to business continuity and disaster recovery (in terms of people assigned /funds committed), as well as the percentage of volume that will be held in a fail-over event.

*Each RNAP and Member must demonstrate BCP/DR capabilities during on-boarding and have at least 1 full time person dedicated to this function. This person or persons would be responsible for compliance with expected controls, tests and documentation for BCP/DR exercises and tests. These deliverables will include detailed DR plans specific DR metrics for RTO’s and RPO’s and a frequency of testing to be no less than annual. Funding for BCP/DR resources and activities would be targeted for approximately 3% of the overall solution annual budget. As vendors, platforms and software are chosen, a preference for those with existing DR capabilities will be given.*

*The industry average among those who do measure DR spending indicated between 2% and 7% of their IT budget is devoted to DR activities*\(^\text{18}\).*

S.9 End-user data protection

Very Effective Effective Somewhat Effective Not Effective Not Assessable

Rationale:
The solution requires controls and cryptographic protections to protect end-user data in transit and at rest from Participants and the central infrastructure (S.9.1). The Directory limits the need for sensitive information to be sent across the network for account setup, transaction setup, problem resolution, and payment completion (S.9.2, S.9.3).

Questions back to proposer
No questions

S.10 End-user/provider authentication

Very Effective Effective Somewhat Effective Not Effective Not Assessable

Rationale:
While Members are responsible for end-user authentication, Payment System Rules define a base level of authentication (S.10.1). The Directory is used to ensure the payment is destined to reach the intended Payee, though other mechanisms such as a pre-notification or “test message” are not addressed. The Solution aligns with regulatory guidance and industry standards for authentication (S.10.3).

The Solution leaves risk-weighting procedures and adoption of new and decommissioning of old authentication models up to the depository institution (S.10.4-5).

Questions back to proposer
S.10.1: What is the base level of authentication that will be required from Members?
As noted in “Component Authentication section (p39), the base level of member authentication will be Multifactor leveraging out-of-band push notifications, TOTP codes and/or digital certificates. The expectation is to authenticate every time-based session or, on a trusted device, providing a re-authentication timeframe determined by a risk score and not to exceed 15 days.

S.11 Participation requirements

Very Effective Effective Somewhat Effective Not Effective Not Assessable

Rationale:
The FPS Regulator will develop the FPs Operating Rules and Guidelines and the Schemes may place additional requirements on Providers. However, these rules are not yet developed (S.11.1, S.11.2).

The Scheme will have a risk management program with annual self-assessment and third party independent audit performed and made available to the public to support compliance and monitoring of all Providers against the rules and requirements (S.11.3).

Questions back to proposer
No questions

To clarify this portion of the proposal further, S.1.2 (p121) of the proposal states that a CAMELS type of rating will be assigned by the FPS Operator to each Participant. As this rating is assigned, areas of deficiency will be addressed with Participants, with plans of action and milestones managed and negotiated between the FPS Operator and Participant.
See Proposers’ Response to QIAT Rationale and Questions in S.1 of this document for more information on Risk Management.

**Speed (Fast)**

**F.1 Fast approval**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**
The Solution expects payment approval within two seconds of payment initiation. However, the scheme operator, providers and operating rules ultimately control the timing of approval.

**Questions back to proposer**
No questions

**F.2 Fast clearing**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**
The Solution expects payments to clear within two seconds of payment initiation. However, the scheme operator, providers and operating rules ultimately control the timing of clearing.

**Questions back to proposer**
No questions

**F.3 Fast availability of good funds to payee**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**
The Solution expects the Payee’s member institution to approve or deny a payment within one minute. After the payee accepts the payment, funds will be immediately available for withdrawal. However, the scheme operator, providers and operating rules ultimately control the timing of availability of good funds.

**Questions back to proposer**
No questions

**F.4 Fast settlement among depository institutions and regulated non-bank account providers**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**
Settlement occurs through NSS, so transactions are settled in the same-day or next day without settlement services on weekends. Thus, the rating is “not effective” since settlement speed can
be next day or longer. Accounts are rebalanced every two hours to reduce the risk associated with Deferred Net Settlement (F.4.1).

The Solution does not address differences in time zones for settlement (F.4.2). Regarding flexibility of settlement timing (F.4.3), if a Member raises a credit or liquidity risk concern, the Solution can conduct an ad hoc settlement.

Questions back to proposer

F.4.3: What settlement mechanism is used for ad-hoc real-time settlement?

The Federal Reserve has outlined a phased plan to enhance the existing National Settlement Service (NSS). With the first two phases focused on expanding business day operations, Phase 3 concentrates on the exploration “weekend and/or 24x7 operating hours” support as early as 201619.

In addition to its public content, the Federal Reserve has explained NSS operations would scale to meet the increase in demand should it be used as settlement mechanism for a real-time payments system.

Based on the outlined volume projections (p101), NSS could be expanded concurrently with the FPS rollout activities over the initial two-year implementation timeline (p70):

- Year 1 - Support the expanded NSS operational hours.
- Year 2 - Full 24x7 expansion of support for NSS operation.

The concurrent approach is ultimately focused on reducing the risk associated with a Deferred Net Settlement solution. Settling every two hours, each calendar day, the settlement risk is greatly minimized to small windows of activity.

In addition to the standard two-hour settlement periods, ad-hoc settlements can be conducted to reduce liquidity risk for any individual participant. The ad-hoc settlements will also leverage NSS and available 24x7.

F.5 Prompt visibility of payment status

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

Rationale:

The Solution expects the Payment status to be visible to end users within five seconds. However, the scheme operator, providers and operating rules ultimately control the timing of availability of good funds.

Questions back to proposer

No questions

Legal

L.1 Legal framework

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

Rationale:

Providers are expected and required to comply with existing laws and regulations, as well as with the FRB’s applicable rules and regulations (L.1.1). There are no gaps in legal sources identified (L.1.2), but also no description of how the Solution plans to address legal gaps and changes that may arise in the future. The Solution requires Members and Providers to enter into agreements with End Users governing use of services (L.1.3). The Solution supports compliance with

relevant U.S. laws by end-users, members, and providers (L.1.4). The proposal does not identify any unique provisions needed to address situations in which end-users would perform the same functions in the payment system but would be subject to different laws or regulatory supervision (L.1.5), but it does not explain how the solution will reconcile potential conflicts between guidance from members’ governing bodies and regulatory guidance.

Questions back to proposer

L.1.2, L.1.5: How will you address gaps in legal sources and different laws or guidance to different Members and Providers coming from governing and regulatory bodies?

As noted in our response to L.1.3 (p148), all Members and Providers will be required to enter into agreements with End Users governing the End Users’ use of the Members’ and Providers’ services, including any services enabled by the Solution. As noted in that same response, the Solution’s Payment System Rules may require the addition of certain language in Members’ and Providers’ agreements with End Users. We will use those End User agreements to address any potential gaps, changes, and/or conflicts in legal sources and different laws or guidance to different Members and Providers coming from governing and regulatory bodies. The governance structure of the Solution allows for amendments or updates to such End User agreements as needed to efficiently deal with those issues as they may arise (e.g., by allowing for unilateral changes to End User agreements by the Members and Providers to address such issues).

L.2 Payment system rules

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

Rationale:

The Solution describes key features of Payment System Rules across the end-to-end payments process (L.2.1).

The proposal acknowledges a need for Payment System Rules and sets out a path to complete them, but they are not yet complete. The QIAT has interpreted the Effectiveness Criteria such that Solutions at this stage of development earn a rating of “Somewhat Effective”; once the element has been completed and/or more details are available, the rating may change.

Questions back to proposer

L.2: Please provide more details regarding the Payment System Rules, including requirements, standards/protocols and procedures that govern the rights and obligations of all End Users, Providers, Payers and Payees. In doing so, please specifically address how the Solution supports the five Payment System Rules subcriteria.

As discussed throughout our Proposal and during our follow-up session with the QIAT, we view the Governance structure and specifically in this context the Payment System Rules as criterion that transcend our individual Solution and a responsibility that should be shared by all stakeholders. We have set forth a Governance framework that is flexible and pragmatic and intended to foster collaboration and stakeholder buy-in, which involves the development of Payment System Rules that specifically address all of the Payment System Rules subcriteria (see cites on pp149-50). Throughout those proposals (see cites on p.) we have clearly set forth the guardrails for the development of Payment System Rules. These guardrails will be the foundation of the Payment System Rules, which will be further refined and adopted by all of the Scheme Owners.
L.3 Consumer protections

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**

The legal framework consists of Reg. E requirements and the rules/regulations for the FRB-supported settlement mechanisms.

The proposal acknowledges a need for consumer protections, but they are not yet complete. The QIAT has interpreted the Effectiveness Criteria such that Solutions at this stage of development earn a rating of “Somewhat Effective”; once the element has been completed and/or more details are available, the rating may change.

**Questions back to proposer**

L.3: Please provide more details regarding consumer protections, including a Legal Framework and procedures that allocate legal and financial responsibility and support Error Resolution. In doing so, please specifically address how the Solution supports the three consumer protections subcriteria.

As set forth in our Proposal (p.150), the legal framework for our Solution will address consumer protection by using the existing consumer protections found in Regulation E as well as any rules and regulations that either exist today or may exist in the future for any Fed-supported rails used by the Solution. This framework for consumer protections exists today and will allocate legal and financial responsibility as required by subcriteria L.3.1. Regulation E also sets forth Error Resolution procedures that the Solution will rely on as required by subcriteria L.3.2. The Solution will also include Error Resolution protections for irrevocable electronic consumer payments, which will require messages built into the Solution to allow the sending financial institution to request the receiving financial institution return the payment in cases of fraud or error by the consumer. The requirement for all End Users to sign an End User agreement allows all participants to offer greater consumer protections than those required under Regulation E and other existing rules and regulations (thus satisfying subcriteria L.3.3)

L.4 Data privacy

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

**Rationale:**

The Solution requires Members and Providers to maintain a privacy policy and data shared with Members and Providers may only be used for the purposes of processing a payment and fraud management, subject to express authorization by an End User to use data for other purposes (L.4.1). Data is secured through operational procedures that ensure protection of data in transit and at rest (L.4.2). The Solution also lists the nature and type of end-user data required for use (L.4.3).

The solution does not provide detail on how end users may get visibility into the Data being collected on them, limit sharing of such data and change privacy preferences (L.4.4), other than stating that end users have a choice to not use the Solution. In addition, more detail is needed on the approach to data breaches at the Payment System or End user/Provider including clarification on how the legal framework allocates financial and other responsibilities among end-users, members, and providers in the event of a data breach (L.4.5), as well as more details about responsibilities related to notification, root-cause analysis, and processes in response to data breaches.

**Questions back to proposer**

L.4.1: Please list specific data privacy laws with which members will be required to comply

*On p147-48 we outline a list of existing laws which members will be required to comply, which list included several data privacy laws or laws with data privacy elements (GLBA, FCRA, Consumer*
Financial Protection Act, Reg E, OFAC, BSA/AML, UIGEA, and state data breach notification rules).
In addition the members will be required to comply with the FTC Act, HIPAA, the CAN-SPAM Act, the Telephone Consumer Protection Act, and any state privacy laws (e.g., the California Online Privacy Protection Act) to the extent such laws apply to them.

L.4.4: How will end users get visibility into the Data collected on them and the ability to change preferences?

The Solution is intentionally designed so that data shared with Member and Providers via the Solution may only be used for the purposes of processing a payment through the Solution (and the Solution will ensure the End User is clearly informed of that), unless the End User expressly authorizes the Member and/or Provider to use the End User’s data for other purposes. Thus the Member and/or Providers must collect authorization from the End User to use the End User’s data for any other purpose and will be required to inform the End User on how such data is being transferred, who has access to it, how the data can be used, and potential risks and allow End Users an easy mechanism to change preferences.

L.4.5: Please describe the processes for responding to a data breach, including steps such as notification (consumers, operators, regulators, governments, etc.), timing of notification, root-cause analysis, and other relevant steps (e.g., remediation for consumers). Please include in the description how financial losses will be accounted for and assigned.

As noted on p151, the Solution will require Members and Providers to comply with existing state and federal laws and regulations in the event of a data breach. The processes for responding to a data breach, including steps such as notification, timing of notification, root-cause analysis, accounting for financial losses, and other relevant steps, will be determined by existing law and/or in conjunction with the other stakeholders if gaps exist.

L.5 Intellectual property

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

Rationale:
The proposer is confident that the solution does not infringe on intellectual property rights, however, more details are needed. Beyond stating that the proposer would undertake an appropriate review when necessary (page 152), there is no proposed approach to handling IP infringement, should issues arise.

Questions back to proposer

L.5.1: What is the approach to resolve or manage legal, operational or financial risks arising from third party intellectual property rights?

As noted on p152, Dwolla will undertake an appropriate review that the Solution does not infringe any third party intellectual property rights. The Solution’s Legal Framework will require each participant to assume liability for any IP infringement by such participant.

Governance

G.1 Effective governance

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

Rationale:
The solution’s governance arrangements are publically disclosed (G.1.2). The solution relies on members to conduct self-assessments and to arrange third-party independent audits (G.1.4).
However, the proposal does not articulate the decision- and rule-making process, arrangements, or approach (G.1.1), nor does it describe the appeals process for decisions (G.1.3).

Questions back to proposer

Please provide more detail on the Governance sub-criteria.

The response below seeks to provide further specificity on Governance while balancing the Proposer’s desire for a more inclusive and collaborative Framework Approach noted on page 3 of this document.

The solution's governance organization could base its model on the COSO Framework covering operations, reporting and compliance activities across the solution. The governance organization would create a board of directors to demonstrate independence and provide oversight to the control environment and organizational proposals and decisions. The governance organization would define a code of conduct to ensure consistency with ethical, legal, and professional standards. The management of the governance organization, with board oversight, would define decision-making criteria for the implementation of rules, agreements and controls using a majority-approved matrix and voting process. Appeals to decisions such as evaluations, control deficiencies or the implementation of governance elements would follow a formal process submitted to management with relevant and required documentation. A formal review will be performed by management and if required, escalation to the board level for mediation. We further elaborate on the appeals process in our response to section G.2.

G.2 Inclusive governance

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
<th>Not Assessable</th>
</tr>
</thead>
</table>

Rationale:

The proposal provides high-level information on inclusive governance plans, but more detail is needed, including: 1) how governance arrangements will allow stakeholders to have input (G.2.2), 2) how stakeholders’ interests and risks will be represented in governance and advisory bodies (G.2.3), and 3) how specific stakeholders will proportionately influence outcomes (G.2.4), 4) how the governance approach would address and manage actual, perceived, or potential conflicts of interest (G.2.5)

Questions back to proposer

Please provide more detail on the Governance sub-criteria.

The response below seeks to provide further specificity on Governance while balancing the Proposer’s desire for a more inclusive and collaborative Framework Approach noted on page 3 of this document.

The governance organization could solicit input from its members using a defined channel for questions, proposals and other considerations. The channel would require authentication and a standard form for submission and will display a workflow as the inquiry is worked by management of the governance organization. The workflow would provide transparency and timely feedback for inquiries.

Stakeholders and their organizational feedback could flow through their scheme representatives that are authorized/defined by the governance organization. The board could follow existing rule making and enforcement organizations, like NACHA, with the notable additions of End-user groups (e.g. consumers, business, government) and standards body representatives to serve directly on the board or as advisors. Board participants capture, consolidate and submit feedback to the governance organization via the previously mentioned workflow. The governance organization’s decision matrix and appeals process would cascade into the workflow status as applicable.

An ethics hotline could be established to capture anonymous complaints and feedback. An independent 3rd party would manage this hotline and a formal channel to the board of directors.
established to review, investigate and act upon hotline submissions based on the previously mentioned code of conduct. The Proposers believe this industry-accepted practice—a combination of the formal stakeholder feedback channel and ethics hotline—would address the actual, perceived or potential conflicts of interest.
Appendix A: Questions for Proposer

Ubiquity

U.1.2: How can a payee be reached if s/he does not bank at a member depository institution? The process for enrollment requires choosing a member FI or an RNAP that is part of the network.

U.1.5: What are the economic incentives to get FIs and RNAPs to adopt and promote the system? How will Dwolla achieve minimum, viable endpoint utility at launch?

U.1.6: Does the Solution include multiple operators or networks? How do payments from one operator/network reach a Payee in another operator/network?

U.2.4: How will the solution ensure a straightforward and simple end-user experience?

U.3.5: If a transaction is completed in error, and the payee does not return the funds, what recourse does the payer have? U.4.1: Please explain in more detail the concept of “customizable metadata.” How would “attributes be easily added and deprecated from the metadata based on provider agreement and adherence” (page 23)? How would business payments that require standardized fields be able to scale quickly in using this payment solution?

U.4.3: Would the operating rules and guidance provide standards for contextual data so that the data could be more easily integrated into common solutions?

Efficiency

E.1.2: If an end user can associate multiple provider accounts with an alias in the directory, how do end users directly update the directory and how do end users send and receive money from and to different accounts?

E.1.2: How would end-users be able to change their payment preferences in the directory? Would they have to go through their provider/member, or would they have direct access?

E.1.3: How will rules and guidelines address requirements for disclosures to end-users?

E.2.1: Please provide more details about the support provided for developers to leverage the open standards to create value-added services.

E.3.1: What is the plan for funding the solution? What type of FI will initially be targeted as members? Please provide further information regarding funding for implementation and partnership plans, or lists of potential providers/members.

E.4.1: Please elaborate on all of the messaging formats that the solution will be able to handle.

E.4.3: What is the mechanism for updating the message format?

E.6.2: At the operator level, what is the transactions-per-second (TPS) capacity of the switch? Please provide further detail as to how the solution is expected to handle peak volumes and the lead-time needed to scale up capacity.

E.7.1, E.7.2: Please provide further details about tools for handling exceptions within a reasonable timeframe and running post-transaction analyses.

Security

S.1.3: How is operational risk (beyond human error) considered in the foreseen framework?

S.5.1: If payments are irrevocable but a dispute arises, what recourse do end-users (particularly payers) have after the request for funds? Please elaborate on the dispute procedure.

S.5.3: Please clarify the timing stipulated for returned transactions.
S.5.4: The proposal states that the solution is Reg. E-compliant, but how are business and government payers protected against losses from fraud or errors?

S.8.1: Please specifically define the solution’s up-time targets

S.8.4: Please comment on the resources allocated to business continuity and disaster recovery (in terms of people assigned/funds committed), as well as the percentage of volume that will be held in a fail-over event.

S.10.1: What is the base level of authentication that will be required from Members?

**Speed (Fast)**

F.4.3: What settlement mechanism is used for ad-hoc real-time settlement?

**Legal**

L.1.2, L.1.5: How will you address gaps in legal sources and different laws or guidance to different Members and Providers coming from governing and regulatory bodies?

L.2: Please provide more details regarding the Payment System Rules, including requirements, standards/protocols and procedures that govern the rights and obligations of all End Users, Providers, Payers and Payees. In doing so, please specifically address how the Solution supports the five Payment System Rules subcriteria.

L.3: Please provide more details regarding consumer protections, including a Legal Framework and procedures that allocate legal and financial responsibility and support Error Resolution. In doing so, please specifically address how the Solution supports the three consumer protections subcriteria.

L.4.1: Please list specific data privacy laws with which members will be required to comply

L.4.4: How will end users get visibility into the Data collected on them and the ability to change preferences?

L.4.5: Please describe the processes for responding to a data breach, including steps such as notification (consumers, operators, regulators, governments, etc.), timing of notification, root-cause analysis, and other relevant steps (e.g., remediation for consumers). Please include in the description how financial losses will be accounted for and assigned.

L.5.1: What is the approach to resolve or manage legal, operational or financial risks arising from third party intellectual property rights?

**Governance**

Please provide more detail on the Governance sub-criteria.
Appendix B – Transcript of Proposer Comments

Proposer Written Comments

< Full written comments submitted from the proposer to the QIAT>
Faster Payments QIAT

DRAFT ASSESSMENT

Property of the Federal Reserve Bank of Kansas City and the Federal Reserve Bank of Chicago ("Banks")

Not for distribution or publication without the express written permission of the Banks
Faster Payments QIAT

**DRAFT ASSESSMENT**

**Proposer:** Dwolla, Inc.

**Summary Description of solution:**

Dwolla is a digital payment network and platform for real-time payments with immediate availability of good funds. The solution is an end-to-end Faster Payments System (FPS) comprising:

- Federal Reserve as the FPS Regulator
- An FPS “Scheme Owner/Operator” that operates the clearing and settlement infrastructure between members. The solution involves real-time clearing and deferred net settlement through the Federal Reserve’s National Settlement Service (NSS). To reduce overall risk exposure, funds are rebalanced across FIs every two hours during the FRB’s hours of operation.
- Depository institutions as member-owners of the FPS scheme. These members can: 1) serve as direct providers of faster payment services to end-users, 2) offer FPS access or services to a third-party service (e.g., Uber) as an access provider, and/or 3) offer FPS access or services to a Regulated Non-bank Account Provider (RNAP) (e.g., PayPal) as a “sponsoring member”
- Providers that deliver, facilitate, or enable access to the FPS by end-users through products, services, or APIs
- A directory or federation of directories serving as a secure, standalone repository that enables anyone to send and receive payments using just an email or phone number. Users may also store payment preferences in the directory
- A Fraud Sharing Service, which the Operator maintains separately, to collect and distribute data and conduct analysis across the platform to spot high risk activity

**EXECUTIVE SUMMARY OF THE PROPOSAL**

**Major strengths**

- The solution facilitates competition by allowing end-users to choose among providers, to use multiple provider accounts, and specify payment preferences in the directory. Providers, both banks and RNAPs, can develop value-added services by integrating with the solution using open, accessible standards through the solution’s Platform Services Layer.
- The solution’s messaging format will help to ensure interoperability. ISO 20022 will be the format for payment messages to and from members and the operator; messaging between providers and members will be determined by the member and translated to ISO 20022. Schemes will be enabled to collaborate with Members and Providers to develop agreed upon standards for contextual data (attributes in the metadata).
- The solution meets the criteria for speed: Payments are expected to be approved and cleared within two seconds of payment initiation. The payee’s member institution is expected to approve or deny a payment within one minute. After the payee accepts the payment, funds will be immediately available for withdrawal. Payment statuses are available within five seconds.

**Areas for improvement and enhancement**

- The solution uses existing settlement systems through its use of NSS, but without enhancement of NSS to 24/7 and weekend operations, the speed of settlement can take over a day.
- The solution’s rules include requirements and processes for resolving unauthorized, fraudulent, erroneous, or otherwise disputed payments but do not include timeframes or a process for cases in which the payee refuses to return the funds, other than indicated disputed payments would be settled outside the solution through civil court. The standard process is limited to a reversal process/request for return of funds and notifications of completion.

- Details on legal and governance yet are to be developed since the proposal notes that governance and rules “transcend the individual systems, stakeholders, and use cases and are uniquely shared and uniformly applied in most cases.” The proposal does articulate a framework approach to legal and governance.

■ Use cases addressed

The solution addresses all four major use cases (P2P, P2B, B2P, and B2B). It does not yet support cross-border payments, deferring the future plan for these to scheme owners.

■ Proposer’s overall ability to deliver proposed solution

- Dwolla is an established payments solution provider that currently provides a bank transfer solution

- The solution uses existing, adapted and improved applications and processes of Dwolla’s current Network, Platform, Services and Immediate Funds Transfer System. Thus, the QIAT has high confidence in the ability to deliver the technical solution
# ASSESSMENT

## Ubiquity

### U.1 Accessibility

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution facilitates payments to/from all types of accounts—savings, checking, and others—across Depository Institutions, Regulated Non-bank Account Providers (RNAP) and third-party providers (U.1.1).

End Users can enroll with a Member depository institution or RNAP. First-time payees that are not part of the directory can also enroll; the Payer’s Member engages the payee via a notification to email or mobile phone, and the payee is then taken through the registration process in order to receive the transfer. This helps ensure that Entities’ payments can reach any and all Payees (U.1.2).

For multi-currency transactions, the solution supports any transfer, so long as end-points can accept the currency (U.1.3). However, the ability to handle multi-currency is dependent on providers, and interbank settlement processing for multi-currency is being explored. It is not clear how solution would ensure the same SLAs for a multi-currency offering.

The ability to send and receive payments from RNAPs and third parties supports the needs of the unbanked and underserved. (U.1.4). In addition, innovations for consumers without access to SMS or email include vouchers for redemption and prepaid cards.

The solution is technically feasible for Providers to adopt and the potential for new revenue generating products and services is the motivation for Providers to adopt the solution (U.1.5). The solution achieves interoperability across operators (U.1.6).

### U.2 Usability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution enables a straightforward, simple end-user experience by allowing Providers to build FPS capabilities and experiences across devices and channels, thereby enabling initiation of payment with just an email or phone number (U.2.1-2). The FPS is available 24x7x365. The payee’s member FI is expected to approve or deny a payment within one minute. After the payee accepts the payment, funds are immediately available for withdrawal (U.2.3).

Providers use the solution’s Platform Services Layer (PSL) to build end-user experiences; the PSL uses APIs and SDKs to deliver and enforce usability requirements while giving Providers the framework to innovate on the end user experience.
U.3 Predictability

**Very Effective**

**Effective**

**Somewhat Effective**

**Not Effective**

**Rationale:**

The solution’s baseline, core features are well-defined and the solution’s design ensures their delivery (U.3.1). The communication of baseline features in the payment experience is the responsibility of the FPS Regulator and Scheme owner, but the Proposer offers suggestions on authentication, timing, and acknowledgment of costs (U.3.2). The solution uses standard messaging and protocols between the FPS operator and providers, but leaves Providers to decide on the messaging standard and protocols used to deliver the end-user’s experience (U.3.3). The error resolution process follows processes similar to the UK’s Faster Payments Service (U.3.5). The solution is “brandless”; however, terms suggested to distinguish the solution from other payment methods include Advanced Clearing Exchange (ACE), Digital Asset Transfer Architecture (DATA), Digital Asset Real-time System (DARTS), and FiSync or Sync (U.3.6). The PSL ensures a base level of predictability through its APIs and SDKs that ensure consistency of experience in feature functionality (U.3.4).

U.4 Contextual data capability

**Very Effective**

**Effective**

**Somewhat Effective**

**Not Effective**

**Rationale:**

The solution enables contextual data capabilities using ISO20022 (U.4.1) and exchanges contextual data on payment orders, payment messages and payment receipts. Integrations of contextual data with interfacing businesses and personal finance systems can be through ISO20022 or JSON (U.4.2). The approach to contextual data is flexible as the solution is “metadata-based” and has core attributes as well as customizable or optional attributes. Members and Providers collaborate across the network to create agreed-upon standards for passing Contextual Data elements such as agreeing to include an “Invoice Number” as an element within Contextual data (U.4.3).

U.5 Cross-border functionality

**Very Effective**

**Effective**

**Somewhat Effective**

**Not Effective**

**Rationale:**

The solution does not yet support cross-border payments. It defers the plan for later inclusion by “scheme owners” (depository institutions that “run their own FPS operator and infrastructure to facilitate and authorize clearing and settlement between members and other operators” - page 6). However the solution’s technical capability can support cross-border, particularly using ISO20022.

Further detail on the plan for implementing cross border payments in the future would be helpful, particularly on addressing typical challenges (e.g., Provider adoption, payment limits, settlement cycles, pre-funding rules) (U.5.5).
U.6 Applicability to multiple use cases

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**

The solution supports all use cases and is extensible to future use cases. The design particularly supports targets consumer payments, such as P2P (person-to-person) payments.

Efficiency

E.1 Enables competition

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**

The solution allows end users to choose among providers, to use multiple provider accounts, and to specify payment preferences in the directory (E.1.1-2). End users cannot update the Directory directly but must update the Directory only through an authorized FI or RNAP and their customer-facing interface. Providers give end users advance disclosure of costs in accordance with the payment system rules (E.1.3). The Platform Services Layer enables all members, RNAPs and Third Party Services access to the FPS to provide services as long as participation requirements are met (E.1.4).

The solution would be enhanced with more clarity on how easy it is for an Entity to switch Providers – while the solution enables end users to use multiple Providers and associate an email address with one Provider and an SMS with another Provider, more clarity would be helpful on how the end user can easily choose to switch the Provider associated with an email or SMS.

E.2 Capability to enable value-added services

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**

Providers integrate with the solution using open, accessible standards through the solution’s Platform Services Layer (E.2.1). The Platform Services Layer allows for tiered access to the FPS, allowing for a broad range of safe participation by a wide variety of providers (E.2.2). For example, a Member brokering access to high-risk Third Party Services may limit daily transaction totals or require additional identity verification from end users. All value-added services are required to be disclosed as optional to customers (E.2.3).
E.3 Implementation timeline

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The proposal outlines a three-phased implementation plan that articulates activities and milestones over three years. It assumes a year for member integration and testing. Funding is provided by Members who are incented to participate through the opportunity for new revenue generating products and services. The new scheme formation to gain adoption by FIs is slated for phase 1 but may take well more than a year unless clear incentives for Member FIs to join over over alternative options.

E.4 Payment format standards

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
ISO 20022 is the standardized format used for Payment Messages between Members and the Operator (E.4.1, E.4.5). The message format between Members and Providers is determined by the Member/Access Provider (e.g., JSON – JavaScript Object Notation or ISO messaging) and translated to ISO 20022. The solution articulates a mechanism for updates (E.4.4). The solution does not yet support cross-border payments, but the message format enables cross border interoperability as ISO 20022 becomes an international standard (E.4.2).

E.5 Comprehensive

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution fully meets the sub-criteria: it enables all aspects of the end-to-end payment process (E.5.1), and its technical design supports all of its features (E.5.2).

E.6 Scalability and adaptability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The technical design supports projected use cases (E.6.1) and has the capacity to handle projected volumes and values, based on adoption rates from the U.K. (E.6.2). Since the solution enables Providers and Members to innovate around the customer experience and focuses on the exchange points of Operator, Directory and Fraud Sharing Service, changes can be made by the Operator, Providers, Members across the end-to-end payments process in response to technology, economics, regulations and customers (E.6.3).

The proposal would be enhanced with articulating the transactions per second capacity of the solution to support its ability to increase capacity and handle transaction volumes at peak times or periods of stress (E.6.2).
E.7 Exceptions and investigations process

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
Timeframes for investigations are also integrated into the system, allowing members to receive alerts to ensure the timely resolution of disputes/exceptions. The solution maintains exceptions data for a minimum of five years (E.7.2). The operator monitors exceptions data to spot patterns and detect fraud. The Operator alerts Members when there is anomalous network activity. In addition the operating rules will define acceptable standards of exceptions by a given party (E.7.3).

The solution includes a mechanism to request a payment reversal and provides end-users with status updates on return requests, however more detail on the tools and related protocols provided to Members or end users to support the ability to resolve transactions would be helpful (E.7.1).

Safety and Security

S.1 Risk management

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution’s scheme owner will maintain a risk management framework that responds to changes such as the unexpected application of a law or regulation (S.1.1). Regarding settlement risk, the Operator manages multilateral net positions by Member based on individual Member risk ratings. Analysis of volume by Member triggers settlement as volume reaches limit amounts. Settlement failures result in suspension of further transaction processing for the Member and its Providers and mitigating actions such as more frequent settlement windows or even suspension from the network (S.1.2). Operational risk is managed through internal process controls and security controls (S.1.3). The risk of fraudulent or erroneous payments is addressed through a variety of prevention mechanisms, including multi-factor authentication to address fraud, and standardized content and presentment requirements to minimize the change of end user error (e.g., chance to confirm information is correct prior to transaction initiation) (S.1.4). The proposal states that the FPS operating rules and guidelines will determine the incentives to providers and other participants to contain risk such as fees, suspensions, fines (S.1.5).

S.2 Payer authorization

Very Effective  Effective  Somewhat Effective  Not Effective

Rationale:
The solution requires payers to authorize to their member when initiating payments (S.2.1). Payers can pre-authorize payments based on a number of parameters (S.2.2) and can revoke pre-authorization easily and quickly (S.2.3).
S.3 Payment finality

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution requires the Payer's Depository Institution or Regulated Non-bank Account Provider to approve each payment following its initiation to assure that the payer's account has good funds (S.3.1). The payment is irrevocable once the payer’s provider receives the final “transaction complete” message (S.3.2). The solution provides mechanisms and processes to protect or compensate the Payer in the event that the payment is disputed through a request for reversal, which gives the Payee the choice of automatically returning the funds or completing a manual review to determine whether or not to do so. In cases of fraud, the Member or Provider of the Payer limits a consumer’s liability as required by regulation (S.3.3).

S.4 Settlement approach

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
Same-day settlement is performed using the Federal Reserve Banks’ National Settlement Service (NSS). To reduce overall risk exposure, funds are rebalanced across FIs every two hours during the FRB’s hours of operation (S.4.1-2). In addition, “If an FI has ongoing concerns about the operational account and negative balance scenarios, optional internal safeguards (e.g., contingency-funded accounts) may be leveraged” (page 133). Obligations are settled in central bank money (S.4.3).

S.5 Handling disputed payments

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution’s rules include requirements and processes for resolving unauthorized, fraudulent, erroneous, or otherwise disputed payments but do not include timeframes (S.5.1, S.5.3). The standard process for resolving exceptions is a reversal process/request for voluntary return of funds (S.5.3), notifications of completion, and the use of a fraud information-sharing service. The process for cases in which the payee refuses to return the funds is to go to civil court as there is no dispute resolution process outlined within the Solution.

Ultimately, the end-user bears responsibility for the accuracy of the information submitted to a member, and there is no guarantee that an erroneous payment can be returned. Members are responsible if the end-user account is compromised.
S.6 Fraud information sharing

**Very Effective**

**Effectiveness Matrix:**

- Effective
- Somewhat Effective
- Not Effective

**Rationale:**
The solution meets all the criteria through its Fraud Sharing Service (S.6.6). The solution requires information sharing in exchange for the aggregated, network-wide data analysis that gives Members real-time information about the status of an End User across the network (S.6.1, S.6.7). The Fraud Sharing Service provides guides with the list of data stored, retention schedule, and explanation of how data is used and how standardized messages are passed back to Members to feed fraud systems of Members (S.6.2, S.6.3).

S.7 Security controls

**Very Effective**

**Effectiveness Matrix:**

- Effective
- Somewhat Effective
- Not Effective

**Rationale:**
The solution meets all criteria across technical access components and controls (S.7.1), operational and procedural components and controls (S.7.2), and managerial policies and oversight (S.7.3).

S.8 Resiliency

**Very Effective**

**Effectiveness Matrix:**

- Effective
- Somewhat Effective
- Not Effective

**Rationale:**
While the approach to meet the solution’s “up-time” targets is clear, the targets themselves need to be specifically defined (S.8.1). The proposal addresses business continuity and disaster recovery plans through routine testing of scenarios (S.8.2). In addition, the system is API-driven with testing and risk-based change processes to mitigate systemic risk (S.8.3). The solution requires at least 1 full time person dedicated to business continuity/disaster recovery at each Member and RNAP along with demonstrated BCP/DR capabilities (S.8.4). Testing of business continuity and disaster recovery controls is supplemented by load testing, vulnerability scanning, penetration testing and simulated abuse (S.8.5).

S.9 End-user data protection

**Very Effective**

**Effectiveness Matrix:**

- Effective
- Somewhat Effective
- Not Effective

**Rationale:**
The solution requires controls and cryptographic protections to protect end-user data in transit and at rest from Participants and the central infrastructure (S.9.1). The Directory limits the need for sensitive information to be sent across the network for account setup, transaction setup, problem resolution, and payment completion (S.9.2, S.9.3).
S.10  End-user/provider authentication

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
While Members are responsible for end-user authentication, Payment System Rules define a base level of authentication (S.10.1). The Directory is used to ensure the payment is destined to reach the intended Payee, though other mechanisms such as a pre-notification or “test message” are not addressed. The solution aligns with regulatory guidance and industry standards for authentication (S.10.3). The solution leaves risk-weighting procedures and adoption of new and decommissioning of old authentication models up to the depository institution (S.10.4-5).

S.11  Participation requirements

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The FPS Regulator will develop the FPs Operating Rules and Guidelines and the Schemes may place additional requirements on Providers. However, these rules are not yet developed (S.11.1, S.11.2).

The Scheme will have a risk management program with annual self-assessment and third party independent audit performed and made available to the public to support compliance and monitoring of all Providers against the rules and requirements (S.11.3).

**Speed (Fast)**

F.1  Fast approval

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution expects payment approval within two seconds of payment initiation. However, the scheme operator, providers and operating rules ultimately control the timing of approval.

F.2  Fast clearing

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution expects payments to clear within two seconds of payment initiation. However, the scheme operator, providers and operating rules ultimately control the timing of clearing.
F.3 Fast availability of good funds to payee

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution expects the Payee’s member institution to approve or deny a payment within one minute. After the payee accepts the payment, funds will be immediately available for withdrawal. However, the scheme operator, providers and operating rules ultimately control the timing of availability of good funds.

F.4 Fast settlement among depository institutions and regulated non-bank account providers

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Settlement occurs through NSS, so transactions are currently settled in the same-day or next day without settlement services on weekends. Accounts are rebalanced every two hours to reduce the risk associated with Deferred Net Settlement (F.4.1). Regarding flexibility of settlement timing (F.4.3), if a Member raises a credit or liquidity risk concern, the solution can conduct an ad hoc settlement. It is the QIAT’s understanding that a working assumption of the proposed solution is that the Federal Reserve will enhance NSS operating hours, although the Fed has not yet committed to make this change. Under these circumstances, the solution will settle in two-hour windows 24x7, including weekends, and will meet the criteria for “Effective”.

F.5 Prompt visibility of payment status

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution expects the Payment status to be visible to end users within five seconds. However, the scheme operator, providers and operating rules ultimately control the timing of availability of good funds.

Legal

L.1 Legal framework

<table>
<thead>
<tr>
<th>Rating</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Providers are expected and required to comply with existing laws and regulations, as well as with the FRB’s applicable rules and regulations (L.1.1). There are no gaps in legal sources identified (L.1.2). The solution requires Members and Providers to enter into agreements with End Users governing use of services (L.1.3). The solution supports compliance with relevant U.S. laws by end-users, members, and providers (L.1.4). The proposal does not identify any
unique provisions needed to address situations in which end-users would perform the same functions in the payment system but would be subject to different laws or regulatory supervision (L.1.5).

L.2  Payment system rules

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution describes key features of Payment System Rules across the end-to-end payments process (L.2.1).

The proposal acknowledges a need for Payment System Rules and sets out a path to complete them, but they are not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

L.3  Consumer protections

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The legal framework consists of Reg. E requirements and the rules/regulations for the FRB-supported settlement mechanisms (L.3.1). The End User agreement allows participants to offer greater consumer protections than those required by Reg E (L.3.3).

The outlines of consumer protection are provided particularly around compliance with Reg E, but the Payment System Rules are not yet developed that support consumer claims from fraud or error (L.3.2).

L.4  Data privacy

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution requires Members and Providers to maintain a privacy policy and data shared with Members and Providers may only be used for the purposes of processing a payment and fraud management, subject to express authorization by an End User to use data for other purposes (L.4.1). Data is secured through operational procedures that ensure protection of data in transit and at rest (L.4.2). The solution also lists the nature and type of end-user data required for use (L.4.3). Providers must collect authorization from the End User to use the End User’s data for any other purpose other than processing a payment (L.4.4).
L.5 Intellectual property

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The proposer is confident that the solution does not infringe on intellectual property rights, however, more details are needed. Beyond stating that the proposer would undertake an appropriate review when necessary (page 152), there is no proposed approach to handling IP infringement, should issues arise.

Governance

G.1 Effective governance

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution provides a governance framework approach to address the subcriteria. A Board of Directors and code of conduct would be established. The management team would develop the decision-making criteria using a majority approved matrix and voting process. The solution’s governance arrangements are publicly disclosed (G.1.2). The solution relies on members to conduct self-assessments and to arrange third-party independent audits (G.1.4).

G.2 Inclusive governance

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution provides a governance framework approach to address the subcriteria. The proposal provides high-level information on inclusive governance plans, including a defined channel for questions and proposals from Members providing input as well as an ethics hotline to capture anonymous complaints and feedback.
APPENDIX A: ASSESSMENT SUMMARY

|= QIAT Assessment  = Proposer Self-Assessment

<table>
<thead>
<tr>
<th>UBIQUITY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.1: Accessibility</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.2: Usability</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.3: Predictability</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.4: Contextual data capability</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>U.5: Cross-border functionality</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>U.6: Multiple use case applicability</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EFFICIENCY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.1: Enables competition</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2: Capability to add value-added services</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.3: Implementation timeline</td>
<td></td>
<td></td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>E.4: Payment format standards</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.5: Comprehensive</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.6: Scalability and adaptability</td>
<td></td>
<td></td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>E.7: Exceptions and investigations process</td>
<td></td>
<td></td>
<td>✓</td>
<td>○</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAFETY AND SECURITY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.1: Risk management</td>
<td></td>
<td></td>
<td>✓</td>
<td>○</td>
</tr>
<tr>
<td>S.2: Payer authorization</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.3: Payment finality</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.4: Settlement approach</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.5: Handling disputed payments</td>
<td></td>
<td>✓</td>
<td></td>
<td>○</td>
</tr>
<tr>
<td>S.6: Fraud information sharing</td>
<td>✓</td>
<td>○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAFETY AND SECURITY (cont'd)</td>
<td>Very Effective</td>
<td>Effective</td>
<td>Somewhat Effective</td>
<td>Not Effective</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------</td>
<td>-----------</td>
<td>--------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>S.7: Security controls</td>
<td>✓  ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.8: Resiliency</td>
<td>✓  ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.9: End-user data protection</td>
<td>✓  ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.10: End-user/provider authentication</td>
<td>✓  ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S.11: Participation requirements</td>
<td>○  ✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SPEED (FAST)</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.1: Fast approval</td>
<td>✓  ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.2: Fast clearing</td>
<td>✓  ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.3: Fast availability of good funds to payee</td>
<td>✓  ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.4: Fast settlement</td>
<td>○  ✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.5: Prompt visibility of payment status</td>
<td>✓  ○</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEGAL</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>L.1: Legal framework</td>
<td>✓  ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.2: Payment system rules</td>
<td>○  ✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.3: Consumer protections</td>
<td></td>
<td>✓  ○</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.4: Data privacy</td>
<td>✓  ○</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.5: Intellectual property</td>
<td></td>
<td>✓  ○</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOVERNANCE</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.1: Effective governance</td>
<td></td>
<td></td>
<td>✓  ○</td>
<td></td>
</tr>
<tr>
<td>G.2: Inclusive governance</td>
<td></td>
<td></td>
<td>✓  ○</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B: PROPOSER RESPONSE TO QIAT ASSESSMENT

Dwolla looks forward to collaborating and refining its submission through the constructive feedback and peer review process of the Task Force commentary period.

About the Proposal

Dwolla\(^1\) provides modern APIs to safely and securely access and leverage the nation’s underlying bank transfer system, ACH. In 2012, Dwolla launched its real-time funds transfer API for financial institutions, called FiSync. To economically and technically provide a functional and sustainable national Faster Payment System (FPS), the proposers have pulled from their technology and experience to provide a slightly modified version of these two components (i.e. an application layer and faster payments engine). You can read more about this system in detail in the proposal.

About the Assessment

It’s important to note that the proposers DID NOT go back and alter the original proposal. Any clarifications or alterations were proposed within the Assessment Response to the QIAT’s Preliminary Assessment.

The comments below address the notable deltas or themes between the QIAT’s evaluation and the proposers’ self-assessment. On a whole, the proposers were pleased by the QIAT’s rapid and thoughtful responses, tacit knowledge of alternative and traditional systems, and ability to quickly adapt and learn.

Our comments focus on 3 key areas:

1. Central bank settlement
2. “Consistency check”
3. Payment System Rules

1. Central bank settlement

<table>
<thead>
<tr>
<th>SPEED (FAST)</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>F.4: Fast settlement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Currently in the United States, only Fed-supported means may be used to settle to central bank funds and ultimately settlement is “an act that discharges obligations in respect of funds between two or more Entities”\(^2\). Unfortunately, the United States does not have a Fed-supported rail that operates 24x7x365.

\(^1\) https://dwolla.com

\(^2\) https://fedpaymentsimprovement.org/resources/glossary/
In an effort to lower costs and time-to-market, the solution builds off the proposed expansion of the existing National Settlement Service, or NSS\textsuperscript{3}. The enhancement would facilitate 2-hour windows and ad hoc settlement through its expansion to 24x7 and weekend availability. The proposed timeline for an NSS expansion aligns with the solution’s Implementation Timeline. With that said, the proposed FPS could be easily adapted to interoperate with a prevailing alternative for Fed-supported real-time settlement in the future.

2. “Consistency Check”

<table>
<thead>
<tr>
<th>EFFICIENCY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.6: Scalability and adaptability</td>
<td>○</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In its Preliminary Assessment by the QIAT, the proposed solution received a “Very effective” rating on E.6. Confident in their rating, the proposers did not provide new information to the E.6 criterion in their official response.

Upon conducting its “consistency check across proposals”, the QIAT lowered the proposal’s effectiveness rating for E.6 from “Very effective” to “Effective” in its Final Assessment.

While Dwolla appreciates the need to properly calibrate scores across solutions to ensure uniform evaluations, the technicality did prevent Dwolla from elaborating on how its cloud-based design, elastic solutions, load balancing, containerization and stack-based scale would allow increased platform throughput in near real-time and without introduced downtime.

This was the only demerit caused by the “consistency check” the proposers received.

3. Payment System Rules (PSR)

Unlike other Criteria, PSR govern individual and national systems, stakeholders, and use cases and are both uniquely and uniformly applied. This creates a significant challenge for any one proposal to posit a comprehensive solution that is further compounded by the current lack of existing regulatory leadership in the U.S.. In an email to proposers on August 3, 2017, the QIAT referenced this recurring theme, stating:

“In many proposals, legal and governance frameworks have yet to be developed. In these cases, the Solution was deemed to be "Somewhat Effective” for these criteria.”

For their part, the proposers made the conscious decision to pursue a “framework approach” throughout the proposal. The proposers believe this approach better supports stakeholder collaboration in designing the necessary future guidelines, relationships, rule sets, and requirements needed to govern schemes, enforce legal action, and secure a faster payment system.

---

Where required, the proposers did make recommendations to provide a foundation for conversation and/or illustrate concepts and ideas. Some of these included, but were not limited to, regulatory governance, incentives, and end-user predictability and usability.

While the proposers believe their framework approach is best suited to foster inclusivity and buy-in from the payments landscape in a Post-Final Report World, it did hinder the proposal’s ability to fully address key criteria, such as…

<table>
<thead>
<tr>
<th>SAFETY AND SECURITY</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.1: Risk management</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAFETY AND SECURITY (cont’d)</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>S.11: Participation requirements</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEGAL</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>L.2: Payment system rules</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.3: Consumer protections</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOVERNANCE</th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.1: Effective governance</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G.2: Inclusive governance</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The proposers of the solution strongly urge the payments community to take swift action in identifying, collaborating, and resolving the gaps posed by these broad governance challenges.
DWOLLA PROPOSAL

TASK FORCE ASSESSMENT COMMENTS

Please share your concerns about this proposal’s assessment against the Effectiveness Criteria.

Interesting technology model, but it is very conceptual and leaves gaps in end-user experience, governance, fraud and legal. Specific/Key elements of the Effectiveness Criteria that are still lagging include: Ubiquity- U.3. U.5, Safety and Security, S.5, Speed (Fast), S.4., Legal, L.5, and Governance G.1 & G.2.

The proposal is not in conformance with the requirements of a full solution proposal. The requirements were designed to ensure that McKinsey and Task Force time and resources are focused on end-to-end solution proposals that can be thoroughly and credibly assessed against the criteria. This proposal does not meet the requirements. Proposal has answered all sections of the template, but in many cases the response does not provide information that would allow the QIAT to evaluate the proposal. The Proposal Template included instructions for Part C: Self-Assessment against Effectiveness Criteria that asked proposers to include a "detailed discussion of why the rating is justified and how the solution meets each criterion" (page 22 of template). It does not include specific information in Part C as to how or why the proposed solution meets each of the criteria. As a result, the QIAT is unable to evaluate the solution with the information provided. Altering the existing process defined to offer an opportunity for the proposer to include more explicit information in its submission to make the proposal “assessable” would be unfair to proposers who provided complete proposals before the submission deadline. A few of the reasons why the proposal did not meet the requirements are as follows: The solution did not address B2B, B2P, P2B, P2P cross-border transactions. Pre-authorization was not addressed.

Please submit any comments about this proposal’s assessment against the Effectiveness Criteria.

This QIAT has a high number of "very effective" and "effective" ratings. This result, in and of itself, is a red flag (to me) that this provider’s results benefited from being assigned to a "high scoring" assessor. However, there are numerous references to specific aspects of the solution that support the results. My concerns are mostly addressed.

The one point I have a question on is S4, settlement approach. This received a "very effective" rating, but the executive summary of the proposal calls out the settlement model and the speed of settlement as an "area for improvement and enhancement." My conclusion is the S4 should be rated lower, either as "effective" or "somewhat effective.”

I have a comment on one Assessment criteria: Under E3—Implementation Timeline—the QIAT Assessment is Effective (Achieves Initial Implementation by 2019 and Ubiquity by 2021). I feel that the proposal’s timeframe does not take into account the required implementation of the Fed as the Regulator of the scheme. An assessment of Somewhat Effective might be more accurate.
Agree as assessed.

Dwolla lacks governance and rules; however, it is quite complete as a technical solution.

A little difficult to know what is built and ready to go today.

Several of the key effectiveness criteria components associated with legal and governance were missing from the proposal to be effective.

Generally agree with the assessment. The proposal needs improvement to ensure clear and robust end-user protections in case of fraud, including victim-assisted fraud.

Governance and rules are not defined. Assumes Fed will serve as the regulator. Directory provider is not clearly defined and is necessary to achieve ubiquity.

PROS:

- Speed effectiveness criteria addressed
- Fraud sharing service
- Federal Reserve as the Regulator allowing for broader adoption
- Has the technical infrastructure for a faster payments system
- Includes ISO20022 messaging formats with cross-border payment capabilities and functionality
- Supports all use cases
- Ubiquity Criteria meets VERY EFFECTIVE: Accessibility, Usability, Predictability, Applicability to multiple use cases
- Generally meets other effectiveness criteria: Effectiveness, Safety & Security, Legal, Speed
- Provides business case/value proposition for: Large FIs, Medium FIs, Consumer End-Users, Business End-Users
- Demonstrates Network Effect
- Provides for Education/Marketing Support
- Meets the standard metrics

CONS:

- Relies on the operator and provider for security, legal and governance
- End-user experience will not be consistent due to the reliance on the operator or provider
- Regulation E framework for dispute handling – unclear on timeframe
- Does not support the following Use Cases: Cross-Border
- Does not meet the following ubiquity Criteria: Contextual data capability, Cross-Border Functionality
- Does not meet the general effectiveness criteria: Governance
- Does not provide business case/value proposition for: Small FIs
Overall the assessment is accurate. The solution, like many, is light on what the end-user experience will be, leaving it to the providers. While this makes sense, it makes it difficult for one to assess the effectiveness criteria attributed to the end-users. In addition, this proposal, like many, could benefit from more substance in the governance and legal areas so I question the ratings. The issue that is hard to assess is how much of what is proposed is built versus a concept on paper. There is not enough substance in the proposal to assess the "tangible aspects" of the solution. With that said, I commend Dwolla and the team for coming forward with a solution, even if it is in concept form.

Although Dwolla has more experience than most of the others, based on the presentation and Q&A they gave at the Task Force meeting I have to assume that their interest is in being part of someone else's faster payments solution, not in offering a solution themselves.

I found the organization structure to be confusing, as were the roles and responsibilities of the actors. The fraud sharing service relies on the participants sharing transaction data information; this could cause some data privacy issues. It is unclear about the total end-to-end processing times and the throughput and latency timings for each of the actors. Settlement was not in real time and relied on a deferred settlement model and would require the Fed to be open 7X24X365 to achieve this.

I think the process looks good, but the question still stands as to who will own the governance. The process itself looks very easy and convenient. Also who will own the directory is a big question that is not answered.

This proposal is confusing regarding its use of ISO 20022 ("proposed solution assumes a future version of ISO 20022"). It does not appear they use such a standard today, but would in the future. As such, the rating for this area should be reviewed—E.4 may be rated too highly due to lack of surety around the standard that is utilized.

S.5, Handling disputes: proposal seems to simply reiterate criteria without much detail. Rated too highly as no detailed information provided. Governance and rules also rated too highly as they are not yet defined.

The movement in the process to a better common understanding on issues like cross-border v. domestic processing demonstrated how the iterative process aided the effort.

I believe that taken at face value the proposal was assessed properly. I think the level of FRB involvement they desire may be a challenge. I like how the proposal can leverage existing Financial Institutions and a directory system in order to provide faster payments.

I generally agree that the proposal was assessed appropriately, but the high ranking for ubiquity is questionable given the proposal didn't speak to how it would address the unbanked. The high ranking for legal/governance could be challenged given the lack of definitions provided in the proposal in that area.

I was somewhat confused by the questions coming back from the assessors regarding end-user experience and accessibility and the three-year implementation plan. I felt as though the criteria were addressed by establishing the owner(s) of the specific end-user experiences and establishing their accountability. I thought the adoption plan was articulated, but I do agree more detail around funding and contingencies was lacking.

I like the simplicity, but feel there are shortcomings in cross-border payments. ACH payments are great, but also difficult in many cases to identify the initiator and cause reconciliation issues.

Settlement approach could have limitations/risks with NSS not operating on the weekends. Suggest this rating is reduced to "effective."

While the proposal delivers a possible end-to-end solution, it leaves several critical questions to be decided by the Schemes. For instance, on governance it states the rules will be developed by the Scheme operators and leaves no room for participation from the stakeholder group. This will slow implementation and possibly keep end-users from adoption until these types of rules are clarified. The proposal is also dependent on the Federal Reserve expanding settlement windows, but even with the expanded windows it does not allow for settlement to occur 365 days a year. There are also gaps on the effectiveness due to a concentration of only allowing depository institutions to participate. It would be a strong proposal if it just identified the requirements for participation based on a risk criteria model.

**TASK FORCE SOLUTION-ENRICHING COMMENTS**

**Ubiquity**

I find this solution to be of particular value as it operates within the existing transfer framework. The credit request design may prove to be a safer design while still being convenient, consistent and scalable.

Some don't feel there should be a central regulator and settlement agent. I like Dwolla's plan because anyone can participate and it becomes a more consistent experience for everyone rather than providers and operators putting their own spin on it. I like this design.

Very strong section for your solution. The flexibility of account types is great.
Need further definition to support interoperability.

Set-up creates inconsistent end-user experiences, small FIs won’t be able to differentiate end-user experience like large FIs, and medium FIs will be able to due to asset and resource size.

With the Fed as the Regulator, it seems to have a higher chance of being rapidly implemented and adopted.

Education from ECCHO & regional payment associations.

Although their written document seems complete, in oral presentation Dwolla's senior personnel seemed more (perhaps exclusively) interested in being hired to be part of someone else's solution.

Using existing framework but does not address how the existing framework will be developed to support 24/7 clearing and settlement.

Concern about small FIs’ ability to stand up a solution like this. It seems it could require more resources than a smaller FI would have available.

U.1 Accessibility – Somewhat Effective, registration enrollment is needed, multicurrency transactions are challenging depending on acceptance at end-point, value to “end-user is not clear” and no plan for interoperability between operators. Regulated Non-Bank Providers (RNAP)- must be sponsored by members and approved by Scheme Owners.

U.2 Usability – Somewhat Effective, solution has members payee’s FI approve or deny within one minute, but “solution does not articulate guidelines or requirements” leaving questions as how effective the solution will be for the end-users.

U.3 Predictability – Not Effective, standards messaging and protocols are left to the providers, which at the end could impact the end-user and the overall Faster Payments concepts, if the providers don’t abide by the Effectiveness Criteria.

U.5 Cross-border functionality – Not Effective, the solution does not support cross-border transactions. It seems to be very complicated for Dwolla as they push everything cross-border to the “scheme owners” thereby possibly impacting the real-time Faster Payments criteria as it will be difficult to have the certainty to rely on operators to be able to process global transactions.

U.6 Applicability to Multiple Use Cases – Somewhat Effective – limitations even within their core use case of P2P. PARTIAL – “auth.” User can send $ to any of the end-users (e.g., e-mail, phone) but nothing available to a bank account) and cross-border is very generic, with limitations.

I know they understand this is not complete and I am hoping to see more of how ubiquity is really implemented.

More clarity should be given to describing the entity that specifically would create and run the proposed directory. Without this definition, it is hard to conceive how ubiquity would be achieved. How is
implementation timeframe impacted by not having a directory provider? Explain how the "reach" to all accounts to send payments to is achieved.

Currently, a few core service providers control a lot of what products small and medium financial institutions are able to provide. In order to be successful, Dwolla will need to connect with many of these providers. To date, these companies have been unwilling to do this without significant compensation, choosing instead to provide their own solutions. I would like to see a road map for how Dwolla will be able to work with these core providers in rolling the solution and thus have it used by small to medium-sized financial institutions.

I think Dwolla's proposal has some very good strengths regarding ubiquity. I believe the fact that it allows access to RNAPs downstream and outside of the banking system helps to ensure that more users, those underbanked or unbanked, have access. It does however rely upon a smartphone or so it seems. While many of us have smartphones some do not and eventually this may not matter if everyone is forced to get a smartphone. What I missed in the proposal was whether or not one could access the scheme from a computer. I realize mobile is the way of the future and computers also represent a barrier to entry, but there didn't seem to be a mention of devices outside of an SMS-enabled phone. Overall I think the setup with FIs and RNAPS could potentially be very successful.

I would have like to see an exploration of a potential approach in Dwolla's interoperability with cross-border solutions already implemented. While I can understand Dwolla's approach in leaving this as a future development among operators, Dwolla is in the best position to understand how this critically-needed function might be handled.

By not filling out the table or adding comments directing the reader to references in the document about cross-border capabilities you made it hard to assess. Concentration on the section and some more thought around specific issues that need to be addressed to bring this to fruition would be beneficial.

I believe it meets the criteria, except for concerns for the Unbanked.

Dwolla's solution, as described in its proposal, is not a complete solution.

**Efficiency**

The directory appears to be a critical part of the solution. You might consider ways to work with existing directories or without (if possible).

The overall settlement of the proposed solution could be enriched by speeding up the deterred net settlement from a 2-hour window to something taking a few seconds.

Too conceptual.
E.1, Enables competition – Somewhat Effective, The directory preferences can be challenging for end-users to switch providers, and participation requirements must be met. And directory is used at this time as a "web-service, not as an End-User interface."

E.3, Implementation timeline – Somewhat Effective – adoption, funding, challenges and how a plan to execute the potential providers and members will be challenging.

E.4, Payment format standards – Somewhat Effective – ISO 20022 is supported but still challenges and limitations with cross-border transactions.

E.7, Exceptions and investigations process – Somewhat Effective, disputes and investigations have a good internal process within the solution, but data is only maintained for 5 years. For many solutions providers, data is kept for a longer time frame.

Not understanding who controls the directories will be a critical part of implementation.

APIs can provide inherent flexibility to various parties, but it may also make it more difficult for various receiver participants to know what to expect relative to incoming payments and information. Expand upon how this factor (the balance required between robustness of APIs and need for consistency in receipt) to support ubiquity will be achieved.

Here there are some concerns. With all of the data breaches that have made headlines in the last few years, there is some hesitancy about having data stored. I think consumers understand that data must be stored somewhere but are rightly somewhat cautious or fearful. My concern revolves around the fact that much of the efficiency, and most like the speed, will come from the use of a directory. If there is not the public will, or if there is public backlash against, instituting a nationwide directory, or a few directories, and directory implementation does not happen, does the scheme fall apart? Is the scheme reliant upon a central infrastructure that doesn’t yet exist or can it function perfectly well without the directory?

It seems to have a long period for the integration and implementation, but I feel the efficiency is there once the implementation is complete.

**Safety and Security**

Good solution meeting the Speed criteria with 2-second funds availability.

No timeline on dispute handling and it complies with Reg E which only covers consumer use cases.

Would encourage a more detailed plan to handle data breaches. Evidenced by the card networks a good plan to handle such events is essential. Also understand this is not priority number one at this stage of the design effort for Dwolla.

The Fraud sharing service relies on the participants sharing transaction data information – this could cause some data privacy issues.
S.1, Risk Management – Somewhat Effective, Risk management framework will be maintained by scheme owner but will be challenging given the ongoing changes with law and regulations related to settlement risk, and related multilateral net positions by the member-based members, as well as operations risks.

S.5, Handling disputed payments – Not Effective, Solution does not include time frames for handling disputes. Timeframes of handling disputes are very important to all participants in the transaction process, as funds can’t be kept without a reasonable timeframe in any reconciling accounts waiting a resolution.

S.10, End-User/provider authentication – Somewhat Effective – “solution leaves risk-weighting procedures and adoption of new and decommissioning of old authentication models up to the depository institution”—this could lead to an inherent risk to all users of this solution.

S.11 Participation requirements – Somewhat Effective, “FPs Operating Rules and Guidelines and the Schemes may place additional requirements on Providers. Rules are not yet developed.”

Describe what organization in particular provides/supports the Fraud Sharing Service (i.e., who is Operator?). Describe what protection provisions are in place for owners of data elements (i.e., those sending the payments or their FIs – do they have protections from the party holding the data?)

Though the proposal leaves the actual rule and guideline development to the regulator and providers, the proposal can set expectations that meet the spirit of the requirements set out by the Fed and highlight the system’s capabilities.

**Speed (Fast)**

It is unclear about the total end-to-end processing times and the throughput and latency timings for each of the actors.

Settlement is not in real time and suggests a deferred settlement model --- That requires the FED by available 7X24X365.

F.1, Fast approval, F.2 Fast clearing, F.3 Fast availability of good funds to payee - Somewhat Effective, through all. F.1 – F.3 ultimate control is shift to the scheme operator, providers, thereby inherently creating an element of risk if the solution is for Faster Payments.

F.4, Fast settlement among depository institutions & regulated non-bank account providers – Not Effective, issue for faster payments as “settlement occurs through NSS, so transactions are settled in the same-day or next day without settlement services on weekends”—thereby creating a risk the lifecycle of real time and faster payments of the transaction.

F.5, Prompt visibility of payment status – Somewhat Effective, even if the transaction is visible in 5 seconds, the solution gives control to the scheme operator and provider.
The speed is very fast, clearing within 2 seconds and deny/approval within 1 minute. However, does this level of speed rely upon the directory and what happens if the directory is not approved?

**Legal**

Having more clear ideas of rules for this solution would be a benefit in attracting full support of this solution.

The proposal could be enriched by providing some insight into the proposed solution set of Rules.

Relies on the providers for legal and governance.

There are no rules in place for this solution. Some of the existing rules will address disputes, etc. but not all of them in a 24/7 environment. Also, does not address disputes for non-consumer transactions.

L.1, Legal framework – Somewhat Effective, there are important items, “legal gaps and changes that may arise in the future” and “unique provisions,” which have not been addressed, including reconciling potential conflicts between members and regulator guidance.

L.2, Payment system rules – Somewhat Effective, payment system rules are not yet complete.

L.3, Consumer protections – Somewhat Effective, need for consumer protections not yet completed.

L.5, Intellectual property – Not Effective, “proposer is confident that the solution does not infringe on intellectual property rights, but has not provided details.”

I would like to see more on how this aligns with our current rules and regulations or if it will be something new.

Providing more information on how the criteria are specifically fulfilled via specific processes, rules, alignment with regulations would be helpful. The proposal states that the solution allows entities to “comply with its own legal obligations” – too general of a statement – requires clarification/specificity.

I would have liked to have seen more substantive information on suggested implementations for legal framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments system.

Though the proposal leaves the actual rule and guideline development to the regulator and providers, the proposal can set expectations that meet the spirit of the requirements set out by the Fed and highlight the system’s capabilities.

**Governance**

The solution could be enriched if more clarity around the proposed solution’s governance model was included within the proposal.
At this stage governance is light but understandable given the stage of development.

G.1, Effective governance – Not effective, Solution relies on members to conduct self-assessment and to arrange 3rd party independent audits, but provide for “decision and rule-making process, arrangement, or approach” and appeals decision process.

G.2, Inclusive governance – Not effective, high level information is provided but a solid plan is important due to the overall participants, operators and providers of this solution.

Discussion of roles of various entities is confusing – clarity around who has responsibility for various governance tasks would be helpful. Does the proposal assume a new regulator (i.e., FPS Regulator) creates all the rules? Then the Scheme Owner also creates rules?

I would have liked to have seen more substantive information on suggested implementations for a governance framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments system.

I would say that governance is lacking in this proposal. From my perspective what I am worried about is financial institutions, who are the scheme owners, getting together and making decisions that are in their best interests but not of their clients. There are an abundance of examples which make the case that could, or will, occur. I would strongly suggest inclusion with end-users on a governance basis, at the beginning, so the end-users are represented. It is a fact that FIs will look at challenges and issues in a completely different way from end-users as the impacts are felt downstream. That is the very nature of differing perspectives why end-users should be included in any kind of governance structure.
The proposers thank the Task Force for its thoughtful feedback. In total, the submission received over 80 assessments responses and solution enhancing comments. When and where appropriate, the proposers merged related comments. The SEC references a Solution Enhancing Comment, while AC indicates it was Assessment Comment.

Ubiquity

<table>
<thead>
<tr>
<th>Category</th>
<th>Comment or Comment Excerpt</th>
<th>Source</th>
<th>Proposer Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td>&quot;limitations even within their core use case of P2P. PARTIAL = “auth.”</td>
<td>SEC</td>
<td>The solution supports the domestic use cases identified by the Effectiveness Criteria.</td>
</tr>
<tr>
<td>Channel</td>
<td>It does however rely upon a smartphone or so it seems. While many of us have smartphones some do not and eventually this may not matter if everyone is forced to get a smartphone. What I missed in the proposal, was whether or not one could access the scheme from a computer. I realize mobile is the way of the future and computers also represent a barrier to entry, but there didn’t seem to be a mention of devices outside of an SMS enabled phone. Overall I think the setup with FIs and RNAPS could potentially be very successful.</td>
<td>SEC</td>
<td>The solution is agnostic to channel, making it uniquely positioned to accommodate nearly any instrument (including, mobile or computer-based access).</td>
</tr>
<tr>
<td>Core providers as an impediment</td>
<td>Currently, a few core service providers control a lot of what products small and medium financial institutions are able to provide. In order to be successful, Dwolla will need to connect with many of these providers. To date, these companies have been unwilling to do this without significant compensation choosing instead to provide their own solutions. I would like to see a road map for how Dwolla will be able to work with these core providers in rolling the solution and thus have it used by small to medium sized financial institutions.</td>
<td>SEC</td>
<td>The proposal mentions a number of different economic pressures, organizational traits, or regulatory requirements that could stimulate a more open banking environment. The Proposers strongly agree with the commenters concern and reinforce the need to address the issue of affordable access in the Task Force’s Final Report. However, the following design elements were considered and would enable a range of required incentives: 1) FIs self-organize a scheme around similar characteristics, such as by region, size, or core providers. 2) Accommodation of Bankers Banks 3) Dynamic API-based design for brokering access and monetizing value-added services to end-users 4) Accommodate existing or pending investments in bank digitization</td>
</tr>
<tr>
<td>Cross-border</td>
<td>It seems to be very complicated for Dwolla as they push everything cross border to the “scheme owners” thereby, possibly impacting the real time Faster Payments criteria as it will be difficult to have the certainty to rely on operators to be able to process global transactions.</td>
<td>SEC</td>
<td>As designed, the FPS is agnostic to use case, currency, and location, making cross-border settlement an additional business objective subject to inclusion by Scheme Owners and regulation by the FPS Regulator. The vendor or protocol for such services will be consistent with the aspirations and technical resources to do so.</td>
</tr>
</tbody>
</table>
**Response to Task Force Comments**

<table>
<thead>
<tr>
<th><strong>Directory ownership</strong></th>
<th><strong>SEC</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>I would have like to see an exploration of a potential approach in Dwolla’s interoperability with cross border solutions already implemented. While I can understand Dwolla’s approach in leaving this as a future development among operators, Dwolla is in the best position to understand how this critically-needed function might be handled.</td>
<td>Numerous cross-border interoperability solutions have been proposed as part of the TF submission process. Banks and Scheme Owners are in strong position to determine the ideal solution, but we do believe Ripple to be a viable cross-border mechanism that complements the FPS.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Directory ownership</strong></th>
<th><strong>SEC</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>More clarity should be given to describing the entity that specifically would create and run the proposed directory. Without this definition, it is hard to conceive how ubiquity would be achieved. How is implementation timeframe impacted by not having a directory provider? Explain how the &quot;reach&quot; to all accounts to send payments to is achieved.</td>
<td>The proposers appreciates the concern (and acknowledges several potential options for Directory custodianship on p. 9 of the proposal submission) regarding ownership.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Directory ownership</strong></th>
<th><strong>SEC</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Given the fragmented nature of today's current directory landscape, the proposers believe that the FPS Regulator and governance structure is best suited to establish or outsource ownership and responsibilities of the Directory as needed. Regardless of custodianship, the Directory, as outlined, is a functional and feasible service designed to safeguard customers and promote Ubiquity.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>End-user experience</strong></th>
<th><strong>AC</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>End user experience will not be consistent due to the reliance on the operator or provider</td>
<td>In its response to its first QIAT assessment, proposers acknowledged and upheld the need for consistent end-user experiences, and further explained how APIs and SDKs would uphold the minimum-required parameters—such as response times, enrollment, dispute processes, presentment of fees, and more—that would be stipulated by the FPS Regulator (p6 of QIAT Response).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>End-user experience</strong></th>
<th><strong>SEC</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>solution has members payee’s FI approve or deny within one minute, but “solution does not articulate guidelines or requirements” leaving questions as how effective the solution will be for the end users.</td>
<td></td>
</tr>
</tbody>
</table>
## Response to Task Force Comments

<table>
<thead>
<tr>
<th>End-user value</th>
<th>value to “end user is not clear”</th>
<th>SEC</th>
<th>See Part B: Section 2: Value Proposition and Competition - End User (p 85 of original proposal)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enrollment</strong></td>
<td>Somewhat Effective, registration enrollment is needed</td>
<td>SEC</td>
<td>All faster payment systems that rely on the abstraction of sensitive information—as recommended by security experts—will need some way to associate a unique identifier (e.g. an email) with a bank account. The proposal outlines a fairly seamless and efficient way of doing just that. The proposers believe that the details and contributions regarding end-user enrollment are a strength, not a weakness.</td>
</tr>
<tr>
<td><strong>Lack of details concerning interoperability</strong></td>
<td>Need further definition to support interoperability.</td>
<td>SEC</td>
<td>Interoperability between multiple operators is a known gap and identified challenge of the Task Force; however, the proposal accounts for such an environment with the inclusion of an Operator ID, Directory, and more. See pages 17-19, 24-37, 109 in the original proposal for more information.</td>
</tr>
<tr>
<td><strong>Small FI's inability to implement, differentiate</strong></td>
<td>Concern about small FIs ability to stand up a solution like this. It seems it could require more resources than a smaller FI would have available.</td>
<td>SEC</td>
<td>A modern, faster payment system will invariably bring challenges to smaller market participants, regardless of which solution is selected.</td>
</tr>
<tr>
<td></td>
<td>small FIs won't be able to differentiate end user experience like large FIs and medium FIs will be able to due to asset and resource size</td>
<td>SEC</td>
<td>To mitigate these challenges and maximize opportunities, the proposers have posited a system that is easily configurable to existing tech-stacks or core providers, and a governance model that could be readily adopted by currently regulated relationships (e.g. Bankers Banks).</td>
</tr>
<tr>
<td><strong>Ubiquity</strong></td>
<td>User can send $ to any of the end users (e.g., e-mail, phone) but nothing available to a bank account</td>
<td>SEC</td>
<td>The proposers, security experts and financial institutions strongly support the abstraction (e.g. tokenization) of sensitive bank information in a faster payment environment.</td>
</tr>
<tr>
<td><strong>Unbanked</strong></td>
<td>I generally agree that the proposal was assessed appropriately, but the high ranking for ubiquity is questionable given the proposal didn't speak to how it would address the unbanked.</td>
<td>AC</td>
<td>As discussed on pages 3, 83, 84, 107, 108, 170, and 171 of the original submission, the proposers offer novel and unique solutions to promoting financial inclusion, including offline payments and the inclusion of RNAPs to cater to the unbanked.</td>
</tr>
<tr>
<td><strong>Standards</strong></td>
<td>Standards messaging and protocols are left to the providers,</td>
<td>SEC</td>
<td>As highlighted throughout the proposal (specifically pages 20-21 and 120-121), the solution provides a standard set of core messaging between components (i.e. Members, Operators, Fraud Sharing Services, and Directories). Providers or Members must conform or translate any messaging format that deviates from this standard prior to sending it to the Operator.</td>
</tr>
</tbody>
</table>

### Efficiency

<table>
<thead>
<tr>
<th>Category</th>
<th>Comment or Comment Excerpt</th>
<th>Source</th>
<th>Proposer Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
<td><strong>Comment or Comment Excerpt</strong></td>
<td><strong>Source</strong></td>
<td><strong>Proposer Response</strong></td>
</tr>
<tr>
<td>Efficiency</td>
<td>The directory appears to be a critical part of the solution. You might consider ways to</td>
<td>SEC</td>
<td>For the purposes of the submission, the proposers assumed a central directory; however, a federated</td>
</tr>
</tbody>
</table>
| Directory and account management | The directory preferences can be challenging for end users to switch providers, and participation requirements must be met. And directory is used at this time as a "web-service, not as an End User interface." | SEC | All providers have direct or indirect access to the Directory (p9 of proposal). The FPS rules and regulations would enforce the availability of consistent end-user interfaces and experiences, like account management of preferences and providers, by providers.

For example, when John associated his email with Bank A, Bank A became required to provide an interface for managing preferences associated John's email address. If John were to associate his email address with Bank B; thus having one email associated with 2 bank accounts, both Bank A and Bank B would now be required to provide a similar interface for managing preferences (e.g. remove associate or select a preferred provider for future funds received). This is achieved by Banks and their sole read/write capabilities to the Directory's web-service.

Consistent end-user experiences would be informed by FPS Operating Rules and Guidelines and enforced through open APIs and SDKs. |
| Contextual Data and Standardization | APIs can provide inherent flexibility to various parties, but it may also make it more difficult for various receiver participants to know what to expect relative to incoming payments and information. Expand upon how this factor (the balance required between robustness of APIs and need for consistency in receipt) to support ubiquity will be achieved. | SEC | In its response to its first QIAT assessment, the proposers acknowledged and upheld the need for consistent end-user experiences. Proposers explained how APIs and SDKs would uphold the minimum-required parameters—such as response times, enrollment, dispute processes, presentation of fees, and more—stipulated by the FPS Regulator (p6 of QIAT Response). |
| Data retention | Data is only maintained for 5 years. | SEC | The proposal cites a timeframe necessitated by applicable laws currently in existence. |
| Security of the directory | My concern revolves around the fact that much of the efficiency, and most like the speed, will come from the use of a directory. If there is not the public will, or if there is public backlash against, instituting a nationwide directory, or a few directories, and directory implementation does not happen, does the scheme fall apart? Is the scheme reliant upon a central infrastructure that doesn’t yet exist or can it function perfectly well without the directory? | SEC | A lightweight central directory service is a core component of the proposal required to deliver not only speed and ubiquity but also security given the cryptographic benefits delivered by the directory entries and associated public keys. It is critically important that the directory service be clearly explained to ensure proper understanding of the lightweight nature as it contains the minimal identity data elements (User Directory ID, Name, Type, Email, Phone, Operator ID, Routing Number and Preference) necessary for signing requests and messages. The scheme is dependent on the creation of the lightweight directory which can be created, loosely-coupled through federation and distributed for resiliency. This is not an entirely new concept and is based off of existing critical and secure central directories such as DNS (with DNSSEC). |
| Timeline | Under E3 - Implementation Timeline - the QIAT Assessment is Effective (Achieves Initial Implementation by 2019 and Ubiquity by 2021). I feel that the proposal's timeframe does not take into account the required implementation of the Fed as the Regulator of the scheme. An assessment of Somewhat | AC | The proposal highlights this concern as a dependency on page 70 of the proposal.

The Fed would not act as the regulator of an individual Scheme, but the system itself. |
## Security

<table>
<thead>
<tr>
<th>Category</th>
<th>Comment or Comment Excerpt</th>
<th>Source</th>
<th>Proposer Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dispute timeline</td>
<td>No timeline on dispute handling</td>
<td>SEC</td>
<td>The proposal cites existing Reg. E timeframes to maintain existing bank and consumer expectations (p 134 of original proposal).</td>
</tr>
<tr>
<td></td>
<td>Solution does not include time frames for handling disputes. Timeframes of handling disputes are very important to all participants in the transaction process, as funds can’t be kept without a reasonable timeframe in any reconciling accounts waiting a resolution.</td>
<td>SEC</td>
<td></td>
</tr>
<tr>
<td>Non-consumer disputes</td>
<td>It complies with Reg E which only covers consumer use cases</td>
<td>SEC</td>
<td>The Reg E timeframes will also be used for commercial disputes. However, the difference in this proposed solution is the finality of payments for non-consumer disputes - if a payment is approved by both the payer and payee member institutions, a transaction will only be reversed in a dispute if approved by the receiver of the payment. This has been shown to be feasible by the UK Faster Payments system.</td>
</tr>
<tr>
<td>Data security</td>
<td>Would encourage a more detailed plan to handle data breaches. Evidenced by the card networks a good plan to handle such events is essential. Also understand this is not priority number one at this stage of the design effort for Dwolla.</td>
<td>SEC</td>
<td>The initial design has focused on the prevention of data breaches through data protection techniques (tokenization, minimal data in lightweight directory with a shared responsibility model (Members will update the directory) and the use of standards-based encryption in-transit and at-rest. The development of data breach plans will certainly be compiled with appropriate details, notification plans and incident response elements; however, without implementation details (for example: data centers, backup strategies, technology stacks) or a more refined governance framework, this remains a future deliverable.</td>
</tr>
<tr>
<td>Fraud Sharing</td>
<td>The Fraud sharing service relies on the participants sharing transaction data information – this could cause some data privacy issues.</td>
<td>SEC</td>
<td>This is an opt-in solution for financial institutions; it is not a requirement, but a system that is intended to improve overall network quality and reduce risk of loss. Data usage would be agreed to by the end user during enrollment and would be used only for fraud and risk management purposes.</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Risk management frame work will be maintained by scheme owner but will be</td>
<td>SEC</td>
<td>The team considered the need for a flexible but a principled risk management foundation which resulted in</td>
</tr>
</tbody>
</table>
### Framework

<table>
<thead>
<tr>
<th>Framework</th>
<th>Challenging given the ongoing changes with law and regulations related to settlement risk, and related multilateral net positions by the member based members, as well as operations risks.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC</td>
<td>The framework approach. Frameworks will be flexible enough to adapt and evolve relative to risk.</td>
</tr>
</tbody>
</table>

“Solution leaves risk-weighting procedures and adoption of new and decommissioning of old authentication models up to the depository institution”—this could lead to an inherent risk to all users of this solution.

### Fraud Sharing Ownership

<table>
<thead>
<tr>
<th>Fraud Sharing Ownership</th>
<th>Describe what organization in particular provides/supports the Fraud Sharing Service (i.e., who is Operator?) Describe what protection provisions are in place for owners of data elements (i.e., those sending the payments or their FIs – do they have protections from the party holding the data?)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC</td>
<td>The proposal leaves flexibility for a multi-Operator system. For practical purposes, one could assume Dwolla as an Operator, but FIs may originate Schemes based on a number of similar characteristics, like size, regionality, or core service providers. The Scheme is responsible for providing the Fraud Sharing service. Member FIs and Operators would ensure the Fraud Sharing service would be built upon sound data protection schemes. Data protection would be delivered via required minimum levels of security configuration (for example, TLS 1.2 and higher) and monitored/maintained through the use of contractual language and ongoing audits and compliance activities.</td>
</tr>
</tbody>
</table>

### Settlement timing

<table>
<thead>
<tr>
<th>Settlement timing</th>
<th>The one point I have a question on is S4 - settlement approach. This received a &quot;very effective&quot; rating; but, the executive summary of the proposal calls out the settlement model and the speed of settlement as an &quot;area for improvement and enhancement&quot;. My conclusion is the S4 should be rated lower, either as &quot;effective&quot; or &quot;somewhat effective&quot;.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>While the proposal’s reliance on enhancements to NSS services and availability is noted, it is not unfounded (see: The Federal Reserve’s “Strategies for Improving the U.S. Payment System”) nor does it preclude the proposal from articulating its ability to timely settle funds and managed liquidity risk. Furthermore, the FPS’ capabilities and modular design make it compatible with a range of potential settlement alternatives (e.g. a pre-funded model or new real-time gross settlement solution product from the Fed).</td>
</tr>
</tbody>
</table>

### Speed

<table>
<thead>
<tr>
<th>Category</th>
<th>Comment or Comment Excerpt</th>
<th>Source</th>
<th>Proposer Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processing time</td>
<td>It is unclear about the total end to end processing times and the throughput and latency timings for each of the actors</td>
<td>SEC</td>
<td>The end-to-end processing time for an approved, clearing, and availability of funds is around 600ms plus internet latency. The proposed systems uses the UK’s rate of adoption to</td>
</tr>
</tbody>
</table>
Response to Task Force Comments

| Settlement 24x7x365 | Settlement is not in real time and suggests a deferred settlement model --- That requires the FED by available 7X24X365 | SEC | While the proposal's reliance on enhancements to NSS services and availability is noted, it is not unfounded (see: The Federal Reserve's "Strategies for Improving the U.S. Payment System") nor does it preclude the proposal from articulating its ability to timely settle funds and managed liquidity risk. Furthermore, the FPS' capabilities and modular design makes it compatible with a range of potential settlement alternatives (e.g. a pre-funded model or new real-time gross settlement solution product from the Fed). |
| Settlement 24x7x365 | The proposal is also dependent on the Federal Reserve expanding settlement windows but even with the expanded windows it does not allow for settlement to occur 365 days a year. | AC |
| Unknown | through all F.1 – F.3 ultimate control is shift to the scheme operator, providers, thereby inherently creating an element of risk if the solution is for Faster Payments. | SEC | Together, the capabilities and controls provided by the Operator, Member, and Provider satisfy the technical and operational requirements of the Effectiveness Criteria F.1-F.3 and a safe and secure FPS. They've been specifically designed to eliminate or mitigate risk, not add to it. |
| Directory and Speed | The speed is very fast, clearing within 2 seconds and deny/approval within 1 minute. However, does this level of speed reliant upon the directory and what happens if the directory is not approved? | SEC | A lightweight, central directory service is a core component of the proposal and is required to deliver not only speed and ubiquity but also security given the cryptographic benefits delivered by the directory entries and associated public keys. |

Legal

<table>
<thead>
<tr>
<th>Category</th>
<th>Comment or Comment Excerpt</th>
<th>Source</th>
<th>Proposer Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer protections</td>
<td>need for consumer protections not yet completed</td>
<td>SEC</td>
<td>As set forth in our proposal, the legal framework for our Solution addresses consumer protection by using existing consumer protections found in Regulation E as well as any rules and regulations that either exist today or may exist in the future for any Fed-supported rails used by the Solution. This framework for consumer protections exists today and will allocate legal and financial responsibility as required by subcriteria L.3.1. Regulation E also sets forth Error Resolution procedures that the Solution will rely on as required by subcriteria L.3.2. The Solution will also include Error Resolution protections for irrevocable electronic consumer payments, which will require messages built into the Solution to allow the sending financial institution to request the receiving financial institution return the payment in cases of fraud or error by the consumer. The requirement for all End Users to sign an End User</td>
</tr>
<tr>
<td>Comment</td>
<td>Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Democratized access for FIs</strong></td>
<td>The agreement allows all participants to offer greater consumer protections than those required under Regulation E and other existing rules and regulations (thus satisfying subcriterion L.3.3).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td>I would have liked to have seen more substantive information on suggested implementations for legal framework, particularly in light of the need to ensure that all financial institutions have equal access to faster payments systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SEC</strong></td>
<td>The FPS does not address the number of different economic pressures, organizational traits, or regulatory requirements that could stimulate a more open banking environment. The Proposers strongly agree with the commenter's concern and reinforce the need for the Task Force to address the issue of fair and open access in the Final Report.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Lack of rule set</strong></td>
<td>“Proposer is confident that the solution does not infringe on intellectual property rights, but has not provided details.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SEC</strong></td>
<td>As noted in our proposal, Dwolla will undertake an appropriate review that the Solution does not infringe any third party intellectual property rights. We strongly believe that review process will confirm that the Solution does not infringe any third party intellectual property rights.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SEC</strong></td>
<td>Having more clear ideas of rules for this solution would be a benefit in attracting full support of this solution.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SEC</strong></td>
<td>As discussed throughout our Proposal, we view the Governance structure and specifically in this context the Payment System Rules as criterion that transcend our individual Solution and a responsibility that should be shared by all stakeholders. We have set forth a Governance framework that is flexible and pragmatic and intended to foster collaboration and stakeholder buy-in, which involves the development of Payment System Rules that specifically address all of the Payment System Rules subcriteria. Throughout our Proposal we have clearly set forth the guardrails for the development of Payment System Rules. These guardrails will be the foundation of the Payment System Rules, which will be further refined and adopted by all of the Scheme Owners.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SEC</strong></td>
<td>There are no rules in place for this solution. Some of the existing rules will address disputes, etc. but not all of them in a 24/7 environment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SEC</strong></td>
<td>Payment system rules are not yet complete.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SEC</strong></td>
<td>I would like to see more on how this aligns with our current rules and regulations or if it will be something new.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SEC</strong></td>
<td>Providing more information on how the criteria are specifically fulfilled via specific processes, rules, alignment with regulations, would be helpful. The proposal states that the solution allows entities to “comply with its own legal obligations” – too general of a statement – requires clarification-specificity.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Non-consumer disputes</strong></td>
<td>Our Solution anticipates that all disputes would be handled in the same way. That process is compliant with Reg E for consumer disputes but can also effectively be used for non-consumer disputes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SEC</strong></td>
<td>Does not address disputes for non-consumer transactions.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Governance

<table>
<thead>
<tr>
<th>Category</th>
<th>Comment or Comment Excerpt</th>
<th>Source</th>
<th>Proposer Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consolidation of power</td>
<td><em>I would say that governance is lacking in this proposal. From my perspective what I am worried about is financial institutions, who are the scheme owners, getting together and making decisions that are in their best interests but not of their clients. There are an abundance of examples which make the case that could, or will, occur. I would strongly suggest inclusion with end users on a governance basis, at the beginning, so the end users are represented. It is a fact that FIs will look at challenges and issues in a completely different way from end users as the impacts are felt downstream. That is the very nature of differing perspectives why end users should be included in any kind of governance structure.</em></td>
<td>SEC</td>
<td>Governance of a multi-operator environments is a known challenge and identified gap of the Task Force. The proposal therefore provides governance details regarding individual schemes (p153-155 of proposal). Where appropriate or possible, however, the proposers did provide suggestions and/or possible frameworks for further multi-operator discussion. Scheme origination and governance call for a pragmatic and inclusive approach to governing individual schemes, which themselves are governed by the FPS Regulator via the FPS Rules and Guidelines. The FPS Rules and Guidelines insure that the policy objectives of a fair, open, fast, secure, and reliable are achieved. These are enforced during Scheme origination as well as yearly audits.</td>
</tr>
<tr>
<td>Lack of governance</td>
<td><em>The solution could be enriched if more clarity around the proposed solutions governance model was included within the proposal.</em></td>
<td>SEC</td>
<td>Governance of a multi-operator environment is a known challenge and identified gap of the Task Force. The proposal therefore provides governance details regarding individual schemes. See pages 153-155 of original submission and page 27-29 of QIAT response.</td>
</tr>
<tr>
<td></td>
<td><em>high level information is provided but a solid plan is important due to the overall participants, operators and providers of this solution.</em></td>
<td>SEC</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Solution relies on members to conduct self-assessment and to arrange 3rd party independent audits, but provide for &quot;decision and rule-making process, arrangement, or approach&quot; and appeals decision process.</em></td>
<td>SEC</td>
<td></td>
</tr>
<tr>
<td>Participation within governance</td>
<td><em>I would have liked to have seen more substantive information on suggested implementations for a governance framework, particularly in light of the need to ensure that all financial institutions have equal access to a faster payments systems.</em></td>
<td>SEC</td>
<td>The FPS does address a number of different economic pressures, organizational traits, or regulatory requirements that could stimulate a more open banking environment, but the proposers recognize that challenges still exist around access for all proposed Solutions. The Proposers strongly agree with the commenters concern and reinforce the need for the Task Force to address the issue of fair and</td>
</tr>
<tr>
<td>Task Force Comments</td>
<td>Open Access in the Final Report</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For instance, on governance it states the rules will be developed by the Scheme operators and leaves no room for participation from the stakeholder group. This will slow implementation and possible keep end users from adoption until these type of rules are clarified.</td>
<td>Governance of a multi-operator environments is a known challenge and identified gap of the Task Force. The proposal therefore provides governance details regarding individual schemes (p153-155 of proposal). Where appropriate or possible, the proposers provide suggestions and/or possible frameworks for further multi-operator discussion:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schemes and their rules are informed by the FPS Regulator's FPS Rules and Guidelines. The FPS Regulator provides rule-making and standardization up and across individual schemes, providing a consistent and holistic enforcement of its policy objectives. The FPS Regulator would have an advisory council composed of industry and end user stakeholders.</td>
<td>Schemes Rules, which are defined and enforced by Scheme Owners, must follow the Rules and Guidelines of the FPS, including requirements around inclusion and participation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Participation within governance</td>
<td>There are also gaps on the effectiveness due to a concentration of only allowing depository institution to participate. It would be a strong proposal if it just identified the requirements for participation based on a risk criteria model.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third-parties and end users receive access through their respective Member FIs. Scheme's board of directors will be comprised of independent representatives and member nominated representatives, including public policy and consumer groups. The FPS Regulator could move to a risk-based model for direct access participation, should it deem it necessary (e.g. Payment Services Directive 2).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule-making and ownership</td>
<td>Discussion of roles of various entities is confusing – clarity around who has responsibility for various governance tasks would be helpful. Does the proposal assume a new regulator(i.e., FPS Regulator) creates all the rules? Then the Scheme Owner also creates rules?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEC</td>
<td>Governance of a multi-operator environments is a known challenge and identified gap of the Task Force. The proposal therefore provides governance details regarding individual schemes (p153-155 of proposal) and their relationship to one another (p6 of proposal). Additional context: FPR Regulator governs Scheme Owners, ensuring policy objectives are met up and across the system via the FPS Rules and Guidelines. FPS Regulator could oversee or outsource the ownership of the Directory. Scheme Owners are comprised of FIs. Aside from owning and operating Fraud Sharing Services and the Operator, they set and enforce Scheme Rules.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>FIs are eligible to be Members of a Scheme. Providers (Third-party service providers, RNAPs, or smaller FIs) must broker access to the FPS through Member FIs.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Response to Task Force Comments*
Faster Payments QIAT

FINAL ASSESSMENT

Proposer: Dwolla, Inc.

Summary Description of solution:
Dwolla is a digital payment network and platform for real-time payments with immediate availability of good funds. The solution is an end-to-end Faster Payments System (FPS) comprising:

■ Federal Reserve as the FPS Regulator

■ An FPS “Scheme Owner/Operator” that operates the clearing and settlement infrastructure between members. The solution involves real-time clearing and deferred net settlement through the Federal Reserve’s National Settlement Service (NSS). To reduce overall risk exposure, funds are rebalanced across FIs every two hours during the FRB’s hours of operation.

■ Depository institutions as member-owners of the FPS scheme. These members can: 1) serve as direct providers of faster payment services to end-users, 2) offer FPS access or services to a third-party service (e.g., Uber) as an access provider, and/or 3) offer FPS access or services to a Regulated Non-bank Account Provider (RNAP) (e.g., PayPal) as a “sponsoring member.”

■ Providers that deliver, facilitate, or enable access to the FPS by end-users through products, services, or APIs

■ A directory or federation of directories serving as a secure, standalone repository that enables anyone to send and receive payments using just an email or phone number. Users may also store payment preferences in the directory.

■ A Fraud Sharing Service, which the Operator maintains separately, to collect and distribute data and conduct analysis across the platform to spot high-risk activity

EXECUTIVE SUMMARY OF THE PROPOSAL

■ Major strengths
  – The solution facilitates competition by allowing end-users to choose among providers, to use multiple provider accounts, and to specify payment preferences in the directory. Providers—both banks and RNAPs—can develop value-added services by integrating with the solution using open, accessible standards through the solution’s Platform Services Layer.

  – The solution’s messaging format will help to ensure interoperability. ISO 20022 will be the format for payment messages to and from members and the operator; messaging between providers and members will be determined by the member and translated to ISO 20022. Schemes will be enabled to allow Members and Providers to develop agreed-upon standards for contextual data (attributes in the metadata).

  – The solution meets the criteria for speed, as payments are expected to be approved and cleared within two seconds of payment initiation. The payee’s member institution is expected to approve or deny a payment within one minute. After the payee accepts the payment, funds will be immediately available for withdrawal. Payment statuses are available within five seconds.

■ Areas for improvement and enhancement
  – The solution uses existing settlement systems through its use of NSS, but without extension of the NSS to 24/7 and weekend operations, the speed of settlement can take over a day.
The solution’s rules include requirements and processes for resolving unauthorized, fraudulent, erroneous, or otherwise disputed payments. They do not include timeframes or a process for cases in which the payee refuses to return the funds, other than indicating that disputed payments would be settled outside the solution through civil court. The standard process is limited to a reversal process/request for return of funds and notifications of completion.

A detailed description of the solution’s legal framework and governance approach has yet to be developed. The proposal notes that governance and rules “transcend the individual systems, stakeholders, and use cases and are uniquely shared and uniformly applied in most cases.” The proposal does articulate a framework to legal and governance.

Use cases addressed

The solution addresses all four major use cases (P2P, P2B, B2P, and B2B). It does not yet support cross-border payments, deferring the future plan for these to scheme owners.

Proposer’s overall ability to deliver proposed solution

Dwolla is an established payments solution provider that currently provides a bank transfer solution.

The solution uses the existing, adapted and improved applications and processes of Dwolla’s current Network, Platform, Services and Immediate Funds Transfer System. Thus, the QIAT has high confidence in the proposer’s ability to deliver the technical solution.
ASSESSMENT

Ubiquity

U.1 Accessibility

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The solution facilitates payments to/from all types of accounts—savings, checking, and others—across Depository Institutions, Regulated Non-bank Account Providers (RNAP) and third-party providers (U.1.1).

End-users can enroll with a Member depository institution or RNAP. First-time payees that are not part of the directory can also enroll; the Payer’s Member engages the payee through notification via email or mobile phone, and the payee is then taken through the registration process in order to receive the transfer. This helps ensure that Entities’ payments can reach any and all Payees (U.1.2).

For multi-currency transactions, the solution supports any transfer, so long as end-points can accept the currency (U.1.3); however, the ability to handle multi-currency transactions is dependent on providers. Interbank settlement processing capability for multi-currency transactions is currently being explored. It is not clear how the solution would ensure the same SLAs for a multi-currency offering.

The ability to send and receive payments from RNAPs and third parties supports the needs of the unbanked and underserved (U.1.4). In addition, innovations for consumers without access to SMS or email include vouchers for redemption and prepaid cards.

The solution is technically feasible for Providers to adopt. The potential for new, revenue-generating products and services is the motivation for Providers to adopt the solution (U.1.5). The solution achieves interoperability across operators (U.1.6).

U.2 Usability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rationale:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The solution facilitates a straightforward, simple end-user experience by allowing Providers to build FPS capabilities and experiences across devices and channels, thereby enabling initiation of payment with just an email or phone number (U.2.1-2). The FPS is available 24x7x365. The payee’s member FI is expected to approve or deny a payment within one minute. After the payee accepts the payment, funds are immediately available for withdrawal (U.2.3).

Providers use the solution’s Platform Services Layer (PSL) to build end-user experiences. The PSL uses APIs and SDKs to deliver and enforce usability requirements while giving Providers the framework to innovate on the end-user experience.
U.3 Predictability

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**

The solution’s core features are well-defined, and the solution’s design ensures their delivery (U.3.1). The communication of baseline features in the payment experience is the responsibility of the FPS Regulator and Scheme owner, but the Proposer offers suggestions on authentication, timing, and acknowledgment of costs (U.3.2). The solution uses standard messaging and protocols between the FPS operator and providers, but leaves Providers to decide on the messaging standard and protocols used to deliver the end-user’s experience (U.3.3).

The error resolution process follows processes similar to the UK’s Faster Payments Service (U.3.5). The solution is “brandless”; however, terms suggested to distinguish the solution from other payment methods include Advanced Clearing Exchange (ACE), Digital Asset Transfer Architecture (DATA), Digital Asset Real-time System (DARTS), and FiSync or Sync (U.3.6). The PSL ensures a base level of predictability through its APIs and SDKs, which ensure consistency of experience in feature functionality (U.3.4).

U.4 Contextual data capability

**Very Effective**  Effective  Somewhat Effective  Not Effective

**Rationale:**

The solution enables contextual data capabilities using ISO 20022 (U.4.1) and exchanges contextual data on payment orders, payment messages and payment receipts. Contextual data can be integrated with interfacing businesses and personal finance systems through ISO 20022 or JSON (U.4.2). The approach to contextual data is flexible, as the solution is “metadata-based” and has core attributes as well as customizable or optional attributes. Members and Providers collaborate across the network to create agreed-upon standards for passing contextual data elements, such as agreeing to include an “Invoice Number” as an element within contextual data (U.4.3).

U.5 Cross-border functionality

**Very Effective**  Effective  **Somewhat Effective**  Not Effective

**Rationale:**

The solution does not yet support cross-border payments. It defers the plan for later inclusion by “scheme owners” [depository institutions that “run their own FPS operator and infrastructure to facilitate and authorize clearing and settlement between members and other operators” (page 6)]. However the solution’s technical capability can support cross-border, particularly using ISO20022.

Further detail on the plan for implementing cross-border payments in the future would be helpful. The plan should address some of the typical challenges encountered in cross-border payments implementation (e.g., Provider adoption, payment limits, settlement cycles, and pre-funding rules) (U.5.5).
U.6 Applicability to multiple use cases

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution supports all use cases and is extensible to future use cases. The design particularly supports consumer payments, such as P2P (person-to-person) payments.

**Efficiency**

E.1 Enables competition

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution allows end-users to choose among providers, to use multiple provider accounts, and to specify payment preferences in the directory (E.1.1-2). End-users cannot directly update the directory; rather, they can only update it through an authorized FI or RNAP and their customer-facing interface. Providers give end-users advance disclosure of costs in accordance with the payment system rules (E.1.3). The Platform Services Layer enables all members, RNAPs and third-party services access to the FPS to provide services as long as participation requirements are met (E.1.4).

The proposal would be enhanced by clarifying the ease with which an Entity may switch Providers. While the solution enables end-users to use multiple Providers and to associate an email address with one Provider and an SMS with another Provider, it would be useful to understand how an end-user might easily switch the Provider associated with an email or SMS.

E.2 Capability to enable value-added services

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Providers integrate with the solution using open, accessible standards through the solution’s Platform Services Layer (E.2.1). The Platform Services Layer allows for tiered access to the FPS, allowing for a broad range of safe participation by a wide variety of providers (E.2.2). For example, a Member brokering access to high-risk third-party services may limit daily transaction totals or require additional identify verification from end-users. All value-added services are required to be disclosed as optional to customers (E.2.3).

E.3 Implementation timeline

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The proposal outlines a three-phased implementation plan that articulates activities and milestones over three years. It assumes a year for member integration and testing. Funding is
provided by Members, who are motivated to participate by the opportunity to offer new, revenue-generating products and services. The formation of a new scheme to gain adoption by FIs is slated for Phase 1, but the effort may take well over a year unless Member FIs are presented with clear incentives to choose the solution over alternative options.

E.4 Payment format standards

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

ISO 20022 is the standardized format used for payment messages between Members and the Operator (E.4.1, E.4.5). The message format between Members and Providers is determined by the Member/Access Provider (e.g., JSON – JavaScript Object Notation or ISO messaging) and translated to ISO 20022. The solution articulates a mechanism for updates (E.4.4). The solution does not yet support cross-border payments, but the message format enables cross border interoperability as ISO 20022 becomes an international standard (E.4.2).

E.5 Comprehensive

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution fully meets the sub-criteria, as it enables all aspects of the end-to-end payment process (E.5.1), and its technical design supports all of its features (E.5.2).

E.6 Scalability and adaptability

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The technical design supports projected use cases (E.6.1) and has the capacity to handle projected volumes and values, based on adoption rates from the U.K. (E.6.2). Since the solution enables Providers and Members to innovate around the customer experience and focuses on the exchange points of Operator, Directory and Fraud Sharing Service, changes can be made by the Operator, Providers, Members across the end-to-end payments process in response to technology, economics, regulations and customers (E.6.3).

The proposal would be enhanced by articulating the solution’s transactions-per-second capacity, as well as its ability to expand capacity to handle transaction volumes at peak times or periods of stress (E.6.2).
E.7 Exceptions and investigations process

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Timeframes for investigations are integrated into the system, and members receive alerts to ensure the timely resolution of disputes/exceptions. The solution maintains exceptions data for a minimum of five years (E.7.2). The operator monitors exceptions data to spot patterns and detect fraud and alerts Members when there is anomalous network activity. In addition, the operating rules will define acceptable standards for exceptions by a given party (E.7.3).

The solution includes a mechanism to request a payment reversal and provides end-users with status updates on return requests; however, more detail on the tools and related protocols provided to Members or end-users to support the resolution of exceptions would be helpful (E.7.1).

Safety and Security

S.1 Risk management

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution’s scheme owner will maintain a risk management framework that responds to changes such as the unexpected application of a law or regulation (S.1.1). Regarding settlement risk, the Operator manages multilateral net positions by Member based on individual Members’ risk ratings. Analysis of volume by Member triggers settlement as volume reaches the established limit. Settlement failures result in suspension of further transaction processing for the Member and its Providers, as well as mitigating actions such as more frequent settlement windows or even suspension from the network (S.1.2). Operational risk is managed through internal process controls and security controls (S.1.3). The risk of fraudulent or erroneous payments is addressed through a variety of prevention mechanisms, including multi-factor authentication to address fraud and standardized content and presentment requirements to minimize the chance of end-user error (e.g., the opportunity to confirm that information is correct prior to transaction initiation) (S.1.4). The proposal states that the FPS operating rules and guidelines will determine the incentives/disincentives (such as fees, suspensions, and fines) to providers and other participants to contain risk (S.1.5).

S.2 Payer authorization

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution requires payers to authorize to their member institution when initiating payments (S.2.1). Payers can pre-authorize payments based on a number of parameters (S.2.2) and can revoke pre-authorization easily and quickly (S.2.3).
S.3 Payment finality

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution requires the Payer's Depository Institution or Regulated Non-bank Account Provider to approve each payment following its initiation to ensure that the payer's account has good funds (S.3.1). The payment is irrevocable once the payer’s provider receives the final “transaction complete” message (S.3.2). If a payment is disputed, the payer may initiate a request for reversal, and the Payee may choose either to automatically return the funds or to manually review the transaction to determine whether or not to return the funds. In cases of fraud, the payer’s Member or Provider limits a consumer’s liability as required by regulation (S.3.3).

S.4 Settlement approach

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
Same-day settlement is performed using the Federal Reserve Banks’ National Settlement Service (NSS). To reduce overall risk exposure, funds are rebalanced across FIIs every two hours during the FRB’s hours of operation (S.4.1-2). In addition, the proposals states that “if an FI has ongoing concerns about the operational account and negative balance scenarios, optional internal safeguards (e.g., contingency-funded accounts) may be leveraged” (page 133). Obligations are settled in central bank money (S.4.3).

S.5 Handling disputed payments

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution’s rules include requirements and processes for resolving unauthorized, fraudulent, erroneous, or otherwise disputed payments but do not include timeframes (S.5.1, S.5.3). The standard process for resolving exceptions is a reversal process/request for voluntary return of funds (S.5.3), notifications of completion, and the use of a fraud information-sharing service. The process for cases in which the payee refuses to return the funds is to go to civil court, as the solution does not outline a dispute resolution process.

Ultimately, the end-user bears responsibility for the accuracy of the information submitted to a member, and there is no guarantee that an erroneous payment can be returned. Members are responsible if the end-user account is compromised.
S.6 Fraud information-sharing

**Rationale:**
The solution meets all the criteria through its Fraud Sharing Service (S.6.6). The solution requires information-sharing in exchange for its aggregated, network-wide data analysis, which gives Members real-time information about the status of an end-user across the network (S.6.1, S.6.7). The Fraud Sharing Service provides guides that include a list of data stored, a retention schedule, an explanation of how data is used, and a description of how standardized messages are passed back to Members to feed their fraud systems (S.6.2, S.6.3).

S.7 Security controls

**Rationale:**
The solution meets all criteria across technical access components and controls (S.7.1), operational and procedural components and controls (S.7.2), and managerial policies and oversight (S.7.3).

S.8 Resiliency

**Rationale:**
While the approach to meet the solution’s “up-time” targets is clear, the targets themselves need to be specifically defined (S.8.1). The proposal addresses business continuity and disaster recovery plans through routine testing of scenarios (S.8.2). In addition, the system is API-driven, with testing and risk-based change processes to mitigate systemic risk (S.8.3). The solution requires that at least one full-time person be dedicated to business continuity/disaster recovery at each Member and RNAP, along with demonstrated BCP/DR capabilities (S.8.4). Testing of business continuity and disaster recovery controls is supplemented by load testing, vulnerability scanning, penetration testing, and simulated abuse (S.8.5).

S.9 End-user data protection

**Rationale:**
The solution requires controls and cryptographic safeguards to protect end-user data in transit and at rest from Participants and the central infrastructure (S.9.1). The presence of a directory limits the need to send sensitive information across the network for account set-up, transaction set-up, problem resolution, and payment completion (S.9.2, S.9.3).
S.10  End-user/provider authentication

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
While Members are responsible for end-user authentication, the solution’s Payment System Rules define a base level of authentication (S.10.1). The Directory helps to ensure that the payment reaches the intended Payee, though other potential mechanisms—such as a pre-notification or “test message”—are not addressed. The solution aligns with regulatory guidance and industry standards for authentication (S.10.3). The solution leaves it to depository institutions to deploy risk-weighting procedures and to adopt new and decommission old authentication models (S.10.4-5).

S.11  Participation requirements

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The FPS Regulator will develop the FPS Operating Rules and Guidelines, and the Schemes may place additional requirements on Providers. However, these rules are not yet developed (S.11.1, S.11.2).

The Scheme will have a risk management program that includes an annual self-assessment as well as independent audits by third parties. The results of these audits will be made public to support compliance and the monitoring of all Providers against the rules and requirements (S.11.3).

**Speed (Fast)**

F.1  Fast approval

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution expects payment approval within two seconds of payment initiation. However, the scheme operator, providers and operating rules ultimately control the timing of approval.

F.2  Fast clearing

<table>
<thead>
<tr>
<th></th>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**
The solution expects payments to clear within two seconds of payment initiation. However, the scheme operator, providers and operating rules ultimately control the timing of clearing.
F.3 Fast availability of good funds to payee

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution expects the Payee’s member institution to approve or deny a payment within one minute. After the payee accepts the payment, funds will be immediately available for withdrawal. However, the scheme operator, providers and operating rules ultimately control the timing of availability of good funds.

F.4 Fast settlement among depository institutions and regulated non-bank account providers

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Settlement occurs through NSS, so transactions are currently settled on the same day or next day, without settlement services on weekends. Accounts are rebalanced every two hours to reduce the risk associated with Deferred Net Settlement (F.4.1). Regarding flexibility of settlement timing (F.4.3), if a Member raises a credit or liquidity risk concern, the solution can conduct an ad hoc settlement. According to the QIAT’s understanding, the proposal assumes that the Federal Reserve will extend NSS operating hours, although the Fed has not yet committed to making this change. If the Fed does indeed extend NSS operating hours, the solution will settle in two-hour windows 24x7—including weekends—and will meet the criteria for an “Effective” rating.

F.5 Prompt visibility of payment status

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution expects the Payment status to be visible to end-users within five seconds. However, the scheme operator, providers and operating rules ultimately control the timing of availability of good funds.

Legal

L.1 Legal framework

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

Providers are expected and required to comply with existing laws and regulations, as well as with the FRB’s applicable rules and regulations (L.1.1). There are no gaps in legal sources identified (L.1.2). The solution requires Members and Providers to enter into agreements with end-users governing the use of services (L.1.3). The solution supports compliance with relevant U.S. laws by end-users, members, and providers (L.1.4). The proposal does not identify any
unique provisions needed to address situations in which end-users would perform the same functions in the payment system but would be subject to different laws or regulatory supervision (L.1.5).

L.2 Payment system rules

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution describes key features of Payment System Rules across the end-to-end payments process (L.2.1). The proposal acknowledges a need for Payment System Rules and sets out a path to complete them, but they are not yet complete. The QIAT has interpreted the Effectiveness Criteria such that solutions at this stage of development earn a rating of “Somewhat Effective.”

L.3 Consumer protections

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The legal framework consists of Reg. E requirements and the rules/regulations for FRB-supported settlement mechanisms (L.3.1). The end-user agreement allows participants to offer greater consumer protections than those required by Reg. E (L.3.3).

The proposal outlines consumer protection measures—particularly around compliance with Reg. E—but Payment System Rules that support consumer claims resulting from fraud or error (L.3.2) have yet to be developed.

L.4 Data privacy

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The solution requires Members and Providers to maintain a privacy policy, and data shared with Members and Providers may only be used to process a payment and/or to manage fraud management. Any other use must be expressly authorized by an end-user (L.4.1, L.4.4).

Data is secured through operational procedures that ensure its protection in transit and at rest (L.4.2). The solution also lists the nature and type of end-user data required for use (L.4.3).

L.5 Intellectual property

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

Rationale:
The proposer is confident that the solution does not infringe on intellectual property rights; however, more details are needed. Beyond stating that the proposer would undertake an
appropriate review when necessary (page 152), there is no proposed approach to handling IP infringement, should issues arise.

**Governance**

**G.1 Effective governance**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution provides a governance framework approach to address the Governance sub-criteria. A board of directors and code of conduct would be established. The management team would develop decision-making criteria using a majority-approved matrix and voting process. The solution’s governance arrangements are publically disclosed (G.1.2). The solution relies on members to conduct self-assessments and to arrange third-party independent audits (G.1.4).

**G.2 Inclusive governance**

<table>
<thead>
<tr>
<th>Very Effective</th>
<th>Effective</th>
<th>Somewhat Effective</th>
<th>Not Effective</th>
</tr>
</thead>
</table>

**Rationale:**

The solution provides a governance framework approach to address the Governance sub-criteria. The proposal provides high-level information on inclusive governance plans, including a defined channel for questions and proposals from Members, as well as an ethics hotline to capture anonymous complaints and feedback.